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 criminalității Date 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

Utilizarea paginilor web pentru distribuirea conținutului cu caracter infracțional reprezintă o problemă globală, inclusiv și pentru Republica Moldova, unde în permanență sunt utilizate tehnologiile informaționale în toate domeniile vieții inclusiv: achitări online, accesarea diferitor pagini pentru studii, activitatea zilnică etc și în general digitalizarea tuturor proceselor, sporește calitatea serviciilor, dar din lipsa supravegherii acestui sector o face tentantă pentru rețelele infracționale de diferite tipuri. Este înregistrată, o creștere semnificativă a exploatării tehnologiei informaționale în scopuri infracționale, de la 75 de infracțiuni anuale în 2006 la 142 în anul 2019. 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, fapt la care fiecare stat aprobă măsuri de combatere a acestui fenomen.

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**

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. e^{1}) 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. 320/2012 cu 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, Legea nr. 20/2009 prevede la art. 7 alin (1) lit. e^1) obligația furnizorilor de servicii de sistarea a accesului la paginile web cu conținut infracțional, însă nu prevede care autorități pot dispune o astfel de sistare. Aceasta 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. e^1) 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.

Conservarea

Legea 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.

Modificările propuse reprezintă expresia juridică a actului de reacţionare faţă de deficienţele identificate care împiedică buna implementare a prevederilor Convenției Europene privind criminalitatea informatică şi are drept scop ajustarea legislației naționale la standardele internaționale.

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 e^{1}) cu obligația furnizorilor de servicii de a sista accesul, însă nu a fost prevăzut care autoritate dispune sistarea. Ca urmare, la momentul de față sistarea este dispusă de subdiviziunea din cadrul MAI, care este specializată în combaterea criminalității informatice, fiind executată de către unii dintre furnizori de servicii de comunicații electronice și totodată o parte dintre furnizori refuză executarea din motivul că Legea nr. 20/2009 nu prevede expresă autoritatea abilitată respectivă.

4. Expunerea sistării exhaustive în 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

Sistarea

1. 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.

Astfel, pe parcursul anului 2020 doar de către subdiviziunea de poliție specializată în combaterea criminalității informatice au fost înregistrate 523 cazuri de infracțiuni informatice, iar în anul 2021-381 de cazuri.

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

1) Aspectul conservării datelor informatice:

Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice prevede la art. 4 alin. (4) lit. b) că Procuratura dispune, în cadrul desfăşurării urmăririi penale, la solicitarea organului de urmărire penală sau din oficiu, conservarea imediată a datelor informatice ori a datelor referitoare la traficul informatic, faţă de care există pericolul distrugerii ori alterării, în condiţiile legislaţiei de procedură penală.

Carența acestei norme intervine la necesitatea de aplicare a acesteia în practică și anume din necesitatea de dispunere a conservării datelor informatice imediat după parvenirea unei plîngeri sau sesizări privind criminalitatea informatică și nu la etapa urmăririi penale care intervine în unele cazuri peste jumătate de an după înregistrarea inițială a cazului. De menționat că Legea nr. 241/2007 „Comunicațiilor electronice" prevede la art. 20 alin. (3) lit. c) obligația furnizorilor de păstrare a datelor ce ţin de reţeaua Internet pe un termen de 6 luni, la expirarea cărora informațiile menționate vor fi distruse ireversibil, prin proceduri automatizate. O prevedere analogică este cuprinsă și în Legea 20/2009 la art. 7 alin. (1) lit. f) - perioadă de 180 de zile calendaristice. Astfel, în multe cazuri la etapa începe urmăririi penale datele informatice cu valoarea probatorie sunt deja nimicite, ceea ce în cele mai multe cazuri face imposibilă investigarea cazului și realizarea dreptului de apărare a victimei. La fel, reieșind din faptul că la prima etapă cazul este investigat de către MAI, este necesar ca autoritatea respectivă să dispună conservarea datelor informatice.
De menționat că Legea 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 (care prevede și atribuția de dispunere a conservării datelor informatice).

