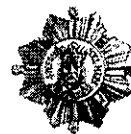




**CENTRUL NAȚIONAL
ANTICORUPȚIE AL
REPUBLICII MOLDOVA**



**НАЦИОНАЛЬНЫЙ ЦЕНТР
ПО БОРЬБЕ С КОРРУПЦИЕЙ
РЕСПУБЛИКИ МОЛДОВА**



MD-2004, mun. Chișinău, bd. Ștefan cel Mare și Sfânt 198
Tel. (+373) 22-25-72-94

Nr. 06/2/3596 din 03.03.2023

La nr. 07-519 din 27.02.2023

Ministerul Economiei

Prin prezenta, Vă remitem atașat raportul de expertiză anticorupție la proiectul de lege privind securitatea cibernetică (număr unic 41/ME/2023).

Anexă: Raportul de expertiză anticorupție – 4 (patru) file.

Director

Digitally signed by Rusu Iulian
Date: 2023.03.03 16:34:35 EET
Reason: MoldSign Signature
Location: Moldova



Iulian RUSU



RAPORT DE EXPERTIZĂ ANTICORUPȚIE

Nr. ELO23/8569 din 03.03.2023

la proiectul de lege privind securitatea cibernetică (număr unic 41/ME/2023)

Prezentul raport de expertiză anticorupție a fost întocmit de Centrul Național Anticorupție al Republicii Moldova în baza Legii nr.100/2017 cu privire la actele normative, a Legii nr.1104/2002 cu privire la Centrul Național Anticorupție, a Legii integrității nr.82/2017 și a Metodologiei de efectuare a expertizei anticorupție a proiectelor de acte legislative și normative, aprobată prin Hotărârea Colegiului Centrului nr.6 din 20 octombrie 2017.

I. Analiza riscurilor de corupere a procesului de promovare a proiectului

I.1. Pertinența autorului, categoriei propuse a actului și a procedurii de promovare a proiectului

Autor al proiectului de act normativ este Guvernul Republicii Moldova, iar autor nemijlocit este Ministerul Economiei, ceea ce corespunde art.73 din Constituția Republicii Moldova și art.47 alin.(3) din Regulamentul Parlamentului, aprobat prin Legea nr.797/1996.

Categoria actului legislativ propus este lege organică, ceea ce corespunde art.72 din Constituție și art. 6-12 din Legea nr.100/2017 cu privire la actele normative.

I.2. Respectarea rigorilor de transparență în procesul decizional la promovarea proiectului

Conform art.8 al Legii nr.239/2008 privind transparența în procesul decizional *"etapele asigurării transparenței procesului de elaborare a deciziilor sunt:*

- a) informarea publicului referitor la inițierea elaborării deciziei;*
- b) punerea la dispoziția părților interesate a proiectului de decizie și a materialelor aferente acestuia;*
- c) consultarea cetățenilor, asociațiilor constituite în corespundere cu legea, altor părți interesate;*
- d) examinarea recomandărilor cetățenilor, asociațiilor constituite în corespundere cu legea, altor părți interesate în procesul de elaborare a proiectelor de decizii;*
- e) informarea publicului referitor la deciziile adoptate."*

Se constată că anunțul privind organizarea consultării publice, proiectul și nota informativă la acesta au fost plasate pe pagina web a Ministerului Economiei www.me.gov.md la compartimentul Transparență decizională/Anunțuri privind consultări publice, precum și pe portalul www.particip.gov.md

În aceste condiții, se consideră că autorul a respectat prevederile legale privind transparența în procesul decizional.

I.3. Scopul anunțat și scopul real al proiectului

În nota informativă se menționează că: *„Proiectul de lege are drept scop asigurarea unui nivel ridicat de securitate a rețelelor 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”.*

În acest context, în Planul de acțiuni al Guvernului pentru anii 2021-2022, aprobat prin Hotărârea Guvernului nr.235/2021, 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 rețelelor și sistemelor informaționale.

Astfel, proiectul de lege privind securitatea cibernetică 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 și care sunt esențiale pentru funcționarea societății, precum și gestionarea incidentelor de securitate.

I.4. Interesul public și interesele private promovate prin proiect

Proiectul promovează interesul public manifestat prin aprobarea de norme generale în domeniul securității cibernetică.

Astfel, după cum se menționează în Analiza de impact la proiectul de lege prenotat - *„Problema principală care urmează a fi soluționată prin inițiativa de reglementare legală propusă poate fi descrisă ca fiind 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”.*

Identificarea în conținutul proiectului a unor lacune de reglementare, precum și a unor norme care creează ambiguități administrative, considerăm că scopul proiectului poate fi periclitat prin implementarea neuniformă a prevederilor proiectului legii.

