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 pentru modificarea Legii nr. 20/2009 privind prevenirea și combaterea criminalității informatice (Monitorul Oficial al Republicii Moldova, 2024, nr. 355-357, art. 535), 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. 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

Aprobat
prin Hotărârea Guvernului nr. /2025

INSTRUCȚIUNE
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. 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 (în continuare – Instrucțiune) stabilește procedurile pentru identificarea paginilor web care conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor, pentru punerea în aplicare a ordinului de sistare a accesului la o pagină web sau de eliminare a conținutului online la sursă, precum și pentru colaborarea între Ministerul Afacerilor Interne și/sau Serviciul de Informații și Securitate și furnizorii de servicii de acces la internet, furnizorii de servicii de găzduire a conținutului online și/sau furnizorii de conținut, în vederea implementării măsurilor de sistare a accesului sau de eliminare a conținutului 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. *adresă 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. *furnizor de servicii de găzduire a conținutului* – companie sau organizație care oferă spațiu pe serverele lor pentru stocarea și gestionarea site-urilor web, aplicațiilor sau altor resurse online;

2.5. *furnizor de conținut* – entitate sau organizație care distribuie sau furnizează conținut digital, precum texte, imagini, video, audio, aplicații sau orice alt tip de material informațional disponibil online;

2.6. *furnizor de servicii/conținut* – furnizor de servicii de acces la Internet, furnizor de servicii de găzduire a conținutului online și furnizor de conținut;

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

3. O pagină web se consideră 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 unui sau mai multor dintre criteriile stabilite la art. 4^2 alin. (1) lit. a)-g) din Legea nr. 20/2009 cu privire la prevenirea și combaterea criminalității informatice.

4. Paginile web care 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 – *subdiviziune specializată*) din oficiu sau în baza sesizării făcute de către orice persoană fizică sau orice 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.

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

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

6.1. întocmește un act privind examinarea paginii/paginilor web, conform modelului din anexă;

6.2. în decurs de 24 de ore:

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

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

6.2.3. dispune refuzul emiterii ordinului de eliminare a conținutului la sursă sau ordinului de sistare a accesului.

7. Ordinul de eliminare a conținutului la sursă sau ordinul de sistare a accesului este comunicat furnizorilor de servicii/conținut în format fizic, după caz,

în format electronic, prin intermediul poștei electronice guvernamentale a subdiviziunii specializate. Adresa URL la care urmează a fi sistat accesul va fi comunicată în format textual.

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

8.1. principiul legalității;

8.2. principiul proporționalității;

8.3. principiul aplicării măsurii tehnice de sistare celei mai puțin restrictive;

8.4. principiul informării privind motivele sistării accesului și căile de atac;

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

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

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

9. Ordinul de sistare a accesului la pagini web sau de eliminare a conținutului online la sursă va conține următoarele elemente:

9.1. informațiile care identifică autoritatea emitentă;

9.2. temeiul juridic al ordinului;

9.3. indicarea motivelor care justifică de ce informațiile sau conținutul online sunt considerate ca informații destinate sau utilizate pentru pregătirea ori comiterea unor infracțiuni, indicând temeiurile legale și argumentele specifice care stau la baza acestei evaluări;

9.4. informații care să permită furnizorilor de servicii/conținut să identifice și să localizeze conținutul în cauză, inclusiv unul sau mai multe adrese URL şi, dacă este necesar, informații suplimentare;

9.5. informații privind modul și termenul de contestare;

9.6. perioada sistării accesului la pagina web în cazurile emiterii ordinului de sistare a accesului.

10. Ordinul de sistare a accesului la pagini web sau de eliminare a conținutului online la sursă se publică pe site-ul web oficial al autorității competente emitente în termen de 10 zile de la emitere.

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 care a emis ordinul, conform prevederilor Legii nr. 20/2009 privind prevenirea și combaterea criminalității informatice, de către orice persoană care revendică încălcarea unui drept al său ca urmare a emiterii ordinului menționat 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. Furnizorii de servicii/conținut vor informa imediat autoritatea emitentă a ordinului, dar nu mai târziu de următoarea zi lucrătoare, cu privire la modul în care s-a dat curs acestuia, indicând data la care s-a realizat punerea în aplicare a 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 care 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 printr-o petiție către subdiviziunea specializată, pentru a-i fi comunicat numărul și data emiterii ordinului respectiv de sistare a accesului, 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 ordin al conducătorului subdiviziunii specializate, este obligată să dispună încetarea sistării accesului la paginile web și

să notifice în scris furnizorilor 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.

În scopul prevăzut la subpct. 18.2, subdiviziunea specializată va revizui lunar lista paginilor web identificate sau comunicate în privința cărora a fost emis ordinul de sistare a accesului.

19. După emiterea ordinului de sistare a accesului și/sau a ordinul de eliminare a conținutului la sursă, persoana interesată poate adresa o petiție către subdiviziunea specializată, prin care 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 de înlăturare a informațiilor destinate și utilizate pentru comiterea infracțiunilor în condițiile pct. 19, 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 emis anterior, 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. 6 și 17, eliminarea conținutului online la sursă sau sistarea accesului la pagini web concepute în întregime pentru distribuirea materialelor privind abuzul sexual asupra copilului *(*pornografia infantilă*)* și care sunt incluse în lista elaborată de către Organizația Internațională a Poliției Criminale *(The INTERPOL „Worst of" List)* se realizează în baza ordinului de sistare a accesului sau a ordinului 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.

22. Subdiviziunea specializată din cadrul Ministerului Afacerilor Interne asigură comunicarea listei paginilor web *The INTERPOL "Worst of" List*, elaborată de către 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.

23. Furnizorii de servicii/conținut pot sista accesul la paginile web concepute în întregime pentru distribuirea materialelor privind abuzul sexual

asupra copilului (pornografiei infantile) și care sunt incluse în lista elaborată de către Organizația Internațională a Poliției Criminale (*The INTERPOL „Worst of" List*) din oficiu, nefiind necesară inițierea procedurii reglementate de prezenta Instrucțiune.

