



GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. ____

din _____ 2023

Chișinău

**Pentru aprobarea proiectului de lege
privind securitatea cibernetică**

Guvernul HOTĂRĂȘTE:

Se aprobă și se prezintă Parlamentului spre examinare proiectul de lege privind securitatea cibernetică.

Prim-ministru

DORIN RECEAN

Contrasemnează:

Viceprim-ministru,
ministrul dezvoltării
economice și digitalizării

Dumitru ALAIBA

Ministrul finanțelor

Veronica Sirețeanu

Ministrul justiției

Veronica Mihailov-Moraru

Lege privind securitatea cibernetică

Parlamentul adoptă prezenta lege organică.

Prezenta Lege transpune art. 1; art. 2; art. 3 alin. (1)-(3); art. 4 alin. (1) și (2); art. 6 alin. (1)-(17); art. 8 alin. (1)-(5); art. 9 alin. (1)-(4); art. 10 alin. (1)-(4); art. 11 alin. (1) lit. (a)-(f), alin. (3) lit. (a)-(e), (g) și (h); art. 12 alin. (1); art. 20; art. 21 alin. (2) și alin. (3); art. 23 alin. (1)-(3), alin. (4) lit. (a), (b), (d) și (e); art. 24 alin. (1); art. 25 alin. (1); art. 29 alin. (1) lit. (a) și (b), alin. (2)-(4); art. 30 alin. (1) lit. (a) și (b), alin. (2); art. 31 alin. (1); art. 32 alin. (1)-(8); art. 33 alin. (1)-(5); art. 34; art. 35 alin. (1); art. 36 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), publicată în Jurnalul Oficial al Uniunii Europene seria L nr.333 din 27 decembrie 2022.

Capitolul I. DISPOZIȚII GENERALE

Articolul 1. Obiectul de reglementare al legii

Prezenta lege reglementează cadrul juridic, organizațional și de cooperare în domeniul securității cibernetică, stabilește competența autorităților și instituțiilor publice în materie de securitate cibernetică, determină cadrul național general de gestionare a crizelor în domeniul securității cibernetică, instituie cerințe, măsuri și mecanisme pentru asigurarea securității rețelelor și sistemelor informatice care sunt esențiale pentru funcționarea societății, precum și gestionarea incidentelor cibernetică.

Articolul 2. Principalele noțiuni și definițiile lor

În sensul prezentei legi, următoarele noțiuni înseamnă:

1) ***amenințare cibernetică*** – orice circumstanță, eveniment sau acțiune potențială care ar putea cauza daune sau perturbări la nivelul rețelelor și al sistemelor informatice, precum și la nivelul utilizatorilor unor astfel de sisteme și al altor persoane, sau care poate avea un alt fel de impact negativ asupra acestora;

2) ***amenințare cibernetică semnificativă*** - amenințare cibernetică despre care se poate presupune, pe baza caracteristicilor sale tehnice, că are potențialul de a afecta grav rețelele și sistemele informatice ale unei persoane juridice care prestează servicii sau utilizatorii serviciilor furnizate de aceasta, cauzând prejudicii materiale sau morale considerabile;

3) ***divulgarea coordonată a vulnerabilităților*** – proces structurat prin care informații privind vulnerabilitățile sunt transmise producătorului sau furnizorului de produse TIC sau de servicii TIC potențial vulnerabile într-o manieră care să îi permită acestuia să diagnosticheze și să remedieze vulnerabilitatea înainte ca informațiile detaliate privind vulnerabilitatea să fie dezvăluite unor terțe părți sau publicului;

4) ***furnizor de servicii*** – persoană juridică de drept public sau de drept privat, înregistrată în Republica Moldova, care prestează servicii în unul sau mai multe sectoare și/sau subsectoare, stabilite de Guvern, și care este identificată de autoritatea competentă în conformitate cu prevederile prezentei legi și a cadrului normativ aprobat pentru punerea acesteia în aplicare;

5) ***gestionarea incidentului cibernetic*** – toate acțiunile și procedurile care vizează prevenirea, detectarea, analizarea, limitarea și izolarea unui incident cibernetic, sau vizează răspunsul la acesta și redresarea în urma acestui incident;

6) ***incident cibernetic*** - orice eveniment care compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor conexe oferite de rețele și sisteme informatice sau accesibile prin intermediul acestora;

7) ***incident cibernetic evitat la limită*** – un eveniment care ar fi putut compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de rețele și sisteme informatice sau accesibile prin intermediul acestora, dar care a fost împiedicat cu succes să se materializeze sau care nu s-a materializat;

8) ***măsuri de securitate*** - operațiuni și/sau resurse organizaționale, fizice și de tehnologie a informației aplicate în scopul obținerii și menținerea securității rețelelor și sistemelor informatice și a datelor procesate prin acestea;

9) proces de tehnologie a informației și comunicații (proces TIC) – un set de activități desfășurate pentru a concepe, a dezvolta, a furniza sau a întreține un produs TIC sau un serviciu TIC;

10) produs de tehnologie a informației și comunicații (produs TIC) - un element sau un grup de elemente al unei rețele sau al unui sistem informatic;

11) rețea și sistem informatic :

a) rețea de comunicații electronice în sensul prevederilor Legii comunicațiilor electronice nr. 241/2007 sau

b) orice dispozitiv sau grup de dispozitive interconectate sau legate între ele, dintre care unul sau mai multe efectuează, în conformitate cu un program, o prelucrare automată de date digitale sau

c) date digitale stocate, prelucrate, recuperate sau transmise de elementele prevăzute la lit. a) și b) în vederea funcționării, utilizării, protejării și întreținerii a unor astfel de date.

12) risc – potențialul de pierderi sau de perturbări cauzate de un incident cibernetic și trebuie exprimat ca o combinație între amploarea unei astfel de pierderi sau perturbări și probabilitatea producerii incidentului cibernetic;

13) securitate cibernetică - activitățile necesare pentru protejarea rețelelor și a sistemelor informatice, a utilizatorilor unor astfel de sisteme și a altor persoane afectate de amenințări cibernetice;

14) securitatea rețelelor și a sistemelor informatice – capacitatea unei rețele și a unui sistem informatic de a rezista, la un nivel de încredere dat, oricărei acțiuni care compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de rețeaua sau de sistemele informatice respective sau accesibile prin intermediul acestora;

15) serviciu de tehnologie a informației și comunicații (serviciu TIC) - un serviciu care constă integral sau preponderent în transmiterea, stocarea, extragerea sau prelucrarea informației prin intermediul rețelelor și al sistemelor informatice;

16) vulnerabilitate - un punct slab, o susceptibilitate sau o deficiență a unor produse TIC sau a unor servicii TIC care poate fi exploatată de o amenințare cibernetică.

Articolul 3. Domeniul de aplicare

(1) Prezenta lege se aplică persoanelor 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 care depășesc plafoanele pentru întreprinderile mijlocii, care furnizează servicii în unul sau mai multe dintre sectoarele sau subsectoarele stabilite de către Guvern, și care sunt identificate ca furnizori de servicii de către autoritatea competentă, desemnată conform articolului 7, în conformitate cu prevederile prezentei legi și a actelor normative de punere a acesteia în aplicare.

(2) Indiferent de dimensiunea lor, prezenta lege se aplică și persoanelor juridice, de tipul stabilit de Guvern, dacă acestea îndeplinesc cel puțin una dintre următoarele condiții:

a) sunt furnizori de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului în sensul legislației privind comunicațiile electronice;

b) sunt prestatori de servicii de încredere în sensul legislației privind identificarea electronică și serviciile de încredere;

c) este Registratorul național al domeniului de nivel superior .md;

d) furnizează servicii de înregistrare a numelor de domenii;

e) este singurul furnizor în Republica Moldova a unui serviciu care este esențial pentru susținerea unor activități societale și economice critice;

f) furnizează un serviciu, dependent de o rețea și/sau de un sistem informatic, perturbarea căruia ar putea avea un impact semnificativ asupra ordinii publice, a securității publice sau a sănătății publice sau ar putea genera un risc sistemic semnificativ, în special pentru sectoarele în care o astfel de perturbare ar putea avea un impact transfrontalier;

g) este critică din cauza importanței sale specifice la nivel național sau regional pentru sectorul sau tipul de servicii în cauză sau pentru alte sectoare interdependente;

h) furnizează un serviciu dependent de o rețea și/sau de un sistem informatic și de un obiectiv al infrastructurii critice și este identificată în conformitate cu cadrul normativ național relevant ca fiind operator al unei astfel de infrastructuri;

i) sunt persoane juridice de drept public.

(3) Prezenta lege nu se aplică

a) activităților desfășurate de autoritățile publice în domeniul protecției secretului de stat în legătură cu mentenanța rețelelor și sistemelor informatice care sunt destinate prelucrării unor astfel de informații;

b) activităților desfășurate de autoritățile publice în domeniile securității naționale, apărării naționale, activității speciale de investigații și urmăririi penale în legătură cu mentenanța rețelelor și sistemelor informatice destinate prelucrării informațiilor din aceste domenii.

(4) În cazul în care tratatele internaționale la care Republica Moldova este parte stabilesc alte norme decât cele prevăzute de prezenta lege, se aplică normele tratatelor internaționale.

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

(6) În cazul în care obligațiile, prevăzute la alineatul (5), stabilite de legile care reglementează activitatea furnizorilor de servicii, sectoarele și subsectoarele stabilite de Guvern, sunt aplicabile unui cerc 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.

(7) Prevederile alineatelor (5) și (6) se aplică de către autoritatea competentă pentru fiecare caz în parte în procesul de identificare a furnizorilor de servicii în conformitate cu prevederile actului normativ stabilit la articolul 4 alineatul (2).

Articolul 4. Identificarea furnizorilor de servicii

(1) Autoritatea competentă întocmește și ține lista furnizorilor de servicii, care cuprinde cel puțin tipul, categoria furnizorului de servicii și sectorul și subsectorul critic în care prestează serviciul respectiv și asigură ori de câte ori este necesar, însă nu mai rar decât o dată la doi ani, actualizarea acesteia.

(2) Guvernul aprobă lista sectoarelor, subsectoarelor critice și, corespunzător, a tipurilor și categoriilor de persoane juridice care prestează servicii în aceste sectoare și subsectoare, stabilește cadrul metodologic privind identificarea persoanelor juridice de drept public și celor de drept privat ca fiind furnizori de servicii, precum și modul de întocmire, ținere și actualizare a listei furnizorilor de servicii.

(3) La solicitarea autorității competente, Serviciul de Informații și Securitate în termen de cel mult 30 de zile din data solicitării, furnizează acesteia lista operatorilor care au în gestiunea lor obiective ale infrastructurii critice, precum și orice modificare a acestei liste în termen de cel mult 30 de zile din data operării modificărilor respective.

(4) Autoritățile publice responsabile de realizarea politicii de stat în sectoarele sau subsectoarele critice, stabilite de Guvern, instituțiile publice responsabile de gestionarea unor domenii conexe sectoarelor și subsectoarelor respective, precum și, dacă e cazul, autoritățile publice de reglementare a acestor sectoare sau subsectoare, asigură suportul necesar autorității competente, la solicitarea acesteia, în procesul de identificare a furnizorilor de servicii.

Articolul 5. Principiile de asigurare a securității cibernetice

În procesul asigurării securității cibernetice, inclusiv a implementării prevederilor prezentei legi, persoanele responsabile trebuie să acționeze luând în considerare următoarele principii:

1) principiul personalității - asigurarea securității rețelelor și a sistemelor informatice este organizată de către furnizorii de servicii;

2) principiul protecției integrale – furnizorii de servicii verifică riscurile potențiale pe care le prezintă rețelele și sistemele informatice pe care le dețin și aplică măsuri organizatorice și tehnice adecvate pentru protecția acestora;

3) principiul reducerii la minimum a efectelor negative - în cazul unui incident cibernetic, furnizorul de servicii aplică măsurile necesare pentru a evita escaladarea efectului incidentului cibernetic și posibila răspândire a acestuia la o altă rețea sau un alt sistem informatic și notifică incidentul cibernetic autorității competente conform prezentei legi;

4) principiul proporționalității - constă în asigurarea unui echilibru între riscurile la care rețelele și sistemele informatice sunt supuse și cerințele de securitate implementate;

5) principiul cooperării - în asigurarea securității cibernetice și în soluționarea incidentelor cibernetice, persoanele responsabile cooperează și, dacă este necesar, iau în considerare conexiunea mutuală dintre sisteme și servicii și dependența acestora.

Capitolul II. CADRUL INSTITUȚIONAL, COOPERAREA ȘI COORDONAREA STRATEGICĂ LA NIVEL NAȚIONAL

Articolul 6. Planificarea și coordonarea strategică în domeniul securității cibernetice la nivel național

(1) Coordonarea strategică la nivel național în domeniul securității cibernetice se realizează de Guvern prin intermediul autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice.

(2) Pentru asigurarea realizării funcției de coordonare strategică, Guvernul instituie și stabilește modul de organizare și funcționare a Consiliului coordonator în domeniul securității cibernetice, organ colegial fără personalitate juridică, a cărui funcție de bază este promovarea și coordonarea, la nivel strategic și operațional, a politicilor în domeniul securității cibernetice.

(3) Strategia națională de securitate cibernetică este un document de politici care definește obiectivele strategice și măsurile de politică și de reglementare care au ca scop atingerea și menținerea unui nivel ridicat de securitate cibernetică. Strategia națională de securitate cibernetică se aprobă de către Parlament la propunerea Guvernului.

