|  |
| --- |
| **Analiza a impactului de reglementare** **la proiectul de lege pentru modificarea Legii nr. 20/2009 privind prevenirea şi combaterea criminalității informatice**  |
| **Titlul analizei impactului**(poate conţine titlul propunerii de act normativ): | **Proiectul de lege pentru** modificarea Legii nr. 20/2009 privind prevenirea și combaterea criminalității informatice |
| **Data:** | 29.11.2022 |
| **Autoritatea administrației publice (autor):** | Ministerul Afacerilor Interne  |
| **Subdiviziunea:** | Direcția politici de prevenire și combatere a criminalității |
| **Persoana responsabilă şi datele de contact:** | Dumitru Vleju- ofițer principal al Direcției politici de prevenire și combatere a criminalitățiiDate de contact: tel. 022 255-750.e-mail: dumitru.vleju@mai.gov.md,  |
| **Compartimentele analizei impactului** |
| **1. Definirea problemei** |
| a) Determinați clar și concis problema și/sau problemele care urmează să fie soluționate |  |
| Factorul-cheie care determină necesitatea intervenției sunt ambiguitățile de implementare a prevederilor cadrului normativ urmare modificării Legii nr. 20/2009 privind prevenirea şi combaterea criminalității informatice, operate prin Legea nr. 257/2020, determinate prin lipsa autorităților cu drept de dispunere a sistării accesului la conținut infracțional și limitarea sistării accesului la conținut infracțional numai prin adresele IP. Subsecvent, a fost constată lipsa coroborării art. 4) din Legea nr. 6/2009 pentru ratificarea Convenției Consiliului Europei privind criminalitatea informatică și Legea nr. 20/2009 privind prevenirea şi combaterea criminalității informatice. |
| b) **Descrieți problema, persoanele/entitățile afectate și cele care contribuie la apariția problemei, cu justificarea necesității schimbării situației curente și viitoare, în baza dovezilor și datelor colectate și examinate** |  |
| Tehnologia informațională a evoluat și a transformat societățile la nivel mondial într-un mod extraordinar. Cu toate acestea, este înregistrată, de asemenea, o creștere semnificativă a exploatării tehnologiei informaționale în scopuri infracționale. Criminalitatea informatică este considerată în prezent de multe state o amenințare gravă la adresa drepturilor omului, a statului de drept și a funcționării societăților democratice. Amenințările reprezentate de criminalitatea informatică sunt numeroase, printre exemple se numără violența sexuală online împotriva copiilor și alte infracțiuni împotriva demnității și integrității persoanelor; furtul și utilizarea abuzivă a datelor cu caracter personal care afectează viața privată a persoanelor. La 16 decembrie 2020 a fost adoptată legea nr. 257 cu privire la modificarea unor acte normative, prin care a fost introdusă modificarea la articolul 7 din Legea nr. 20/2009 privind prevenirea şi combaterea criminalității informatice și anume completarea cu lit. e1) cu următorul cuprins: *să sisteze, în condițiile legii, folosind metodele şi mijloacele tehnice din posesie, accesul din propriul sistem informatic la toate adresele IP pe care sunt amplasate pagini web, inclusiv cele găzduite de furnizorul respectiv, ce contribuie la comiterea infracțiunilor sau la încălcarea prevederilor legislației în vigoare ori conțin/difuzează instrucțiuni privind modul de comitere a acestora*”. Introducerea acestei reglementări, lipsită de autoritățile care sunt abilitate cu dreptul de a dispune o astfel de măsură, generează apariția diferitor interpretări și devine dificilă executarea acestei obligații de către furnizorii de servicii. Un exemplu elocvent de sistarea accesului la conținutul infracțional este împiedicarea utilizatorilor să acceseze site-uri web care prezintă materiale de abuz sexual asupra copiilor, reprezentând o parte importantă a luptei împotriva acestei infracțiuni. Prin sistarea accesului, se oprește re-victimizarea copiilor abuzați și are un efect pedagogic asupra utilizatorilor care ar putea fi pe cale să comită o infracțiune gravă prin vizualizarea sau descărcarea de materiale ilegale. Rolul