24. În cazul identificării pe pagina web a informațiilor destinate și utilizate pentru comiterea infracțiunilor asupra copilului și a deținerii datelor cu privire la un copil identificat, se acționează în conformitate cu Hotărârea Guvernului nr. 270/2014 cu privire la aprobarea Instrucțiunilor privind mecanismul intersectorial de cooperare pentru identificarea, evaluarea, referirea, asistența și monitorizarea copiilor victime și potențiale victime ale violenței, neglijării, exploatării și traficului.

Anexă
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 respectiv la sursă

ACT
privind examinarea paginii/paginilor web

_____
(funcția, gradul, numele și prenumele angajatului)

_____,
în conformitate cu prevederile pct. 6 din Instrucțiunea privind procedura de sistare a accesului la pagini web ce conțin informații destinate și utilizate pentru comiterea infracțiunilor și de eliminare a conținutului respectiv 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 paginii web și/sau ale furnizorului de servicii de găzduire a paginii web sunt/nu sunt disponibile.
(se evidențiază)
_____
(în caz afirmativ, datele de contact se indică succint)

_____ _____
(data) (funcția, gradul, numele și prenumele 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 sistarea 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:

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.

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

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.

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.

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.

Punctul 6 reglementează procesul de intervenție al subdiviziunii specializate în cazul identificării unor pagini web care conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor, stabilind procedurile concrete pe care autoritățile trebuie să le urmeze pentru a combate difuzarea acestor informații online. În primul rând, subdiviziunea specializată trebuie să examineze paginile web identificate ca fiind posibile surse de informații ce sprijină

comiterea infracțiunilor, iar în urma acestei examinări autoritatea întocmește un act de evaluare detaliată care va reflecta conținutul considerat ilegal, motivând astfel necesitatea intervenției. În termen de 24 de ore, autoritățile sunt obligate să ia măsuri concrete pentru a elimina riscurile asociate acestor informații periculoase, iar dacă conținutul ilegal este găzduit de furnizori din Republica Moldova, se poate emite un ordin de eliminare a conținutului la sursă, cerând furnizorului să elimine respectivul conținut de pe platformele sale, pentru a preveni răspândirea acestuia. În caz contrar, dacă nu este posibilă eliminarea conținutului, se va emite un ordin de sistare a accesului, prin care se va solicita restricționarea accesului la pagina web respectivă, împiedicând utilizatorii din Republica Moldova să acceseze acea pagină. Scopul general al acestei proceduri este protejarea utilizatorilor de internet din Republica Moldova de conținuturi periculoase ce ar putea sprijini infracțiuni, prevenind astfel răspândirea unor informații ce pot fi folosite în scopuri ilegale, iar procedura impune un termen scurt de acțiune de 24 de ore pentru a asigura o intervenție rapidă și eficientă în fața riscurilor reprezentate de aceste site-uri.

Punctul 7 reglementează modalitatea de comunicare a ordinelor emise de autoritățile competente către furnizorii de servicii de găzduire sau furnizorii de conținut. În cazul emiterii unui Ordin de eliminare a conținutului la sursă sau a unui Ordin de sistare a accesului, acestea vor fi comunicate furnizorilor în două forme: în format fizic, dacă este necesar, și în format electronic prin intermediul poștei electronice guvernamentale a subdiviziunii specializate, asigurându-se astfel că ordinul ajunge rapid și în mod oficial la destinatar. De asemenea, ordinul va conține informațiile necesare, inclusiv adresa URL a paginii web unde urmează a fi restricționat accesul, care va fi comunicată în format textual, pentru a fi ușor identificată de către furnizorii de servicii sau conținut, astfel încât aceștia să poată lua măsurile necesare.

Punctul 8 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.

Punctul 9 reglementează conținutul și structura unui Ordin de sistare a accesului la pagini web sau de eliminare a conținutului online la sursă, stabilind elementele esențiale care trebuie să fie incluse în document pentru a asigura transparența și legalitatea măsurii. Ordinul trebuie să conțină informații clare care identifică autoritatea emitentă, pentru a asigura transparența și responsabilitatea acțiunii, precum și temeiul juridic al măsurii, pentru a justifica măsurile impuse și a se asigura că procedura respectă cadrul normativ existent. De asemenea, ordinul trebuie să motiveze de ce informațiile sau conținutul online sunt considerate destinate sau utilizate pentru pregătirea ori comiterea infracțiunilor, prin prezentarea argumentelor specifice care susțin evaluarea autorităților și a temeiurilor legale invocate, astfel încât furnizorii să înțeleagă clar rațiunea luării acestor măsuri. În plus, ordinul va include informații suficiente pentru ca furnizorul de servicii să poată localiza și identifica conținutul care trebuie eliminat sau la care trebuie să se restricționeze accesul, incluzând cel puțin adrese URL specifice și, dacă este necesar, informații suplimentare. În final, Ordinul va informa furnizorul despre posibilitatea de a contesta măsura și despre termenul în care poate face acest lucru, garantând astfel dreptul de apărare al părților implicate.

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, în termen de 10 zile.

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.

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.

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.

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.

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

Punctul 17 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.

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.

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

Punctul 20 din Instrucțiune reglementează acțiunile autorității competente în condițiile recepționării unei cereri primite în baza punctului 19. Actul procesual prin care se va dispune anularea parțială sau integrală a Ordinul de sistare a accesului și/sau Ordinul de eliminare a conținutului la sursă va fi Ordinul.

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.

Punctul 22 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.

Punctul 23 din Instrucțiune oferă posibilitatea furnizorilor de servicii să sisteze materialele ilegale din oficiu. Astfel, furnizorii de servicii de internet pot lua măsuri pro-activ pentru a sista 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.

Punctul 24 reglementează mecanismul intersectorial de cooperare pentru identificarea, evaluarea, referirea, asistența și monitorizarea copiilor victime și potențiale victime ale violenței, neglijării, exploatării și traficului.

