GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. ____

din 2025

Chișinău

pentru aprobarea Instrucțiunii privind procedura de sistare a accesului la pagini web care conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor și de eliminare a conținutului respectiv la sursă

În temeiul art. II alin. (2) din Legea nr. 200/2024 privind modificarea Legii nr. 20/2009 privind prevenirea și combaterea criminalității informatice (Monitorul Oficial al Republicii Moldova, 2010, nr.11-12, art.17) cu modificările ulterioare, Guvernul HOTĂRĂŞTE:

1. Se aprobă Instrucțiunea privind procedura de sistare a accesului la pagini web care conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor și de eliminare a conținutului respectiv la sursă, conform anexei.

2. Instrucțiunea privind procedura de sistare a accesului la pagini web care conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor și de eliminare a conținutului respectiv la sursă se aplică doar în scopul executării Legii nr. 20/2009 privind prevenirea și combaterea criminalității informatice și nu afectează actele normative care reglementează alte proceduri de sistare a accesului la materiale ilegale.

3. Ministerul Afacerilor Interne și Serviciul de Informații și Securitate vor întreprinde măsurile ce se impun pentru implementarea Instrucțiunii privind procedura de sistare a accesului la pagini web care conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor și de eliminare a conținutului respectiv la sursă.

4. Serviciul Tehnologia Informației și Securitate Cibernetică va asigura accesul neîntrerupt al subdiviziunii specializate în prevenirea și combaterea criminalității informatice din cadrul Ministerului Afacerilor Interne și Serviciului de Informații și Securitate la toate paginile web din rețeaua internet.

5. Prezenta hotărâre intră în vigoare la data publicării în Monitorul Oficial al Republicii Moldova.

Prim-ministru **Dorin RECEAN**

Contrasemnează:

Ministrul afacerilor interne Daniella MISAIL-NICHITIN

Ministrul justiției Veronica MIHAILOV-MORARU

Aprobat
prin Hotărârea Guvernului nr.____/2025

INSTRUCȚIUNEA
privind procedura de sistare a accesului la pagini web care conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor și de eliminare a conținutului respectiv la sursă

Capitolul I.
DISPOZIȚII GENERALE

1. Prezenta Instrucțiunea stabilește procedura de identificare a paginilor web care conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor și de interacțiune dintre Ministerul Afacerilor Interne și/sau Serviciul de Informații și Securitate, pe de o parte, și furnizorii de servicii de acces la Internet, furnizorii de servicii de găzduire a conținutului online și/sau furnizorii de conținut, pe de altă parte, în ceea ce privește sistarea accesului la paginile web respective sau eliminarea conținutului respectiv la sursă.

2. În sensul prezentei Instrucțiuni, se definesc următoarele noțiuni:

2.1. *adresă IP (Internet Protocol Address)* – adresă numerică care permite identificarea unei resurse din Internet și schimbul de date cu resursa respectivă.

2.2. *adresa URL (Uniform Resource Locator)* – adresă unitară cu format textual care identifică o resursă (pagină web) din Internet;

2.3. *furnizor de servicii de acces la Internet* – furnizor de servicii de comunicații electronice care furnizează servicii de acces la Internet;

2.4. *furnizorii de servicii de găzduire a conținutului* - companii sau organizații care oferă spațiu pe serverele lor pentru stocarea și gestionarea site-urilor web, aplicațiilor sau altor resurse online.

2.5. *furnizorii de conținut* - entități sau organizații care creează, distribuie sau oferă acces la conținut digital, precum texte, imagini, video, audio, aplicații, sau orice alt tip de material informațional disponibil online.

2.6. *furnizorii de servicii/conținut* - furnizorii de servicii de acces la Internet, furnizorii de servicii de găzduire a conținutului online și furnizorii de conținut.

2.4. *sistem de nume de domen (DNS - Domain Name System)* – sistemul distribuit de nume utilizat pentru identificarea calculatoarelor din Internet sau din alte rețele pe bază de Internet Protocol (IP);

3. O pagină web poate fi considerată ca fiind destinată și utilizată pentru pregătirea sau comiterea infracțiunilor în cazul în care informația publicată sau oferită în orice mod pe aceasta, inclusiv sub formă de linkuri, corespunde unuia sau mai multor dintre criteriile stabilite la art. 4^2 din Legea nr. 20/2009 cu privire la prevenirea și combaterea criminalității informatice.

4. Paginile web ce conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor se identifică de către subdiviziunea specializată în prevenirea și combaterea criminalității informatice din cadrul Ministerului Afacerilor Interne sau din cadrul Serviciului de Informații și Securitate (în continuare – *subdiviziunea specializată*) din oficiu sau în baza sesizării făcute de către orice persoană fizică persoană juridică de drept public sau privat.

5. O comunicare privind existența unei pagini web care conține informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor, adresată subdiviziunii specializate de către o persoană fizică sau juridică, urmează să întrunească cerințele unei petiții.

6. Furnizorii de serviciu de găzduire sau conținut pot să ia, dacă este cazul, măsuri pro active proporționale și specifice de sistare a accesului la pagini web sau de eliminare a conținutului online la sursă în cazul informațiilor destinate și utilizate pentru pregătirea sau comiterea infracțiunilor în conformitate cu legislația.