de prevenire și combaterea acestui fenomen fiind în competența subdiviziunii specializate a Ministerului Afacerilor Interne, care nu este indicată în lista autorităților cu dreptul de a dispune această măsură, astfel dispunând de capacități limitate în domeniul prevenirii acestui fenomen.Totodată, subdiviziunea centrală specializată în prevenirea și combaterea criminalității informatice a MAI numai la compartimentul sustragere a mijloacelor financiare de pe cardurile bancare ale cetățenilor Republicii Moldova, în primul semestrului I 2022, a înregistrat 218 de infracțiuni, cu un prejudiciu de 4,5 milioane MDL, iar în perioada analogică a anului 2021 au fost înregistrate 550 de infracțiuni cu un prejudiciu de 9 milioane MDL.Astfel în scopul prevenirii cazurilor din domeniul infracțiunilor informatice, pentru care este necesar să fie acordat prioritate maximă, este necesar de reglementat la nivel normativ, autoritățile abilitate cu dreptul de a dispune sistare accesului la conținut infracțional, care să fie compatibilă cu drepturile fundamentale, protecția datelor, protecția consumatorilor, comerțul electronic etc. Respectiv, subdiviziunea centrală specializată în prevenirea și combaterea criminalității informatice a MAI, care conform atribuțiilor, realizează atât combaterea, cât și prevenirea infracțiunilor, atribuții prevăzute de legea nr. 320/2012cu privire la activitatea Poliției și statutul polițistului. În acest sens, poliția asigură reacționarea promptă la sesizările despre infracțiuni, constată cauzele şi condițiile ce pot genera sau contribui la săvârșirea infracțiunilor care sunt în competența Poliției, cu sesizarea, potrivit legii a persoanei cu funcții de răspundere cu privire la necesitatea de întreprindere a măsurilor de înlăturare a acestor cauze și condiții. Subsecvent, un moment important în vederea atribuirii funcției de sistare a accesului la conținut infracțional către Ministerul Afacerilor Interne și Serviciul de Informații și Securitate, va duce într-o stare organizată și strict controlată ingerința dată, din considerentul că la moment dispunerea acesteia, poate fi atribuită oricărei autorități prevăzute de legea nr. 20/2009 privind prevenirea şi combaterea criminalității informatice, posibil și de către angajați care nu dispun de cunoștințe tehnice speciale în acest domeniu, ceea ce generează aplicare incorectă a acestei prevederi.Dispunerea de către subdiviziunile centrale specializate în prevenirea și combaterea criminalității informatice din cadrul MAI și SIS, reiese din stoparea conținutului infracțional și a apariției de noi victime, dar nu are scopul de stabilire a făptuitorului, care uneori este imposibilă datorită faptului că site-ul este găzduit în afara teritoriului RM, aceste măsuri sunt stipulate în Codul de procedură penală. La moment, incertitudinea creată, împiedică prevenirea infracțiunilor informatice și celor comise cu utilizarea tehnologiilor informaționale, ca urmare sunt afectați :* Utilizatorii de sisteme informatice care accesează în continuare conținutul infracțional, deoarece accesul nu este sistat. Iar măsura de sistare a accesului este o măsură de prevenire, considerent din care dispunerea se va efectua în termeni proximi de către subdiviziunile centrale specializate în prevenirea și combaterea criminalității informatice din cadrul MAI și SIS;
* Entitățile economice, care sunt supuși atacurilor prin intermediul tehnologiilor informaționale, prin accesarea site-urilor phishing, astfel documentele comerciale (contabile, cu secret comercial), bazele de date sunt criptate sau sustrase, iar pentru întoarcerea acestor se estorchează mijloace financiare;
* Furnizorii servicii , deoarece nu cunosc a cui solicitări trebuie să fie executate, astfel ori o execută solicitarea primită de orice autoritate ori refuză la toți, respectiv neîndeplinind obligațiile sale prevăzute de art. 7 alin. (1) lit. e1)din legea nr. 20/2009 privind prevenirea şi combaterea criminalității informatice;
* Statul care întâmpină dificultăți în asigurarea protecției în mediul online.

