UE

L E G E

privind securitatea cibernetică

Parlamentul adoptă prezenta lege organică.

Prezenta lege transpune art. 1, 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) și 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

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

Articolul 2. Noțiuni principale

În sensul prezentei legi, următoarele noțiuni semnifică:

amenințare cibernetică – circumstanță, eveniment sau acțiune potențială, care ar putea cauza daune, perturba sau avea un alt fel de impact negativ asupra rețelelor

și sistemelor informatice, asupra utilizatorilor unor astfel de sisteme sau asupra altor persoane;

amenințare cibernetică semnificativă – amenințare cibernetică despre care se poate presupune, pe baza caracteristicilor tehnice ale acesteia, 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 și/sau nonmateriale considerabile;

divulgare coordonată a vulnerabilităților – proces structurat prin care informațiile privind vulnerabilitățile sunt transmise producătorului sau furnizorului de produse TIC ori de servicii TIC, potențial vulnerabile, într-un mod care să le permită acestora să diagnosticheze și să remedieze vulnerabilitățile respective înainte ca informațiile detaliate privind vulnerabilitatea să fie dezvăluite unor părți terțe sau publicului;

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 critice, stabilite de către Guvern, și care este identificată de autoritatea competentă în conformitate cu prevederile prezentei legi și ale actelor normative pentru punerea acesteia în aplicare;

gestionarea incidentului cibernetic – totalitatea acțiunilor și procedurilor care vizează prevenirea, detectarea, analizarea, limitarea și izolarea unui incident cibernetic sau care vizează răspunsul la incidentul respectiv și redresarea situației în urma acestuia;

incident cibernetic – eveniment care compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de rețelele și sistemele informatice sau accesibile prin intermediul acestora;

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

măsuri de securitate – operațiuni și/sau resurse organizaționale, fizice și de tehnologie a informației, aplicate în scopul obținerii și menținerii securității rețelelor și sistemelor informatice și a securității datelor procesate prin acestea;

proces al tehnologiei informației și comunicațiilor (proces TIC) – set de activități desfășurate pentru a concepe, a dezvolta, a furniza și/sau a întreține produse TIC sau servicii TIC;

produs al tehnologiei informației și comunicațiilor (produs TIC) – element ori grup de elemente ale rețelelor și/sau sistemelor informatice;

rețea și sistem informatic:

a) rețea de comunicații electronice, astfel cum este definită conform Legii comunicațiilor electronice nr. 241/2007; sau

b) dispozitiv sau grup de dispozitive interconectate ori legate între acestea, dintre care unul sau mai multe efectuează, conform unui program, prelucrarea automată de date digitale; sau

c) date digitale stocate, prelucrate, recuperate sau transmise de elementele prevăzute la lit. a) și b) în vederea operării, utilizării, protejării și întreținerii datelor respective;

risc – potențial de pierdere sau de perturbare, cauzat de un incident cibernetic, care trebuie exprimat ca o combinare între amploarea unei astfel de pierderi sau perturbări și probabilitatea producerii incidentului cibernetic;

securitate cibernetică – activități necesare pentru protejarea rețelelor și sistemelor informatice, a utilizatorilor unor astfel de sisteme și a altor persoane expuse amenințărilor cibernetice;

securitatea rețelelor și sistemelor informatice – capacitate a rețelelor și sistemelor informatice de a rezista, la un anumit nivel de încredere, oricărei acțiuni care ar putea compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de rețelele și/sau de sistemele informatice respective sau accesibile prin intermediul acestora;

serviciu al tehnologiei informației și comunicațiilor (serviciu TIC) – serviciu care constă integral sau preponderent în transmiterea, stocarea, extragerea sau prelucrarea informației prin intermediul rețelelor și sistemelor informatice;

vulnerabilitate – punct slab, susceptibilitate sau deficiență a unor produse TIC ori 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 ce depășesc criteriile pentru întreprinderile mijlocii, care furnizează servicii în unul sau mai multe dintre sectoarele sau subsectoarele critice, stabilite de către Guvern, și care sunt identificate ca furnizori de servicii de către autoritatea competentă, desemnată potrivit art. 7, în conformitate cu prevederile prezentei legi și ale actelor normative de punere în aplicare a acesteia.