Articolul 7. Autoritatea competentă

(1) Guvernul desemnează autoritatea competentă la nivel național în domeniul securității cibernetice și stabilește modul de organizare și funcționare a acesteia.

(2) Autoritatea competentă exercită și funcțiile de punct național unic de contact și echipă de răspuns la incidentele cibernetice la nivel național.

(3) Autoritatea competentă exercită următoarele atribuții principale:

a) identifică și ține evidența furnizorilor de servicii pe teritoriul Republicii Moldova;

b) elaborează și asigură promovarea celor mai bune practici pentru gestionarea incidentelor cibernetice și a riscurilor;

c) asigură interacțiunea strategică la nivel internațional și schimbul de experiență cu alte state, organizații internaționale sau entități create de acestea privind aspecte legate de securitatea cibernetică;

d) asigură interacțiunea în domeniul securității cibernetice cu autoritățile și instituțiile publice naționale și cu furnizorii de servicii;

e) exercită supravegherea și controlul respectării de către furnizorii de servicii a obligațiilor ce le revin conform prezentei legi;

f) emite acte cu caracter obligatoriu, recomandări și orientări metodologice pentru furnizorii de servicii în vederea conformării și remedierii deficiențelor constatate și stabilește termenul până la care aceștia trebuie să se conformeze;

g) examinează sesizări cu privire la neîndeplinirea sau îndeplinirea necorespunzătoare a obligațiilor de către furnizorii de servicii;

h) alte atribuții care decurg din prevederile prezentei legi și actele normative.

(4) În exercitarea funcției de echipă de răspuns la incidentele cibernetice la nivel național, autoritatea competentă exercită următoarele atribuții principale:

1) coordonează procesul de asigurare a securității cibernetice, de prevenire și de soluționare a incidentelor cibernetice în conformitate cu prevederile prezentei legi și actele normative aprobate în scopul punerii acestora în aplicare;

2) monitorizează și analizează amenințările cibernetice, vulnerabilitățile și incidentele cibernetice la nivel național, precum și acordă asistență furnizorilor de servicii, la solicitarea acestora, în procesul de monitorizare de către aceștia a rețelilor și sistemelor lor informatice;

3) emite avertizări timpurii, alerte, anunțuri și diseminează informații privind amenințările cibernetice, vulnerabilitățile și incidentele cibernetice;

4) recepționează notificări privind incidentele cibernetice;

5) asigură răspunsul la incidente cibernetice, în conformitate cu procedurile stabilite de prezenta lege și actele normative de punere în aplicare a acestora, inclusiv acordă asistență în acest sens furnizorilor de servicii;

6) colectează și analizează date criminalistice și furnizează analize dinamice de risc și de incident și conștientizare a situației în materie de securitate cibernetică;

7) cooperează, la nivel național și internațional, cu echipele de răspuns la incidentele cibernetice, inclusiv în cadrul unei platforme de management al incidentelor cibernetice și pentru schimbul de informații;

8) efectuează, la cererea unui furnizor de servicii, scanări proactive a rețelilor și a sistemelor informatice ale solicitantului pentru a detecta vulnerabilitățile cu un impact potențial semnificativ, în conformitate cu actul normativ aprobat de Guvern în temeiul articolului 12 alineatul (9);

9) implementează în schimbul de informații cu furnizorii de servicii și alte persoane relevante instrumente și soluții tehnice securizate, precum și asigură, în conformitate cu legislația, protecția informațiilor de care ia cunoștință în procesul exercitării atribuțiilor sale;

10) exercită atribuțiile de coordonator al procesului de divulgare coordonată a vulnerabilităților conform cadrului normativ aprobat de Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice, inclusiv:

a) intermedierea și facilitarea interacțiunii dintre persoana fizică sau juridică care raportează o vulnerabilitate și producătorul sau furnizorul de produse TIC sau servicii TIC potențial vulnerabile, la cererea oricăreia dintre aceste persoane;

b) identificarea și contactarea persoanelor fizice sau juridice implicate;

c) acordarea asistenței persoanelor fizice sau juridice care raportează o vulnerabilitate;

d) negocierea calendarelor de divulgare și gestionarea vulnerabilităților care afectează mai multe entități;

e) asigurarea anonimatului persoanelor fizice sau juridice care raportează o vulnerabilitate, atunci când acestea o solicită.

(5) În exercitarea funcției de punct național unic de contact, autoritatea competentă exercită următoarele atribuții principale:

a) asigură o legătură a autorităților și instituțiilor publice naționale cu autoritățile similare din alte state și/sau cu organizații internaționale sau entități constituite de către acestea;

b) transmite, la cererea autorităților și instituțiilor publice sau a echipelor de răspuns la incidente cibernetice către punctele unice de contact din alte state notificări și solicitări privind incidentele cibernetice;

c) transmite autorităților și instituțiilor publice naționale, conform competenței acestora, notificări și cereri în materie de securitate cibernetică primite din alte state sau de la organizații internaționale ori de la entitățile constituite de către acestea.

Articolul 8. Centrul guvernamental de răspuns la incidente cibernetice

(1) Pentru asigurarea securității cibernetice la nivel guvernamental, Guvernul instituie centrul guvernamental de răspuns la incidentele cibernetice la nivelul rețelelor și sistemelor informatice ale căror proprietar este statul, desemnează

persoana juridică de drept public responsabilă de exercitarea funcțiilor respective și stabilește modul de organizare și funcționare al centrului respectiv.

(2) Guvernul este responsabil de asigurarea cu resursele necesare a centrului guvernamental de răspuns la incidentele cibernetice pentru prevenirea, analiza, identificarea și răspunsul la incidentele cibernetice la nivelul rețelelor și sistemelor informatice ale căror proprietar este statul.

(3) Centrul guvernamental de răspuns la incidentele cibernetice este responsabil de asigurarea securității rețelelor și sistemelor informatice ale căror proprietar este statul și de facilitarea realizării de către furnizorii de servicii – persoane juridice de drept public a obligațiilor de asigurare a securității cibernetice prevăzute de prezenta lege, inclusiv a celor de notificare, și a interacțiunii acestora cu autoritatea competentă și echipa de răspuns la incidente cibernetice la nivel național.

Articolul 9. Cadrul național de gestionare a crizelor în domeniul securității cibernetice

(1) Autoritatea competentă este responsabilă de gestionarea incidentelor cibernetice și a crizelor în domeniul securității cibernetice la nivel național.

(2) În acest scop autoritatea competentă elaborează și aprobă planul național de răspuns la incidentele cibernetice și crizele în domeniul securității cibernetice în care sunt stabilite obiectivele și modalitățile de gestionare a incidentelor cibernetice și a crizelor de securitate cibernetică la nivel național.

(3) Planul național de răspuns la incidente cibernetice și crize în domeniul securității cibernetice trebuie să includă cel puțin însă fără să se limiteze la acestea:

- a) obiectivele măsurilor și ale activităților naționale de pregătire;
- b) sarcinile și responsabilitățile autorităților naționale competente;
- c) procedurile de gestionare a crizelor și canalele de schimb de informații;
- d) măsurile de pregătire, inclusiv exerciții și activități de formare;
- e) furnizorii de servicii, interacțiunea dintre aceștia și autoritățile sau instituțiile publice responsabile, precum și infrastructura implicată;
- f) procedurile și mecanismele de interacțiune dintre autoritățile și instituțiile publice responsabile la nivel național, precum și de interacțiune coordonată a acestora în gestionarea incidentelor și a crizelor de securitate cibernetică de mare amploare, inclusiv a celor la nivel european și internațional.

(4) Guvernul aprobă cadrul metodologic privind elaborarea, actualizarea și implementarea prevederilor planului național de răspuns la incidente cibernetice și crize de securitate cibernetică, interacțiunea dintre autoritățile și instituțiile publice cu atribuții în procesul de elaborare și actualizare, precum și interacțiunea acestora cu sectorul privat.

Articolul 10. Registrul de stat al incidentelor cibernetice

(1) În scopul evidenței datelor privind apariția, evoluția și soluționarea incidentelor cibernetice, precum și a automatizării proceselor de identificare, înregistrare, documentare, clasificare, analiză și gestionare a astfel de incidente, a monitorizării și evidenței alertelor, amenințărilor cibernetice și vulnerabilităților de securitate cibernetică, Guvernul, la propunerea autorității competente instituie și reglementează modul de organizare și funcționare a Registrului de stat al incidentelor cibernetice și, corespunzător, a sistemului informațional destinat ȋnerii acestuia.

(2) Accesul la registru este limitat, iar datele din registru sunt destinate utilizării interne, cu excepția cazului ȋn care cadrul normativ prevede altfel.

Capitolul III. OBLIGAȚII PRIVIND ASIGURAREA SECURITĂȚII CIBERNETICE

Articolul 11. Măsurile de securitate

(1) Furnizorul de servicii este obligat să aplice continuu măsuri de securitate ȋn scopul:

- a) prevenirii incidentelor cibernetice;
- b) soluționării incidentelor cibernetice;
- c) prevenirii și atenuării impactului asupra continuității serviciului sau a securității rețelei și/sau a sistemului informatic cauzat de un incident cibernetic;
- d) prevenirii și atenuării unui posibil impact asupra continuității unui serviciu ori rețea sau sistem informatic dependente de cele ale furnizorului de servicii.

(2) ȋn procesul aplicării măsurilor de securitate, furnizorul de servicii este obligat:

- a) să evalueze vulnerabilitățile și riscurile rețelei și sistemului informatic, să determine severitatea impactului unui eventual incident cibernetic survenit urmare a

materializării riscurilor, să descrie măsurile pentru soluționarea unui incident cibernetic, precum și să întocmească un raport de evaluare în acest sens;

b) să implementeze măsuri tehnice și organizatorice corespunzătoare și proporționale, în conformitate cu standardele menționate la alineatul (4) litera a), pentru a gestiona riscurile legate de securitatea rețelelor și a sistemelor informatice pe care le utilizează în activitatea sa. Măsurile de securitate trebuie să includă cel puțin următoarele:

1) politici referitoare la analiza riscurilor și securitatea rețelelor și sistemelor informatice;

2) politici și proceduri privind gestionarea incidentelor (prevenire, detectare și răspuns la incidente);

3) politici și proceduri privind utilizarea criptografiei și a criptării în special a criptării de la un capăt la altul;

4) politici și proceduri pentru a evalua eficacitatea măsurilor de securitate implementate;

5) măsuri privind continuitatea activității, inclusiv gestionarea copiilor de rezervă și recuperarea în caz de dezastru, precum și gestionarea crizelor;

6) măsuri de securitate aplicate în achiziționarea, dezvoltarea și întreținerea rețelelor și a sistemelor informatice, inclusiv gestionarea vulnerabilităților și divulgarea acestora;

7) măsuri de securitate a resurselor umane, politici de control al accesului și gestionarea activelor;

8) măsuri privind securitatea lanțului de aprovizionare, inclusiv aspectele legate de securitate referitoare la relațiile furnizorului de servicii cu prestatorii sau furnizorii săi direcți de servicii;

9) practici de bază în materie de igienă cibernetică și formare în domeniul securității cibernetice;

10) utilizarea soluțiilor de autentificare, de comunicații securizate voce, video și text și de sisteme securizate de comunicații de urgență în cadrul furnizorului de servicii;

c) să mențină în stare de actualitate documentația privind măsurile de securitate;

d) să asigure monitorizarea situației privind securitatea rețelelor și sistemelor sale informatice, inclusiv în scopul detectării serviciilor TIC, proceselor TIC sau produselor TIC care compromit aceste rețele sau sisteme;

e) să întreprindă măsuri orientate spre reducerea impactului și a răspândirii unui incident cibernetic, inclusiv, dacă este necesar, restricționarea utilizării sau accesului la rețeaua sau sistemul informatic;

f) verifică suficiența și conformitatea aplicării măsurilor de securitate, inclusiv prin efectuarea auditurilor de securitate, și documentează rezultatele acestei verificări.

(3) În cazul în care furnizorul de servicii autorizează un terț să administreze rețeaua și/sau sistemul informatic ori utilizează serviciile unui terț pentru găzduirea sistemului informatic, acesta este responsabil pentru aplicarea măsurilor de securitate a rețelei și/sau sistemului informatic de către terț.

(4) În vederea asigurării îndeplinirii obligațiilor prevăzute în prezentul articol și a securității rețelelor și sistemelor informatice ale furnizorilor de servicii, Guvernul:

a) prin intermediul organismului național de standardizare, asigură aprobarea standardelor naționale în domeniul securității informației și securității cibernetice în baza standardelor și a specificațiilor tehnice europene și internaționale relevante pentru securitatea rețelelor și a sistemelor informatice;

b) la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice, aprobă cerințele specifice de securitate a rețelelor și sistemelor informatice, în funcție de sectorul, subsectorul, categoria și/sau tipul furnizorului de servicii.

Articolul 12. Obligațiile de notificare

(1) Furnizorul de servicii informează imediat autoritatea competentă, dar nu mai târziu de 24 de ore din momentul în care a luat cunoștință despre:

a) un incident cibernetic care are un impact semnificativ asupra securității rețelei sau sistemului informatic ori asupra continuității serviciului;

b) un incident cibernetic al cărui impact semnificativ asupra securității rețelei sau sistemului informatic ori asupra continuității serviciului nu este evident, dar poate fi presupus în mod rezonabil;

c) impactul semnificativ al unui incident cibernetic, care a afectat un terț, asupra continuității serviciului său dacă prestarea acestui serviciu depinde de serviciile prestate de acest terț.