Totodată excluderea obligațiunii de sistare a accesului anume în baza adreselor IP, va asigura realizarea acestei acțiuni prin diferite metode posibile, cum ar fi: în baza adresei URL a paginii web, în baza DNS (numelui de domeniu) ori adreselor IP, precum și alte metode existente sau care vor apărea, fără a interveni legislativ în viitor. Un alt aspect important privind sintagma „*la toate adresele IP*” este existența riscului ca mai multe site-uri web să împartă aceeași adresă IP, astfel pot fi afectate alte site-uri web, care nu au contribuit la comiterea infracțiunilor și activează în conformitate cu legislația. ConservareaLegea nr. 6/2009 pentru ratificarea Convenţiei Consiliului Europei privind criminalitatea informatică prevede că Ministerul Afacerilor Interne desemnează punctul de contact responsabil de realizarea prevederilor articolului 35 din Convenție (inclusiv sub aspectul dispunerii conservării datelor informatice). Conservarea datelor informatice este prima acțiune care necesită a fi realizată în vederea neadmiterii ștergerii sau alterării datelor cu valoare probatorie. Aceasta este o acțiune foarte importantă și sub aspectul cooperării internaționale, luînd în considerației că criminalitatea informatică este un fenomen transfrontalier care persistă și evoluează la nivel global. Astfel, lipsa atribuției de dispunere a conservării datelor informatice de către MAI duce la neîndeplinirea de către Republic Moldova a obligațiilor prevăzute de Convenția de la Budapesta.Articolul 29 din Convenția de la Budapesta asigură conservarea rapidă a datelor, astfel încât să permită un timp suficient pentru a obține datele prin intermediul asistenței juridice internaționale. Conform Raportului explicativ a Convenției de la Budapesta, cererea de conservare rapidă a datelor informatice stocate este o "*măsură provizorie destinată să aibă loc mult mai rapid decât executarea unei cereri de asistență internațională tradițională (pct. 282)”* și ar trebui să precizeze autoritatea care solicită conservarea cererii. Astfel, cererea de conservare rapidă a datelor nu trebuie să îndeplinească condițiile formale ale unei cereri de asistență juridice internaționale tradițională (prevăzută de Codul de procedură penală) și nici nu trebuie să fie emisă de aceeași autoritate care va trimite ulterior cererea de asistență juridică internațională, privind divulgarea datelor conservate.Conservarea datelor informatice în sine reprezintă solicitarea adresată furnizoului de servicii de comunicații electronice de a păstra și a nu șterge datele informatice administrate în contextul furnizării de servicii. Astfel, conservarea datelor informatice nu presupune obținerea datelor de către autoritățile abilitate, acestea fiind păstrate de către furnizorul de servicii pînă la momentul ridicării datelor conform procedurii prevăzute de lege, sau în cazul în care datele respective nu sunt ridicate în termenul asigurării conservării, prevăzute de Legea nr. 20/2009, acestea sunt șterse de către furnizorul de servicii. Respectiv, conservarea datelor informatice nu reprezintă o ingerință în viața privată, fiind o măsură de asigurare a integrității datelor cu valoare probatorie și este necesară pornind de la faptul că furnizorii de servicii de comunicații electronice păstrează datele generate sau procesate pentru o perioadă limitată de timp, după care le nimicesc.În redacția actuală a art. 4 alin. (4) lit. b) din Legea nr. 20/2009, Procuratura dispune în cadrul desfășurării urmăririi penale conservarea datelor informatice. Ca urmare, a apărut o contradicție cu Legea nr. 6/2009 pentru ratificarea Convenţiei Consiliului Europei privind criminalitatea informatică raportată la prevederile Convenției și a fost generată apariție unor interpretări precum că măsura conservării datelor informatice poate fi dispusă doar de către procuror și doar în cadrul urmăririi penale. Respectiv, posibilitatea conservării datelor în baza cooperării internaționale prevăzută de Convenției este dificilă în cazul în care aceasta este dispusă din partea Ministerului Afacerilor Interne, care este desemnat punctul de contact responsabil să asigure cooperarea internațională imediată și permanentă în domeniul combaterii criminalității informatice. Aceasta are ca rezultat dispariția datelor informatice cu valoare probatorie și pune în pericol funcționarea rețelei 24/7 a Convenției de la Budapesta, având în vedere că majoritatea punctelor de contact sunt autoritățile polițienești. Menționăm, că în cazul infracțiunilor comise prin sistemele informatice datele informatice reprezintă cea mai valoroasă și în unele cazuri unica sursă de informații cu valoare probatorie pentru stabilirea subiectului infracțiunii și altor circumstanțe pe caz.Persoanele/entitățile afectate:1. Autoritățile responsabile de prevenirea și combaterea criminalității informatice, ale căror activitate devine ineficientă ca urmare a ștergerii datelor informatice în mod automat de către furnizorii de servicii după scurgerea termenului de păstrare.