Capitolul II.
PROCEDURA SISTĂRII ACCESULUI LA PAGINILE WEB CE CONȚIN INFORMAȚII DESTINATE ȘI UTILIZATE PENTRU COMITEREA INFRACȚIUNILOR ȘI DE ELIMINARE A CONȚINUTULUI RESPECTIV LA SURSĂ

7. După identificarea uneia sau mai multor pagini web ce conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor, subdiviziunea specializată întreprinde următoarele acțiuni:

7.1. întocmește un Act privind examinarea paginii/paginilor web, conform modelului din anexa nr. 1 la prezenta Instrucțiune;

7.2. în decurs de 24 de ore:

7.2.1. emite Ordinul de eliminare a conținutului online la sursă (în continuare – *Ordinul de eliminare a conținutului la sursă*), dacă conținutul poate fi eliminat la sursă de către furnizorii de servicii de găzduire a conținutului online sau de către furnizorii de conținut de pe teritoriul Republicii Moldova; și/sau

7.2.2. emite Ordinul de sistare a accesului la paginile web ce conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor (în continuare – *Ordinul de sistare a accesului*), dacă eliminarea conținutului la sursă nu este posibilă;

8. Ordinul de eliminare a conținutului la sursă sau Ordinul de sistare a accesului este comunicat furnizorilor de servicii și/sau conținut, după caz, în format electronic prin intermediul unui canal securizat. Adresa URL la care urmează a fi sistat accesul va fi comunicată în format textual.

9. Emiterea Ordinului de sistare a accesului sau de eliminare a conținutului online la sursă are loc cu respectarea următoarelor principii:

9.1. legalității;

9.2. proporționalității;

9.3. aplicării măsurii tehnice de sistare cel mai puțin restrictive;

9.4. informării privind motivele sistării accesului și căile de atac;

9.5. revizuirii periodice a necesității sistării în continuare a accesului la o anumită pagină web;

9.6. respectării dreptului furnizorilor de servicii de a aplica, din proprie inițiativă, alte măsuri pentru prevenirea utilizării abuzive a serviciilor sale;

9.7. respectării prevederilor Legii nr. 284/2004 privind serviciile societății informaționale.

10. Ordinul de sistare a accesului la pagini web sau de eliminare a conținutului online la sursă se publică pe pagina web a autorității competente emitente.

11. Ordinul de sistare a accesului sau de eliminare a conținutului la sursă poate fi contestat direct în instanța de judecată în raza teritorială a căreia este amplasat sediul autorității ce a emis ordinul, în ordinea contenciosului administrativ, de către orice persoană care revendică încălcarea unui drept al său urmare emiterii Ordinului sau de către furnizorul de servicii/conținut. Depunerea contestației nu suspendă acțiunea Ordinului de sistare a accesului sau de eliminare a conținutului la sursă.

12. Actele ce țin de punerea în aplicare a prevederilor prezentei Instrucțiuni se păstrează în conformitate cu dispozițiile actelor normative.

13. Refuzul subdiviziunii specializate de a emite Ordinul de sistare a accesului sau de eliminare a conținutului la sursă, în urma primirii unei sesizări, poate fi contestat direct în instanța de judecată în ordinea contenciosului administrativ.

14. Furnizorii de servicii/conținut sunt obligați să execute Ordinul de sistare a accesului sau de eliminare a conținutului la sursă, emis de subdiviziunea specializată imediat, dar nu mai târziu de următoarea zi lucrătoare de la recepționarea acestuia.

15. Furnizorii de servicii de acces la Internet realizează sistarea accesului din propriul sistem informatic la pagini web, folosind metodele și mijloacele tehnice din posesie.

16. Ministerul Afacerilor Interne și Serviciul de Informații și Securitate creează o pagină web dedicată autorității respective, care este comunicată furnizorilor de servicii de acces la Internet și cuprinde următoarele informații:

16.1. anunțul despre faptul că pagina web sau conținutul pe care utilizatorul încearcă să le acceseze conține informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor și accesul la aceasta este sistat;

16.2. mențiunea privind căile de contestare a Ordinului de sistare a accesului;

16.3. adresa de email la care utilizatorul se poate adresa către subdiviziunea specializată printr-o petiție, pentru a-i fi comunicat numărul și data emiterii Ordinului de sistare a accesului respectiv, precum și motivele sistării, în vederea posibilității de contestare a acestuia.

17. După executarea Ordinului de sistare a accesului, furnizorii de servicii de acces la Internet redirecționează tentativele de acces la paginile web în cauză către adresa IP a paginii web dedicate a autorității care a emis Ordinul de sistare a accesului.

18. Autoritatea emitentă, prin intermediul conducătorului subdiviziunii specializate, este obligată să dispună încetarea sistării accesului la paginile web și să notifice în scris furnizorii de servicii de acces la Internet despre acest fapt, în următoarele cazuri:

18.1. a expirat perioada pentru care a fost dispusă sistarea accesului;

18.2. înainte de expirarea perioadei pentru care a fost dispusă sistarea accesului, au dispărut temeiurile și motivele care au justificat sistarea accesului;

18.3. dacă Ordinul de sistare a fost suspendat sau anulat parțial sau integral print-un act judecătoresc.

19. După ce a fost emis Ordinul de sistare a accesului și/sau Ordinul de eliminare a conținutului la sursă, persoana interesată poate adresa o petiție către subdiviziunea specializată, prin care se comunică despre înlăturarea din conținutul unei pagini web a informațiilor destinate și utilizate pentru comiterea infracțiunilor. Subdiviziunea specializată va examina petiția în cauză în termenul stabilit de actele normative.