(2) Autoritatea competentă prezintă, fără întârzieri nejustificate însă nu mai târziu de 24 de ore de la primirea informației menționate la alineatul (1), furnizorului

de servicii un răspuns inițial cu privire la incidentul semnificativ și, dacă furnizorul de servicii solicită, orientări sau instrucțiuni operaționale privind punerea în aplicare a unor eventuale măsuri de soluționare a incidentului cibernetic, inclusiv de atenuare a impactului acestuia, precum și de continuitate a activității, inclusiv de aplicare a unor mecanisme de recuperare în caz de dezastru.

(3) Furnizorul de servicii, prezintă autorității competente, imediat, dar nu mai târziu de 72 de ore din momentul în care a luat cunoștință despre incidentul cibernetic, o actualizare a informațiilor prezentate în conformitate cu alineatul (1) și o evaluare inițială a incidentului cibernetic cu impact semnificativ, inclusiv a gravității și a impactului acestuia, precum și a indicatorilor de compromitere, dacă sunt disponibili.

(4) În cazul în care rețeaua sau sistemul informatic al furnizorului de servicii este administrat și/sau găzduit de un terț, furnizorul de servicii trebuie să se asigure că terțul îl informează în termenii stabiliți la alineatele (1) și (3) despre un incident cibernetic, specificat în alineatul (1) sau că terțul informează concomitent în aceiași termeni autoritatea competentă despre faptul producerii unui astfel de incident cibernetic.

(5) Un incident cibernetic are un impact semnificativ dacă este îndeplinită cel puțin una dintre următoarele condiții:

a) severitatea consecințelor incidentului cibernetic este determinat ca fiind cel puțin înalt în raportul de evaluare a riscurilor rețelei și sistemului informatic, întocmit în conformitate cu prevederile articolul 11 alineatului (2) litera a) și în cerințele prevăzute de actele menționate la articolul 11 alineatul (4);

b) din cauza incidentului cibernetic, prestarea serviciului nu poate fi continuată după expirarea perioadei de timp maxime admise stabilite în acordul privind nivelul agreeat al serviciilor încheiat în cadrul relațiilor contractuale ale furnizorului de servicii cu alte persoane, sau prevăzute de cerințele privind continuitatea serviciului stabilite în documentația prevăzută la articolul 11 alineatul (2) literele a), b), și c);

c) continuitatea serviciului unui alt furnizor de servicii este perturbată de incidentul cibernetic;

d) furnizorului de servicii care notifică incidentul cibernetic, altui furnizor de servicii sau utilizatorilor serviciilor le-au fost cauzate sau le-ar putea fi cauzate prejudicii materiale sau non-materiale considerabile din cauza incidentului cibernetic.

(6) Furnizorul de servicii este obligat să informeze fără întârzieri nejustificate, însă nu mai târziu de 24 de ore din momentul în care a luat cunoștință despre o amenințare cibernetică semnificativă, destinatarii serviciilor pe care le prestează, care ar putea fi afectați de o astfel de amenințare, privind măsurile, inclusiv de ordin corectiv, pe care aceștia le-ar putea lua pentru a evita materializarea amenințării respective. În cazul în care, furnizorul de servicii este în imposibilitate de a identifica și notifica în mod individual destinatarii potențial afectați, acesta informează publicul. În cazul în care constată că materializarea amenințării cibernetice semnificative este iminentă, furnizorul de servicii informează destinatarii serviciilor sale despre amenințarea cibernetică semnificativă propriu-zisă.

(7) În cazul în care furnizorul de servicii nu realizează obligațiunile de notificare prevăzute de alineatul (6) în termenul respectiv, autoritatea competentă solicită expres furnizorului de servicii realizarea obligațiunii de notificare și, dacă acesta nu o realizează în termen de cel mult 3 ore din momentul solicitării, autoritatea competentă asigură notificarea destinatarilor posibil afectați sau publicul, informând despre aceasta furnizorul de servicii. Modul de informare a destinatarilor de către furnizorii de servicii sau de către autoritatea competentă constituie obiect de reglementare a actului normativ prevăzut de alin (9).

(8) În cazul soluționării unui incident cibernetic cu impact semnificativ, furnizorul de servicii este obligat, în termen de cel mult o lună de la transmiterea informației actualizate în temeiul alineatului (3), să transmită autorității competente un raport care să includă cel puțin informații despre cauzele producerii incidentului cibernetic, timpul de soluționare a acestuia, măsurile aplicate și impactul incidentului cibernetic.

(9) Procedura de notificare a incidentelor cibernetice, inclusiv interacțiunea dintre furnizorul de servicii și autoritatea competentă, modul de stabilire a impactului unui incident cibernetic și formatul informațiilor evaluărilor și rapoartelor prezentate în procesul de gestionare a unui incident cibernetic sunt stabilite de Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice.

(10) Obligația prevăzută la alineatul (1) nu limitează dreptul furnizorului de servicii de a notifica autoritatea competentă cu privire la amenințările cibernetice și la incidentele evitate la limită, precum și la incidentele cibernetice care nu au un impact semnificativ prevăzut la alineatul (5)

(11) Furnizorii de servicii – persoane juridice de drept public notifică centrul guvernamental de răspuns la incidente cibernetice cu privire la incidentele cibernetice în vederea îndeplinirii obligațiilor prevăzute de prezentul articol. Centrul guvernamental de răspuns la incidente cibernetice informează autoritatea competentă cu privire la incidentele cibernetice prevăzute de literele a) – c).

Articolul 13. Notificarea voluntară

(1) Persoanele juridice de drept public sau de drept privat care nu sunt identificate de autoritatea competentă ca furnizori de servicii, precum și persoanele fizice, pot transmite acesteia notificări cu privire la incidente cibernetice semnificative, amenințări cibernetice și incidente cibernetice evitate la limită.

(2) Notificările menționate la alineatele (1) și (2), sunt soluționate de către autoritatea competentă conform procedurilor stabilite de prezenta lege și a actului aprobat în temeiul articolului 12 alineatului (8), acordând prioritate examinării și soluționării notificărilor obligatorii conform prevederilor prezentei legi și asigurând confidențialitatea și protecția adecvată a informațiilor furnizate de către persoana care a notificat.

(3) Notificarea voluntară nu impune persoanelor menționate la alineatele (1) și (2) nicio obligație suplimentară care nu le-ar fi revenit dacă nu ar fi transmis notificarea, exceptând obligațiile care le revin sau le-ar putea reveni conform legislației corespunzătoare în contextul desfășurării acțiunilor de prevenire, investigare, depistare și urmărire penală a infracțiunilor.

Articolul 14. Măsurile de securitate ale rețelelor și sistemelor informatice ale persoanelor juridice de drept public

(1) Persoane juridice de drept public sunt obligate să aplice măsurile stabilite la articolului 11 alineatele (1), (2) și (3) și cerințele de notificare obligatorie a unui incident cibernetic prevăzute la articolul 12.

(2) Măsurile de securitate minime obligatorii pentru persoanele juridice de drept public, sunt stabilite de Guvern la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice.

Articolul 15. Prevenirea și soluționarea incidentelor cibernetice

(1) În scopul asigurării securității cibernetice, autoritatea competentă monitorizează numele de domenii din spațiul de adrese în Internet al Republicii Moldova și legate de domeniul de nivel superior .md, analizează riscurile, precum și impactul acestora asupra statului, societății și securității rețelelor și sistemelor informatice.

(2) Pentru contracararea unei amenințări cibernetice semnificative imediate asupra securității rețelelor și sistemelor informatice sau pentru eliminarea sau atenuarea consecințelor unui incident cibernetic semnificativ, autoritatea competentă restricționează utilizarea sau accesul la o rețea sau un sistem informatic, dacă sunt îndeplinite cumulativ următoarele condiții:

a) incidentul cibernetic compromite sau dăunează securității altei rețele sau sistem informatic;

b) administratorul rețelei sau sistemului informatic nu poate în timp util să contracareze amenințarea semnificativă sau să elimine perturbarea gravă provocată de incidentul cibernetic;

c) nu este posibilă contracararea amenințării grave sau eliminarea perturbării grave provocate de incidentul cibernetic prin aplicarea unei alte măsuri;

d) nu se provoacă un prejudiciu disproporționat prin contracararea amenințării grave sau prin eliminarea perturbării provenite din incidentul cibernetic.

(3) Autoritatea competentă notifică în cel mai scurt timp însă nu mai târziu de 24 de ore, referitor la aplicarea măsurilor prevăzute la alineatul (2), destinatarul și, în cazul unui furnizor de servicii, autoritatea publică care realizează politica de stat în domeniul respectiv și, dacă e cazul, autoritatea cu funcții regulatorii pe piața din domeniul în care se prestează serviciul respectiv.

(4) În exercitarea competenței sale în procesul gestionării incidentelor cibernetice, autoritatea competentă este obligată să țină cont de interesele de afaceri ale furnizorului de servicii, să asigure păstrarea secretului comercial în condițiile legislației. Autoritatea competentă asigură protecția informațiilor atribuite la secretul de stat și a datelor cu caracter personal în conformitate cu prevederile actelor normative din aceste domenii

(5) Autoritatea competentă informează Serviciul de Informații și Securitate imediat, însă nu mai târziu de 24 de ore din momentul în care a luat cunoștință despre incidente cibernetice cu impact semnificativ, prevenite sau soluționate, care au vizat obiectivele infrastructurii critice.

Articolul 16. Schimbul transfrontalier de informații

În contextul realizării atribuțiilor funcționale prevăzute de prezenta lege, sau în temeiul unei obligații care decurge dintr-un tratat internațional, autoritatea competentă are dreptul de a transmite unui alt stat sau unei organizații internaționale informații privind prevenirea și soluționarea unui incident cibernetic, în cazul în care nu există riscul ca informațiile transmise să prejudicieze securitatea națională sau desfășurarea procedurilor de urmărire penală.

Articolul 17. Schimbul de informații voluntar

(1) Furnizorii de servicii și, după caz, alte persoane juridice care nu intră în domeniul de aplicare al prezentei legi, pot face schimb reciproc de informații relevante în materie de securitate cibernetică, în mod voluntar, inclusiv schimb de informații referitoare la amenințări cibernetice, incidente cibernetice evitate la limită, vulnerabilități, tehnici și proceduri, indicatori de compromitere, tactici adversariale, informații specifice entității care generează amenințări, alerte de securitate cibernetică și recomandări privind configurația instrumentelor de securitate cibernetică pentru detectarea atacurilor cibernetice, în cazul în care un astfel de schimb de informații:

a) vizează prevenirea și detectarea incidentelor, răspunsul la incidente sau redresarea în urma acestora sau atenuarea impactului lor;

b) sporește nivelul de securitate cibernetică, în special prin sensibilizarea cu privire la amenințările cibernetice, prin limitarea sau împiedicarea posibilității răspândirii unor asemenea amenințări, sprijinirea gamei de capacități defensive, remedierea și divulgarea vulnerabilităților, detectarea amenințărilor, tehnicile de limitare și prevenire a amenințărilor, strategiile de atenuare sau etapele proceselor de răspuns și de recuperare sau promovarea colaborării dintre persoanele juridice de drept public și cele de drept privat în domeniul cercetării amenințărilor cibernetice.

(2) Autoritatea competentă intermediază schimbul de informații între persoanele juridice menționate la alineatul (1) prin crearea și gestionarea unor platforme, inclusiv tehnico-tehnologice, și comunități de încredere. Pentru a asigura protecția informațiilor ce au un caracter potențial sensibil, autoritatea competentă facilitează semnarea acordurilor de schimb de informații între participanții la astfel de platforme și comunități. Modul de semnare, conținutul și alte aspecte privind acordurile de schimb de informații se stabilesc de autoritatea competentă.

(3) Persoanele juridice de drept public pot semna acorduri de schimb de informații în materie de securitate cibernetică în condițiile stabilite de regulamentul aprobat de Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii statului în domeniul securității cibernetică.

(4) Furnizorii de servicii sunt obligați să informeze autoritatea competentă despre semnarea acordurilor privind schimbul de informații în materie de securitate cibernetică menționate la alineatul (2) sau retragerea din astfel de acorduri, în termen de 3 zile din data semnării sau, după caz, a retragerii.

Capitolul IV. SUPRAVEGHERE ȘI CONTROL DE STAT

Articolul 18. Supravegherea

(1) Autoritatea competentă exercită funcția de supraveghere a respectării prevederilor prezentei legi de către furnizorii de servicii prin monitorizarea continuă a modului în care aceștia realizează obligațiile ce le revin conform prevederilor prezentei legi și a actelor normative de punere în aplicare a acestora, inclusiv prin efectuarea auditurilor de securitate.

(2) În cazul în care un furnizor de servicii responsabil de gestionarea incidentului cibernetic nu este în măsură să răspundă sau să soluționeze în timp util un incident cibernetic, autoritatea competentă asigură aplicarea măsurilor necesare pentru soluționarea incidentului cibernetic.

(3) Modul de aplicare a măsurilor de supraveghere se stabilesc de Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetică.

Articolul 19. Controlul de stat

(1) Autoritatea competentă exercită controlul respectării prezentei legi de către furnizorii de servicii persoane juridice de drept privat, aplicând prevederile Legii nr.131/2012 privind controlul de stat a activității de întreprinzător.

(2) Autoritatea competentă realizează controlul exclusiv în baza unui act motivat emis în acest scop, în baza evaluării riscurilor pentru securitatea rețelelor și sistemelor informaționale ale furnizorilor de servicii, precum și cu înștiințarea în prealabil a furnizorului de servicii despre controlul preconizat.