(2) Indiferent de categoria acesteia, prezenta lege se aplică și persoanei juridice, de tipul stabilit de Guvern, dacă aceasta îndeplinește cel puțin una dintre următoarele condiții:

a) este furnizor de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului, în sensul legislației privind comunicațiile electronice;

b) este prestator de servicii de încredere, în sensul legislației privind identificarea electronică și serviciile de încredere;

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

d) furnizează servicii de înregistrare a numelor de domenii;

e) este singurul furnizor în Republica Moldova al 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 ori 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 ori tipul de servicii respective 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 relevant ca fiind operator al unei astfel de infrastructuri;

i) este persoană juridică de drept public.

(3) Prezenta lege nu se aplică:

a) activităților desfășurate de către 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 către autoritățile publice în domeniul securității naționale, al apărării naționale, al activității speciale de investigații și al urmăririi

penale, în legătură cu mentenanța rețelelor și sistemelor informatice destinate prelucrării informațiilor din domeniile respective.

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

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

(7) Prevederile alin. (5) și (6) din prezentul articol 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 aprobat potrivit art. 4 alin. (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 critice în care prestează serviciul respectiv. Autoritatea competentă asigură, ori de câte ori este necesar, însă nu mai rar decât o dată la doi ani, actualizarea listei respective.

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

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

(4) Autoritățile publice responsabile de realizarea politicii de stat în sectoarele sau subsectoarele critice, stabilite de către Guvern, instituțiile publice responsabile de gestionarea unor domenii conexe sectoarelor și subsectoarelor respective, precum și, după caz, autoritățile publice de reglementare a activității în aceste sectoare sau subsectoare asigură acordarea suportului 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 al implementării prevederilor prezentei legi, persoanele responsabile acționează luând în considerare următoarele principii:

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

b) *principiul protecției integrale* – furnizorii de servicii verifică riscurile la care sunt supuse rețelele și sistemele informatice pe care le dețin și aplică măsuri de securitate adecvate pentru protecția acestora;

c) *principiul reducerii la minimum a efectelor negative* – în cazul unui incident cibernetic, furnizorul de servicii aplică măsurile necesare pentru a evita amplificarea efectelor incidentului cibernetic și posibila răspândire a acestuia către alte rețele și alte sisteme informatice și notifică incidentul cibernetic autorității competente, conform prezentei legi;

d) *principiul proporționalității* – asigurarea unui echilibru între riscurile la care sunt supuse rețelele și sistemele informatice și măsurile de securitate implementate;

e) *principiul cooperării* – în procesul asigurării securității cibernetice și al soluționării incidentelor cibernetice, persoanele responsabile cooperează și, în caz de necesitate, iau în considerare conexiunea mutuală dintre sisteme și servicii și interdependența 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) Planificarea și coordonarea strategică la nivel național în domeniul securității cibernetice se realizează de către Guvern, prin intermediul autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice.

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

(3) Strategia națională de securitate cibernetică este un document de politici care definește obiectivele strategice, măsurile de politică și cele de reglementare, având ca scop atingerea și menținerea unui nivel sporit 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 inclusiv funcția de echipă de răspuns la incidentele cibernetice la nivel național și cea de punct național unic de contact.

(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 aspectele legate de securitatea cibernetică;

d) asigură interacțiunea în domeniul securității cibernetice cu autoritățile și instituțiile publice 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 îndrumări metodologice pentru furnizorii de servicii, în vederea conformării acestora cu prevederile legislației și a remedierii deficiențelor constatate, și stabilește termenul în care aceștia trebuie să se conformeze;

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

h) exercită alte atribuții care decurg din prevederile legislației.

(4) În realizarea 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 ale actelor normative de punere în aplicare a acesteia;

2) monitorizează și analizează amenințările cibernetice, vulnerabilitățile și incidentele cibernetice la nivel național; acordă asistență furnizorilor de servicii, la solicitarea acestora, în procesul de monitorizare de către aceștia a rețelelor și sistemelor informatice pe care le dețin;

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 incidentele cibernetice, în conformitate cu procedurile stabilite de prezenta lege și actele normative de punere în aplicare a acesteia, și acordă asistență, în acest sens, furnizorilor de servicii;

6) colectează și analizează date criminalistice, furnizează analize dinamice privind riscurile, incidentele cibernetice și conștientizarea 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, scanarea proactivă a rețelelor și sistemelor informatice ale solicitantului pentru a detecta vulnerabilitățile cu un impact potențial semnificativ, în conformitate cu actul normativ aprobat de Guvern potrivit art. 12 alin. (9);

9) implementează, în procesul schimbului de informații cu furnizorii de servicii și cu alte persoane relevante, instrumente și soluții tehnice securizate și asigură, în conformitate cu prevederile legislației, protecția informațiilor de care ia cunoștință în exercitarea atribuțiilor;