Analiza detaliată a acestor norme este efectuată în compartimentul III al prezentului raport de expertiză anticorupție.

I.5. Justificarea soluțiilor proiectului

I.5.1. Suficiența argumentării din nota informativă.

În conformitate cu art.30 al Legii nr.100/2017 cu privire la actele normative, proiectele de acte normative sunt însoțite de *„nota informativă care cuprinde:*

a) denumirea sau numele autorului și, după caz, a participanților la elaborarea proiectului actului

normativ;

b) condițiile ce au impus elaborarea proiectului actului normativ și finalitățile urmărite;

c) descrierea gradului de compatibilitate, pentru proiectele care au ca scop armonizarea legislației naționale cu legislația Uniunii Europene;

d) principalele prevederi ale proiectului și evidențierea elementelor noi;

f) modul de încorporare a actului în cadrul normativ în vigoare".

Nota informativă stabilește condițiile ce au impus elaborarea proiectului, evidențiază elementele noi și finalitățile urmărite prin promovarea proiectului.

Examinând conținutul notei informative a proiectului supus expertizei se constată că aceasta întrunește condițiile menționate în art.30 al Legii nr.100/2017 cu privire la actele normative.

I.5.2. Argumentarea economică-financiară.

Conform art.30 lit.e) al Legii nr.100/2017 cu privire la actele normative, nota informativă trebuie să conțină „e) fundamentarea economico-financiară”.

În nota informativă se menționează că:

„Impactul economico-financiar al implementării proiectului de lege este detaliat descris în capitolul corespunzător al analizei de impact. 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”.

I.5.3. Efectuarea analizei impactului de reglementare.

Potrivit art.30, pct.2 din anexa nr.1 la Legea nr.100/2017 cu privire la actele normative, „În cazul proiectelor actelor normative ce reglementează activitatea de întreprinzător, suplimentar se descriu concluziile și propunerile înaintate în cadrul studiilor de cercetare, precum sau 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”.

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

Metodologia de analiză a impactului în procesul de fundamentare a proiectelor de acte normative a fost aprobată prin Hotărârea Guvernului nr.23 din 18.01.2019.

La proiectul de lege privind securitatea cibernetică a fost elaborată Analiza Impactului de Reglementare care definește problema, stabilește obiectivele, identifică opțiunile și analizează și compară opțiunile. La fel, se menționează despre aspectele privind implementarea și monitorizarea.

În nota informativă autorul proiectului menționează că „Proiectul a fost examinat în cadrul ședinței Grupului de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător și a fost susținut condiționat”.

II. Analiza generală a factorilor de risc ale proiectului

II.1. Limbajul proiectului

Potrivit art.54 al Legii nr.100/2017 cu privire la actele normative „textul proiectului actului normativ se elaborează [...] cu respectarea următoarelor reguli: [...]

a) se expune într-un limbaj simplu, clar și concis [...]

c) terminologia utilizată este constantă, uniformă și corespunde celei utilizate în alte acte normative, în legislația Uniunii Europene și în alte instrumente internaționale la care Republica Moldova este parte, cu respectarea prevederilor prezentei legi; [...]

e) se interzice folosirea neologismelor dacă există sinonime de largă răspândire, [...]

f) se evită folosirea [...] a cuvintelor și expresiilor [...] care nu sînt utilizate sau cu sens ambiguu;

g) se evită tautologiile juridice;

h) se utilizează, pe cât este posibil, noțiuni monosemantice, [...]”.

Textul proiectului este expus în mare parte într-un limbaj simplu, clar și concis, cu respectarea regulilor gramaticale și de ortografie, întrunind cerințele prevăzute de art.54 din Legea nr.100/2017.

Considerăm că utilizarea în conținutul normelor a textelor „poate solicita expres realizarea obligației”, „poate aroga obligația de notificare” și „poate restricționa utilizarea sau accesul la un sistem informativ” ar putea fi interpretate diferit de la caz la caz, generând manifestări de corupție.

Astfel, se va examina suplimentar oportunitatea păstrării acestor sintagme în conținutul normelor analizate.

Analiza detaliată a acestor aspecte este efectuată în compartimentul III al prezentului raport de expertiză anticorupție.

II.2. Coerența legislativă a proiectului

În textul proiectului nu au fost identificate norme contradictorii sau conflicte dintre prevederile acestuia cu reglementările altor acte normative în vigoare.