(3) În vederea efectuării controlului, autoritatea competentă are dreptul să beneficieze de acces la informațiile, bunurile și încăperile deținute de furnizorul de servicii supus controlului, care sunt necesare realizării obiectivelor controlului.

(4) Autoritatea competentă efectuează controale numai în cazul în care:

a) a depistat și, urmare a unei investigații preliminare, a confirmat fapte de încălcare a prevederilor prezentei legi; și/sau

b) a fost sesizată cu privire la încălcări, neîndeplinirea sau îndeplinirea necorespunzătoare a obligațiilor prevăzute de prezenta lege de către furnizorul de servicii.

(5) Guvernul, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice, stabilește separat, pentru furnizorii de servicii – persoane juridice de drept privat și furnizorii de servicii – persoane juridice de drept public, procedurile detaliate privind modul de efectuare a controlului de către autoritatea competentă asupra respectării de către aceștia a obligațiilor ce le revin conform prezentei legi.

Capitolul V. PROTECȚIA DATELOR CU CARACTER PERSONAL. RĂSPUNDEREA. FINANȚAREA

Articolul 20. Protecția datelor cu caracter personal

(1) În exercitarea competenței cu care este investită prin prezenta lege autoritatea competentă prelucrează date cu caracter personal în condițiile stabilite de legislația în acest domeniu.

(2) În cazul în care, în procesul exercitării funcțiilor sale autoritatea competentă ia cunoștință de faptul că o încălcare de către un furnizor de servicii a obligațiilor prevăzute de prezenta lege poate atrage după sine o încălcare a legislației privind protecția datelor cu caracter personal, autoritatea competentă informează imediat organul de control al prelucrărilor de date cu caracter personal.

Articolul 21 Răspunderea

(1) Personalul autorității competente poartă răspundere, în conformitate cu legislația, pentru neîndeplinirea sau îndeplinirea necorespunzătoare a atribuțiilor funcționale stabilite de actele normative.

(2) Personalul autorităților/instituțiilor publice, furnizorilor de servicii care interacționează cu autoritatea competentă în condițiile prezentei legi, poartă

răspundere, în conformitate cu legislația, pentru neîndeplinirea sau îndeplinirea necorespunzătoare a atribuțiilor funcționale stabilite de actele normative.

Articolul 22. Finanțarea implementării prezentei legi

(1) Finanțarea activității autorității competente se efectuează din bugetul de stat în limita alocațiilor aprobate prin legea bugetară anuală.

(2) Implementarea prevederilor prezentei legi de către furnizorii de servicii – persoane juridice de drept public este finanțată din contul bugetul de la care se finanțează activitatea persoanelor juridice respective în limita alocațiilor aprobate prin legea/decizia bugetară anuală.

(3) Implementarea prevederilor prezentei legi de către furnizorii de servicii – persoane juridice de drept privat - se efectuează din contul mijloacelor acestor persoane juridice.

(4) Pentru punerea în aplicare a prevederilor prezentei legi Guvernul poate atrage mijloace financiare provenite din proiecte de asistență externă.

Capitolul VI. DISPOZIȚII FINALE ȘI TRANZITORII

Articolul 23. Intrarea în vigoare a legii și măsuri de implementare

(1) Prezenta lege intră în vigoare la data de 1 ianuarie 2025.

(2) Guvernul:

a) în termen de 9 luni de la data publicării prezentei legi, va întreprinde măsurile necesare pentru desemnarea autorității competente, precum și reglementarea modului de organizare și funcționare și stabilirea structurii și efectivului limită a acesteia;

b) în termen de 6 luni de la data publicării prezentei legi va prezenta propuneri Parlamentului privind aducerea actelor normative în concordanță cu prezenta lege;

c) în termen de 12 luni de la data publicării prezentei legi va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi, inclusiv va determina autoritatea administrației publice centrale de specialitate responsabilă de realizarea politicii de stat în domeniul securității cibernetice;

d) în termen de 12 luni de la data intrării în vigoare a prezentei legi va elabora, va aproba și va prezenta Parlamentului spre examinare Strategia națională în domeniul securității cibernetice.

(3) Autoritatea competentă:

în termen de 3 luni de la data intrării în vigoare a actelor normative prevăzute la articolul 4 alineatul (2), va identifica furnizorii de servicii, îi va notifica în modul stabilit și îi va include în Lista furnizorilor de servicii, întocmită în condițiile prezentei legi;

va aproba actele normative necesare punerii în aplicare a prevederilor prezentei legi.

Notă informativă
la proiectul de lege privind securitatea cibernetică

1. Denumirea autorului și, după caz, a participanților la elaborarea proiectului

(În calitate de denumire a autorului se indică denumirea autorității publice responsabile, conform competențelor, de elaborarea și promovarea proiectului actului normativ. Dacă în vederea elaborării proiectului a fost constituit un grup de lucru, se indică numărul și data documentului prin care s-a constituit grupul de lucru respectiv.)

Proiectul a fost elaborat de Ministerul Economiei, cu suportul proiectului Uniunii Europene „Moldova Cybersecurity Rapid Assistance”

2. Condițiile ce au impus elaborarea proiectului de act normativ și finalitățile urmărite

(La acest compartiment se indică prevederile concrete din documentele de politici din care rezultă necesitatea elaborării proiectului actului normativ.

De asemenea, se indică finalitățile urmărite prin adoptarea actului normativ, precum și rezultatele scontate după adoptarea și implementarea acestuia, se descrie viziunea clară privind efectele actului normativ după implementarea prevederilor acestuia.

În cazul proiectelor actelor normative ce reglementează activitatea de întreprinzător, suplimentar se descriu concluziile și propunerile înaintate în cadrul studiilor de cercetare, precum și rezultatele analizei ex ante sau ale analizei impactului de reglementare.

Se prezintă argumentarea, în baza evaluării beneficiilor, a necesității adoptării actului normativ și, după caz, analiza de impact al acestuia asupra activității de întreprinzător, inclusiv prin prisma respectării drepturilor și intereselor întreprinzătorilor și ale statului.

Se prezintă lista lucrărilor științifice, studiilor de cercetare, rapoartelor, recomandărilor internaționale și a altor materiale care au fost luate în considerare la elaborarea proiectului actului normativ)

1. Condițiile ce au impus elaborarea proiectului de act normativ (documentele de politici din care rezultă necesitatea elaborării proiectului de lege)

Cadrul politicii de securitate cibernetică este oferit de un set de documente de politici adoptate de Parlament sau Guvern și care oferă viziunea strategică pentru țară cu privire la modul de înființare, consolidare și asigurare a rezilienței sistemului de securitate cibernetică în Republica Moldova.

Astfel, **Concepția securității informaționale**¹, aprobată prin Legea nr. 299/2017, reprezintă o viziune de ansamblu asupra scopului, obiectivelor, principiilor și direcțiilor de bază ale activității de asigurare a unui nivel înalt al securității informaționale a Republicii Moldova, ca parte componentă a sistemului național de securitate. Potrivit acestei concepții măsurile de prevenire, depistare și contracarare a amenințărilor complexe și persistente la adresa securității informaționale pot fi întreprinse doar cu condiția existenței și funcționării unui cadru normativ corespunzător în domeniu, a unor instrumente și metode bine definite, a unor mecanisme de colaborare la nivel național și internațional.

Concepția a constituit baza pentru elaborarea **Strategia securității informaționale**² a Republicii Moldova pentru anii 2019-2024 și **Planul de acțiuni** pentru implementarea acesteia, aprobate prin Hotărârea Parlamentului nr. 257/2018. Scopul principal al acestei Strategii este de a lega și integra din punct de vedere juridic domeniile prioritare cu responsabilități și competențe de asigurare a securității informațiilor la nivel național, bazată inclusiv pe reziliența cibernetică. Problemele abordate de Strategie, într-un context mai larg al securității informaționale, se referă la cinci componente de bază: securitate cibernetică și investigarea criminalității cibernetică, securitatea spațiului mediatic, contrainformații și securitate, probleme de natură legală și, în final, probleme de conștientizare a maselor.

Dintre acestea, cu referire la componenta securității cibernetică, Strategia evidențiază ca cele mai proeminente probleme lipsa unui CERT național (Centrul de răspuns la incidente de

¹ https://www.legis.md/cautare/getResults?doc_id=105660&lang=ro

² https://www.legis.md/cautare/getResults?doc_id=111979&lang=ro

securitate cibernetică), responsabil de prevenirea și răspunsul la incidente din domeniul securității cibernetice la scară largă, lipsa unui sistem integrat de management al securității cibernetice și un mecanism viabil de audit al securității cibernetice. În acest context, Strategia stabilește un set de obiective de diferită natură, dintre care evidențiem în mod special următoarele:

- crearea/desemnarea entității care va exercita rolul de Centru național de reacție la incidente de securitate cibernetică și care va constitui punctul unic de raportare a incidentelor de securitate cibernetică pentru autoritățile publice competente și persoanele fizice și juridice – cu termen limită de realizare în anul 2021 (*Obiectivul 1, acțiunea 1) din Planul de acțiuni de implementare a Strategiei*);

- elaborarea cadrului normativ pentru asigurarea unui nivel înalt de securitate a rețelelor și a sistemelor informatice la nivel național în baza bunelor practici ale UE cu termen limită de realizare în anul 2024 (*Obiectivul 1, acțiunea 5) din Planul de acțiuni de implementare a Strategiei*).

Diverse aspecte ale securității cibernetice sunt abordate și în alte documente de politici, interconectate cu Strategia securității informaționale, cum sunt:

- Strategia de securitate națională, aprobată prin Hotărârea Parlamentului nr. 153/2011³ (pct. 4.7)

- Strategia Națională de Apărare și Planul de Acțiuni privind implementarea Strategiei Naționale de Apărare 2018–2022, aprobate prin Hotărârea Parlamentului nr. 134/2018⁴ (pct. 2.8.2)

- Planul individual de acțiuni de parteneriat Republica Moldova – NATO pentru anii 2022–2023, aprobat prin Hotărârea Guvernului nr. 26/2022⁵ (obiectivul 1.7, partea II).

Conform *Programul de activitate al Guvernului „Moldova prosperă, sigură, europeană”*⁶ unul dintre obiectivele fundamentale este prevenirea și combaterea amenințărilor hibride pe palierul securității cibernetice și informaționale. În acest context una dintre priorități în domeniul asigurării securității statului este fortificarea structurilor responsabile pentru lupta împotriva amenințărilor hibride și asigurarea securității cibernetice în vederea sporirii nivelului de siguranță pentru oameni, instituțiile statului și pentru mediul privat. De asemenea inițiativa elaborării unei legi în domeniul securității cibernetice se înscrie și în contextul consacării în Programul de activitate a Guvernului a unor astfel de repere în procesul de integrare europeană, ca obiectiv fundamental al programului,

realizarea deplină a celor nouă pași înaintați de Comisia Europeană în Avizul cu privire la cererea de aderare la Uniunea Europeană;

transpunerea legislației europene care să asigure un nivel bun de pregătire pe toate capitolele de negocieri și operaționalizarea grupurilor de lucru de negociere cu Uniunea Europeană⁷;

³ https://www.legis.md/cautare/getResults?doc_id=105346&lang=ro

⁴ https://www.legis.md/cautare/getResults?doc_id=110013&lang=ro

⁵ https://www.legis.md/cautare/getResults?doc_id=129865&lang=ro

⁶ https://gov.md/sites/default/files/document/attachments/program_de_guv-final_ro.pdf

⁷ Este important de menționat că raportul analitic al Comisiei privind alinierea Republicii Moldova la acquis-ul UE (publicat la 2 februarie 2023) subliniază, la capitolul privind transformarea digitală și mass-media, că Moldova va trebui să se alinieze la cerințele cadrului NIS (Directiva 2016/1148)

https://neighbourhood-enlargement.ec.europa.eu/system/files/2023-02/SWD_2023_32_%20Moldova.pdf, pagina 25

elaborarea și punerea în aplicare a planului național de transpunere a acquis-ului comunitar.

În dezvoltarea acestor obiective și priorități în proiectul Planului de acțiuni al Guvernului⁸ este prevăzută aprobarea și transmiterea Parlamentului spre examinare în trimestrul I al anului 2023 a proiectului de lege privind securitatea cibernetică.

O acțiune similară este prevăzută și de *Planul de acțiuni al Guvernului pentru anii 2021-2022*⁹, aprobat prin Hotărârea Guvernului nr. 235/2021, actualmente în vigoare. Conform acestui Plan Guvernul și-a propus ca obiectiv implementarea unui cadru eficient de securitate cibernetică după modelul statelor cu experiență în acest domeniu (p.2.7) prin elaborarea proiectului de lege privind securitatea rețelor și sistemelor informaționale (p. 2.7.1) cu termen de realizare decembrie 2022, stabilind ca responsabil principal de realizarea acestei acțiuni Ministerul Economiei.

2. Finalitățile urmărite

Proiectul de lege are scopul să creeze cadrul normativ primar care, prin implementarea cerințelor, măsurilor și mecanismelor instituite, să asigure un nivel suficient de ridicat de securitate a rețelor și sistemelor informaționale în Republica Moldova, capabil să asigure protecția intereselor vitale ale persoanelor fizice și juridice, ale societății și ale statului, precum și a intereselor naționale ale Republicii Moldova. Un nivel ridicat de protecție a rețelor și sistemelor informatice în prestarea unor servicii critice în ambele domenii, public și privat, poate fi atins prin asigurarea unui nivel de reziliență cibernetică adecvată provocărilor și amenințărilor atât din mediul cibernetic, cât și din cel non-cibernetic.