20. În cazul constatării faptului înlăturării informațiilor destinate și utilizate pentru comiterea infracțiunilor în condițiile pct. 17, subdiviziunea specializată întocmește un Act privind examinarea paginii/paginilor web și anulează în întregime sau parțial Ordinul de sistare a accesului și/sau Ordinul de eliminare a conținutului la sursă corespunzător, fapt despre care comunică furnizorilor de servicii de acces la Internet pentru acordarea accesului utilizatorilor la pagina/paginile web în cauză.

21. Prin derogare de la prevederile pct. 7 și 17, eliminarea conținutului online la sursă sau sistarea accesului la pagini web concepute în întregime pentru distribuirea materialelor privind abuzul sexual asupra minorului *(pornografia infantilă)* și care sunt incluse în lista elaborată de Organizația Internațională a Poliției Criminale *(The INTERPOL „Worst of" List)* se realizează în baza Ordinului de sistare a accesului sau de eliminare a conținutului online la sursă, fără întocmirea unui Act privind examinarea paginilor web în cauză și fără adresarea prealabilă către furnizorul de găzduire sau de conținut, pe o perioadă nelimitată de timp.

22. Furnizorii de servicii/conținut pot sista accesul la web site-uri concepute în întregime pentru distribuirea materialelor privind abuzul sexual asupra minorului (pornografiei infantile) și care sunt incluse în lista elaborată de Organizația Internațională a Poliției Criminale (*The INTERPOL „Worst of" List*) din oficiu, nefiind necesară inițierea procedurii reglementate de prezenta instrucțiune.

23. Subdiviziunea specializată din cadrul Ministerului Afacerilor Interne asigură comunicarea listei paginilor web *The INTERPOL "Worst of" List*, elaborată de Organizația Internațională a Poliției Criminale, către furnizorii de servicii de acces la Internet și furnizorii de servicii de găzduire a conținutului online de pe teritoriul Republicii Moldova.

Anexa nr. 1
la Instrucțiunea privind procedura de sistare a accesului la paginile web care conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor și de eliminare a conținutului online la sursă

Act
privind examinarea paginii/paginilor web

_____
(funcția, gradul, numele angajatului)

_____

în conformitate cu prevederile pct. 7 din Instrucțiune privind procedura de sistare a accesului la pagini web ce conțin informații destinate și utilizate pentru comiterea infracțiunilor și de eliminare a conținutului online la sursă, aprobat prin Hotărârea Guvernului Republicii Moldova nr. ____ din _____, am întocmit prezentul Act privind examinarea paginii/paginilor web.

Obiectul examinării reprezintă pagina/paginile web:

1. _____
fiind stabilit că aceasta conține/nu conține informații destinate și utilizate pentru
(se evidențiază)
comiterea infracțiunilor:
_____
(în caz afirmativ, informațiile se descriu succint)
_____

2. _____
fiind stabilit că aceasta conține/nu conține informații destinate și utilizate pentru
(se evidențiază)
comiterea infracțiunilor:
_____
(în caz afirmativ, informațiile se descriu succint)
_____

3. Datele de contact ale administratorului website-ului și/sau ale furnizorului de servicii de găzduire a website-ului sunt/nu sunt disponibile.
(se evidențiază)
_____
(în caz afirmativ, datele de contact se indică succint)

_____ _____
(data) (funcția, gradul, numele angajatului, semnătura)
_____
_____
_____

NOTA DE FUNDAMENTARE
la proiectul Hotărârii de Guvern pentru aprobarea Instrucțiunii privind procedura de sistare a accesului la pagini web care conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor și de eliminare a conținutului respectiv la sursă