2. Persoanele fizice și juridice – deoarece în cadrul investigațiilor inițiate în baza plângerilor acestora nu pot fi acumulate date informatice necesare. Respectiv, investigațiile nu se finalizează cu succes.

În același timp, intervenția preconizată prin proiectul menționat, nu presupune adoptarea unor noi mecanisme, acestea fiind deja în vigoare, dar din contra stipulează expres autoritățile abilitate cu atribuția de dispunere a sistării accesului la conținut infracțional *(cu cunoștințe tehnice în domeniu)*, ceea ce nu va admite limitării eronate sau excesive a accesului la conținutul web, fiind în beneficiul furnizorilor de servicii  |
| c) Expuneți clar cauzele care au dus la apariţia problemei |  |
| 1. Legea nr. 20/2009 a fost adoptată imediat după ratificarea Convenţiei Consiliului Europei privind criminalitatea informatică și nu a fost suficient corelată cu prevederile convenției.
2. De la momentul ratificării Convenţiei Consiliului Europei privind criminalitatea informatică au trecut 12 ani, tehnologiile informaționale s-au dezvoltat, fiind aplicate în toate domeniile vieții economice, sociale, astfel la moment există necesitatea unui răspuns prompt în raport cu criminalitatea informatică.
3. Legea nr. 20/2009 a fost completată la art. 7 alin.(1) cu litera e1) cu obligația furnizorilor de servicii de a sista accesul, însă nu a fost prevăzut care autoritate dispune sistarea.
4. Expunerea sistării exhaustiveîn baza adreselor IP**, a** exclus realizarea acestei acțiuni prin diferite metode posibile, cum ar fi: în baza adresei URL a paginii web, în baza DNS (numelui de domeniu), astfel persistând riscul de a afectata alte site-uri web, care nu au contribuit la comiterea infracțiunilor sau la încălcarea prevederilor legislației, dar împart aceeași adresă IP.
 |
| d) Descrieți cum a evoluat problema şi cum va evolua fără o intervenție  |  |
| Sistarea1. În perioada anilor 2020-2021 persoanele fizice și juridice din Republica Moldova au devenit tot mai mult afectate de fraude în spațiul online, unde infractorii expediază, prin metoda Phising, linkuri către adrese URL de pe care la accesare sunt descărcate și instalate programe malițioase care criptează computerul și estorcă mijloace financiare.
2. Fenomenul de criminalitate tradițional migrează în spațiul online, permițând, spre exemplu, comercializarea drogurilor în mediul online pe pagini web create în acest sens.
3. În lipsa unei intervenții, vor fi victimizate și alter persoane fizice și juridice prin intermediul paginilor web create în scop infracțional care deja există. De asemenea, reieșind din faptul lipsei răspunsului prompt a statului în raport cu fenomenul dat, va fi încurajată apariția de noi pagini web cu conținut infracțional.