2) Aspectul sistării accesului la pagini web cu conținut ilegal:
Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice prevede la art. 7 alin. (1) lit. e[1]) că furnizorii de servicii sînt obligaţi 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.
Carența acestei norme constă în următoarele:

- Nu este prevăzut expres care autorități sunt abilitate cu dreptul de a dispune o astfel de măsură, ceea ce a generat apariția diferitor interpretări.
- Prin stipularea expresă privind sistarea accesului în baza adreselor IP, au fost omise și alte modalități de realizare a măsurii date, precum sistarea accesului în baza numelui de domeniu (DNS) sau în baza adresei web concrete (URL). În cazul sistării accesului în baza adreselor IP, pe aceeași adresă IP pot fi mai multe site-uri web simultan, inclusiv cu conținut legal.

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)

Prezentul proiect urmărește două obiective de bază:

1) Asigurarea bazei probatorii pe cazurile privind criminalitate informatică, prin ajustarea procedurii de conservare a datelor informatice stocate de furnizorii de servicii de comunicații electronice, în cazul în care acestea sunt relevante pe cazurile privind criminalitatea informatică examinate de MAI și Procuratura;

2) Stoparea activității infracționale informatice, care este realizată prin intermediu site-urilor web cu conținut ilegal și prevenirea apariției de victimei noi care accesează site-urile de Phising, linkuri către adrese URL de pe care la accesare sunt descărcate și instalate programe malițioase care criptează computerul și estorcă mijloace financiare.

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 informatice include 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 e[1])*", 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.

Prin analogie, prin Dispoziția nr. 1 din 01.04.2021 a Comisiei pentru Situații Excepționale a Republicii Moldova, Serviciul de Informații și Securitate a fost abilitat cu atribuția de identificare a paginilor web ce promovează știri false cu privire la evoluția COVID-19, în vederea sistării accesului la acestea.

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 e[1]) a textului „în condițiile legii,", „*toate adresele IP pe care sunt amplasate*" și a cuvintelor „în vigoare".

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 exhaustivă în 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.

b[1]) 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.

2. 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 exhaustive 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, 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.

b[2]) 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
-Conservarea datelor informatice nu implică suportarea unor costuri suplimentare, întrucât reprezintă doar extinderea termenului de păstrarea a acestor date. Sistarea accesului la pagini web nu implică suportarea unor costuri suplimentarea, deoarece acesta va fi realizată de către furnizori prin adăugarea unor noi pagini web la „lista neagră” a paginilor web precum cele prin care sunt răspândite programe malițioase (viruși). De menționat că furnizorii de servicii aplică astfel de filtre pentru asigurarea propriei securități informatice. În cazul în care o parte interesată va considera că sistarea accesului a fost dispusă abuziv, aceasta o va putea contesta conform prevederilor Codului Administrativ nr. 116/2018.
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
-Nu au fost identificate riscuri iminente care pot duce la eșecul intervenției și/sau schimba substanțial valoarea beneficiilor și costurilor estimate.

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

-Atât conservarea datelor informatice cît și sistarea accesului la pagini web nu implică suportarea unor costuri suplimentare, respectiv nu necesită suportarea unor costurile de conformare.

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.

Modificările propuse sub aspectul conservării datelor informatice vor contribui la asigurarea bazei probatorii pe cazurile privind criminalitatea informatică și asigurarea drepturilor victimelor acestor infracțiuni la apărare, urmare prevenirii situațiilor de dispariție a acestor probe odată cu scurgerea termenului legal de păstrare a datelor informatice.

Propunerile sub aspectul sistării accesului la paginile web cu conținut infracțional vor contribui la stoparea activității infracționale prin intermediul paginilor web și la prevenirea apariției unor noi victime, în special celor care accesează pagini web de tip Phishing sau care infectează computerul, îl criptează și estorcă mijloace financiare.