1. Denumirea sau numele autorului și, după caz, a/al participanților la elaborarea proiectului actului normativ
Autor: Ministerul Afacerilor Interne. *Alte autorități publice participante:* Inspectoratul General al Poliției. *Sectorul privat:* Asociația națională a companiilor din sectorul tehnologii informaționale și comunicare; Moldcell S.A; Orange Moldova S.A; Moldtelecom S.A; StarNet S.R.L.
2. Condițiile ce au impus elaborarea proiectului actului normativ
2.1. Temeiul legal sau, după caz, sursa proiectului actului normativ
Temeiul legal din care rezultă prezentul proiect de lege reprezintă: 1. acțiunea nr. 172 din Planul național de reglementări pentru anul 2025, aprobat prin Hotărârea Guvernului nr. 841/2024; 2. Art. II alin. (2) din Legea nr. 200/2024 pentru modificarea Legii nr. 20/2009 privind prevenirea și combaterea criminalității informatice.
2.2. Descrierea situației actuale și a problemelor care impun intervenția, inclusiv a cadrului normativ aplicabil și a deficiențelor/lacunelor normative
Progresele considerabile în domeniul tehnologiilor informației și comunicațiilor au favorizat interconectarea unei societăți globale, ceea ce, din păcate, a dus la apariția unor noi infracțiuni de diferit calibru: criminalitatea informatică/cibernetică. Criminalitatea informatică/cibernetică reprezintă activitatea de utilizare a sistemelor, rețelelor de calculatoare și în special a internetului pentru a comite infracțiuni. Termenul a fost creat la sfârșitul anilor 1990, când internetul a început să se răspândească în America de Nord. Atunci a fost momentul cînd criminalitatea informatică/cibernetică a devenit o preocupare globală. Astfel, *„criminalitatea informatică/cibernetică”* a fost folosită pentru a desemna infracțiunile comise pe internet, în special cele legate de piraterie, pornografie și atacuri asupra sistemelor informatice. Prin urmare, criminalitatea informatică/cibernetică se referă la un set de infracțiuni comise prin rețele de calculatoare și, în special, prin internet. Aceste infracțiuni includ pirateria, pornografia, fraudele prin telemarketing și altele. Conform Comisiei Europene, termenul include trei categorii de activități criminale: - infracțiuni tradiționale, cum ar fi frauda informatică și falsificarea; - difuzarea de conținut ilegal prin mijloace electronice, cum ar fi pornografia sau incitarea la ură rasială, etc.; - atacuri asupra rețelelor electronice, cum ar fi atacurile asupra sistemelor informatice, atacurile de tip „*deny of service*”, „hacking-ul”, etc. În contextul acestor amenințări, statele membre al Consiliului Europei, fiind conștiente de profundele schimbări determinate de digitalizarea, convergenta si globalizarea continuă a rețelelor de calculatoare; preocupate de riscul că rețelele de calculatoare si informația electronică ar putea fi utilizate si pentru comiterea de infracțiuni si că probele privind asemenea infracțiuni ar putea fi stocate și transmise prin intermediul acestor rețele; recunoscând necesitatea cooperării între state și industria privată în lupta împotriva criminalității informatice, precum și nevoia de a proteja interesele legitime în utilizarea si dezvoltarea tehnologiilor informației; considerând că lupta eficientă purtată împotriva criminalității informatice impune o cooperare internațională intensificată, rapidă si eficace în materie penală; au adoptat, la 23.11.2001, la Budapesta, Convenția privind criminalitatea informatică – act normativ care reglementează măsuri de prevenire și combatere a criminalității informatice/cibernetice. Totodată, la 28.01.2003, Consiliul Europei a adoptat Protocol adițional la Convenția Consiliului Europei privind criminalitatea informatică, referitor la incriminarea actelor de natură rasistă și xenofobă

săvârșite prin intermediul sistemelor informatice. În final, la 28.02.2023, Consiliul Europei a adoptat al doilea protocol adițional la Convenția privind criminalitatea informatică referitor la cooperarea consolidată și la divulgarea probelor electronice.

În paralel, cu unele mici întârzieri, Republica Moldova a înregistrat progrese semnificative în domeniul combaterii criminalității informatice/cibernetice, care pot fi listate după cum urmează:

1. La 02.02.2009, Parlamentul Republicii Moldova a adoptat Legea nr. 6/2009 pentru ratificarea Convenției Consiliului Europei privind criminalitatea informatică;

2. La 03.02.2009, Parlamentul Republicii Moldova a adoptat Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice;

3. La 03.02.2009, Parlamentul Republicii Moldova a adoptat Legea nr. 302/2016 pentru ratificarea Protocolului adițional la Convenția Consiliului Europei privind criminalitatea informatică, referitor la incriminarea actelor de natură rasistă și xenofobă comise prin intermediul sistemelor informatice;

4. La 09.11.2022, a fost semnat Decretul Președintelui Republicii Moldova, Maia Sandu, pentru aprobarea semnării celui de-al doilea Protocol adițional la Convenția Consiliului Europei privind criminalitatea informatică referitor la cooperarea consolidată și divulgarea probelor electronice.

Aceste progrese normative au apropiat Republica Moldova tot mai mult de standardele Uniunii Europene de prevenire și combatere a criminalității informatice/cibernetice. Le fel, se menționează că, în anul 2024, au fost operate unele modificări în Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice, care au dus la dezvoltarea instrumentelor de conservare a datelor informatice și de sistare a accesului la paginile web care conțin informații destinate și utilizate pentru comiterea infracțiunilor.

Potrivit noilor prevederi legale, subdiviziunea specializată din cadrul Ministerului Afacerilor Interne și Serviciul de Informații și Securitate dispun sistarea accesului la paginile web care sunt destinate și utilizate pentru pregătirea sau comiterea infracțiunilor în cazul în care informația publicată sau oferită în orice mod pe aceasta, inclusiv sub formă de linkuri, se referă la fapte infracționale. Pe de altă parte, furnizorii de servicii sunt obligați să sisteze, la solicitarea autorităților competente, folosind metodele și mijloacele tehnice din posesie, accesul din propriul sistem informatic la paginile web ce cuprind informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor.

Totuși, prevederile legale referite mai sus nu oferă o reglementare completă a procedurii de sistare, fapt ce naște necesitatea elaborării prezentului proiect de hotărâre de Guvern, care vine să aprobe Instrucțiunile privind procedura de sistare a accesului la paginile web care conțin informații destinate și utilizate pentru comiterea infracțiunilor și de eliminare a conținutului respectiv la sursă. Altfel spus, prezentul proiect de lege are ca scop crearea unui mecanism de interacțiune dintre organele de drept și furnizorii de servicii în vederea implementării prevederilor legale introduse în Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice.