 |
| e) Descrieți cadrul juridic actual aplicabil raporturilor analizate şi identificați carenţele prevederilor normative în vigoare, identificați documentele de politici şi reglementările existente care condiționează intervenția statului |  |
| Legea nr. 20/2009privind prevenirea și combaterea criminalității informatice**.** |
| **2. Stabilirea obiectivelor** |
| a) Expuneți obiectivele (care trebuie să fie legate direct de problemă și cauzele acesteia, formulate cuantificat, măsurabil, fixat în timp și realist) |  |
|

|  |
| --- |
| Obiectivul principal al acestui proiect constă în perfecționarea și actualizarea actului normativ prin sporirea gradului de claritate și coerență al reglementării, corelarea cu alte prevederi legale, creșterea eficacității practice și înlăturarea lacunelor identificate, asigurarea unui răspuns prompt și eficient în prevenirea și descoperirea infracțiunilor, care pot fi remediate doar prin intervenție legislativă.  |

 |
| **3. Identificarea opțiunilor** |
| a) Expuneți succint opțiunea „a nu face nimic”, care presupune lipsa de intervenție |  |
| Opțiunea „a nu face nimic” este opțiunea prin care nu se vor opera modificările propuse în legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice, iar situația actuală va rămâne neschimbată, precum și conform tendințelor ar putea să se înrăutățească. |
| b) Expuneți principalele prevederi ale proiectului, cu impact, explicând cum acestea țintesc cauzele problemei, cu indicarea novațiilor și întregului spectru de soluții/drepturi/obligații ce se doresc să fie aprobate |  |
| Proiectul Legii pentru modificarea Legii nr. 20/2009 privind prevenirea și combaterea criminalității informaticeinclude următoare propuneri:1. Se propune completarea articolului 4 alineatul (1) din lege cu textul „ , *dispun prin intermediul subdiviziunii sale centrale specializate în prevenirea şi combaterea criminalității informatice sistarea accesului la pagini web în condițiile prevăzute la articolul 7 alineatul (1) litera e1)*”, astfel Ministerul Afacerilor Interne și Serviciul de Informații și Securitate vor dispune prin intermediul subdiviziunii sale centrale specializate în prevenirea și combaterea criminalității informatice sistarea accesului la pagini web ce contribuie la comiterea infracțiunilor sau la încălcarea prevederilor legislației ori conțin/difuzează instrucțiuni privind modul de comitere a acestora.
2. Se propune completarea articolului 4 alineatul (2) din lege cu textul „ , *dispune conservarea imediată a datelor informatice ori a datelor referitoare la traficul informatic*”.
3. Se propune excluderea la articolul 7 alineatul (1) litera e1) a textului „în condițiile legii,”, „*toate adresele IP pe care sunt amplasate*” și a cuvintelor „în vigoare”.

Astfel,  |
| c) Expuneți opțiunile alternative analizate sau explicați motivul de ce acestea nu au fost luate în considerare |  |
|  Pe marginea problemelor care au stat la baza elaborării proiectului actului normativ nu există opțiuni alternative de intervenție, alegerea putând fi realizată doar între soluția de a modifica cadrul normativ existent și în aceea de nu se interveni. |
| **4. Analiza impacturilor opțiunilor** |
| a) Expuneți efectele negative și pozitive ale stării actuale și evoluția acestora în viitor, care vor sta la baza calculării impacturilor opțiunii recomandate |  |
| Efectele negative ale stării actuale sunt:* capacitate de reacție insuficientă a autorităților responsabile de prevenirea și combaterea criminalității informatice;
* persoane fizice și juridice victimizate prin intermediul paginilor web create în scop infracțional care deja există;
* perturbarea funcționării rețelei 24/7 a Convenției de la Budapesta;
* sistarea exhaustivăîn baza adreselor IP, poate afecta alte site-uri web, care nu au contribuit la comiterea infracțiunilor sau la încălcarea prevederilor legislației, dar împart aceeași adresă IP.

Efecte pozitive nu au fost identificate. |
| b1) Pentru opțiunea recomandată, identificați impacturile completând tabelul din anexa la prezentul formular. Descrieți pe larg impacturile sub formă de costuri sau beneficii, inclusiv părțile interesate care ar putea fi afectate pozitiv și negativ de acestea |  |
| 1. Stabilirea expresă a entităților cu dreptul de a dispune sistarea accesului la pagini web ce contribuie la comiterea infracțiunilor sau la încălcarea prevederilor legislației ce contribuie la comiterea infracțiunilor sau la încălcarea prevederilor legislației ori conțin/difuzează instrucțiuni privind modul de comitere a acestora, exclude interpretările confuze și discreționare. Concomitent, luând în considerație aspectul tehnologic al măsurii, care necesită cunoștințe tehnice în domeniu, măsura va fi dispusă anume de către subdiviziunea centrală specializată în prevenirea și combaterea criminalității informatice din cadrul celor două autorități (MAI și SIS), ceea ce nu va admite limitări eronate sau excesive a accesului la conținutul web.