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.

  Instrucțiunile respective urmează să cuprindă aspecte pur tehnice în domeniul tehnologiilor informaționale, privind sistarea accesului la paginile web cu conținut infracțional, care nu pot fi incluse în Legea nr. 20/2009 reieșind din tehnica legislativă.

  Pentru analogie, menționăm procedura de intervenție pe cazurile copiilor victime ale violenţei, neglijării, exploatării şi traficului:

  - Codul penal prevede un șir de infracțiuni precum: Articolul 201[1] (Violenţa în familie), Art. 206 (Traficul de copii), Articolul 163 (Lăsarea în primejdie);
  - Codul de procedură penală prevede drepturile și modalitatea de audiere a copilului-victimă;
  - Legea nr. 45/2007 reglementează prevenirea şi combaterea violenței în familie;
  - Legea nr. 140/2013 reglementează protecția specială a copiilor aflați în situație de risc şi a copiilor separați de părinți;
  - HG nr. 270/2014 prevede Instrucţiunile privind mecanismul intersectorial de cooperare pentru identificarea, evaluarea, referirea, asistenţa şi monitorizarea copiilor victime şi potenţiale victime ale violenţei, neglijării, exploatării şi traficului;

- 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 și 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 și combaterea criminalității informatice și 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. (https://particip.gov.md/ro/document/stages/anunt-privind-initierea-consultarilor-publice-asupraanalizei-impactului-de-reglementare-la-proiectului-de-lege-pentru-modificarea-legii-nr-202009-privind-prevenirea-si-combaterea-criminalitatii-informatice/8289)
Cu termen de la **30.11.2022 - 14.12.2022.**

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)

Asociației Naționale a Companiilor din sectorul TIC (ATIC):

ATIC nu a menționat careva costuri suplimentare.

În contextul lansarii consultărilor publice a proiectului Analizei de impact la proiectul de lege pentru modificarea Legii nr. 20/2009 privind prevenirea și combaterea criminalității informatice, ATIC a examinat proiectul Legii, nota informativă şi analiza impactului de reglementare la acest proiect şi prezintă următoarele observații şi propuneri privind acest subiect.

1. Sistarea accesului la paginile web

ATIC susține, de principiu, stabilirea autorităților abilitate să dispună sistarea accesului la paginile web, precum şi înlocuirea obligației de sistare a accesului la adresele IP pe care sunt amplasate paginile web contestate cu obligația de sistare a accesului la paginile web propriu-zise. Totuși, aceste modificări nu sunt suficiente pentru a aduce această prevedere în conformitate cu normele internaționale și constituționale.

Remarcăm că o normă similară cu cea stabilită la art. 7 alin. (1) lit. e[1]) din Legea nr. 20/2009 a fost examinată anterior de Comisia de la Veneția, care a formulat mai multe observații și recomandări față de aceasta.

Potrivit Comisiei, în Recomandarea sa către statele membre privind măsurile de promovare a respectării libertății de exprimare și de informare în legătură cu filtrarea conținutului de pe Internet (CM/Rec(2008)6)4, Comitetul de Miniștri al Consiliului Europei a declarat, inter alia, că statele ar trebui să se abțină de la filtrarea conținutului de pe Internet din alte motive decât cele prevăzute la articolul 10, paragraful 2 Convenția Europeană a Drepturilor Omului (CEDO), astfel cum este interpretat de Curtea Europeană a Drepturilor Omului (CtEDO), și ar trebui să garanteze că măsurile generale de blocare sau filtrare la nivel național sunt introduse numai dacă condițiile de la articolul 10, paragraful 2 CEDO sunt îndeplinite.