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) intermediază și facilitează interacțiunea dintre persoana fizică sau juridică, care raportează o vulnerabilitate, și producătorul sau furnizorul de produse TIC ori servicii TIC, potențial vulnerabile, la cererea oricărei dintre persoanele respective;

b) identifică și contactează persoanele fizice sau juridice implicate;

c) acordă asistență persoanelor fizice sau juridice care raportează o vulnerabilitate;

d) negociază calendarele de divulgare și gestionare a vulnerabilităților care afectează mai multe persoane;

e) asigură anonimatul persoanelor fizice sau juridice care raportează o vulnerabilitate, în cazul în care acestea o solicită.

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

a) asigură interacțiunea autorităților și instituțiilor publice naționale cu autoritățile similare din alte state și/sau cu organizațiile internaționale ori entitățile instituite de acestea;

b) transmite, la cererea autorităților și instituțiilor publice sau a echipelor de răspuns la incidentele cibernetice, punctelor 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 instituite de acestea.

Articolul 8. Centrul guvernamental de răspuns la incidentele cibernetice

(1) Pentru asigurarea securității cibernetice la nivel guvernamental, Guvernul instituie Centrul guvernamental de răspuns la incidentele cibernetice la nivelul rețelelor și sistemelor informatice proprietate a statului, desemnează persoana juridică de drept public responsabilă de exercitarea funcțiilor corespunzătoare și stabilește modul de organizare și funcționare a centrului respectiv.

(2) Guvernul este responsabil de asigurarea Centrului guvernamental de răspuns la incidentele cibernetice cu resursele necesare pentru prevenirea, analizarea, identificarea și răspunsul la incidentele cibernetice la nivelul rețelelor și sistemelor informatice proprietate a statului.

(3) Centrul guvernamental de răspuns la incidentele cibernetice este responsabil de asigurarea securității rețelelor și sistemelor informatice proprietate a statului, de facilitarea îndeplinirii de către furnizorii de servicii persoane juridice de drept public a obligațiilor privind asigurarea securității cibernetice prevăzute de prezenta lege, inclusiv a celor privind notificarea, și de facilitarea interacțiunii acestora cu autoritatea competentă și echipa de răspuns la incidentele 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 și a crizelor respective la nivel național.

(3) Planul național de răspuns la incidentele cibernetice și crizele în domeniul securității cibernetice trebuie să includă cel puțin:

a) obiectivele măsurilor și ale activităților de pregătire la nivel național;

b) sarcinile și atribuțiile autorităților și instituțiilor publice responsabile;

c) procedurile de gestionare a crizelor și căile de schimb de informații;

d) măsurile de pregătire, inclusiv exercițiile și activitățile de formare;

e) furnizorii de servicii, interacțiunea dintre aceștia și autoritățile și instituțiile publice responsabile, precum și infrastructura implicată;

f) procedurile și mecanismele de interacțiune dintre autoritățile și instituțiile publice responsabile, precum și de interacțiune coordonată a acestora în gestionarea incidentelor cibernetice și a crizelor în domeniul securității cibernetice de mare amploare, inclusiv a celor la nivel european și internațional.

(4) Guvernul aprobă cadrul normativ metodologic privind elaborarea, actualizarea și implementarea prevederilor planului național de răspuns la incidentele cibernetice și crizele în domeniul securității cibernetice, privind interacțiunea dintre autoritățile și instituțiile publice cu responsabilități în procesul de elaborare și actualizare a planului respectiv 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, al automatizării proceselor de identificare, înregistrare,

documentare, clasificare, analizare și gestionare a unor astfel de incidente, al monitorizării și evidenței alertelor, amenințărilor cibernetice și vulnerabilităților, Guvernul, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii statului în domeniul securității cibernetice, creează Registrul de stat al incidentelor cibernetice și reglementează modul de organizare și funcționare a acestuia și, corespunzător, creează sistemul informațional destinat ținerii registrului respectiv și reglementează modul de administrare și funcționare a acestui sistem.

(2) Accesul la Registrul de stat al incidentelor cibernetice este limitat, iar datele din registru sunt destinate utilizării interne, cu excepția cazului în 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 în scopul:

a) prevenirii incidentelor cibernetice;

b) soluționării incidentelor cibernetice;

c) prevenirii și atenuării impactului asupra continuității serviciului ori asupra securității rețelei și/sau sistemului informatic, cauzat de un incident cibernetic;

d) prevenirii și atenuării impactului potențial asupra continuității serviciilor ori asupra securității rețelelor și/sau sistemelor informatice dependente de cele ale furnizorului de servicii.