În acest context, urmare a implementării prevederilor proiectului de lege Guvernul își propune următoarele:

- desemnarea unei autorități competente în domeniul securității cibernetică cu funcții de identificare a persoanelor juridice care vor intra în cercul de subiecți asupra cărora se vor răsfărge prevederile proiectului (furnizori de servicii) și menținere în stare de actualitate a unei liste a furnizorilor de servicii; de supraveghere și control a măsurilor de securitate pe care furnizorii de servicii trebuie să le implementeze pentru a asigura bun nivel adecvat de securitate a rețelor și sistemelor sale informatice, de stabilire a unor practici comune în gestionarea incidentelor cibernetică și de coordonare operațională a situațiilor de criză, de cooperare și interacțiune la nivel național și internațional și de schimb de experiență cu organizații, state sau alte entități relevante la nivel european în primul rând. În context ținem să evidențiem faptul că Guvernului i se acordă marja discreționară ca, în contextul exercitării prerogativei de desemnare a autorității competente, să decidă fie să desemneze o autoritate publică existentă, fie să instituie o autoritate publică nouă în structura sa administrativă și să o desemneze în calitate de autoritate competentă conform proiectului de lege.

- instituirea unei echipe de răspuns la incidentele de securitate cibernetică (CSIRT) cu competențe la nivel național, asigurarea recunoașterii internaționale a acesteia, în mod special la nivel european, care să exercite atribuții de monitorizare și analiză a amenințărilor cibernetică, vulnerabilităților și incidentelor cibernetică, de răspuns la incidente cibernetică, de asigurare a schimbului de informații și coordonare a procesului de divulgare a vulnerabilităților. Potrivit

⁸ <https://gov.md/sites/default/files/document/attachments/subiect-03-nu-77-cs-2023.pdf>

⁹ https://www.legis.md/cautare/getResults?doc_id=128407&lang=ro

proiectului de lege se propune ca la nivel național CSIRT să fie stabilit în cadrul autorității competente;

- definirea cadrului general strategic și operațional de coordonare și cooperare dintre sectorul public și privat în domeniul securității cibernetice, inclusiv în ce privește gestionarea crizelor și aprobarea unui plan național de răspuns care să asigure pregătirii, a capacității de reacție și a recuperării în caz de incidente cibernetice. În același context, proiectului de lege cuprinde norme juridice primare care vor avea ca efect aprobarea de către Guvern a Strategiei naționale privind securitatea cibernetică și instituirea Consiliului coordonator în domeniul securității cibernetice;

- stabilirea obligativității de a implementa măsuri de securitate de către furnizorii de servicii ale căror servicii sunt critice pentru funcționarea economiei și a societății care să asigure atingerea unui nivel minim comun de securitate a rețelelor și sistemelor informaționale și reziliența serviciilor, ceea ce implicit va avea ca efect pozitiv creșterea nivelului de pregătire și de răspuns la incidentele cibernetice și amenințările de acest fel;

- instituirea unui mecanism obligatoriu de raportare a incidentelor cibernetice semnificative de către furnizorii de servicii, și creare a unui regim de notificare voluntară a incidentelor cibernetice de orice categorie de persoane;

- crearea și asigurarea funcționării adecvate a mecanismelor de cooperare eficiente la nivel național și internațional, prin difuzarea de către autoritatea competentă întregii societăți și în mod deosebit entităților ce furnizează servicii în domenii critice, a informațiilor relevante, a avertizărilor și alertelor, precum și a celor mai bune practici internaționale;

- dezvoltarea unor capacități înalte de reacție la incidentele semnificative sau care ar putea avea impacturi cu potențiale prejudicii considerabile, atât a autorităților responsabile de implementarea politicii de stat în domeniul securității cibernetice, cât și a furnizorilor de servicii.

În conformitate cu prevederile art. 25 din Legea nr.100/2017 privind actele normative și ale Metodologiei de analiză a impactului în procesul de fundamentare a proiectelor de acte normative, aprobată prin Hotărârea Guvernului nr. 23/2019, pentru a estima efectele și consecințele adoptării și implementării actului normativ în speță, a fost elaborată **analiza de impact**. Conform concluziilor relevante de analiza de impact, opțiunea reglementării problematicei securității cibernetice printr-o lege cadru s-a dovedit, din perspectiva raportului pozitiv dintre beneficii și costuri, a fi opțiunea cea mai plauzibilă, inclusiv din punctul de vedere al necesității de a transpune legislația Uniunii Europene în legislația națională.¹⁰ Este de remarcat stringența soluționării chestiunilor ce vizează aspectele instituționale și organizaționale ale acestui domeniu, prin desemnarea unei autorități competente și a unui CSIRT național cu capacități suficiente și necesare pentru a preveni, detecta și răspunde adecvat amenințărilor și incidentelor de securitate cibernetică. Prin intervenția propusă vor fi instituite premisele fundamentale necesare pentru stabilirea clară a responsabilităților și a răspunderii, precum și a mecanismelor orientate spre promovarea unei mai mari încrederi atât la nivel de autorități, cât și la nivel de întreprinderi, stimulând schimbul de informații și asigurând o asistență reciprocă bazată pe încredere și diligență.

Implementarea proiectului de lege bineînțeles va presupune costuri de implementare atât pentru sectorul public, a căror sinteză este prevăzută în capitolul 5 din prezenta notă, cât și pentru cel privat, dar în rezultatul implementării măsurilor și cerințelor propuse se va asigura o

¹⁰ A se vedea nota de referință nr.7

creștere consecventă a nivelului de reziliență cibernetică a entităților-cheie din Republica Moldova, vor fi generate, economii de costuri atât pentru sectorul privat, cât și pentru societate.

Pe termen mediu și lung, atingerea unei creșteri a capacităților în materie de securitate cibernetică la nivel național ar aduce beneficii substanțiale printr-o cooperare la nivel operațional, stimulare și asistență reciprocă și o mai bună interacțiune cu mediul privat.

Elaborarea proiectului de lege a fost precedată de *analiza informațiilor conținute în diferitele studii de cercetare și rapoarte de evaluare*, recomandări metodologice, dedicate atât nemijlocit contextului actual de securitate cibernetică în Republica Moldova, cât și contextului european și internațional în acest domeniu.

Astfel, potrivit *Analizei*¹¹ *modelelor de guvernare națională în domeniul securității cibernetice și recomandări pentru Moldova*, efectuat de proiectul Asistență Rapidă în domeniul Securității Cibernetice pentru Republica Moldova au fost analizate modelele de guvernare a 6 state membre ale UE (Republica Cehă, Estonia, Finlanda, Grecia, Regatul Țărilor de Jos și România) și furnizate recomandări ce au vizat în special:

necesitatea adoptării unei Strategii dedicată exclusiv domeniului securității cibernetice, aliniată la cerințele prevăzute în legislația europeană (Directiva NIS2), cu o mai bună coordonare a implementării și corelată cu alte documente de politici relevante;

modelul de guvernare pentru securitatea cibernetică la nivel național ar trebui să fie mai degrabă unul centralizat, adică să concentreze funcțiile de autoritate competentă, CSIRT național și punct național unic de contact într-o singură autoritate, model caracteristic pentru statele cu resurse limitate;

inițierea în paralel cu o nouă lege privind securitatea cibernetică și a modificărilor în legislația relevantă, inclusiv cea privind infrastructura critică.

elaborarea, aprobarea și dezvoltarea continuă a legislației în domeniul respectiv trebuie însoțită de un amplu proces de consultare publică cu toate părțile interesate, precum și de instruire și dialog constant pentru implementarea legii, dar și pentru conștientizarea sancțiunilor ce urmează a fi aplicate pentru nerespectare.

De asemenea, *Raportul de evaluare*¹² *privind instituirea unei echipe de răspuns la incidente de securitate cibernetică din Republica Moldova*, efectuat de ITU în septembrie 2022 a înaintat mai multe recomandări, dintre care relevăm în mod deosebit recomandarea privind necesitatea unui CSIRT național, mandatat oficial și recunoscut clar ca entitatea competentă să răspundă la incidente și să coordoneze acest proces, acționând ca punct focal în gestionarea incidentelor și ca centru de coordonare pentru a gestiona schimbul de informații și fluxurile de informații, astfel încât toate părțile relevante să poată raporta incidentele către acest punct central, precum și să dispună de capacitățile necesare pentru a furniza cunoștințe despre cele mai bune practici disponibile, etc.

De rând cu studiile menționate mai sus, în procesul elaborării proiectului de lege au fost luate în considerare următoarele:

Ghid de bune practici¹³ al Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA) privind modul de constituire și organizare a unui CSIRT;

¹¹ Analysis of Cybersecurity National Governance Models and Recommendations to Moldova, efectuat de Moldova Cybersecurity Rapid Assistance Project, septembrie, 2022.

¹² Assessment Report of Moldova National Computer Incident Response Team (cirt-mdmd), efectuat de ITU, în septembrie 2022

¹³ <https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc>

Raportul¹⁴ ENISA privind investițiile în rețele și sisteme informatice (NIS);

Evaluarea de impact¹⁵, realizată de Comisia Europeană, la propunerea de Directivă a Parlamentului European și a Consiliului privind măsurile de asigurare a unui nivel ridicat de securitate a rețelelor și a informațiilor în întreaga Uniune (Directiva NIS1), etc.

Raport de evaluare a impactului¹⁶ pentru propunerea de directivă a Parlamentului European și a Consiliului privind măsuri pentru un nivel comun ridicat de securitate cibernetică în întreaga Uniune, de abrogare a Directivei (UE) 2016/1148 (propunerea de Directivă NIS2).

3. Descrierea gradului de compatibilitate pentru proiectele care au ca scop armonizarea legislației naționale cu legislația Uniunii Europene

(În cazul în care actul normativ are ca scop armonizarea legislației naționale cu legislația Uniunii Europene, se indică:

a) dacă intervenția rezultă din angajamentele asumate de Republica Moldova în baza acordurilor bilaterale cu Uniunea Europeană;

b) lista actelor Uniunii Europene cu care se realizează armonizarea;

c) mențiunea privind elaborarea tabelului de concordanță.

După caz, se face referire la reglementările similare existente în legislația statelor membre ale Uniunii Europene.)

Potrivit Programului de Asociere¹⁷ dintre Uniunea Europeană și Republica Moldova pentru perioada 2021-2027 (Recomandarea nr. 1/2022 a Consiliului de Asociere UE-Republica Moldova din 22 august 2022 privind Programul de asociere UE-Republica Moldova [2022/1997]), unul dintre obiectivele generale ale cooperării dintre UE și Republica Moldova este transformarea digitală rezilientă, ceea ce presupune și asigurarea unor cadre juridice, de politică și operaționale solide în materie de securitate cibernetică, pe baza legislației și a bunelor practici ale UE. În continuare acest document determină prioritățile pe termen scurt și lung ale programului în domeniul „Libertate, securitate și justiție”, stabilind colaborarea părților în materie de securitate cibernetică prin implementarea următoarelor măsuri:

- asigurarea punerii în aplicare a măsurilor legate de componenta de securitate cibernetică a Strategiei securității informaționale a Republicii Moldova pentru anii 2019-2024 și a Planului de acțiuni pentru implementarea acesteia;

- consolidarea securității cibernetice prin *transpunerea în dreptul intern a Directivei (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 („Directiva NIS”);

- identificarea și desemnarea în mod oficial a unei echipe naționale de răspuns la urgențe cibernetice (CERT) și stabilirea unei diviziuni clare a muncii și a competențelor între agențiile implicate în asigurarea securității cibernetice;

- elaborarea unei abordări în vederea consolidării cooperării în domeniul securității cibernetice prin intermediul schimbului de informații și de bune practici, în special cu privire la utilizarea setului de instrumente pentru securitatea rețelelor 5G, elaborat de UE.

În același context, una dintre acțiunile, prevăzute de *Planul de acțiuni pentru implementarea măsurilor propuse de către Comisia Europeană în Avizul său privind cererea de aderare a Republicii Moldova la Uniunea Europeană, aprobat de către Comisia Națională pentru Integrare Europeană pe data de 4 august 2022*, ce urmează a fi realizată de Republica Moldova pentru implementarea măsurii de *consolidare a luptei împotriva criminalității organizate, pe baza unor evaluări detaliate ale amenințărilor, a unei cooperări sporite cu*

¹⁴ Report on network and information systems (NIS) investments, ENISA, 2021
(<https://www.enisa.europa.eu/publications/nis-investments-2021>)

¹⁵ <https://data.consilium.europa.eu/doc/document/ST-6342-2013-ADD-2/en/pdf>

¹⁶ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020SC0345>

¹⁷ <https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:2022D1997&from=EN>

partenerii regionali ai UE și internaționali și a unei mai bune coordonări a autorităților de aplicare a legii, propuse de Comisia Europeană, este adoptarea Legii privind securitatea rețelelor și a sistemelor informatice, în conformitate cu Directiva UE privind securitatea rețelelor și a informației (NIS), în vederea stabilirii unui cadru eficient de securitate cibernetică.

La data de 27 decembrie 2022, în Jurnalul Oficial al Uniunii Europene a fost publicată 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). Această Directivă vine să înlocuiască Directiva NIS1 și, potrivit art. 45 al primei, a intrat în vigoare în a douăzecea zi de la data publicării, 16 ianuarie 2023. În același timp Directiva NIS2, în art. 41, prevede obligativitatea statelor membre ale UE ca până la 17 octombrie 2024 să adopte și să publice măsurile necesare pentru a se conforma acestei directive, iar de la 18 octombrie să le pună în aplicare. Până la această data Directiva NIS1 continuă să rămână în vigoare urmând a fi abrogată la data de 18 octombrie 2024 (art.44).