Articolul 10 CEDO și art. 32, 34 și 54 din Constituția RM garantează că orice persoană are dreptul la libertate de exprimare. Acest drept include libertatea de opinie și libertatea de a primi sau a comunica informații ori idei fără amestecul autorităților publice și fără a ține seama de frontiere. Exercitarea acestor libertăți poate fi supusă unor restrângeri sau sancțiuni prevăzute de lege care, într-o societate democratică, constituie măsuri necesare pentru securitatea națională, integritatea teritorială sau siguranța publică, apărarea ordinii și prevenirea infracțiunilor, protecția sănătății, a moralei, a reputației sau a drepturilor altora, pentru a împiedica divulgarea informațiilor confidențiale sau pentru a garanta autoritatea și imparțialitatea puterii judecătorești.

Potrivit Comisiei, aceasta înseamnă că trebuie prevăzute motive și garanții deosebit de puternice pentru limitarea accesului publicului la Internet, măsură care, făcând cantități mari de informații inaccesibile, restrânge substanțial drepturile utilizatorilor de internet și este probabil să aibă efecte colaterale semnificative.

În opinia CtEDO, restricțiile, cum ar fi ordinele de blocare a internetului „nu sunt neapărat incompatibile cu Convenția, ca principiu. Cu toate acestea, este necesar un cadru legal, care să

asigure atât un control strict asupra întinderii interdicțiilor, cât și un control judiciar eficient pentru a preveni orice abuz de putere [...]. În această privință, controlul judiciar al unei astfel de măsuri, bazat pe o cântărire a intereselor concurente în joc și menit să stabilească un echilibru între ele, este de neconceput fără un cadru care să stabilească norme precise și specifice privind aplicarea restricțiilor preventive asupra libertății de exprimare […]" (Ahmet Yıldırım v. Turkey, Cerere Nr 3111/10, Hotărâre din 18.12.2012, § 67).

De asemenea, Recomandarea precizează că „așa acțiuni de către stat ar trebui luate numai dacă filtrarea se referă la conținut specific și clar identificabil, o autoritate națională competentă a luat o decizie privind ilegalitatea acestuia și decizia poate fi revizuită de un tribunal sau de un organism de reglementare independent și imparțial, în conformitate cu cerințele articolului 6 din Convenția Europeană a Drepturilor Omului".

Totodată, în Recomandarea sa CM/Rec(2016)5 privind libertarea Internetului, Comitetul Miniștrilor subliniază că „înainte de a se aplica măsuri restrictive privind accesul la Internet, o instanță sau autoritate administrativă independentă stabilește că deconectarea de la Internet este cea mai puțin restrictivă măsură pentru atingerea scopului legitim".

Pentru a asigura respectarea normelor internaționale citate, se impune, în primul rând, limitarea temeiurilor pentru sistarea accesului. Referința la pagini web "*ce contribuie la comiterea infracțiunilor sau la încălcarea prevederilor legislației în vigoare ori conține/difuzează instrucțiuni privind modul de comitere a acestora*" este prea largă.

Ținând cont de faptul că Legea nr. 20/2009 are ca obiect prevenirea și combaterea criminalității informatice şi de principiul proporționalității, "*încălcarea prevederilor legislației în vigoare*" care nu constituie infracțiune, nu trebuie să servească temei pentru sistarea accesului în baza Legii nr. 20/2009 sau Codului de procedură penală (în continuare – CPP).

De asemenea, Comisia de la Veneția recomandă excluderea prevederii potrivit căreia poate servi drept temei pentru sistarea accesului faptul că o pagină web "conține/difuzează instrucțiuni privind modul de comitere a [infracțiunilor]".

Totodată, norma respectivă trebuie să prevadă că sistarea accesului poate fi dispusă numai referitor la paginile web care sunt destinate şi utilizate în scopul comiterii infracțiunilor, și nu doar să contribuie la comiterea lor. Contribuirea la comiterea unei infracțiuni are un sens prea larg, care poate conduce la sistarea accesului la paginile web ale terților, destinate și utilizate pentru activități legale.