Nu au fost identificate costuri suplimentare de implementare a acestei opțiuni din considerentul că, sistarea accesului la conținut infracțional deja este stipulată în lege, iar opțiunea propusă stabilește concret cine va dispune această măsură. 1. Dispunerea conservării datelor informatice de către MAI va asigura îndeplinirea de către Republic Moldova a obligațiilor prevăzute de art. 35 a Convenției Consiliului Europei privind criminalitatea informatică, ratificată prin Legea nr. 6/2009, în care MAI este desemnat punct de contact în scopul asigurării unei asistențe imediate pentru investigațiile referitoare la infracțiunile privind sisteme sau date informatice, inclusiv prin aplicarea măsurii de conservare a datelor informatice.

Esența conservării datelor informatice constă în prevenirea dispariției datelor informatice cu valoarea probatorie ca urmare a alterării sau ștergerii, inclusiv în urma expirării termenului legal de păstrare a datelor cu privire la traficul informatic – 6 luni. Conservarea datelor informatice nu prezintă în sine o ingerință în viața privată deoarece nu presupune oferirea datelor respective către autoritățile abilitate, ci este o măsură de asigurare a integrității datelor, iar obținerea datelor informatice conservate se efectuează în baza reglementărilor stabilite de legislația procesual penală.Datele informatice reprezintă cea mai valoroasă și în unele cazuri unica sursă de informații cu valoare probatorie pentru stabilirea subiectului infracțiunii și altor circumstanțe pe caz. Astfel respectând principiul operativității prevăzut de art. 3 lit. c) din Legea nr. 20/2009 și dispunerea de către MAI a conservării datelor informatice, va asigura protecția adecvată în mediul online, precum și va facilita descoperirea infracțiunilor din acest domeniu.Nu au fost identificate costuri suplimentare de implementare a acestei opțiuni din considerentul că, în conformitate cu Legea nr. 241/2007 *comunicaţiilor electronice,* furnizorii de reţele şi/sau servicii de comunicaţii electronice, indiferent de tipul de proprietate, sunt obligați: „ *să păstreze toate informațiile disponibile, generate sau procesate în procesul furnizării propriilor servicii de comunicaţii electronice, necesare pentru identificarea şi urmărirea sursei de comunicaţii electronice, identificarea destinaţiei, tipului, datei, orei şi duratei comunicaţiei, identificarea echipamentului de comunicaţii al utilizatorului sau al altui dispozitiv utilizat pentru comunicaţie, identificarea coordonatelor echipamentului terminal de comunicaţii mobile şi să asigurare prezentarea acestor informaţii organelor împuternicite în condiţiile legii. Informaţiile ce ţin de serviciile de telefonie mobilă sau fixă vor fi păstrate o perioadă de un an, iar cele ce ţin de reţeaua Internet - de 6 luni, la expirarea cărora informațiile menționate vor fi distruse ireversibil, prin proceduri automatizate, cu excepția informațiilor și documentelor prelucrate în conformitate cu art. 73 și a celor care, conform actelor normative în vigoare, se păstrează pentru o perioadă mai îndelungată. Obligația de păstrare se referă inclusiv la tentativele de apel eşuate.”*Excluderea sistării exhaustiveîn baza adreselor IP**,** va asigura realizarea acestei acțiuni prin diferite metode posibile, cum ar fi: în baza adresei URL a paginii web, în baza DNS (*numelui de domeniu*) ori adreselor IP, precum și alte metode existente sau care vor apărea, fără a interveni legislativ în viitor, fiind în beneficiul furnizorilor de servicii care vor alege singuri modalitatea disponibilă de echipamentele sale. Subsecvent va fi exclus riscul de a afecta alte site-uri web, care nu au contribuit la comiterea infracțiunilor sau la încălcarea prevederilor legislației, dar împart aceeași adresă IP.  |