În comparație cu Directiva NIS1, Directiva NIS2 urmărește să îmbunătățească situația existentă în materie de securitate cibernetică în întreaga UE și:

- să creeze structura necesară în gestionarea crizelor în materie de securitate cibernetică (Cyber Crises Liaison Organisation Network, CyCLONe);
- extinde cercul de entități și sectoare/subsectoare care sunt vizate de normele de securitate cibernetică;
- elimină diferențierea dintre operatorii de servicii esențiale și furnizorii de servicii digitale, care s-a dovedit a fi caducă;
- instituie o uniformizare mai aprofundată a normelor de securitate cibernetică în statele membre ale UE;
- stabilește aplicarea unor norme care prevăd cerințe mai stricte în materie de securitate cibernetică.
- stabilește un cadru pentru o mai bună cooperare cibernetică și un schimb de informații între diferitele state membre ale UE și creează o bază de date europeană privind vulnerabilitățile, etc.

Obiectivul Directivei NIS2 este de a atinge un nivel mai ridicat de securitate cibernetică în UE decât cel atins până acum în mare parte prin implementarea Directivei NIS începând cu 2016. Cu alte cuvinte Directiva NIS2 este o nouă treaptă în procesul de asigurare a securității rețelelor și sistemelor informatice în statele membre ale UE. Necesitatea unei astfel de îmbunătățiri a fost determinată de deficiențele constatate în procesul reexaminării Directivei NIS1, care o împiedică să soluționeze în mod eficace provocările actuale și cele emergente în materie de securitate cibernetică.¹⁸

Este important de relevat că, spre deosebire de contextul Republicii Moldova, contextul european de implementare a Directivei NIS2 este determinat în primul rând de faptul că statele membre au atins deja un anumit nivel de securitate cibernetică implementând prevederile Directivei NIS1, ceea ce nu este caracteristic pentru Republica Moldova. Chiar dacă în Republica Moldova anumite progrese în acest domeniu au fost realizate, acestea nicidecum nu pot fi catalogate ca fiind în armonie cu cele existente în Uniunea Europeană.

Din această perspectivă transpunerea în dreptul intern a Directivei NIS2 va fi una parțială și nu doar din perspectiva faptului că Republica Moldova nu este un stat membru al UE, ci și

¹⁸ Considerentul (2) din Directiva NIS2: <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2555>

din punctul de vedere a necesității de a asigura implementarea treptată a unor măsuri care, pe de o parte, să garanteze o creștere substanțială a nivelului de reziliență cibernetică a serviciilor critice, iar pe de altă parte să nu constituie o povară insurmontabilă pentru persoanele juridice, în special pentru cele din sectorul privat, dar și pentru bugetul de stat.

În acest context, proiectul de lege cuprinde reglementări care, din punctul de vedere al armonizării legislației naționale cu cea europeană, au ca obiectiv general de a transpune Directiva NIS2. Totuși, proiectul legii asigură o armonizare parțială, creând în principiu doar premisele legale primare pentru acțiuni viitoare cu caracter unic sau permanent, care vor asigura transpunerea într-un volum mai mare a Directivei NIS2. Adicional, este extrem de important de a lua în considerare și alte acte legislative europene, în paralel cu NIS2, care sunt relevante în dezvoltarea domeniului securității cibernetice în Moldova și sunt aplicabile în statele membre ale UE. Într-o etapă imediat următoare publicării proiectului, Guvernul, în comun cu autoritățile responsabile, urmează să aprobe un set de acte normative de punere în aplicare a prevederilor legii, precum și să asigure desemnarea/instituirea, organizarea, dotarea cu resurse necesare și asigurarea funcționalității autorității competente.

Astfel, ținem să evidențiem că Directiva NIS2, ca de altfel și Directiva NIS, sunt acte cu un efect orizontal fundamental, nefiind un instrument de sine stătător. Concomitent cu Directiva NIS2 au fost aprobate alte două acte fundamentale din perspectiva rezilienței cibernetice, și anume:

- Directiva (UE) 2022/2557 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a Consiliului (Directiva CER)¹⁹;

- Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (Regulamentul DORA).

Prin urmare, transpunerea Directivei NIS2 în legislația națională nu poate fi concepută fără demararea imediată a proceselor de transpunere și a celorlalte două acte, parte a pachetului legislativ european direcționat spre creșterea și îmbunătățirea rezilienței sectoarelor de o importanță critică fundamentală pentru funcționarea economiei și a statului. Importanța acestui exercițiu este determinată și de interconexiunile dintre cele trei documente. Regulamentul DORA are un caracter de *lex specialis* față de prevederile conținute în Directiva NIS2²⁰, iar interconexiunile²¹ dintre Directiva CER și Directiva NIS2 urmează a fi abordate din perspectiva unor cadre de politici coerente pentru o coordonare consolidată și cooperare eficientă dintre autoritățile competente conform ambelor directive, inclusiv din punctul de vedere al raționalizării activităților de supraveghere și reducerii la minimum a sarcinii administrative.²²

¹⁹ Noua directivă CER propune un nou cadru de cooperare, precum și obligații pentru statele membre și entitățile critice, în vederea consolidării rezilienței fizice non-cibernetice împotriva amenințărilor naturale și antropice a acelor entități care furnizează servicii esențiale pe piața internă, cu unsprezece sectoare specificate. Directiva NIS2 instituie o acoperire sectorială mai largă a obligațiilor în materie de securitate cibernetică. Textul Directivei CER poate fi accesat aici: <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2557>

²⁰ Considerentul (28) din Directiva NIS2: <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2555>

²¹ Considerentul (30) din Directiva NIS2: <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2555>

²² Considerentul 24 din Directiva CER evidențiază că este important ca statele membre să se asigure că cerințele prevăzute în prezenta directivă și în Directiva (UE) 2022/2555 sunt puse în aplicare în mod complementar și că entitățile critice nu sunt supuse unei sarcini administrative mai mari decât cea necesară pentru a atinge obiectivele prezentei directive și pe cele ale directivei menționate.

Desincronizarea acestor procese la nivel național, de transpunere a celor trei acte europene, constituie un risc serios de implementare a prevederilor proiectului de lege. Având în vedere importanța securității cibernetice pentru reziliența entităților critice și din motive de consecvență, ar trebui să se asigure o abordare coerentă, ori de câte ori este posibil, între Directiva CER și Directiva NIS²³. După cum se subliniază în propunerea privind o abordare coordonată de către Uniune pentru consolidarea rezilienței infrastructurilor critice, având în vedere interconexiunile dintre securitatea cibernetică și securitatea fizică a operatorilor, este important ca lucrările de pregătire pentru transpunerea și aplicarea noii directive NIS2 să înceapă cât mai curând posibil și ca aceste lucrări în cadrul noii directive CER să progreseze, de asemenea, în paralel²⁴.

De asemenea, autoritățile administrației publice centrale de specialitate responsabile de realizarea politicii de stat în sectoarele și subsectoarele enumerate în anexele II și III ale directivei NIS2 urmează să efectueze o evaluare a gradului de transpunere a legislației UE la care se face referire în aceste anexe, și după caz, să inițieze modificarea legislației sectoriale relevante.

Rezultatele procesului de transpunere în proiectul de lege a prevederilor Directivei NIS2, gradul de transpunere a acesteia și explicațiile de rigoare privind relația dintre componentele acestei directive și părțile corespunzătoare ale proiectului de lege sunt reflectate în tabelul de concordanță, care este parte a dosarului de însoțire a proiectului.

4. Principalele prevederi ale proiectului și evidențierea elementelor noi

(Se indică actele normative existente care reglementează domeniul vizat de proiectul actului normativ, precum și cauzele în virtutea cărora normele în vigoare nu sunt suficiente să ofere soluții problemelor abordate în proiectul actului normativ.)

Se descriu elementele noi din proiect, modificările propuse, urmările implementării acestora.

Se indică rezultatele studiilor, recomandărilor și se prezintă argumentele în favoarea intervenției în legislație cu un nou act normativ.

De asemenea, se iau în calcul sesizările parvenite de la diferiți subiecți (instituții de stat sau private, asociații, persoane etc.) care interacționează în cadrul relațiilor sociale ce urmează a fi reglementate.)

Domeniul protecției și asigurării securității rețelelor și sistemelor informatice în Republica Moldova nu a constituit până în prezent obiectul unei legi cadru care să reglementeze sistemic problemele de securitate cibernetică. Norme juridice care reglementează aspectele organizatorice, instituționale și funcționale în domeniul asigurării protecției și securității rețelelor și sistemelor informaționale sunt dispersate în câteva legi, principalele dintre acestea fiind:

Legea nr. nr 467/2003²⁵ cu privire la informatizare și resursele informaționale de stat (art.23) și **Legea nr. 71/2007²⁶ cu privire la registre** (art.24) reglementează, pe de o parte, responsabilitățile autorităților publice în asigurarea securității cibernetice a sistemelor și resurselor informaționale ale statului, iar pe de altă parte, responsabilitățile entităților, inclusiv private, în protecția informațiilor conținute de resursele și prelucrate de sistemele informaționale pe care le creează.

În același timp, cerințele de securitate pentru rețelele publice de comunicații electronice și serviciile de comunicații electronice accesibile publicului sunt prevăzute la articolele 21 și 22 din **Legea comunicațiilor electronice nr. 241/2007²⁷**. Această lege reglementează activitatea în domeniul comunicațiilor electronice civile a tuturor furnizorilor de rețele sau servicii de

²³ Recitalul (9) al Directivei CER: <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2557>

²⁴ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0551&qid=1666351317270>

²⁵ https://www.legis.md/cautare/getResults?doc_id=132933&lang=ro

²⁶ https://www.legis.md/cautare/getResults?doc_id=131038&lang=ro

²⁷ https://www.legis.md/cautare/getResults?doc_id=133262&lang=ro

comunicații electronice, fie din sectorul public sau privat, și stabilește drepturile și obligațiile utilizatorilor. Legea nu se extinde la rețelele de comunicații speciale. Din punct de vedere al securității rețelelor și serviciilor de comunicații electronice, Agenția Națională pentru Reglementare în Comunicațiile Electronice și Tehnologia Informației este responsabilă de implementarea măsurilor minime de securitate pe care toți furnizorii ar trebui să le implementeze. Agenția poate verifica și evalua măsurile stabilite de furnizori pentru a garanta securitatea și integritatea rețelelor și serviciilor de comunicații electronice.

De asemenea, **Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate** are ca scop să faciliteze și să eficientizeze schimbul de date și interoperabilitatea în cadrul sectorului public, precum și între sectorul public și cel privat, în vederea creșterii calității serviciilor publice prestate, a creării noilor servicii publice electronice și a *asigurării securității informaționale*.

Pentru punerea în aplicare a acestor legi, Guvernul a aprobat:

- **Hotărârea Guvernului nr. 201/2017**²⁸ privind aprobarea cerințelor minime obligatorii de securitate cibernetică, care se adresează atât autorităților guvernamentale, cât și autorităților care nu intră în structura administrativă a Guvernului. Obiectul de reglementare al acestei hotărâri se limitează la aspecte de organizare a sistemului intern de securitate cibernetică, documentația ce necesită a fi aprobată și actualizată periodic, a responsabilităților angajaților entităților care intră în cercul de subiecți ai reglementărilor, a cerințelor propriu-zise ce urmează a fi aplicate atunci când în activitatea instituțiilor respective sunt utilizate soluții de tehnologie a informației și comunicațiilor și, respectiv, de prestare a serviciilor bazate pe astfel de soluții, a cerințelor specifice la achiziția sistemelor informaționale noi sau actualizarea celor existente, precum și a celor ce urmează a fi aplicate la externalizarea administrării/mentenanței sistemelor.

- **Hotărârea Guvernului nr. 482/2020**²⁹ privind aprobarea măsurilor necesare asigurării securității cibernetice la nivel guvernamental, prin care Guvernul reglementează din punct de vedere instituțional, organizatoric, procedural și funcțional sistemul de asigurare a securității cibernetice la nivelul structurii sale administrative, inclusiv desemnează Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică în calitate de Centru guvernamental de reacție la incidente de securitate cibernetică, care constituie și punctul unic de contact și de raportare a incidentelor de securitate cibernetică pentru structurile de tip CERT (echipă de răspuns la incidentele cibernetice) departamentale ale Guvernului.

- **Hotărârea Guvernului nr. 388/2022**³⁰ privind aprobarea Concepției Sistemului Informațional „Registrul de Stat al Incidentelor de Securitate Cibernetică”, este una dintre măsurile preliminare pentru stabilirea unei platforme informaționale pentru comunicarea strategică cu entitățile publice, precum și pentru asigurarea evidenței amenințărilor, vulnerabilităților în spațiul cibernetic și a incidentelor de securitate cibernetică identificate sau raportate.

Cu toate că actele normative sus-menționate abordează protecția rețelelor și sistemelor informatice, normele conținute de acestea au un caracter dispart și îngust, limitat la obiectivul de a legifera anumite aspecte ale securității cibernetice doar din perspectiva necesităților de reglementare a domeniului care constituie obiectul actului normativ respectiv, în detrimentul unei abordări sistemice, care să coaguleze din punct de vedere normativ la nivel național întregul

²⁸ https://www.legis.md/cautare/getResults?doc_id=98644&lang=ro

²⁹ https://www.legis.md/cautare/getResults?doc_id=122272&lang=ro

³⁰ https://www.legis.md/cautare/getResults?doc_id=132011&lang=ro

spectru de măsuri de ordin organizatoric, instituțional, funcțional, procedural și coercitiv în acest domeniu.