În al doilea rând, se impune detalierea condițiilor de aplicare a acestei măsuri. În acest scop, este necesară completarea Codului de procedură penală (în continuare – CPP). Observăm că art. 2 alin. (4) CPP stabilește că normele juridice cu caracter procesual din alte legi naționale pot fi aplicate numai cu condiția includerii lor în cod. În avizul său, Comisia de la Veneția, de asemenea, recomandă de a include cel puțin o parte din prevederile necesare în CPP. Prin urmare, la art. 7 alin. (1) lit. e1) din Legea nr. 20/2009 trebuie păstrată sintagma „în condițiile legii".

Printre detaliile care trebuie să fie reglementate în CPP pot fi evidențiate următoarele:

1. Stabilirea infracțiunilor sau categoriilor de infracțiuni pentru comiterea cărora se permite sistarea accesului la pagina web.
2. Stabilirea procedurii de autorizare a măsurii de sistare a accesului (poate fi similară cu cea stabilită pentru autorizarea măsurilor procesuale de constrângere), inclusiv:

a. organului abilitat de a autoriza asemenea măsură, la propunerea cui şi prin care act procesual, de exemplu, ordonanța procurorului, emisă din oficiu sau la propunerea organului de urmărire penală, sau încheierea instanței de judecată, emisă la demersul procurorului).

b. etapei procesului penal la care este posibilă dispunerea unei asemenea măsuri, de exemplu, doar după pornirea urmăririi penale.

c. elementelor pe care trebuie să le conțină actul procesual prin care se autorizează măsură respectivă, de exemplu, conținutul online ilicit sau activitatea ilicită desfășurată prin intermediul paginii web, încadrarea juridică a acestei activități, motivarea necesității aplicării acestei măsuri, precum și adresa URL a paginii web accesul la care trebuie sistat.

d. La soluționarea chestiunii privind necesitatea aplicării măsurii respective, procurorul și instanța de judecată trebuie să evalueze și să stabilească dacă măsura este proporțională cu

circumstanțele individuale ale cauzei penale, inclusiv dacă sistarea accesului la pagina web este cea mai puțin restrictivă măsură pentru atingerea scopului legitim, de exemplu, dacă este posibilă eliminarea a conținutului online ilicit la sursă de către furnizorul acestuia sau de către furnizorul serviciilor de găzduire a conținutului online.

e. Copia de pe ordonanța procurorului sau prin încheierea instanței de judecată trebuie adusă la cunoștința furnizorului de conținut online ilicit (dacă este posibilă identificarea acestuia), în termenul care să fie stabilit prin lege.

3. Stabilirea actului prin care se dispune măsura respectivă şi conţinutul acestuia.
4. Stabilirea procedurii de atac a actelor privind autorizarea şi dispunerea unei asemenea măsuri (poate fi similară cu cea stabilită pentru autorizarea măsurilor procesuale de constrângere)16. Recomandarea CM/Rec(2008)6 clarifică faptul că prevederea privind „mijloacele eficiente și ușor accesibile de recurs și remediere, inclusiv suspendarea filtrelor" este crucială pentru a răspunde „cazurilor în care utilizatorii și/sau autorii de conținut susțin că conținutul a fost blocat nerezonabil".
5. Stabilirea procedurii de revocare şi încetare a actelor privind autorizarea şi dispunerea unei asemenea măsuri (poate fi similară cu cea stabilită pentru autorizarea măsurilor procesuale preventive), inclusiv temeiurile revocării şi încetării, organul abilitat să să dispună acest lucru, la propunerea cui şi prin care act procesual. De exemplu, măsura se revocă de către organul care a dispus-o dacă temeiurile care au servit la aplicarea acesteia au dispărut şi măsura nu mai este justificată, cu înştiinţarea furnizorului de conţinut online respectiv.