Intrarea în vigoare:

Potrivit dispozițiilor tranzitorii ale Legii nr. 200/2024 pentru modificarea Legii nr. 20/2009 privind prevenirea și combaterea criminalității informatice:

Art. II. – (1) Prezenta lege intră în vigoare la expirarea a 3 luni de la data publicării în Monitorul Oficial al Republicii Moldova.

(2) 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.

Astfel, Legea nr. 200/2024 a fost publicată în Monitorul Oficial la 15.08.2024 și a intrat în vigoare la 14.11.2024. Prin urmare, Guvernul avea obligația ca până la 13.02.2025 să aprobe această instrucțiune.

Potrivit art. 56 alin. (3) din Legea nr. 100/2017 cu privire la actele normative, intrarea în vigoare a actelor normative poate fi stabilită pentru o altă dată doar în cazul în care se

urmăreşte protecţia drepturilor şi libertăţilor fundamentale ale omului, realizarea angajamentelor internaţionale ale Republicii Moldova, conformarea cadrului normativ hotărîrilor Curţii Constituţionale, eliminarea unor lacune din legislație sau contradicţii între actele normative ori dacă există alte circumstanţe obiective.

Prin urmare, având în vedere circumstanțele de drept și de fapt menționate mai sus, se consideră justificat și necesar ca prezenta hotărâre să intre în vigoare la data publicării în Monitorul Oficial al Republicii Moldova.

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. Creşterea 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 conținutul 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: potrivit celor comunicate Asociația națională a companiilor din sectorul tehnologii informaționale și comunicare; Moldcell S.A; Orange Moldova S.A; Moldtelecom S.A; StarNet S.R.L nu sunt preconizate costuri suplimentare, fiindcă mecanismul a fost deja implementat.

3. Creşterea costurilor operaționale: nu este aplicabil.

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 paginii web. 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.
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. Avizarea a fost realizată, avizele au fost recepționate și Sinteza a fost elaborată 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: https://particip.gov.md/ro/document/stages/proiectul-hotararii-de-guvern-pentru-aprobarea-instructiunii-privind-procedura-de-sistare-a-accesului-la-pagini-web-care-contin-informatii-destinate-si-utilizate-pentru-pregatirea-sau-comiterea-infractiunilor-si-de-eliminare-a-continutului-respectiv-la-sursa/14136.

7. Concluziile expertizelor

Ministerul Justiției

Raportul de expertiză nu conține o Concluzie separată. Totuși toate propunerile au fost examinate, iar proiectul Instrucțiunii a fost racordat la cerințele formulate de Ministerul Justiției (a se vedea Sinteza).

Centrul Național Anticorupție

Proiectul hotărârii Guvernului 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 scopul creării 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.

Proiectul corespunde normelor de tehnică legislativă și respectă parțial rigorile de transparență impuse de Legea nr.239/2008 privind transparența în procesul decizional.

Proiectul corespunde interesului public general, în cazul în care prevederile acestuia vor fi aplicate cu respectarea strictă a cadrului legal, adică evitarea unor eventuale abuzuri din partea entităților responsabile de sistarea accesului la paginile web.

În normele proiectului supus expertizei anticorupție au fost identificați următorii factori de corupție:

– utilizarea neuniformă a termenilor;

– formulare ambiguă care admite interpretări abuzive;

– concurența normelor de drept.

În scopul preîntâmpinării apariției manifestărilor de corupție la aplicarea în practică a prevederilor proiectului, considerăm oportună redactarea acestuia în contextul obiecțiilor și recomandărilor din prezentul raport de expertiză anticorupție.

8. Modul de încorporare a actului în cadrul normativ existent

Nu este aplicabil

9. Măsurile necesare pentru implementarea prevederilor proiectului actului normativ

Nu este aplicabil.

Ministru afacerilor interne /semnat/ Daniella MISAIL-NICHITIN

S I N T E Z A

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

Participantul la avizare, consultare publică, expertizare	Nr. crt.	Conținutul obiecției, propunerii, recomandării, concluziei	Argumentarea autorului proiectului
Avizare și consultare publică			
Ministerul Culturii	1.	Prin prezenta, Ministerul Culturii Vă comunică că a examinat proiectul de hotărâre 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 (număr unic 152/MAI/2025) și vine cu următoarele propuneri: 1. În denumire și pe tot parcursul textului se propune ca sintagma „pagina web” să fie înlocuită cu sintagma „site-ul”, deoarece este mai corectă din punct de vedere și tehnic și logic. Însuși cuvântul „pagina” presupune o cantitate limitată de informații publicată pe o adresă (hiperlink) electronică, în timp ce „site” este o culegere de pagini. În același sens, dacă se decide sistarea accesului la pagina web (cu conținutul respectiv), spre exemplu cu adresa https://raufacator.md/terror, la pagina web https://raufacator.md/home (sau orice altă pagină site-lui respectiv) nu trebuie să fie sistat accesul, deoarece este o altă pagină. Sistarea accesului anume la o pagina a site-ului nu este posibilă fără o intervenție în conținutul site-ului, ce presupune o altă activitate din punct de vedere tehnic și juridic.	**Nu se acceptă** Sintagma „***pagina web***” nu poate să fie înlocuită cu sintagma „*site-ul*”, deoarece s-ar încălca dreptul la libera exprimare. Așa cum a menționat și avizatorul, *pagina web* se referă la o unitate individuală de conținut pe internet. Este o pagină de pe un site, care poate include text, imagini, videoclipuri și alte tipuri de informații. Pe de altă parte, *site-ul web* este un ansamblu de pagini web interconectate între ele, care sunt accesibile pe internet. Un *site web* poate include mai multe *pagini web,* care formează un întreg, cu o structură ierarhică. Prin urmare, sistarea întregului *site* din cauza unei *pagini web* poate duce la încălcarea