În același timp, prezentul proiect vine spre realizarea sarcinii trasate Guvernului, la Art. II alin. (2) din Legea nr. 200/2024 pentru modificarea Legii nr. 20/2009 privind prevenirea și combaterea criminalității informatice, unde este indicat că Guvernul, în termen de 3 luni de la data intrării în vigoare a prezentei legi, va aproba instrucțiunile privind modul de emitere și executare a ordinelor emise în temeiul art. 4 alin. (1) lit. b) din Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice, adică a ordinelor de sistare a accesului la paginile web.

Prin urmare, prezentul proiect are ca scop definitivarea, perfecționarea mecanismului de sistare a accesului la paginile web destinate și utilizate pentru pregătirea sau comiterea infracțiunilor instituit prin Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice.

3. Obiectivele urmărite și soluțiile propuse

3.1. Principalele prevederi ale proiectului și evidențierea elementelor noi

Scopul și obiectivele Instrucțiunii:

Scopul Instrucțiunii constă în stabilirea procedurii de identificare a paginilor web care conțin informații destinate și utilizate pentru comiterea infracțiunilor și de interacțiune dintre Ministerul Afacerilor Interne și/sau Serviciul de Informații și Securitate, pe de o parte, și furnizorii de servicii de acces la Internet, furnizorii de servicii de găzduire a conținutului online și/sau furnizorii de conținut, pe de altă parte, în ceea ce privește sistarea accesului la paginile web respective sau eliminarea conținutului respectiv la sursă.

Obiectivele Instrucțiunii sunt:

1. Prevenirea și combaterea criminalității informatice: reglementează identificarea și eliminarea paginilor web care conțin informații destinate și utilizate pentru comiterea infracțiunilor, contribuind astfel la protejarea securității cibernetice;

2. Colaborarea eficientă între autorități și furnizorii de servicii de internet: stabilește proceduri clare pentru interacțiunea dintre Ministerul Afacerilor Interne, Serviciul de Informații și Securitate și furnizorii de servicii de acces la internet și găzduire de conținut online, pentru a asigura implementarea măsurilor de prevenire a criminalității informatice;

3. Protecția utilizatorilor de internet: prin sistarea accesului la site-uri infracționale și eliminarea conținutului ilegal, Instrucțiunea protejează utilizatorii de informații periculoase, cum ar fi cele legate de abuzuri sau activități ilegale;

4. Asigurarea unui cadru legal și proporțional de aplicare a măsurilor: reglementează aplicarea măsurilor într-un mod legal, proporțional și transparent, respectând drepturile fundamentale ale utilizatorilor și furnizorilor de servicii de internet;

5. Crearea unui mecanism de revizuire și contestare: oferă posibilitatea contestării măsurilor luate în instanță și stabilește proceduri de revizuire periodică a paginilor web care au fost sistate, asigurând astfel corectitudinea și echitatea în aplicarea Instrucțiunii.

Principalele prevederi ale proiectului și elementele noi care se conțin în cuprinsul acestuia:

1. Punctul 1 al Instrucțiunii reglementează procesul prin care autoritățile competente (Ministerul Afacerilor Interne și Serviciul de Informații și Securitate) pot identifica și lua măsuri împotriva paginilor web care conțin informații destinate și utilizate pentru comiterea infracțiunilor. De asemenea, stabilește cum vor interacționa autoritățile cu furnizorii de servicii de internet și găzduire de conținut pentru a opri accesul la aceste pagini sau pentru a elimina conținutul ilegal de pe ele. Scopul este protejarea securității cibernetice și prevenirea utilizării internetului pentru activități infracționale.

2. Punctul 2 definește noțiunile cheie utilizate în Instrucțiune pentru a asigura o înțelegere corectă a termenilor.

3. Punctul 3 din Instrucțiune explică când o pagină web va fi considerată ca având scop infracțional, menționându-se că acest lucru se poate întâmpla dacă pagina web oferă informații care încurajează sau facilitează comiterea de infracțiuni, conform legislației naționale (Legea nr. 20/2009). Aceasta include, de exemplu, site-uri care promovează activități ilegale, cum ar fi fraudele sau distribuirea de materiale ilegale.

4. Punctul 4 din Instrucțiune prevede că paginile web destinate sau utilizate pentru comiterea infracțiunilor pot fi identificate fie din oficiu, adică autoritățile descoperă site-urile pe cont propriu, fie pe baza unei sesizări din partea oricărei persoane fizice sau juridice.

5. Punctul 5 din Instrucțiune stabilește faptul că în situațiile când o persoană sau instituție sesizează autoritățile că o pagină web conține informații infracționale, această sesizare trebuie să fie formală, sub forma unei petiții, care va include detalii suficiente pentru ca autoritățile să poată evalua situația.

6. Punctul 6 din Instrucțiune specifică faptul că furnizorii de servicii de găzduire a conținutului sau de internet pot lua măsuri pentru a opri accesul la paginile web ilegale sau pentru a elimina conținutul ilegal, fără a aștepta întotdeauna un ordin oficial din partea

autorităților, dacă consideră că este necesar pentru a preveni infracțiunile, exclusiv în cazurile în care legislația le permite realizarea unei astfel de acțiuni.