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

1) să evalueze vulnerabilitățile și riscurile de securitate ale rețelelor și sistemelor informatice, să determine gravitatea impactului unui eventual incident cibernetic survenit ca urmare a materializării riscurilor, să descrie măsurile pentru soluționarea unui incident cibernetic și să întocmească un raport de evaluare în acest sens;

2) să implementeze măsuri tehnice și organizatorice corespunzătoare și proporționale, în conformitate cu standardele aprobate potrivit alin. (4) lit. a), pentru a gestiona riscurile de securitate a rețelelor și a sistemelor informatice pe care le utilizează. Măsurile respective trebuie să includă cel puțin următoarele:

a) politicile referitoare la analizarea riscurilor și asigurarea securității rețelelor și sistemelor informatice;

b) politicile și procedurile privind gestionarea incidentelor cibernetice (prevenirea, detectarea și răspunsul la incidentele respective);

c) politicile și procedurile privind utilizarea criptografiei și a criptării, în special a criptării de la un capăt la altul;

d) politicile și procedurile referitoare la evaluarea eficacității măsurilor de securitate implementate;

e) măsurile privind continuitatea activității și privind gestionarea crizelor;

f) măsurile de securitate aplicate în achiziționarea, dezvoltarea și întreținerea rețelelor și sistemelor informatice, inclusiv în divulgarea și gestionarea vulnerabilităților;

g) măsurile de securitate privind resursele umane, politicile de control al accesului și de gestionare a activelor;

h) măsurile privind asigurarea securității lanțului de aprovizionare, inclusiv aspectele, legate de securitate, referitoare la relațiile furnizorului de servicii cu prestatorii sau cu furnizorii direcți de servicii ai acestuia;

i) practicile de bază în materie de igienă cibernetică și formarea în domeniul securității cibernetice;

j) soluțiile de autentificare, de comunicații securizate voce, video și text; sistemele securizate de comunicații de urgență în cadrul furnizorului de servicii;

3) să asigure actualitatea documentației privind măsurile de securitate;

4) să asigure monitorizarea situației privind securitatea rețelelor și sistemelor sale informatice, inclusiv în scopul detectării serviciilor TIC, proceselor TIC sau produselor TIC care compromit rețelele sau sistemele respective;

5) să întreprindă măsuri orientate spre reducerea impactului și răspândirii incidentelor cibernetice, inclusiv, dacă este necesar, să restricționeze utilizarea sau accesul la rețelele și sistemele informatice;

6) să verifice plenitudinea și conformitatea aplicării măsurilor de securitate, inclusiv prin efectuarea auditurilor de securitate, și să documenteze rezultatele verificării respective.

(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, furnizorul respectiv de servicii este responsabil pentru aplicarea de către terț a măsurilor de securitate referitoare la rețeaua și sistemul informatic.

(4) În vederea asigurării îndeplinirii obligațiilor prevăzute de prezentul articol și asigurării 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 al securității

cibernetice în baza standardelor și a specificațiilor tehnice europene și celor 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 privind rețelele și sistemele informatice în funcție de sectorul, subsectorul, categoria și/sau tipul furnizorului de servicii.

Articolul 12. Obligațiile de notificare

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

a) incidentul cibernetic cu impact semnificativ asupra securității rețelei sau sistemului informatic ori asupra continuității serviciului;

b) incidentul 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 furnizorului respectiv de servicii – dacă prestarea acestui serviciu depinde de serviciile prestate de terțul respectiv.

(2) Autoritatea competentă prezintă, fără întârzieri nejustificate și nu mai târziu de 24 de ore de la recepționarea informației indicate la alin. (1), furnizorului de servicii un răspuns inițial cu privire la incidentul cibernetic cu impact semnificativ și, la solicitarea furnizorului de servicii, recomandări sau instrucțiuni operaționale privind punerea în aplicare a unor eventuale măsuri de soluționare a incidentului respectiv, inclusiv de atenuare a impactului acestuia și de continuitate a activității.

(3) Furnizorul de servicii prezintă autorității competente, fără întârzieri nejustificate și nu mai târziu de 72 de ore din momentul în care a luat cunoștință despre incidentul cibernetic, actualizarea informațiilor prezentate în conformitate cu alin. (1) și evaluarea inițială a incidentului cibernetic cu impact semnificativ, inclusiv a gravității și a impactului acestuia, 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 termenele stabilite la alin. (1) și (3), despre incidentele cibernetice specificate la alin. (1) sau că terțul informează concomitent, în aceleași termene, autoritatea competentă despre producerea unor astfel de incidente cibernetice.