		Totodată, referitor la sintagmă „pagina web”, ca precedent, facem trimitere la hotărârea guvernului cu o formulare similară – Hotărârea Guvernului nr. 728/2023 cu privire la site-urile web oficiale ale autorităților și instituțiilor publice și cerințele minime privind profilurile de socializare ale acestora.	dreptului la libera exprimare din moment ce restul paginilor de pe același site ar putea să nu conțină date sau informații cu privire la pregătirea sau comiterea infracțiunilor.
	2.	La punctul 9 se propune excluderea sau reformularea subpunctului 9.3 și excluderea subpunctului 9.5, reieșind din următoarele considerente. În cazul în care site-ul a fost hackuit de către infractori, blocarea unei anumite pagini nu are sens, deoarece accesul la conținutul sitului este deja obținut de către infractori și blocarea unei pagini nu exclude generarea conținutului dăunător la celelalte pagini ale aceleași resurse. În cazul în care conținutul dăunător a apărut de la intenția persoanei care are acces legal la conținutul site-ului, blocarea unei pagini cu atât mai mult nu are sens.	**Nu se acceptă** Se atestă o lipsă de concordanță între argumentarea avizatorului și norma la care se face trimitere. Punctul 9 din proiect reglementează principiile care urmează a fi respectate la emiterea Ordinului de sistare a accesului sau de eliminare a conținutului online la sursă, principii reglementate și de Legea nr. 20/2009. În speță, este vorba de: a) subpunctului 9.3 - aplicării măsurii tehnice de sistare cel mai puțin restrictive; b) subpunctului 9.5 - revizuirii periodice a necesității sistării în continuare a accesului la o anumită pagină web. În pofida acestor neconcordanțe, se pare că argumentele avizatorului vin spre susținerea sistării integrale a site-lui în cazurile când una din paginile

			web ale acestui site a fost compromisă. Așa cum s-a menționat mai sus, nu este corect de sistat un site întreg din cauza unei singure pagini web, chiar dacă, ipotetic, există riscul sau presupunerea că, în viitor, vor fi publicate date sau informații compromițătoare.
	3.	3. Se propune introducerea punctului referitor păstrarea de către furnizorii de servicii de găzduire a conținutului copiilor de rezervă ca dovadă a cauzei sistării accesului.	**Nu se acceptă** Informațiile și datele care au servit la sistarea unei pagini web se vor păstra de subdiviziunea specializată a Ministerului Afacerilor Interne și/sau a Serviciului de Informații și Securitate – autorități publice ce sunt în drept să emite Ordine de sistare. Furnizorii de servicii execută aceste Ordine și nu este corect de pus în sarcina acestora păstrarea unor asemenea informații, mai ales că aceste măsuri implică costuri de păstrare/arhivare.
	4.	4. Se propune introducerea punctului referitor la blocarea de către furnizorii de servicii de găzduire a conținutului pentru excluderea restabilirii din copiile de rezervă ale conținutului infracțional.	**Nu se acceptă** Nu este clară propunerea. Totuși, se pare că avizatorul nu a pătruns în esența proiectului. Cadrul legal oferă 2 posibilități:

			1) eliminarea conținutului la sursă în cazurile când serverele sunt în RM; și 2) sistarea accesului la pagina web, atunci când organele de drept nu pot șterge informația se sistează accesul. În cazul celei de-a 2 măsuri, accesul se sistează doar de către operatorii de servicii din RM, nu și din străinătate.
Ministerul Muncii și Protecției Sociale	1.	Ministerul Muncii și Protecției Sociale a examinat demersul nr. 18-69-2657 din 10 martie 2025, referitor la avizarea/expertizare proiectului de hotărâre 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 (număr unic 152/MAI/2025), și reieșind din competența funcțională comunică următoarele: La proiectul hotărârii de Guvern se propune: 1. După punctul 3, de inclus un punct nou cu următorul cuprins „Paginile web care conțin informații destinate și utilizate prin prisma aspectelor Legii nr. 45/2007 cu privire la violența împotriva femeilor si violenței în familie, vor fi considerate, de asemenea, ca fiind destinată și utilizată pentru pregătirea sau comiterea infracțiunilor.” În acest context este de remarcat că noțiunea de violență psihologică conține elemente de utilizare a tehnologiilor informaționale și comunicațiilor electronice. Iar Parlamentul a lansat la 6 martie o inițiativă legislativă ce vizează inclusiv modificarea legii citate cu noțiuni specifice violenței facilitate de tehnologii informaționale.	**Nu se acceptă** Potrivit art. 3 alin. (4) lit. b) din Legea nr. 100/2017 cu privire la actele normative, proiectul actului normativ întocmit în temeiul unui act normativ de nivel superior nu poate depăși limitele competenței instituite prin actul de nivel superior și nici nu poate contraveni scopului, principiilor și dispozițiilor acestuia. În prezent, criteriile privind sistarea accesului la o pagină web ce cuprinde informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor sau privind eliminarea la sursă a conținutului online ce cuprinde informații destinate și utilizate pentru

			pregătirea sau comiterea infracțiunilor sunt reglementate expres și exhaustiv în art. 4^2 alin. (1) din Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice. Prezentul proiect nu poate să reglementeze și alte situații decât cele ce se referă la Legea nr. 20/2009. Reglementarea altor situații ar presupune încălcarea art. 3 alin. (4) lit. b) din Legea nr. 100/2017, conținutul căruia s-a menționat mai sus.
	2.	2. Punctul 21 de redat în următoarea redacție „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) precum privind violența față de femeie, inclusiv pornografie sau materialele care sunt dăunătoare pentru femei 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."	**Nu se acceptă** Pornind de la prevederile art. 3 alin. (4) lit. b) din Legea nr. 100/2017, unde este menționat că proiectul actului normativ întocmit în temeiul unui act normativ de nivel superior nu poate depăși limitele competenței instituite prin actul de nivel superior și nici nu poate contraveni scopului, principiilor și dispozițiilor acestuia, se comunică faptul imposibilității modificării punctului 21 din proiect. Totuși, în cazurile în care lista elaborată de Organizația Internațională a Poliției