7. Punctul 7 și 8 din Instrucțiune reglementează faptul că autoritățile, după ce identifică o pagină web ilegală, întocmesc un act oficial care descrie evaluarea acelei pagini. În termen de 24 de ore, autoritățile pot decide dacă vor emite un ordin pentru eliminarea conținutului ilegal de pe site sau pentru sistarea accesului la site. Dacă conținutul poate fi eliminat de pe serverele din Republica Moldova, autoritățile vor emite un Ordin de eliminare a conținutului la sursă. Dacă nu este posibilă eliminarea, vor emite un Ordin de sistare a accesului, care va bloca accesul utilizatorilor la respectiva pagină web.

8. Punctul 9 din Instrucțiune enumeră principiile de care se ghidează actorii implicați la aplicarea măsurilor, astfel încât activitatea respectivă să fie corectă și proporțională. Autoritățile trebuie să aplice cele mai puțin restrictive tehnici pentru a preveni accesul, fără a afecta inutil alte aspecte ale internetului. De asemenea, trebuie să informeze furnizorii de servicii despre motivele măsurii și despre cum pot contesta ordinul emis.

9. Punctul 10 din Instrucțiune precizează faptul că Ordinul de sistare a accesului sau de eliminare a conținutului trebuie să fie publicat pe site-ul autorităților competente, pentru a asigura transparența și pentru ca persoanele afectate să fie informate.

10. Punctul 11 din Instrucțiune ne spune că Ordinul poate fi contestat în instanță de către orice persoană care consideră că i-au fost încălcate drepturile, inclusiv de către furnizorii de servicii sau conținut. Contestarea nu va suspenda efectele ordinului, adică măsurile vor rămâne în vigoare până la o decizie judecătorească.

11. Punctul 12 din Instrucțiune precizează că toate documentele legate de aplicarea Instrucțiunii trebuie păstrate conform legii pentru a fi utilizate în cazul unui control sau a unei verificări ulterioare.

12. Punctul 13 din Instrucțiune menționează că în situațiile în care autoritățile specializate refuză să emită un ordin de sistare a accesului sau de eliminare a conținutului, persoanele interesate pot contesta acest refuz în instanță.

13. Punctele 14 și 15 din Instrucțiune stabilesc că furnizorii de servicii de internet sunt obligați să aplice ordinul de sistare a accesului imediat, dar nu mai târziu de ziua lucrătoare următoare primirii acestuia. Ei pot utiliza diverse metode tehnice pentru a bloca accesul la site-urile respective.

14. Punctul 15 din Instrucțiune comunică faptul că, după aplicarea măsurii de sistare a accesului, furnizorii de internet vor redirecționa utilizatorii care încearcă să acceseze pagini web blocate către o pagină web dedicată, administrată de autoritățile competente, care va informa utilizatorii despre motivul blocării.

15. Punctul 16 din Instrucțiune precizează faptul că autoritățile competente vor crea o pagină web care va conține informații despre paginile blocate, motivele pentru care accesul a fost sistat și modalitățile de contestare a ordinului.

16. Punctul 17 din Instrucțiune explică faptul că furnizorii de servicii de acces la Internet redirecționează tentativele de acces la paginile web sistate către adresa IP a paginii web dedicate a autorității care a emis Ordinul de sistare a accesului.

17. Punctul 18 din Instrucțiune este despre restabilirea accesului. Dacă autoritățile decid să ridice măsura de sistare a accesului, furnizorii de internet trebuie să restabilească accesul la paginile web respective. Acest lucru poate apărea după ce au fost înlăturate informațiile infracționale sau dacă măsurile nu mai sunt justificate.

18. Punctul 19 din Instrucțiune reglementează procedura deblocării paginii web care a fost supusă procedurii de sistare la cererea persoanei interesate.

19. Punctul 20 din Instrucțiune reglementează acțiunile autorității competente în condițiile recepționării unei cereri primite în baza punctului 18.

20. Punctul 21 din Instrucțiune reglementează o procedură simplificate pentru paginile care distribuie materiale de abuz sexual asupra minorilor (pornografie infantilă). În aceste cazuri, Ordinul de sistare se emite fără întocmirea unui Act privind examinarea paginilor web

în cauză și fără adresarea prealabilă către furnizorul de găzduire sau de conținut, pe o perioadă nelimitată de timp.

21. Punctul 22 din Instrucțiune oferă posibilitatea furnizorilor de servicii să elimine materialele ilegale din oficiu. Astfel, furnizorii de servicii de internet pot lua măsuri pro-activ pentru a elimina paginile care distribuie materiale de abuz sexual asupra minorilor și care sunt incluse în lista elaborată de Organizația Internațională a Poliției Criminale (The INTERPOL "Worst of" List), fără a fi necesar să urmeze procedura prevăzută în Instrucțiune.

22. Punctul 23 din Instrucțiune prevede că autoritățile vor comunica furnizorilor de servicii de internet și de găzduire a conținutului lista cu paginile web care promovează pornografia infantilă, astfel încât aceștia să poată lua măsuri imediate pentru a le bloca.

3.2. Opțiunile alternative analizate și motivele pentru care acestea nu au fost luate în considerare

Menționăm că, în urma analizelor efectuate, nu au fost identificate opțiuni alternative.

4. Analiza impactului de reglementare

4.1. Impactul asupra sectorului public

Proiectul nu presupune impact structural și instituțional asupra sistemului administrației publice. Ceea ce se schimbă este faptul că autoritățile competente din subordinea Ministerului Afacerilor Interne și/sau Serviciul de Informații și Securitate vor avea competența să dispună sistarea accesului la paginile web ce conțin date și informații utilizate sau destinate pentru comiterea infracțiunilor.