Deși la nivel guvernamental anumite mecanisme coordonate de interacțiune sunt deja instituite în art. 23 din Legea nr. 467/2003 și, subsidiar în Hotărârea Guvernului 482/2020 și reflectă o anumită maturitate în gestionarea incidentelor, riscurilor, vulnerabilităților și amenințărilor cibernetice la rețelele și sistemele informaționale, ale căror proprietar este statul, totuși în sectorul public există anumite lacune și inconsistențe referitoare în mod special la aplicabilitatea prevederilor normative asupra autorităților administrației publice locale și la cooperarea CERT-Gov cu autoritățile publice care sunt plasate în afara structurii administrative guvernamentale.

În ce privește sectorul privat, problematica asigurării securității cibernetice este abordată într-o formă limitată în contextul realizării prevederilor Legii nr. 120/2017 cu privire la prevenirea și combaterea terorismului și a actelor de punere în aplicare a acesteia (*Regulamentului privind protecția antiteroristă a infrastructurii critice, aprobat prin Hotărârea Guvernului nr. 701/2018, Regulamentului privind organizarea și desfășurarea testelor antiteroriste, aprobat prin Hotărârea Guvernului nr. 996 /2018 și Ordinul SIS cu privire la aprobarea modelului Pașaportului antiterorist*), din perspectiva protecției antiteroriste a infrastructurii critice.

Această situație are ca efect un nivel general insuficient de protecție împotriva incidentelor, riscurilor și amenințărilor legate de securitatea rețelelor și a sistemelor informatice, ceea ce poate submina sau subminează buna funcționare, pe de o parte, a activității administrative, în mod special prestarea serviciilor publice, de către administrația publică centrală și locală, iar pe de altă parte buna funcționare a activității economice desfășurată de către întreprinderile din mediul privat, ceea ce afectează în consecință întreaga economie națională și, implicit, activitatea socială.

Proiectul de lege are ca **obiect reglementarea** cadrului juridic, organizațional și de cooperare în domeniul securității cibernetice a persoanelor juridice, competenței autorităților și instituțiilor publice în materie de securitate cibernetică, cadrului național general de gestionare a crizelor în domeniul securității cibernetice, cerințelor, măsurilor și mecanismelor pentru asigurarea securității rețelelor și sistemelor informatice care sunt esențiale pentru funcționarea societății, precum și modul de gestionare a incidentelor cibernetice. Proiectul este structurat în 6 capitole după cum urmează:

În **capitolul I – Dispoziții generale** sunt reglementate aspecte ce țin de domeniul de aplicare al legii, principalele noțiuni utilizate și definițiile acestora, aspecte generale privind procesul de identificare a persoanelor juridice asupra cărora prevederile legii urmează să fie aplicate, precum și principiile generale conform cărora subiecții legii urmează să le aplice în procesul de asigurare a securității cibernetice.

Acest capitol de asemenea stabilește principalele criterii în baza cărora autoritatea competentă urmează să identifice persoanele juridice ca furnizori de servicii, criterii ce au la bază regula principală a dimensiunii organizației, dar și criterii specifice precum categoria de servicii prestate (ex. prestatorii de servicii de încredere, furnizorii de rețele și servicii de comunicații electronice accesibile publicului, etc), calitatea prestatorului de servicii (operator al obiectivelor infrastructurii critice), impactul pe care l-ar putea avea perturbarea prestării serviciului, dependența serviciului de rețelele și sistemele informatice, importanța și interconexiunile cu alte servicii sau sectoare și subsectoare.

Capitolul II „Cadrul instituțional, cooperarea și coordonarea strategică la nivel național” cuprinde norme juridice ce reglementează problematici generale ale raporturilor juridice instituite în procesul de planificare și coordonare strategică în domeniul securității cibernetice la nivel național, inclusiv competența Guvernului de aprobare a Strategiei naționale de securitate cibernetică, misiunea Consiliului coordonator în domeniul securității cibernetice, aspecte funcționale ale Autorității competente în domeniul reglementat de prevederile legii, modul de desemnare, atribuții specifice funcției de CSIRT național și de punct unic de contact la nivel național. De asemenea capitolul vizat stabilește norme legale primare de reglementare a cadrului național general de gestionare a crizelor în materie de securitate cibernetică, inclusiv responsabilitatea autorității competente de a elabora și aproba Planul național de răspuns la incidentele și crizele de securitate cibernetică, în baza cadrului metodologic aprobat de Guvern în ce privește elaborarea, actualizarea și implementarea prevederilor acestui plan. În același context, în acest capitol sunt propuse reglementări fundamentale ce vizează instituirea, organizarea și funcționarea Registrului de stat al incidentelor cibernetice și a sistemului informațional ce-l formează. De notat că Guvernul a aprobat deja Conceptul acestui Registru de stat și sistem informațional ce-l formează prin Hotărârea sa nr. **nr. 388/2022, menționată mai sus.**

Capitolul III – Obligații privind asigurarea securității cibernetice – cuprinde reglementări privind măsurile obligatorii de securitate ce urmează a fi întreprinse de către persoanele juridice, identificate de autoritatea competentă ca furnizorii de servicii, pentru a asigura un nivel înalt de securitate a rețelelor și sistemelor informatice proprii, responsabilitățile acestora în legătură cu măsurile respective, aspecte procedurale generale și obligațiile concrete în procesul de gestionare a incidentelor cibernetice semnificative, responsabilitățile în relațiile cu persoanele juridice terțe care nu cad sub incidența prevederilor legii.

De asemenea, capitolul cuprinde reglementări generale privind asigurarea de către autoritatea competentă prin intermediul echipei de răspuns la incidente cibernetice a procesului de gestionare a acțiunilor orientate spre prevenirea și soluționarea a incidentelor, dar și spre prevenirea și atenuarea impactului asupra continuității serviciului sau a securității rețelei și/sau a sistemului informatic cauzat de un incident cibernetic.

De rând cu acestea, acest capitol include și prevederi privind notificarea voluntară, ceea ce presupune dreptul furnizorilor de servicii să notifice autoritatea competentă cu privire la incidente cibernetice, amenințări cibernetice și incidente evitate la limită, iar persoanele juridice de drept public sau de drept privat care nu sunt identificate de autoritatea competentă ca furnizori de servicii – să transmită acesteia notificări cu privire la incidente cibernetice semnificative, amenințările cibernetice și incidentele evitate la limită.

În contextul acestor reglementări, capitolul în speță abordează și problematica schimbului de informații voluntar, prin instituirea contextului juridico-normativ suficient pentru crearea unor comunități și platforme de schimb de informații, între furnizorii de servicii și dintre aceștia și alte persoane juridice care nu intră în domeniul de aplicare al prezentei legi. Astfel subiecții respectivi pot face schimb reciproc de informații relevante în materie de securitate cibernetică, în mod voluntar, inclusiv de informații referitoare la amenințări cibernetice, incidente evitate la limită, vulnerabilități, tehnici și proceduri, indicatori de compromitere, tactici adversariale, informații specifice actorului care generează amenințări, alerte de securitate cibernetică și recomandări privind configurația instrumentelor de securitate cibernetică pentru detectarea atacurilor cibernetice. Conform proiectului de act normativ autoritatea competentă trebuie să intermedieze acest schimb de informații prin crearea și gestionarea unor platforme,

inclusiv tehnico-tehnologice, și comunități de încredere, iar pentru a asigura protecția informațiilor ce au un caracter potențial sensibil, autoritatea competentă urmează să-și aroge funcția de a facilita semnarea acordurilor de schimb de informații între participanții la astfel de platforme și comunități.

În **Capitolul IV – Supraveghere și control de stat** sunt cuprinse normele juridice ce reglementează aspectele privind exercitarea de către autoritatea competentă a funcțiilor de supraveghere și control de stat. Aceste funcții urmează a fi realizate prin monitorizarea continuă a modului în care aceștia realizează obligațiile ce le revin conform prevederilor legii și a actelor normative de punere în aplicare a acesteia. Atunci când un furnizor de servicii responsabil de gestionarea incidentului cibernetic nu este în măsură să răspundă sau să soluționeze în timp util un incident cibernetic, autoritatea competentă asigură aplicarea măsurilor necesare pentru soluționarea incidentului cibernetic utilizând, dacă este necesar, asistență profesionistă terță.

În același context, pentru a contracara o amenințare gravă imediată asupra securității rețelelor și sistemelor informatice sau pentru a elimina o perturbare gravă în cazul unui incident cibernetic sunt stabilite expres condițiile în care autoritatea competentă poate restricționa utilizarea sau accesul la un sistem informatic. În ce privește controlul sunt stabilite reglementările primare minime necesare pentru asigurarea legalității intervenției autorității competente pe această dimensiune.

În ambele cazuri, ale supravegherii și controlului de stat, pentru implementarea prevederilor legii conform articolelor corespunzătoare din capitolul respectiv al proiectului de lege, Guvernul urmează să adopte acte normative care să reglementeze mai detaliat modul de aplicare a măsurilor de supraveghere și modul de realizare a controlului de către autoritatea competentă asupra respectării de către furnizorii de servicii a obligațiilor ce le revin.

Capitolul V – Răspunderea – abordează generic, în scop de interconexiune cu legislația cadru din domeniul administrativ, contravențional, penal și de altă natură, problematica răspunderii, pe de o parte a autorității competente inclusiv a personalului acesteia, iar pe de altă parte a persoanelor juridice care cad sub incidența prevederilor legii în calitate de furnizori de servicii, inclusiv angajații acestora. Aici este necesar de evidențiat că o etapă importantă în procesul de implementare a proiectului de lege va constitui elaborarea și aprobarea proiectului de lege pentru modificarea legilor existente astfel încât intercalarea noilor norme legale să evite coliziuni sau lacune ale normelor juridice primare și, implicit, deficiențe de implementare ale prevederilor proiectului de lege în speță.

Capitolul VI – Dispoziții finale și tranzitorii – prevede termenul de intrare în vigoare al legii – 1 ianuarie 2025, precum și termenele concrete și sarcinile stabilite:

Guvernului: de a întreprinde măsurile necesare pentru instituirea/desemnarea autorității competente, reglementarea modului de organizare și funcționare a acesteia și dotarea ei cu resurse umane, financiare și tehnice necesare pentru îndeplinirea atribuțiilor stabilite de lege, de a prezenta propuneri Parlamentului privind aducerea actelor normative în concordanță cu prezenta lege și de a aduce în concordanță actele proprii;

Autorității competente: de a identifica furnizorii de servicii, de a-i notifica în modul stabilit și de a-i include în Lista furnizorilor de servicii, întocmită în condițiile legii, precum și de a aproba actele normative necesare punerii în aplicare a legii.

Totodată în acest capitol sunt stabilite cerințele față de CSIRT național din perspectiva obligării Guvernului de a dota autoritatea competentă, astfel încât aceste cerințe să fie îndeplinite nu doar în faza inițială de înființare a acestei entități, ci și să fie aplicate într-o manieră continuă și permanentă.

Evidențiem că termenul de intrare în vigoare a legii de 1 ianuarie 2025, este suficient pentru a permite tuturor părților implicate, autorități sau întreprinderi, să își concentreze resursele în pregătirea pentru noile obligații la momentul potrivit.

5. Fundamentarea economico-financiară

(Se descrie impactul economico-financiar, cu indicarea cheltuielilor (bugetare și nebugetare) necesare pentru implementarea prevederilor noului act normativ și, după caz, a veniturilor generate de noile reglementări.)

În principiu, impactul economico-financiar al implementării proiectului de lege este detaliat descris în capitolul corespunzător al analizei de impact la proiectul respectiv. Totuși, rezumând cele expuse în analiza de impact, implementarea acestei inițiative va implica costuri:

- pentru bugetul de stat, determinate de necesitatea instituirii/desemnării autorității competente, creării și dotării corespunzătoare cu resurse a unui CSIRT național sau, eventual, atribuirii competenței unui astfel de CSIRT către CERT-Gov,
- pentru furnizorii de servicii din sectorul privat - privind necesitatea conformării cu cerințele noi stabilite de noul cadru legal în domeniul securității cibernetice.

În ce privește costurile privind autoritatea competentă și CSIRT național modelul³¹ de cost estimat pentru înființarea acestora este în mare măsură determinat de obiectivele stabilite pentru această organizație, de poziția sa juridică și de grupul de interese (constituenții).

Pentru realizarea funcțiilor enunțate mai sus autoritatea competentă, în cazul în care va include în competența sa și realizarea funcției de CSIRT național va avea necesarul de **minim 25 de angajați**, fără a include aici conducătorii, personalul de suport (în cazul creării unei entități noi) și personalul dedicat realizării funcției de supraveghere (numărul acestuia este direct dependent de numărul furnizorilor de servicii). Având în vedere prevederile cadrului normativ național în domeniul salarizării, și presupunând că personalul respectiv este divizat în patru subdiviziuni (numărul funcțiilor fundamentale ce urmează a fi realizate de autoritatea competentă) remunerarea anuală a muncii acestui personal (autoritate administrativă în subordinea unui minister ar constitui **circa 2 mil. lei anual**.

La aceste cheltuieli de personal, urmează a fi adăugate cheltuieli investiționale unice inițiale de **circa 10 mil. lei (0,5 mil Euro)** în echipamentul și instrumentarul tehnic al CSIRT.

De asemenea, o estimare a costurilor ce țin de asigurarea cu sediu ce corespunde cerințelor Directivei NIS2 urmează a fi efectuat atunci când Guvernul, în temeiul prevederilor legale propuse în proiect va exercita dreptul său discreționar de a decide înființarea unei noi entități sau atribuirea competențelor unei autorități existente.