			Criminale (The INTERPOL „Worst of" List) va conține pagini web în partea ce se referă la violența față de femei, atunci aceste pagini vor fi sistate.
	3.	3. La 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, după pct. 22 se propune de completat cu un punct nou, pct. 23, cu următorul cuprins: „23. În cazul identificării pe pagina web a informațiilor destinate și utilizate pentru comiterea infracțiunilor asupra copilului și deținerii datelor cu privire la un copil identificat, se acționează în conformitate cu Hotărârea Guvernului nr. 270/2014 cu privire la aprobarea Instrucțiunii privind mecanismul intersectorial de cooperare pentru identificarea, evaluarea, referirea, asistența și monitorizarea copiilor victime și potențiale victime ale violenței, neglijării, exploatării și traficului." Atragem atenția că, actualmente conform prevederilor Hotărârii Guvernului nr. 270/2014 sus-menționate - persoanele fizice care dețin informații despre un caz suspect de violență, neglijare sau exploatare a copilului sunt obligate să le comunice autorității tutelare locale/teritoriale sau organelor de drept. 4. Urmare a completării cu punctul vizat, punctul 23 urmează a fi renumerotat în punctul 24.	**Se acceptă**
	4.	5. Totodată, pe tot parcursul textului proiectului de hotărâre, precum și în Nota de fundamentare la proiectul vizat cuvântul minor în orice formă gramaticală se va substitui cu cuvântul copil la forma gramaticală corespunzătoare, luând în considerare Convenției cu privire la drepturile copilului,	**Se acceptă**

		Codului Familiei, Legii nr. 370/2023 privind drepturile copilului și altor acte normative naționale și internaționale, care reglementează semnificația cuvântului copil.	
Ministerul Dezvoltării Economice și Digitalizării	1.	Ca urmare examinării proiectului de hotărâre 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 (număr unic 152/MAI/2025), în limita competențelor, comunicăm următoarele. I. Obiecții/propunerii la proiectul de Instrucțiune. La pct. 4, după cuvintele ,,persoană fizică” se completează cu cuvântul ,,sau”.	**Se acceptă**
	2.	La pct. 6, textul ,,serviciu de găzduire sau conținut” propunem de substituit cu textul ,,servicii de găzduire a conținutului”. Totodată, la același punct, de exclus textul ,,și specifice de sistare a accesului la pagini web sau”.	**Nu se acceptă** În spațiul online, „*serviciul de găzduire*” și „*serviciul de conținut*” sunt considerate două concepte distincte, deși adesea pot interacționa sau se pot suprapune într-o anumită măsură. *Serviciul de găzduire* (hosting) se referă la furnizarea de infrastructură tehnică pentru stocarea și accesarea datelor pe internet. Furnizorii de servicii de găzduire (*de exemplu, servere, cloud, centre de date*) pun la dispoziție resursele necesare pentru ca utilizatorii să poată încărca, stoca și distribui informații online.

			Serviciul de conținut se referă la furnizarea, distribuirea sau crearea de conținut pe internet. Conținutul poate include texte, imagini, videoclipuri, audio, aplicații sau orice alt tip de material digital. În Republica Moldova activează ambele tipuri de servicii, iar formula propusă de avizator presupune excluderea unui tip de serviciu.
	3.	La pct. 8, se propune excluderea cuvintelor „și sau”. Suplimentar, la punctul dat, după cuvintele „canal securizat” se propune completarea cu următorul text „în baza unor acorduri de colaborare între subdiviziunea specializată pentru fiecare furnizor în parte. Acest acord va fi încheiat în scopul creării și gestionării canalului securizat în care se vor stabili condiții de transmitere/recepționare a Ordinului de eliminare a conținutului din sursă sau Ordinului de sistare a accesului.”.	**Se acceptă parțial** Cuvintele *„și/sau”* nu se vor exclude din considerentele menționate la punctul precedent. Punctul 8 din Instrucțiune a fost modificat după cum urmează: *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, în baza unor acorduri de colaborare. Adresa URL la care urmează a fi sistat accesul va fi comunicată în format textual.*
	4.	După pct. 10, se propune completarea cu un nou punct, cu următorul text „Sistarea accesului la pagina web, ce	**Nu se acceptă**

		conține informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor, poate fi dispus pe un termen de 30 de zile, cu posibilitatea de prelungire a acestuia, dar nu mai mult de 90 de zile. Fiecare prelungire nu poate depăși 30 de zile.”	Această normă este reglementată de art. 4^1 alin. (2) din Legea nr. 20/2009 și nu este necesară repetarea acesteia, chiar dacă se va observa că, în cazul altor prevederi, indicarea repetată a acestora în Instrucțiune s-a admis. La etapa elaborării proiectului Instrucțiunii s-a constatat că, în practică, pot apărea situații în care paginile web – create exclusiv pentru comiterea infracțiunilor, ar urma să fie sistate pe un termen nelimitat, aspect omis la etapa elaborării și promovării proiectului de lege de modificare al Legii nr. 20/2009. Astfel, există o prezumție rezonabilă că, în curând, Legea nr. 20/2009 va trebui să suporte anumite modificări în sensul în care ar permite sistarea unor pagini web pe perioade nedeterminate de timp. Prin urmare, pentru a evita modificarea ulterioară a Instrucțiunii, s-a decis că prevederile referitoare la perioadele de sistare a paginilor