4.2. Impactul financiar și argumentarea costurilor estimative

Proiectul nu presupune costuri financiare suplimentare.

4.3. Impactul asupra sectorului privat

În partea ce se referă la sectorul privat, se menționează că furnizorii de servicii de acces la Internet, furnizorii de servicii de găzduire a conținutului online și furnizorii de conținut vor începe să execute obligațiile ce le-au revenit conform modificărilor operate în Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice. Aceste obligații pot fi sumarizate după cum urmează:

1. Creșterea responsabilității în monitorizarea și filtrarea conținutului: furnizorii de servicii de internet și de găzduire a conținutului vor avea o responsabilitate mult mai mare în ceea ce privește monitorizarea și gestionarea conținutului găzduit pe platformele lor. Aceștia vor fi obligați să acționeze rapid pentru a elimina sau bloca accesul la paginile care conțin informații ilegale, cum ar fi site-uri care promovează infracțiuni, fraude, sau pornografia infantilă. În unele cazuri, furnizorii pot fi obligați să intervină imediat, fără a aștepta un ordin formal, dacă detectează conținut care poate avea un impact dăunător;

2. Costuri suplimentare și investiții în tehnologie: există o probabilitate că furnizorii vor trebui să investească în soluții care să permită blocarea rapidă a site-urilor vizate, respectând termenii legali stabiliți;

3. Creșterea costurilor operaționale: implementarea acestor măsuri posibil, pentru unele categorii de furnizori, va implica costuri administrative și operaționale suplimentare. Furnizorii vor trebui să angajeze personal dedicat pentru a răspunde sesizărilor și pentru a urmări implementarea măsurilor de blocare a site-urilor sau de eliminare a conținutului ilegal. Acest lucru poate crește costurile operaționale, mai ales pentru furnizorii mai mici care nu dispun de resurse mari.

4. Necesitatea conformării rapide cu ordinele autorităților: furnizorii de internet vor fi obligați să acționeze rapid pentru a implementa măsurile de blocare a site-urilor sau de eliminare a conținutului ilegal. Aceste măsuri trebuie implementate în termen de 24 de ore de la primirea unui ordin.

4.4. Impactul social

Implementarea acestei Instrucțiuni va aduce un impact pozitiv semnificativ asupra cetățenilor, asigurând un mediu online mai sigur și mai protejat. Prin blocarea și eliminarea rapidă a conținutului ilegal și periculos, cetățenii vor fi expuși mai puțin la informații dăunătoare, cum ar fi fraudele online, pornografia infantilă sau incitarea la violență. De

asemenea, Instrucțiunea asigură transparență și protecția drepturilor utilizatorilor, oferindu-le posibilitatea de a contesta măsurile luate și de a fi informați în mod clar despre motivele blocării sau eliminării unui site. În acest fel, cetățenii vor avea acces la o experiență online mai sigură și mai responsabilă, protejându-le integritatea și securitatea personală.

4.4.1. Impactul asupra datelor cu caracter personal

Implementarea acestei instrucțiuni va avea un impact pozitiv asupra protecției datelor cu caracter personal, întrucât măsurile de blocare a accesului la site-uri sau eliminare a conținutului ilegal vor contribui la reducerea riscurilor de expunere a datelor personale pe platformele online periculoase. Prin prevenirea accesului la pagini web care promovează activități infracționale, cum ar fi fraudele sau furtul de identitate, cetățenii vor fi mai bine protejați împotriva riscurilor de abuzuri și atacuri cibernetice. În plus, reglementările asigură transparență în procesul de luare a măsurilor, ceea ce contribuie la încrederea cetățenilor că datele lor personale sunt gestionate în mod responsabil și securizat.

4.4.2. Impactul asupra echității și egalității de gen

Implementarea acestei instrucțiuni poate avea un impact pozitiv asupra echității și egalității de gen, prin crearea unui mediu online mai sigur și mai protejat pentru toate persoanele, indiferent de sex sau gen. Prin eliminarea conținutului ilegal și dăunător, inclusiv materialele care pot incita la discriminare, violență de gen sau hărțuire online, Instrucțiunea va contribui la protejarea drepturilor femeilor, bărbaților și persoanelor non-binare. De asemenea, măsurile de prevenire a accesului la pagini web care promovează comportamente abuzive sau infracționale vor ajuta la asigurarea unui spațiu virtual mai echitabil, în care toate persoanele se pot simți în siguranță, fără teama de a fi expuse unor tratamente inechitabile sau abuzuri pe baza genului.

4.5. Impactul asupra mediului

Deși Instrucțiunea se concentrează pe securitatea cibernetică și protecția cetățenilor online, aplicarea sa poate aduce și un impact pozitiv indirect asupra mediului. Prin eliminarea paginilor web care conțin conținut dăunător, precum infracțiuni informatice sau fraude, se reduce utilizarea de resurse tehnologice, cum ar fi lățimea de bandă și capacitatea serverelor, care sunt necesare pentru a găzdui și distribui acest conținut. Astfel, se poate reduce consumul de energie asociat cu aceste activități online. Mai mult, prin încurajarea furnizorilor de servicii să implementeze măsuri proactive și tehnologii eficiente de control și eliminare a conținutului dăunător, se poate contribui la un sistem digital mai sustenabil, care minimizează impactul asupra resurselor energetice.