Condițiile sistării accesului la paginile web în afara procesului penal urmează a fi reglementate prin legile speciale (de exemplu, art. 46 din Legea nr. 120/2017 cu privire la prevenirea şi combaterea terorismului, art. 48 din Legea nr. 291/2016 cu privire la organizarea şi desfăşurarea jocurilor de noroc, Legea nr. 30/2013 cu privire la protecţia copiilor împotriva impactului negativ al informaţiei, art. 114 din Legea nr. 230/2022 privind dreptul de autor şi drepturile conexe).

2. Conservarea datelor informatice şi a datelor privind traficul informatic

Așa cum am remarcat mai sus, art. 2 alin. (4) CPP stabilește că normele juridice cu caracter procesual din alte legi naționale pot fi aplicate numai cu condiția includerii lor în cod. Prin urmare, norma prevăzută la art. 4 alin. (2) şi art. 7 alin. (1) lit. c) din Legea nr. 20/2009 trebuie dublată și detaliată în CPP.

Procedura și garanțiile procesuale pentru efectuarea acestei măsuri sunt stabilite la art. 16, 17 şi 29 din Convenția privind criminalitatea informatică. În conformitate cu aceste norme, se propune următoarea redacție a articolului dedicat din CPP:

Articolul [XXX]. Conservarea rapidă a datelor informatice

(1) Prin conservarea rapidă a datelor informatice se înțelege păstrarea şi protejarea integrității datelor informatice, inclusiv a datelor referitoare la trafic, stocate prin intermediul unui sistem informatic, efectuată în scopul de a permite autorităților competente să obțină dezvăluirea acestora.

(2) Conservarea rapidă a datelor informatice se dispune atunci când există motive de a crede că acestea sunt în mod special susceptibile de pierdere sau de modificare.

(3) Conservarea se dispune de procuror, prin ordonanță motivată, din oficiu sau la cererea organului de urmărire penală, pentru atât timp cât este necesar, dar nu mai mult de [120] de zile.

(4) În ordonanța de conservare trebuie să fie indicate:

a) autoritatea care solicită conservarea;

b) persoana asupra căreia se pune obligația de conservare;

c) infracțiunea care face obiectul urmăririi penale şi prezentarea succintă a faptelor care au legătură cu aceasta;

d) datele informatice specifice ce urmează a fi conservate, inclusiv numele şi prenumele persoanei sau persoanelor ale căror date trebuie să fie conservate (dacă acestea sunt disponibile), genul de date care trebuie conservate, perioada de referinţă pentru care trebuie conservate datele;
e) motivele dispunerii conservării: natura legăturii acestor date cu infracţiunea, motivarea îndeplinirii condiţiilor prevăzute în alin. (2).
f) obligaţia persoanei asupra căreia se pune obligaţia de conservare de a păstra datele informatice şi de a le menţine integritatea, cu păstrarea confidenţialităţii cu privire la aplicarea acestei măsuri; şi g) perioada de păstrare a datelor informatice ce urmează a fi conservate.
(5) Măsura conservării poate fi prelungită de către procuror o singură dată pentru motive temeinic justificate, pe o durată maximă de 90 de zile.
(6) Extrasul din ordonanţa procurorului, care trebuie să cuprindă informațiile specificate la literele a), b), d), f) şi g) din alin. (4), se transmite persoanei în posesia sau sub controlul căreia se află datele stocate, aceasta fiind obligată să asigure conservarea lor rapidă, cu păstrarea confidențialității cu privire la aplicarea acestei măsuri.
(7) În cazul în care în transmiterea comunicaţiei au fost implicaţi mai mulţi furnizori de servicii, procurorul, prin ordonanţa de conservare sau o altă ordonanţă, poate dispune dezvăluirea rapidă de către persoana în posesia sau sub controlul căruia se află datele referitoare la trafic a unei cantităţi de date referitoare la trafic, suficiente pentru a permite identificarea furnizorilor de servicii şi a canalelor prin intermediul căruia comunicaţia a fost transmisă.
(8) Procurorul este obligat să dispună încetarea conservării, înaintea expirării perioadei pentru care a fost dispusă, de îndată ce au dispărut temeiurile şi motivele care au justificat-o.
(9) Procurorul dispune ridicarea datelor conservate de la persoana care le-a conservat în termenul prevăzut în alin. (3) sau (5), după caz. Ridicarea datelor conservate se efectuează în conformitate cu prevederile art. 125-132.
(10) Până la terminarea urmăririi penale, procurorul este obligat să anunțe, în scris, utilizatorii ale căror date au fost conservate."