			web să fie reflectate doar în Legea nr. 20/2009.
	5.	La pct. 16, propunem excluderea cuvintelor ,,autorității respective". Aceeași obiecții și la punctul 17, de exclus textul ,,a autorității care a emis Ordinul de sistare a accesului", dat fiind faptul că va fi o pagină comună creată pentru acest scop.	Nu se acceptă Ordinul de sistare a accesului la paginile web sau de eliminare a conținutului la sursă va reprezenta actul administrativ al subdiviziunii specializate din cadrul Ministerului Afacerilor Interne, fie din cadrul Serviciului de Informații și Securitate, adică două autorități publice distincte. Prin urmare, nu este corect și practic ca subdiviziunea specializată din cadrul Ministerului Afacerilor Interne să comunice utilizatorului (solicitantului) motivele sistării paginii web sau eliminării conținutului la sursă, ce a fost realizată de subdiviziunea specializată din cadrul Serviciul de Informații și Securitate și invers. Fiecare autoritate publică va fi responsabilă să-și argumenteze legalitatea Ordinului emis.
	6.	La pct. 18.3., de completat cu următorul text ,,În scopul prevăzut la pct. 18.2., subdiviziunea specializată va revizui lunar, până în ziua a 15-a a lunii următoare, lista paginilor web identificate sau comunicate, în privința cărora a fost emis Ordinul de sistare a accesului."	**Se acceptă** S-a indicat că subdiviziunea specializată va revizui lunar lista paginilor web identificate sau comunicate în privința cărora a

			fost emis Ordinul de sistare a accesului sau de eliminare a conținutului.
	7.	Referitor la Anexă, recomandăm excluderea numerotării, deoarece este doar una. Totodată, propunem excluderea cuvântului „online” de pe tot textul acestuia. În contextul celor relatate, solicităm revizuirea proiectului conform aspectelor enunțate supra.	**Se acceptă**
Ministerul Educației și Cercetării	1.	Ministerul Educației și Cercetării a examinat proiectul de hotărâre 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* (număr unic 152/MAI/2025) și, în limitele competențelor, comunică lipsă de obiecții și propuneri.	**S-a luat act**
Ministerul Finanțelor	1.	La indicația Cancelariei de Stat nr.18-69-2657 din 10 martie 2025, Ministerul Finanțelor a examinat proiectul de hotărâre 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 (număr unic 152/MAI/2025) și, în limita competențelor funcționale, comunică următoarele. La 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 propune: La pct. 4 după cuvintele „orice persoană fizică” de completat cu cuvântul „ori”, în continuare după text.	**Se acceptă** S-a introdus cuvântul *„sau”*.
	2.	La pct. 7, subpct. 7.1 textul „anexa la prezenta Instrucțiune” se va substitui cu textul „anexa la prezenta Instrucțiune”, ținând cont că există doar o anexă.	**Se acceptă**

	3.	La Anexa Instrucțiunii se propune: La parafa de aprobare a Actului privind examinarea paginii/paginilor web a Anexei Instrucțiunii, de exclus textul „nr. 1” după cuvântul „Anexa”. La parafa de aprobare și în textul Actului privind examinarea paginii/paginilor web anexat la Instrucțiune, cuvântul „online” se va substitui cu cuvântul „respectiv”, întru respectarea denumirii instrucțiunii indicate în titlul proiectului actului de hotărâre. Prin urmare, proiectul urmează a fi revizuit, prin prisma celor invocate.	**Se acceptă**
Serviciul Tehnologia Informației și Securitate Cibernetică	1.	Prin prezenta, în ordinea examinării proiectului de hotărâre 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 (număr unic 152/MAI/2025), în limita competențelor funcționale, I.P. „Serviciul Tehnologia Informației și Securitate Cibernetică” (în continuare IP STISC) comunică următoarele propuneri și obiecții. Din proiectul de hotărâre se va exclude pct. 4 întrucât are un sens echivoc și irelevant. În acest context, subliniem că în conformitate cu prevederile pct. 8 sbp. 1) din Statutul IP STISC aprobat prin Anexa nr. 1 la Hotărârea Guvernului nr. 414/2018, IP STISC asigură crearea, administrarea, asigurarea funcționării și dezvoltarea infrastructurii de tehnologie a informației și Sistemului de telecomunicații al autorităților administrației publice ca parte a rețelei de comunicații speciale. Astfel, Ministerul Afacerilor Interne și Serviciul de Informații și Securitate, fiind incluse în Lista entităților publice, asigurate cu serviciile Sistemului de telecomunicații al autorităților	**Se acceptă**

		administrației publice, aprobată prin Anexa nr. 1 la Hotărârea de Guvern nr. 840/2004, beneficiază inclusiv de serviciile de acces al autorităților publice la resursele rețelei globale Internet prestate de către IP STISC.	
	2.	În vederea uniformizării terminologiei utilizate, în tot cuprinsul 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 precum și a Notei de fundamentare la proiect, cuvintele „site” și „website” se vor substitui cu cuvântul „pagină” și respectiv sintagma „pagină web”, la forma gramaticală corespunzătoare. Dacă totuși autorul utilizează aceste noțiuni ca fiind cu sensuri diferite, urmează să le definească.	**Se acceptă**
Consiliul Superior al Magistraturii	1.	La 11 martie 2025 Cancelaria de Stat a Republicii Moldova a adresat Consiliului Superior al Magistraturii un demers prin care a solicitat avizarea proiectului 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 (număr unic 152/MAI/2025). Analizând proiectul hotărârii și argumentele prezentate în nota informativă, Plenul Consiliului Superior al Magistraturii consideră oportună avizarea proiectului elaborat de Ministerul Afacerilor Interne al Republicii Moldova reținând următoarele. Conform notei informative, 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;	**Nu se acceptă** Instrucțiunea reprezintă un act normativ care urmează a fi aplicat împreună cu actul normativ superior, adică Legea nr. 20/2009. Se va observa că punctul 3 din instrucțiune este primul pas spre identificarea paginilor web. În continuare, punctele 4 și 5 din Instrucțiune indică, cu lux de amănunte, cine poate sesiza organele de drept cu privire la existența unei pagini web ce conține informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor. Bineînțeles că acest proces și

		2. 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 Legii nr. 200/2024, 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 sau de eliminare a conținutului la sursă. Drept 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. Este de reținut că, Instrucțiunea propusă spre aprobare 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. 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;	înseamnă identificarea paginilor web.