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

a) gravitatea consecințelor incidentului cibernetic este determinată ca fiind cel puțin înaltă în raportul de evaluare a riscurilor de securitate a rețelelor și sistemelor informatice, întocmit în conformitate cu prevederile art. 11 alin. (2) pct. 1) sau cu cerințele prevăzute de actele aprobate potrivit art. 11 alin. (4);

b) din cauza incidentului cibernetic, prestarea serviciului nu poate fi continuată după expirarea perioadei maxime admise prevăzute în acordul privind nivelul agreat al serviciilor, încheiat în cadrul relațiilor contractuale ale furnizorului de servicii cu alte persoane, sau prevăzute de cerințele privind continuitatea serviciului stabilite în documentația indicată la art. 11 alin. (2) pct. 1)–3);

c) continuitatea serviciului altui 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 nonmateriale considerabile din cauza incidentului cibernetic.

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

(7) În cazul în care furnizorul de servicii nu își îndeplinește obligațiile de notificare prevăzute la alin. (6) în termenul respectiv, autoritatea competentă solicită expres furnizorului de servicii executarea obligației de notificare și, dacă acesta nu o execută în termen de cel mult 3 ore din momentul solicitării, autoritatea competentă asigură notificarea utilizatorilor posibil afectați sau a publicului larg, informând despre aceasta furnizorul de servicii. Modul de informare a utilizatorilor de către furnizorii de servicii sau de către autoritatea competentă este reglementat de actul normativ emis conform alin. (9).

(8) În cazul soluționării unui incident cibernetic cu impact semnificativ, furnizorul de servicii este obligat, în termen de o lună de la transmiterea informației actualizate conform alin. (3), să transmită autorității competente un raport care să

includă cel puțin informațiile despre cauzele producerii incidentului cibernetic, durata 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 către Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice.

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

(11) Furnizorii de servicii persoane juridice de drept public notifică Centrul guvernamental de răspuns la incidentele cibernetice cu privire la incidentele cibernetice în vederea îndeplinirii obligațiilor prevăzute de prezentul articol. Centrul guvernamental de răspuns la incidentele cibernetice informează autoritatea competentă cu privire la incidentele cibernetice prevăzute la alin. (1).

Articolul 13. Notificarea voluntară

(1) Persoanele juridice de drept public și cele 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 incidentele cibernetice cu impact semnificativ, amenințările cibernetice și incidentele cibernetice evitate la limită.

(2) Notificările menționate la alin. (1) din prezentul articol și la art. 12 alin. (10) sunt examinate și soluționate de către autoritatea competentă conform procedurilor stabilite de prezenta lege și actului aprobat potrivit art. 12 alin. (9), 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 efectuat notificarea.

(3) Notificarea voluntară nu impune persoanelor menționate la alin. (1) din prezentul articol și la art. 12 alin. (10) nicio obligație suplimentară care nu le-ar fi revenit dacă nu ar fi efectuat 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 privind rețelele și sistemele informatice ale persoanelor juridice de drept public

(1) Persoanele juridice de drept public sunt obligate să aplice măsurile stabilite la art. 11 alin. (1)–(3) și să respecte obligațiile de notificare a unui incident cibernetic stabilite la art. 12.

(2) Măsurile de securitate minime obligatorii pentru persoanele juridice de drept public sunt stabilite de către 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 potențial al acestora asupra statului, societății și securității rețelelor și sistemelor informatice.

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

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

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

c) nu este posibilă contracararea amenințării cibernetice semnificative sau eliminarea perturbării grave provocate de incidentul cibernetic prin aplicarea altei măsuri;

d) prin contracararea amenințării cibernetice semnificative sau prin eliminarea perturbării grave provocate de incidentul cibernetic nu este cauzat un prejudiciu disproporționat.

(3) Autoritatea competentă notifică, fără întârzieri nejustificate și nu mai târziu de 24 de ore, cu privire la aplicarea măsurilor prevăzute la alin. (2), utilizatorii și, în cazul furnizorului de servicii, autoritatea publică care realizează politica de stat în domeniul respectiv și, după caz, autoritatea cu funcții regulatorii pe piața din domeniul în care se prestează serviciul respectiv.