II.3. Activitatea agenților publici și a entităților publice reglementată în proiect

Proiectul reglementează activitatea entităților publice și a agenților publici din cadrul acestora responsabile/responsabili de implementarea normelor acestuia.

Normele proiectului atribuie unele competențe neclare prin riscul interpretării acestora, ceea ce poate duce la comiterea manifestărilor de corupție.

Analiza acestor aspecte este efectuată în compartimentul III al prezentului raport de expertiză anticorupție.

II.4. Atingeri ale drepturilor omului care pot fi cauzate la aplicarea proiectului

Prevederile proiectului nu aduc atingere drepturilor fundamentale ale omului consacrate de Constituția Republicii Moldova, Declarația Universală a Drepturilor Omului și Convenția Europeană a Drepturilor Omului.

III. Analiza detaliată a factorilor de risc și a riscurilor de corupție ale proiectului

- 1 -

Art.8 din proiect -

Art.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.

Obiecții:

Prin norma articolului 8, Guvernul este investit cu atribuția de a institui Centrul guvernamental de răspuns la incidentele cibernetice la nivelul rețelelor și sistemelor informatice ale căror proprietar este statul.

Potrivit alin.(3) al art.8, 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 lege, inclusiv a celor de notificare și a interacțiunii acestora cu autoritatea competentă și echipa de răspuns la incidente cibernetice la nivel național.

În acest sens, constatăm că norma art.8 nu stabilește expres funcția Centrului, precum și atribuțiile acestuia, lăsând acest aspect pentru a fi reglementat de către Guvern.

Or, considerăm că odată ce, potrivit art.7 din lege, autorității competente îi sunt stabilite expres atribuții, necesită reglementarea expresă și a atribuțiilor Centrului, în vederea excluderii riscurilor de stabilire a unor atribuții paralele între aceste entități sau a unor atribuții care pot depăși scopul instituirii Centrului.

Astfel, atât în cazul autorității competente, cât și în cazul Centrului guvernamental de răspuns la incidente cibernetice, Guvernul urmează să stabilească doar modul de organizare și funcționare a acestora.

În final, menționăm că nestabilirea atribuțiilor Centrului în lege, va crește riscul stabilirii unor atribuții paralele sau a unor atribuții care pot depăși atribuțiile autorității competente în anumite direcții, ceea ce se poate răsfrânge negativ asupra finalității scopului instituirii autorității competente și a Centrului guvernamental în partea ce ține de asigurarea eficientă a securității cibernetice.

Recomandări:

Propunem autorului includerea în norma articolului 7 a atribuțiilor Centrului Guvernamental de răspuns la incidentele cibernetice.

Factori de risc:

- Atribuții excesive, improprie sau contrare statutului entității publice
- Lacună de drept

Riscuri de corupție:

- Generale

- Atribuții extensive de reglementare
- Lipsa/ambiguitatea procedurilor administrative

- 2 -

Art.12 alin.(7) din proiect -

Art.12 Obligațiile furnizorilor de servicii de a notifica incidentele cibernetice

(...)

(7) În cazul în care furnizorul de servicii nu realizează obligațiunile de notificare prevăzute de alineatul (6) în termenul respectiv, autoritatea competentă poate solicita expres realizarea obligațiunii de către furnizorul de servicii sau își poate aroga obligația de notificare a 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 la alin.(9).

Obiecții:

Norma instituie dreptul autorității competente de a decide aplicarea normei în dependență de interes. Astfel, autoritatea competentă poate solicita expres realizarea obligațiunii de către furnizorul de servicii, totodată, poate notifica, unilateral, destinatarii posibil afectați sau publicul.

Norma nu stabilește careva condiții sau cazuri de aplicare a normei diferențiate, or, norma face referință doar la faptul că modul de informare a destinatarilor de către furnizorii de servicii sau de către autoritatea competentă constituie obiectul de reglementare a unui act normativ aprobat de Guvern.

În aceste condiții, prin utilizarea în normă a textului „poate solicita expres realizarea obligațiunii de către furnizorul de servicii sau își poate aroga obligația de informare” va permite autorității competente de a decide, în aceleași situații, în mod diferit, în dependență de interes.

Totodată, norma nu stabilește un termen în care autoritatea competentă, după constatarea neîndeplinirii de către furnizorul de servicii a obligației prevăzute la alin.(6), urmează să fie obligată să solicite expres acestuia realizarea obligațiunii legale.