		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. Analizând conținutul proiectului Plenul Consiliului Superior al Magistraturii intervine cu unele obiecții de care urmează să se țină cont. 1. La pct. 1 sintagma „Prezenta Instrucțiunea stabilește procedura de identificare a paginilor web care conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor ...” nu corespunde conținutului documentului. Or, niciun punct ulterior din proiectul actului normativ nu reglementează propriu-zis procedura de identificare a paginilor web, iar din titlul actului normativ	

		rezultă că acesta reglementează procedura de sistare a accesului la pagini web și de eliminare a conținutului, nu și cea de identificare. Identificarea propriu-zisă este reglementată de din Legea nr. 20/2009 care la art. 4^2 alin. 1 lit.a)-g) stabilește criteriile pentru identificarea paginilor web pasibile de sistare și eliminare.	
	2.	2. La pct. 3 din proiect se propune introducerea după art. 4^2 a textului „alin. 1 lit. a)-g)”, deoarece anume aceste prevederi reglementează criteriile pentru sistarea și eliminarea unei pagini web.	**Se acceptă**
	3.	3. La pct. 6 se declară că furnizorii de servicii pot sista accesul sau elimina conținutul online la sursă. La pct. 22, care reglementează mecanismul de implementare a pct. 6, este menționat că furnizorii de servicii pot doar sista accesul, nu și elimina conținutul la sursă. Din păcate nici nota informativă nu face lumină în acest caz. În comentariul la pct. 22 autorul proiectului scrie că furnizorii de servicii pot elimina materialele. Se recomandă de coroborat conținutul acestor norme.	**Se acceptă** Punctul 6 din Instrucțiune a fost exclus la propunerea Grupului de lucru al Comisiei de Stat privind Activitatea de Întreprinzător. Totodată, se menționează că lista paginilor web The INTERPOL *“Worst of” List* pot fi doar sistate, eliminarea conținutului fiind imposibilă tehnic, fiindcă serverele nu se află pe teritoriul Republicii Moldova.
	4.	4. La pct. 8 sintagma „furnizorilor de servicii și/sau conținut” de uniformizat cu sintagma de la pct. 2.6.	**Se acceptă**
	5.	5. Prevederile pct. 9 reproduc conținutul alin. (1) din art. 4^1 din Legea nr. 20/2009. Nu este binevenită o astfel de repetare. Propun următoarea redacție „Emiterea Ordinului de sistare a accesului sau de eliminare a conținutului online la sursă are loc cu respectarea alin. 1 din art. 4^1 din Legea nr. 20/2009”.	**Se acceptă parțial** Potrivit art. 3 alin. (4) lit. b) din Legea nr. 100/2017, unica limitare impusă Guvernului în procesul de elaborare și adoptare a Hotărârilor de Guvern reprezintă interdicția de depășire

			a limitelor competenței instituite prin actul normativ de nivel superior. Altfel spus, nu este interzis ca proiectele Hotărârilor de Guvern să reglementeze (repetat) prevederile legii puse în aplicare. Practica națională de legiferare arată că, de regulă, Hotărârile Guvernului conțin prevederile legilor pe care le pun în aplicare. Aceasta se face pentru ca executorul Hotărârilor de Guvern să aibă la îndemână întreg cadrul legal aplicabil.
	6.	6. La pct. 10 este reprodus conținutul alin. 3 din art. 4¹ din Legea nr. 20/2009 precum că „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”. Ar fi binevenit dacă autorul proiectului ar indica termenul în decursul căruia urmează a fi publicate aceste ordine pe pagina web. Astfel, ar crea un mecanism de implementare a prevederii din alin. 3 din art. 4¹ din Legea nr. 20/2009.	**Se acceptă**
	7.	7. La pct. 18 în sintagma „Autoritatea emitentă, ... este obligată să dispună încetarea sistării accesului la paginile web ...” ar fi binevenit să se specifice actul procesual prin care se dispune încetarea sistării (e.g., dispoziție, încheiere, decizie etc.).	**Se acceptă**
	8.	8. La pct. 20 în sintagma „în condițiile pct. 17” cifra 17 de înlocuit cu cifra 19, deoarece pct. 20 este continuitatea	**Se acceptă**

		pct. 19. Mai mult ca atît, în Nota informativă se face trimitere la pct.19. De asemenea, la pct. 20 în sintagma „... anulează în întregime sau parțial...” ar fi binevenit să se specifice actul procesual (dispoziție, încheiere, decizie etc.) prin care se dispune anularea ordinului.	Actul procesual prin care se va dispune anularea parțială sau integrală a Ordinul de sistare a accesului și/sau Ordinul de eliminare a conținutului la sursă va fi Ordinul. Acest fapt poate fi dedus din pct. 18 al proiectului. Totodată, pentru eliminarea oricăror interpretări Nota de fundamentare a fost completată cu explicații suplimentare.
	9.	9. La pct. 22 sintagma „pot sista accesul” este în contradicție cu explicația din nota informativă, autorul folosind termenul de eliminare a paginilor. Ar fi binevenit ca autorul proiectului să înlăture aceste neconcordanțe pentru a evita apariția divergențelor la practică. În asemenea circumstanțe, Plenul Consiliului Superior al Magistraturii avizează cu obiecții pe marginea conținutului proiectului 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 (număr unic 152/MAI/2025). Avizul se remite Ministerului Ministerul Afacerilor Interne al Republicii Moldova, Cancelariei de Stat și se publică pe pagina web a Consiliului Superior al Magistraturii (www.csm.md).	**Se acceptă** Nota de fundamentare a fost modificată.
Serviciul de Informații și Securitate	1.	Serviciul de Informații și Securitate al Republicii Moldova (în continuare – Serviciul), a examinat 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	**Se acceptă**