În analiza de impact la Directiva NIS1, experții Comisiei Europene au stabilit că „*Pentru cele trei state membre care nu au înființat încă CERT-uri naționale/guvernamentale (Cipru, Irlanda și Polonia), costul estimat al punerii în funcțiune a infrastructurii și serviciilor aferente, pe baza interviurilor realizate cu CERT-uri care sunt deja operaționale, ar fi de aproximativ 2,5 milioane EUR pentru fiecare CERT.*”³².

În același context, Agenția Europeană pentru Securitate Cibernetică a publicat un ghid³³ privind modul de creare și asigurare a funcționalității unui CSIRT care oferă informații și privind costurile estimative la nivelul țărilor membre, necesare pentru instituirea unui CSIRT național.

În ce privește costurile de conformare pentru persoanele juridice din sectorul privat, estimarea costurilor de implementare a legii pentru întreprinderile care vor cădea sub incidența

³¹ The cost model of Competent Cyber Authority, Moldova Cybersecurity Rapid Assistance Project, October 2022;

³² <https://data.consilium.europa.eu/doc/document/ST-6342-2013-ADD-2/en/pdf>, pag. 53

³³ <https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc>.

obligărilor stabilite de lege actualmente este o provocare în condițiile unei lipse acute a datelor statistice primare în domeniu securității cibernetice, precum și lipsei unor evaluări și analize financiare bazate pe astfel de date la nivel național. Totuși anumite orientări pe această dimensiune sunt acordate de Comisia Europeană în procesul de evaluare³⁴ a costurilor de conformare pentru mediul privat în procesul de pregătire a propunerii de Directivă NIS1: „Pornind de la costurile totale de conformare pentru sectorul privat, care variază între 360 și 720 de milioane de euro, costul de conformare pentru fiecare întreprindere mică și mijlocie s-ar situa între 2 500 și 5 000 de euro.”³⁵

În ce privește costurile pentru entitățile administrației publice și furnizorii de servicii asociați cu raportarea obligatorie a unui incident semnificativ, Comisia Europeană a estimat în aceeași analiză de impact că *costul preconizat pentru fiecare notificare de încălcare ar fi de 125 EUR....., iar în ceea ce privește posibilele investigații care pot fi inițiate de către autoritățile competente de securitatea rețelilor și informațiilor (NIS) cu privire la respectarea obligațiilor de gestionare a riscurilor și de notificare a incidentelor NIS..... costul maxim pentru entitatea afectată ar fi de maximum 25 000 EUR pe investigație*³⁶.

6. Modul de încorporare a actului în cadrul normativ în vigoare

(Se indică lista actelor normative ce urmează a fi modificate sau abrogate. În cazul în care urmează a fi adoptate acte normative noi în scopul implementării prevederilor în cauză, se indică expres aceste acte.)

1. Cadrul juridic ce necesită a fi modificat și/sau elaborat și aprobat

În conformitate cu prevederile art. 20 alin (2) din proiectul de lege, Guvernul urmează, în termen de cel mult 9 luni din data publicării Legii privind securitatea cibernetică să asigure elaborarea și să prezinte Parlamentului propuneri de modificare a legilor în vigoare care sunt conexe domeniului reglementat de actul normativ în speță. Astfel, deși la momentul actual este destul de ambițios de a identifica prevederile specifice ale unor legi-cadru ce reglementează alte domenii și care cu certitudine necesită a fi modificate în contextul aducerii în concordanță cu prevederile legii în speță, totuși ar putea fi anticipată necesitatea, cel puțin a examinării, în contextul realizării acestui obiectiv, a următoarelor legi care cuprind reglementări privind securitatea și protecția rețelilor și sistemelor informatice:

- Legea nr. 1069/2000 cu privire la informatică;
- Legea nr.467/2003 cu privire la informatizare și la resursele informaționale de stat;
- Legea nr.71/2007 cu privire la registre;
- Legea nr. 241/2007 comunicațiilor electronice;
- Legea nr.133/2011 privind protecția datelor cu caracter personal;
- Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere;

În același context, unei examinări aprofundate urmează a fi supuse legile cadru care reglementează sectoarele, subsectoarele și tipurile de entități ce prestează servicii în acestea, enumerate în anexele I și II la Directiva NIS2, în contextul în care Guvernul urmează să aprobe lista acestor sectoare și subsectoare de rând cu tipurile persoanelor juridice. Examinarea acestei categorii de acte normative naționale urmează a fi efectuată în primul rând din perspectiva armonizării acestora cu actele sectoriale relevante ale Uniunii Europene, menționate de altfel în anexele respective ale Directivei NIS2.

³⁴ <https://data.consilium.europa.eu/doc/document/ST-6342-2013-ADD-2/en/pdf>

³⁵ <https://data.consilium.europa.eu/doc/document/ST-6342-2013-ADD-2/en/pdf>, pag.55

³⁶ <https://data.consilium.europa.eu/doc/document/ST-6342-2013-ADD-2/en/pdf>, pag.56

În continuare pentru a asigura implementarea prevederilor legale noi, urmează a fi supuse dacă nu unei revizuiri, cel puțin unei examinări aprofundate în scopul confirmării conformității cu prevederile noii legi și cu prevederile Directivei NIS2 a următoarelor acte normative guvernamentale:

- Hotărârea Guvernului nr. 201/2017 privind aprobarea cerințelor minime obligatorii de securitate cibernetică;
- Hotărârea Guvernului nr. 482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetice la nivel guvernamental;
- Hotărârea Guvernului nr. 388/2022 cu privire la aprobarea Concepției Sistemului informațional „Registrul de stat al incidentelor de securitate cibernetică”.

În același context, Guvernul urmează să aprobe un set de acte normative de punere în aplicare a noului cadru normativ în domeniul securității cibernetice, prevăzute de proiectul de lege:

- a) lista sectoarelor, subsectoarelor și, respectiv, a tipurilor și categoriilor de persoane juridice care prestează servicii în aceste sectoare și/sau subsectoare (art. 4 alin. (2));
- b) cadrul metodologic privind identificarea persoanelor juridice de drept public sau privat ca fiind furnizori de servicii (art. 4 alin. (2));
- c) instituirea și reglementarea modului de organizare și funcționare a Consiliului coordonator în domeniul securității cibernetice (art.6 alin. (2));
- d) Strategia națională de securitate cibernetică (art.6 alin. (3)), având la bază pe de o parte rezultatele și concluziile procesului de analiză a modului de implementare a Strategiei naționale de securitate informațională, aprobată prin Hotărârea Parlamentului nr. 257/2018, și pe de altă parte prevederile articolului 7 al Directivei NIS 2;
- e) modul de organizare și funcționare a entității care va exercita funcțiile autorității competente (art. 7 alin. (1));
- f) modul de coordonare de către autoritatea competentă a procesului de divulgare a vulnerabilităților (art. 7 alin. (4) pct.10);
- g) cadrul metodologic privind elaborarea, actualizarea și implementarea prevederilor planului național de răspuns la incidente cibernetice și crize de securitate cibernetică, interacțiunea dintre autoritățile și instituțiile publice cu atribuții în procesul de elaborare și actualizare, precum și interacțiunea acestora cu sectorul privat (art. 9 alin. (4));
- h) modul de organizare și funcționare a Registrului de stat al incidentelor cibernetice și a sistemului informațional corespunzător art. 10 alin. (1));
- i) asigurarea, prin intermediul organismului național de standardizare și în cooperare cu autoritatea competentă, aprobarea Standardului național în domeniul securității informațiilor, securității cibernetice și protecția confidențialității în baza standardelor și a specificațiilor tehnice europene și internaționale relevante pentru securitatea rețelelor și a sistemelor informatice art. 11 alin. (4));
- j) cerințele specifice privind măsurile de securitate a rețelelor și sistemelor informatice, în funcție de sectorul, subsectorul, categoria și/sau tipul furnizorului de servicii (art. 11 alin. (4));
- k) procedura de notificare a incidentelor cibernetice, inclusiv interacțiunea dintre furnizorul de servicii și autoritatea competentă, modul de stabilire a impactului unui incident cibernetic, formatul informațiilor evaluărilor și rapoartelor prezentate în procesul de gestionare a unui incident cibernetic și modul de informare a destinatarilor de către furnizorii de servicii sau de către autoritatea competentă (art. 12 alin. (7) și alin. (9)).

l) regulamentul privind condițiile și cerințele în care sunt semnate de către autoritățile și instituțiile publice acordurile de schimb de informații în materie de securitate cibernetică (art. 17 alin. (3));

m) modul de aplicare a măsurilor de supraveghere de către autoritatea competentă (art. 18 alin. (5));

n) modul de realizare a controlului de către autoritatea competentă asupra respectării de către furnizorii de servicii a obligațiilor ce le revin conform Legii privind securitatea cibernetică (art. 19 alin. (5)).

2. Schimbările instituționale preconizate prin aprobarea proiectului de act normativ

În temeiul art. 7 alin. (1) din proiectul de act normativ Guvernul urmează să desemneze autoritatea competentă la nivel național în domeniul securității cibernetică. De asemenea, potrivit prevederilor art. 23 alin. (2) Guvernul urmează să asigure dotarea ei cu resurse umane, financiare și tehnice necesare pentru îndeplinirea atribuțiilor stabilite de lege.

Potrivit proiectului de act normativ Guvernului i se conferă o marjă discreționară în procesul de desemnare a acestei autorități competente fie prin instituirea unei autorități/instituții publice noi fie prin identificarea și atribuirea competenței prevăzute de proiectul de act normativ unei entități publice existente. În oricare dintre cazurile menționate Guvernul urmează, după aprobarea sau, după caz, revizuirea modului de organizare a entității desemnate ca fiind autoritatea competentă în sensul prevederilor proiectului de lege, să inițieze procesul de ajustare a structurii, efectivului-limită și organigramei entității respective și să asigure aprobarea statelor de personal noi și a schemei de încadrare corespunzătoare.

De asemenea, Guvernul conform art. 23 alin. (2) lit. a) urmează să asigure dotarea autorității competente, inclusiv CSIRT național, cu resurse umane, financiare și tehnice necesare pentru îndeplinirea atribuțiilor stabilite de lege. Pentru realizarea acestei sarcini conform prevederilor art. 23 alin. (3) din proiectul legii, Guvernul trebuie să doteze autoritatea competentă, astfel încât CSIRT național să corespundă cerințelor stipulate la acest alineat, care sunt în principiu cerințele față de astfel de echipe stabilite de Directiva NIS2 la art. 11 alin. (1).

7. Avizarea și consultarea publică a proiectului

(Se menționează acțiunile întreprinse în vederea respectării prevederilor Legii nr. 239/2008 privind transparența în procesul decizional (crearea grupurilor de lucru, organizarea dezbaterilor publice, meselor rotunde, publicarea proiectului pentru consultare publică etc.). Se indică autoritățile publice, instituțiile și alte persoane juridice care au avizat pozitiv proiectul fără obiecții și propuneri, cele care au prezentat obiecții și propuneri și cele care au avizat negativ proiectul sau nu au prezentat avize/recomandările.)

În conformitate cu prevederile art. 9 din Legea nr. 239/2008 privind transparența în procesul decizional pe pagina web oficială a Ministerului Economiei **me.gov.md** și pe platforma de consultare **particip.gov.md**, la data de 23 decembrie 2022 a fost publicat anunțul referitor la inițierea elaborării proiectului de lege la care au fost anexate analiza de impact la proiect și versiunea inițială a acestuia.

Proiectul a fost supus procesului de avizare conform prevederilor actelor normative în vigoare.

8. Constatările expertizei anticorupție

(Se indică rezultatele expertizei respective, în special constatările privind identificarea normelor din proiect care ar favoriza corupția, precum și recomandările pentru excluderea sau diminuarea efectelor acestora.)

Proiectul definitivat în rezultatul primei avizări a fost transmis Centrului Național Anticorupție pentru examinare și expertiză anticorupție.

9. Constatările expertizei de compatibilitate

*(Compartimentul se completează pentru proiectele care au ca scop armonizarea legislației naționale cu legislația Uniunii Europene, în acesta fiind incluse concluziile expertizei de compatibilitate
Pentru proiectele cu sigla „UE” se indică expres numărul și denumirea actului/actelor Uniunii Europene. Se indică gradul de compatibilitate a proiectului de act normativ cu legislația Uniunii Europene și concluzia expertizei de compatibilitate.)*

Proiectul a fost supus expertizei de compatibilitate de către Centrul de Armonizare a Legislației.

10. Constatările expertizei juridice

(Se prezintă concluziile expertizei privind compatibilitatea proiectului de act normativ cu prevederile Constituției, cu actele normative în vigoare, privind respectarea naturii juridice a propunerilor de reglementare, privind asigurarea concordanței proiectului cu jurisprudența Curții Constituționale și cu prevederile tratatelor internaționale la care Republica Moldova este parte, privind respectarea normelor de tehnică legislativă, precum și alte aspecte indicate în constatările expertizei.)

Proiectul a fost examinat și avizat de Ministerul Justiției și a fost definitivat conform obiecțiilor și propunerilor parvenite.

11. Constatările altor expertize

*(În cazul în care au fost efectuate și alte expertize ale proiectului, concluziile acestora se reflectă în nota informativă.
În cazul proiectelor de acte normative ce se referă la reglementarea activității de întreprinzător, se prezintă și concluziile grupului de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător privind expertiza efectuată.)*

Proiectul a fost examinat în cadrul ședinței Grupului de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător și a fost susținut condiționat.

Ministru



Dumitru ALAIBA