(4) În exercitarea competenței aferente gestionării incidentelor cibernetice, autoritatea competentă este obligată să țină cont de interesele de afaceri ale furnizorului de servicii și 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 domeniile respective.

(5) Autoritatea competentă informează Serviciul de Informații și Securitate, fără întârzieri nejustificate și nu mai târziu de 24 de ore din momentul în care a luat cunoștință, cu privire la incidentele cibernetice cu impact semnificativ, prevenite sau soluționate, care au vizat obiectivele infrastructurii critice.

Articolul 16. Schimbul transfrontalier de informații

În contextul realizării atribuțiilor prevăzute de prezenta lege sau în temeiul obligațiilor care decurg dintr-un tratat internațional, autoritatea competentă este în drept să transmită altui stat sau organizații internaționale informații privind prevenirea și soluționarea incidentelor cibernetice în cazul în care nu există riscul ca informațiile transmise să prejudicieze securitatea națională sau desfășurarea procedurilor de urmărire penală.

Articolul 17. Schimbul voluntar de informații

(1) Furnizorii de servicii și, după caz, alte persoane juridice care nu intră în domeniul de aplicare al prezentei legi pot face schimb de informații relevante în materie de securitate cibernetică în mod voluntar, inclusiv schimb de informații referitoare la amenințările cibernetice, incidentele cibernetice evitate la limită, vulnerabilități, tehnici și proceduri, indicatorii de compromitere, tacticile adversariale, informații specifice entității care generează amenințări cibernetice, alertele de securitate cibernetică și de 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 cibernetice, răspunsul la incidentele cibernetice sau redresarea în urma acestora ori atenuarea impactului acestora;

b) sporește nivelul de securitate cibernetică, în special prin sensibilizarea cu privire la amenințările cibernetice; prin limitarea sau împiedicarea posibilității răspândirii unor asemenea amenințări; prin sprijinirea unei game de capacități defensive, de remediere și divulgare a vulnerabilităților, de detectare a amenințărilor, de tehnici de limitare și prevenire a amenințărilor, strategii de atenuare sau etape ale proceselor de răspuns și de recuperare; prin 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 indicate la alin. (1) prin crearea și gestionarea unor platforme, inclusiv tehnico-tehnologice, și a comunităților de încredere. Pentru a asigura protecția informațiilor ce au un caracter 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 cibernetice.

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

Capitolul IV
SUPRAVEGHEREA ȘI CONTROLUL 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 își îndeplinesc obligațiile ce le revin conform prevederilor prezentei legi și ale actelor normative de punere în aplicare a acesteia, 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 respectiv.

(3) Măsurile de supraveghere și modul de aplicare a acestora se stabilesc de către Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice.

Articolul 19. Controlul de stat

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

(2) Autoritatea competentă realizează controlul de stat 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 prealabilă a furnizorului de servicii despre controlul preconizat.

(3) În vederea efectuării controlului de stat, autoritatea competentă este în drept 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 dacă:

a) a depistat și, în urma 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 separat pentru furnizorii de servicii persoane juridice de drept public, procedurile detaliate privind modul de efectuare a controlului de stat de către autoritatea competentă asupra respectării obligațiilor ce le revin acestora 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 învestită prin prezenta lege, autoritatea competentă prelucrează date cu caracter personal în condițiile stabilite de legislația în domeniul respectiv.

(2) În cazul în care, în procesul exercitării funcțiilor, autoritatea competentă ia cunoștință despre faptul că încălcarea de către un furnizor de servicii a obligațiilor prevăzute de prezenta lege poate atrage încălcarea legislației privind protecția datelor cu caracter personal, autoritatea competentă informează, fără întârzieri nejustificate, organul de control al prelucrărilor de date cu caracter personal.

Articolul 21. Răspunderea

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

(2) Personalul autorităților și al instituțiilor publice, al furnizorilor de servicii, care interacționează cu autoritatea competentă în condițiile prezentei legi, poartă răspundere, în conformitate cu prevederile legislației, pentru neîndeplinirea sau îndeplinirea necorespunzătoare a atribuțiilor stabilite de actele normative.

Articolul 22. Finanțarea

(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 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 persoanelor juridice respective.

(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 și măsuri de implementare

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

(2) Guvernul:

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

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

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 stabili 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:

a) în termen de 3 luni de la data intrării în vigoare a actelor normative aprobate potrivit art. 4 alin. (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;

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

PREȘEDINTELE PARLAMENTULUI

IGOR GROSU

Chișinău, 16 martie 2023.
Nr. 48.