Propuneri sau obiecții pe marginea documentului de analiză a impactului nu au fost indicate.

Poziția MAI cu referire la aviz:

1. Cu referire la procedura de sistare a accesului la paginile web.

În cadrul elaborării proiectului de modificare, a fost studiată practica altor state, în special a celor din spațiul UE.

Astfel, un exemplu clasic de dispunere a sistării de către organele de poliției a fost stabilit în legislația **Republicii Franceze** - Decretul președintelui nr. 2015-125 din 2015 (*Décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique*, link: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000030195477/), care stabilește în Art. 1 că autoritatea administrativă menționată la articolul 6-1 din Legea nr. 2004-575 pentru încredere în economia digitală (autoritatea care poate solicita persoanelor a căror activitate este de a oferi acces la serviciile de comunicații publice online retragerea conținutului) este Direcția Generală a Poliției Naționale, Biroul Central pentru lupta împotriva criminalității legate de tehnologiile informației și comunicațiilor.

La fel, avizul comun al Comisiei de la Veneția și al Direcției Generale Drepturile Omului și statul de drept (DGI) a Consiliului Europei pe marginea proiectului de lege nr.161), menționat în avizul ATIC prevede că „înainte de aplicarea măsurilor restrictive asupra accesului la Internet, o instanță sau o autoritate administrativă competentă determină dacă deconectarea de la Internet este cea mai puțin restrictivă măsură pentru atingerea scopului legitim". În acest sens, menționăm că aspectele tehnice privind procedura respectivă urmează a fi desfășurate în cadrul unei hotărâri de Guvern.

Astfel, art. II. din proiectul de lege prevede următoarele:
(1) Prezenta lege intră în vigoare în termen de 3 luni de la data publicării în Monitorul Oficial al Republicii Moldova.
(2) Guvernul, până la intrarea în vigoare a prezentei legi, va elabora instrucțiunile privind punerea în aplicare a prevederilor din articolul 7 alineatul (1) litera e^1) din Legea nr. 20/2009.

Cu referire la procedura de contestare a deciziei de sistare a accesului la o pagină web, sunt aplicabile prevederile generale privind procedura de Contencios administrativ. În cele ce urmează, menționăm prevederile relevante din Codul administrativ nr. 116/2018:
„Articolul 5. Activitatea administrativă.
Activitatea administrativă reprezintă totalitatea actelor administrative individuale și normative, a contractelor administrative, a actelor reale, precum și a operațiunilor administrative realizate de autoritățile publice în regim de putere publică, prin care se organizează aplicarea legii și se aplică nemijlocit legea.
Articolul 20. Acțiunea în contencios administrativ
Dacă printr-o activitate administrativă se încalcă un drept legitim sau o libertate stabilită prin lege, acest drept poate fi revendicat printr-o acțiune în contencios administrativ, cu privire la care decid instanțele de judecată competente pentru examinarea procedurii de contencios administrativ, conform prezentului cod."