| b2) Pentru opțiunile alternative analizate, identificați impacturile completând tabelul din anexa la prezentul formular. Descrieți pe larg impacturile sub formă de costuri sau beneficii, inclusiv părțile interesate care ar putea fi afectate pozitiv și negativ de acestea |  |
| - |
| c) Pentru opțiunile analizate, expuneți cele mai relevante/iminente riscuri care pot duce la eșecul intervenției și/sau schimba substanțial valoarea beneficiilor și costurilor estimate și prezentați presupuneri privind gradul de conformare cu prevederile proiectului a celor vizați în acesta |  |
| - |
| d) Dacă este cazul, pentru opțiunea recomandată expuneți costurile de conformare pentru întreprinderi, dacă există impact disproporționat care poate distorsiona concurența și ce impact are opțiunea asupra întreprinderilor mici și mijlocii. Se explică dacă sînt propuse măsuri de diminuare a acestor impacturi |  |
| - |
| **Concluzie**e) Argumentați selectarea unei opțiunii, în baza atingerii obiectivelor, beneficiilor și costurilor, precum și a asigurării celui mai mic impact negativ asupra celor afectați  |  |
| Opțiunea propusă remediază problemele în domeniu, atât de ordin practic cât și juridic. Argumentele expuse la identificarea opțiunilor sunt valabile prin prisma atingerii obiectivelor, fiind clarificate inclusiv în nota informativă la proiectul de lege. |
| **5. Implementarea şi monitorizarea** |
| a) Descrieți cum va fi organizată implementarea opțiunii recomandate, ce cadru juridic necesită a fi modificat și/sau elaborat și aprobat, ce schimbări instituționale sînt necesare  |  |
|

|  |
| --- |
| * Se modifică doar Lege nr. 20/2009 privind prevenirea și combaterea criminalității informatice.
 |
| * De asemenea, ca urmare a intrării în vigoare a proiectului de lege se vor elabora instrucțiunile privind punerea în aplicare a prevederilor din articolul 4 alineatul (1) și articolul 7 alineatul (1) litera e 1) din Legea nr. 20/2009.

|  |
| --- |
| - Nu necesită schimbări instituționale.  |

 |

 |
| b) Indicați clar indicatorii de performanță în baza cărora se va efectua monitorizarea |  |
| - |
| c) Identificați peste cât timp vor fi resimțite impacturile estimate și este necesară evaluarea performanței actului normativ propus. Explicați cum va fi monitorizată şi evaluată opțiunea |  |
| După intrarea în vigoare a amendamentelor propuse. |
| **6. Consultarea** |
| a) Identificați principalele părți (grupuri) interesate în intervenția propusă |  |
| 1. Furnizorii de servicii de comunicații electronice
2. Autoritățile competente în prevenirea şi combaterea criminalității informatice (Ministerul Economiei, Serviciul de Informații și Securitate, Procuratura Generală, Serviciul Tehnologia Informației și Securitate Cibernetică, Agenția de Guvernare Electronică)
3. Utilizatorii de sisteme informatice
 |
| b) Explicați succint cum (prin ce metode) s-a asigurat consultarea adecvată a părților |  |
| Analiza a impactului de reglementare la proiectul de lege pentru modificarea Legii nr. 20/2009 privind prevenirea şi combaterea criminalității informaticeși proiectul de lege au fost plasate pe pagina web oficială a Ministerului Afacerilor Interne mai.gov.md, în rubrica: Transparența, secțiunea: Anunțuri privind consultările publice și pe platforma guvernamentală [www.particip.gov.md](http://www.particip.gov.md). |
| c) Expuneți succint poziția fiecărei entități consultate față de documentul de analiză a impactului și/sau intervenția propusă (se expune poziția a cel puțin unui exponent din fiecare grup de interese identificat) |  |
|  |
| **Anexă** **Tabel pentru identificarea impacturilor** |
| **Categorii de impact** | **Punctaj atribuit** |
|  | *Opțiunea* *propusă* | *Opțiunea alterativă 1* | *Opțiunea alterativă 2* |