Riscurile identificate constau în aplicarea neuniformă a normei, precum și în tergiversarea intenționată de către unii participanți a luării măsurilor urgente în privința limitării impactului negativ al unui incident cibernetic semnificativ.

Recomandări:

Propunem autorului delimitarea cazurilor în care autoritatea competentă urmează să fie obligată să solicite expres realizarea obligațiunii de către furnizorii de servicii și a cazurilor în care autoritatea competentă poate să notifice, în mod unilateral, destinatarii posibil afectați sau publicul.

La fel, propunem stabilirea unui termen de conformare de către autoritatea competentă de solicitare a realizării de către furnizorii de servicii a obligațiilor ce reies din norma alin.(6).

Factori de risc:

- Formulare ambiguă care admite interpretări abuzive
- Lacună de drept
- Atribuții care admit derogări și interpretări abuzive
- Temeiuri neexhaustive/ambigui/subiective pentru refuzul sau inacțiunea entității publice
- Lipsa/ambiguitatea procedurilor administrative
- Stabilirea unui drept al entității publice în loc de o

Riscuri de corupție:

- Generale

obligație ● Lipsa unor termene concrete/termene nejustificate/prelungirea nejustificată a termenilor	
---	--

- 3 -

Art.15 alin.(2) din proiect -

Art.15 Gestionarea incidentelor cibernetice

(...)

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

Obiecții:

Norma art.15 stabilește dreptul autorității competente de a restricționa sau nu utilizarea sau accesul la sistemul informativ.

Cu toate acestea, norma stabilește foarte clar întrunirea unor condiții cumulative pentru a restricționa utilizarea sau accesul la un sistem informativ.

Or, în cazul în care sunt întrunite condițiile (expres stabilite), considerăm că autoritatea competentă urmează să acționeze într-un mod ferm, norma urmând să fie una imperativă, care să impună o anumită conduită de urmat (o normă cu caracter prescriptiv).

Totodată, autoritatea competentă urmează să-și exercite atribuțiile eficient și într-un mod care să trateze într-o manieră justă și echitabilă toți subiecții ce se află în situații identice.

În acest sens, în redacția din proiect, s-ar putea ca acțiunile pe care le va întreprinde autoritatea competentă să difere de la caz la caz, cu riscuri iminente comiterii manifestărilor de corupție.

Recomandări:

Propunem autorului substituirea sintagmei „poate restricționa utilizarea”cu sintagma „restricționează utilizarea”.

Factori de risc:

- Formulare ambiguă care admite interpretări abuzive
- Atribuții care admit derogări și interpretări abuzive
- Temeiuri neexhaustive/ambigui/subiective pentru refuzul sau inacțiunea entității publice
- Lipsa/ambiguitatea procedurilor administrative
- Stabilirea unui drept al entității publice în loc de o obligație

Riscuri de corupție:

- Generale

IV. Concluzia expertizei

În nota informativă se menționează că: „Proiectul de lege are drept scop asigurarea unui nivel ridicat de securitate a rețelelor 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”.

În acest context, în Planul de acțiuni al Guvernului pentru anii 2021-2022, aprobat prin Hotărârea Guvernului nr.235/2021, 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 rețelelor și sistemelor informaționale.

Astfel, proiectul de lege privind securitatea cibernetică 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 și care sunt esențiale pentru funcționarea societății, precum și gestionarea incidentelor de securitate.

În conținutul proiectului au fost identificate unele norme, care, în opinia noastră, comportă pericol de coruptibilitate.

Astfel, normele care utilizează în conținut textele „poate solicita expres realizarea obligației”, „poate aroga obligația de notificare” și „poate restricționa utilizarea sau accesul la un sistem informativ” ar putea fi interpretate diferit de la caz la caz, generând manifestări de corupție.

În acest sens, normele ar putea cauza dificultăți în interpretare și aplicare uniformă a acestora.

Totodată, lipsa stabilirii exprese în lege a atribuțiilor Centrului guvernamental de răspuns la incidentele cibernetică va crește riscul aprobării acestora într-un mod care ar putea depăși scopul instituirii Centrului de către legiuitor (Parlament).

În final, pentru a evita confuziile și diferențele de tratare a sensului normelor, precum și în vederea interpretării uniforme a normelor juridice propunem autorului reexaminarea normelor analizate prin prisma prezentului raport de expertiză anticorupție.

03.03.2023

Expert al Direcției legislație și expertiză anticorupție:
Vadim CURMEI, Inspector principal

Digitally signed by Curmei Vadim
Date: 2023.03.03 14:43:25 EET
Reason: MoldSign Signature
Location: Moldova