De asemenea, la elaborarea proiectului a fost studiată practica Curții Europene a Drepturilor Omului la compartimentul libertății internetului:
Cazul Akdeniz împotriva Turciei, din 11.03.2014, privind blocarea accesului la două site-uri pe motiv că acestea au difuzat cu încălcarea drepturilor de autor. Reclamantul, care este un utilizator al site-urilor în cauză, s-a plâns, în special, pe o încălcare a libertății sale de exprimare.
CtEDO a declarat inadmisibilitatea cererii și a constatat: cele două site-uri de streaming au fost blocate deoarece au funcționat cu încălcarea legislației privind dreptul de autor. Curtea a observat în continuare că reclamantul a avut la dispoziție multe mijloace de a accesa o serie de lucrări muzicale, fără încălcarea normelor care reglementează drepturile de autor.

Menționăm că revederi similare celor din proiectul de lege deja există în legislația națională, după cum urmează.
1) Legea nr. 291 din 16.12.2016 cu privire la organizarea și desfășurarea jocurilor de noroc.
Conform art. 5 și 50^1 din Lege, Agenția Servicii Publice identifică paginile web prin intermediul cărora sunt accesate jocurile de noroc care nu sunt autorizate în modul stabilit, aprobă lista de pagini web/platforme/aplicații prin intermediul cărora pot fi accesate jocurile de noroc care nu sunt autorizate în condițiile prezentei legi, iar furnizorii de servicii de comunicații electronice accesibile publicului, la decizia Agenției Naționale pentru Reglementare în Comunicații Electronice și Tehnologia Informației, bazată pe lista de surse făcută publică de către Agenția Servicii Publice, au obligația de a bloca imediat accesul utilizatorilor din Republica Moldova la sursele respective.
2) Legea Nr. 284/2004 privind comerţul electronic.
Art. 17 din Lege (Stocarea permanentă a informaţiei) prevede următoarele:
(1) În cazul în care un serviciu al societății informaţionale constă în stocarea informaţiilor furnizate de un destinatar al serviciului *[...]*
(2) Din momentul în care furnizorului de servicii îi devine cunoscut faptul că activitatea sau informaţia stocată este ilicită, acesta este obligat să acţioneze prompt pentru a elimina informaţia sau pentru a bloca accesul la aceasta.
(3) Se consideră că furnizorul de servicii are cunoştinţă despre faptul că activitatea sau informaţia stocată este ilicită ori despre fapte sau circumstanţe din care să rezulte că activitatea sau informaţia în cauză este vădit ilicită în cazul în care acesta: a) primeşte o dispoziţie scrisă din partea unei instanţe de judecată sau a unei autorităţi publice abilitate, emisă în conformitate cu prevederile legale, prin care se constată caracterul ilicit al activităţii sau al informaţiei specifice

stocate pe serverele furnizorului de servicii sau pe cele care se află sub controlul acestuia şi se solicită eliminarea paginii web respective sau blocarea accesului la aceasta; *[...]*

Totodată, urmează a fi respinsă propunerea de includere a măsurii în Codul de procedură penală sub formă de măsură procesuală de constrînger, din următoarele considerente:
Articolul 300 din CPP (Sfera controlului judiciar) prevede:
„(1) Judecătorul de instrucţie examinează demersurile procurorului privind autorizarea efectuării acţiunilor de urmărire penală, măsurilor speciale de investigaţii şi de aplicare a măsurilor procesuale de constrîngere care limitează drepturile şi libertăţile constituţionale **ale persoanei**."
Astfel, limitarea accesului la conținutul din internet nu poate fi atribuită la măsurile procesuale de constrîngere, întrucît măsurile procesuale de constrîngere sunt aplicate în privința unei persoane concrete, dar nu în privința publicului care ar fi limitat să acceseze resursele respective din spațiul online.

2. Cu referire la procedura de conservare a datelor informatice.

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 pentru ulterioara obținere în condițiile legii.
Totodată, legea nr. 6/2009 pentru ratificarea Convenției 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).
Ca urmare, limitarea procedurii de conservare doar la atribuțiile procuraturii, nu și a Ministerul Afacerilor Interne contravine prevederilor Convenției și Legii de ratificare a acesteia.

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. b[1]) și, după caz, b[2]), privind analiza impacturilor opțiunilor.