| **Economic** |
| costurile desfășurării afacerilor | 1 |  |  |
| povara administrativă | 1 |  |  |
| fluxurile comerciale și investiționale | -1 |  |  |
| competitivitatea afacerilor | -1 |  |  |
| activitatea diferitor categorii de întreprinderi mici și mijlocii | 1 |  |  |
| concurența pe piață | 0 |  |  |
| activitatea de inovare și cercetare | -2 |  |  |
| veniturile și cheltuielile publice | -2 |  |  |
| cadrul instituțional al autorităților publice | 0 |  |  |
| alegerea, calitatea și prețurile pentru consumatori | 0 |  |  |
| bunăstarea gospodăriilor casnice și a cetățenilor | -2 |  |  |
| situația social-economică în anumite regiuni | -2 |  |  |
| situația macroeconomică | -2 |  |  |
| alte aspecte economice | -1 |  |  |
| **Social** |
| gradul de ocupare a forței de muncă | -2 |  |  |
| nivelul de salarizare | -1 |  |  |
| condițiile și organizarea muncii | 0 |  |  |
| sănătatea și securitatea muncii | -2 |  |  |
| formarea profesională | -1 |  |  |
| inegalitatea și distribuția veniturilor | -1 |  |  |
| nivelul veniturilor populației | 0 |  |  |
| nivelul sărăciei | -3 |  |  |
| accesul la bunuri și servicii de bază, în special pentru persoanele social-vulnerabile | 0 |  |  |
| diversitatea culturală și lingvistică | 0 |  |  |
| partidele politice și organizațiile civice | 0 |  |  |
| sănătatea publică, inclusiv mortalitatea și morbiditatea | 1 |  |  |
| modul sănătos de viață al populației | 0 |  |  |
| nivelul criminalității și securității publice | 3 |  |  |
| accesul și calitatea serviciilor de protecție socială | 1 |  |  |
| accesul și calitatea serviciilor educaționale | 1 |  |  |
| accesul și calitatea serviciilor medicale | 0 |  |  |
| accesul și calitatea serviciilor publice administrative | 1 |  |  |
| nivelul și calitatea educației populației | 1 |  |  |
| conservarea patrimoniului cultural | 0 |  |  |
| accesul populației la resurse culturale și participarea în manifestații culturale | 0 |  |  |
| accesul și participarea populației în activități sportive | 0 |  |  |
| discriminarea | 1 |  |  |
| alte aspecte sociale | 0 |  |  |
| **De mediu** |
| clima, inclusiv emisiile gazelor cu efect de seră și celor care afectează stratul de ozon | 0 |  |  |
| calitatea aerului | 0 |  |  |
| calitatea și cantitatea apei și resurselor acvatice, inclusiv a apei potabile și de alt gen | 0 |  |  |
| biodiversitatea | 0 |  |  |
| flora | 0 |  |  |
| fauna | 0 |  |  |
| peisajele naturale | 0 |  |  |
| starea și resursele solului | 0 |  |  |
| producerea și reciclarea deșeurilor | 0 |  |  |
| utilizarea eficientă a resurselor regenerabile și neregenerabile | 0 |  |  |
| consumul și producția durabilă | 0 |  |  |
| intensitatea energetică | 0 |  |  |
| eficiența și performanța energetică | 0 |  |  |
| bunăstarea animalelor | 0 |  |  |
| riscuri majore pentru mediu (incendii, explozii, accidente etc.) | 0 |  |  |
| utilizarea terenurilor | 0 |  |  |
| alte aspecte de mediu | 0 |  |  |
| *Tabelul se completează cu note de la -3 la +3, în drept cu fiecare categorie de impact, pentru fiecare opțiune analizată, unde variația între -3 și -1 reprezintă impacturi negative (costuri), iar variația între 1 și 3 – impacturi pozitive (beneficii) pentru categoriile de impact analizate. Nota 0 reprezintă lipsa impacturilor. Valoarea acordată corespunde cu intensitatea impactului (1 – minor, 2 – mediu, 3 – major) față de situația din opțiunea „a nu face nimic”, în comparație cu situația din alte opțiuni și alte categorii de impact. Impacturile identificate prin acest tabel se descriu pe larg, cu argumentarea punctajului acordat, inclusiv prin date cuantificate, în compartimentul 4 din Formular, lit. b1) și, după caz, b2), privind analiza impacturilor opțiunilor.* |