4.6. Alte impacturi și informații relevante

Nu este aplicabil.

5. Compatibilitatea proiectului actului normativ cu legislația UE

5.1. Măsuri normative necesare pentru transpunerea actelor juridice ale UE în legislația națională

Nu este aplicabil.

5.2. Măsuri normative care urmăresc crearea cadrului juridic intern necesar pentru implementarea legislației UE

Nu este aplicabil.

6. Avizarea și consultarea publică a proiectului actului normativ

Lista autorităților și instituțiilor a căror avizare este necesară:

1. Ministerul Finanțelor;
2. Ministerul Muncii și Protecției Sociale;
3. Ministerul Dezvoltării Economice și Digitalizării;
4. Ministerul Educației și Cercetării;
5. Ministerul Culturii;
6. Serviciul de Informații și Securitate
7. Procuratura Generală;
8. Consiliul Superior al Magistraturii

Proiectul a fost elaborat cu sprijinul Asociației naționale a companiilor din sectorul tehnologii informaționale și comunicare. Totodată, împreună cu Asociația națională a companiilor din sectorul tehnologii informaționale și comunicare, a companiilor Moldcell S.A; Orange Moldova S.A; Moldtelecom S.A; StarNet S.R.L s-a organizat o ședință comună de lucru în care a fost abordat fiecare punct al proiectului, decizându-se versiunea finală al acestora.

De asemenea, proiectul a fost prezentat la Masa rotundă „*Parteneriat pentru siguranța copiilor online: reglementări și soluții pentru eliminarea conținutului ilegal*" organizat de La Strada, la 24 ianuarie 2025.

Anunțul privind inițierea elaborării proiectului a fost plasat pe site-ul web Particip.gov.md la adresa: https://particip.gov.md/ro/document/stages/proiectul-hotararii-de-guvern-pentru-aprobarea-regulamentului-privind-procedura-de-sistare-a-accesului-la-paginile-web-care-contin-informatii-destinate-si-utilizate-pentru-comiterea-infractiunilor/13515

Anunțul despre inițierea procedurii de avizare a proiectului, număr unic /MAI/2025, autor Ministerul Afacerilor Interne a fost plasat pe site-ul web Particip.gov.md la adresa:

7. Concluziile expertizelor

Ministerul Justiției
Se va completa ulterior.

Centrul Național Anticorupție
Se va completa ulterior.

8. Modul de încorporare a actului în cadrul normativ existent

Nu este aplicabil

9. Măsurile necesare pentru implementarea prevederilor proiectului actului normativ

Pentru implementarea prezentului proiect de lege Ministerul Afacerilor Interne și Inspectoratul General al Poliției vor desfășura acțiuni pentru:
1. Elaborarea cadrului normativ intern pentru punerea în aplicare a legii și reglementarea cooperării Poliției și altor autorități responsabile de menținerea, asigurarea și restabilirea ordinii și securității publice.

Secretar de stat **Alexandru BEJAN**

Ministerul Afacerilor Interne
al Republicii Moldova

Nr. 38/660 din 27 februarie 2025

Cancelaria de Stat

CERERE
privind înregistrarea de către Cancelaria de Stat a proiectelor de acte ale Guvernului

Nr. crt.	Criterii de înregistrare	Nota autorului
1.	Categoria și denumirea proiectului	Proiectul Hotărârii Guvernului pentru aprobarea Regulamentului privind procedura de sistare a accesului la pagini web care conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor și de eliminare a conținutului respectiv la sursă.
2.	Autoritatea care a elaborat proiectul	Ministerul Afacerilor Interne
3	Justificarea depunerii cererii	Crearea cadrului normativ subsecvent necesar pentru aplicabilitatea modificărilor operate în Legea nr. 20/2009 privind prevenirea și combatrerea criminalității informatice, operate prin Legea nr. 200/2024 pentru modificarea unor acte normative.
4.	Referința la documentul de planificare care prevede elaborarea proiectului (PNA, PND, PNR, alte documente de planificare sectoriale)	Acțiunea nr. 172 din Planul național de reglementări pentru anul 2025, aprobat prin Hotărârea Guvernului nr. 841/2024;
5.	Lista autorităților și instituțiilor a căror avizare este necesară	1. Ministerul Finanțelor; 2. Ministerul Muncii și Protecției Sociale; 3. Ministerul Dezvoltării Economice și Digitalizării; 4. Ministerul Educației și Cercetării; 5. Ministerul Culturii;

		6. Serviciul de Informații și Securitate 7. Asociația națională a companiilor din sectorul tehnologii informaționale și comunicare; 8. Cancelaria de Stat;
6.	Termenul-limită pentru depunerea avizelor/expertizelor	10 zile
7.	Persoana responsabilă de promovarea proiectului	Petru Jalbă, ofițer principal al Direcției politici în domeniul ordinii și securității publice, combaterii criminalității, a Ministerului Afacerilor Interne. Tel: 069929950/ 022 255-625 e-mail: petru.jalba@mai.gov.md
8.	Anexe	1. Proiectul acului normativ; 2. Nota de fundamentare;
9.	Data și ora depunerii cererii	
10.	Semnătura	**Secretar general al ministerului** **Vladislav COJUHARI**