		comiterea infracțiunilor și de eliminare a conținutului respectiv la sursă (număr unic 152/MAI/2025) și Vă comunică următoarele obiecții și propuneri. 1. În textul proiectului hotărârii de Guvern, Serviciul propune excluderea punctului 4, în contextul în care Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică (în continuare – I.P. STISC) în calitate de CERT-Gov, are atribuția de a bloca accesul utilizatorilor la pagini web multipcase, pentru a nu permite compromiterea infrastructurii TIC guvernamentale, iar din punct de vedere tehnic, I.P. STISC nu poate asigura acces neîntrerupt la toate paginile web. 2. Din alt punct de vedere, subdiviziunile specializate, în cadrul activității de identificare a paginilor web, ce necesită a fi blocate și monitorizate privind eficiența blocării, trebuie să dețină acces la Internet mobil/fix din diferite rețele ale operatorilor naționali a comunicații – iar faptul respectiv trebuie organizat de către entitățile vizate în proiect.	
	2.	3. La punctul 2 al proiectului Instrucțiunii, Serviciul propune revizuirea noțiunilor (de ex. DNS) în contextul în care unele din ele nu se utilizează în textul proiectului, iar altele sunt utilizate eronat (de ex. blocarea se va efectua la nivel de nume de domeniu, dar nu la nivel de adresă URL).	**Se acceptă parțial** Noțiunile au fost consultate și coordonate suplimentar cu reprezentanții furnizorilor de servicii. În plus, potrivit art. 32 alin. (5^1) din Legea nr. 100/2017, avizele și recomandările conțin obiecții și propuneri motivate, cu anexarea, după caz, a versiunii redactate a proiectului sau a unor prevederi. Se menționează că propunerea avizatorului nu este clară, fiindcă

			nu propune soluții alternative și nu explică deficiențele pe care le-a identificat.
	3.	4. La punctul 8 al proiectului Instrucțiunii – textul „adresa URL” urmează a fi înlocuită cu textul „numele domeniului”.	**Nu se acceptă** Propunerea avizatorului de înlocuire a termenului „adresa URL” cu „numele domeniului” nu este adecvată în contextul procedurii de sistare a accesului la pagini web. Scopul acestei proceduri este de a bloca accesul nu doar la domeniul principal al unui site, ci și la anumite pagini specifice sau resurse de pe acel domeniu care conțin informații ilegale sau destinate comiterii de infracțiuni. Adresa URL completă este necesară pentru a identifica în mod precis pagina web care conține informațiile incriminate. URL-ul cuprinde atât domeniul (ex: www.exemplu.com), cât și calea către resursa specifică (ex: www.exemplu.com/pagina-infractiune), care poate fi o sub-pagină sau o resursă particulară. Înlocuirea acestuia cu doar „numele domeniului” (ex: www.exemplu.com) ar duce la sistarea accesului la întregul domeniu, ceea ce ar fi mult mai

			puțin precis și mai puțin eficient în combaterea infracționalității informatice. Procedura de sistare a accesului se aplică pentru a opri utilizarea unor pagini web care conțin informații destinate și utilizate pentru comiterea infracțiunilor. Așadar, identificarea exactă a unei pagini (prin URL) este esențială, iar restrângerea la „numele domeniului” nu ar asigura o intervenție precisă asupra paginilor specifice care trebuie blocate.
	4.	5. În punctul 8 al proiectului Instrucțiunii, se menționează despre „canal securizat” prin care se va remite Ordinul, iar adresa URL se va comunica în format textual. Respectiv, apar următoarele neclarități: 5.1. vor fi organizate 2 canale de comunicații, unul securizat și altul în format textual? 5.2. formatul textual nu trebuie securizat? 5.3. „canalul securizat” - nu este în format textual, e format video/audio? 5.4. Cum este organizat canalul securizat? Astfel, procedura de utilizare a unui „canal securizat” pentru comunicarea ordinelor, urmează a fi definită mai clar pentru a asigura securitatea comunicării între autoritățile implicate.	**Se acceptă** Punctul 8 a fost modificat, *canalul securizat* se va stabili prin acorduri de colaborare dintre subdiviziunea specializată și furnizorii de servicii.
	5.	6. Totodată, Serviciul propune modificarea punctului 16 din proiectul Instrucțiunii, care va avea următorul conținut: *„Ministerul Afacerilor Interne și Serviciul de*	**Nu se acceptă** Ordinul de sistare a accesului la paginile web sau de eliminare a

		Informații și Securitate de comun cu I.P. Serviciul Tehnologia Informației și Securitate Cibernetică, creează o pagină web dedicată, găzduită în infrastructura mCloud, care este comunicată furnizorilor de servicii de acces la Internet și cuprinde următoarele informații:”.	conținutului la sursă va reprezenta actul administrativ al subdiviziunii specializate din cadrul Ministerului Afacerilor Interne, fie din cadrul Serviciului de Informații și Securitate, adică două autorități publice distincte. Prin urmare, nu este corect și practic ca subdiviziunea specializată din cadrul Ministerului Afacerilor Interne să comunice utilizatorului (solicitantului) motivele sistării paginii web sau eliminării conținutului la sursă, ce a fost realizată de subdiviziunea specializată din cadrul Serviciul de Informații și Securitate și invers. Fiecare autoritate publică va fi responsabilă să-și argumenteze legalitatea Ordinului emis.
Procuratura Generală	1.	Procuratura Generală a examinat proiectul de hotărâre pentru aprobarea Instrucțiunii privind procedura de sistare a accesului la pagini web care conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor, precum şi de eliminare a conținutului respectiv la sursă (număr unic 152/MAI/2025), remis spre avizare. Apreciind conținutul proiectului prin prisma principiilor activității de legiferare prevăzute la art. 3 din Legea nr. 100/2017 privind actele normative, în limita	**Se acceptă** Punctul 1 a fost modificat după cum urmează: *„Prezenta Instrucțiune stabileşte proceduri pentru identificarea paginilor web care conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor, pentru punerea în aplicare a Ordinului*

		domeniului de competență al Procuraturii Generale, expunem mai jos următoarele propuneri: 1. Cu privire la punctul 1 din Instrucțiune, propunem reformularea acestuia conform următoarei redacții: *„Prezenta Instrucțiune stabilește proceduri pentru identificarea paginilor web care conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor, pentru punerea în aplicare a ordinului de sistare a accesului la o pagină web sau de eliminare a conținutului online la sursă, precum și pentru cooperarea și coordonarea între autoritățile competente (Ministerul Afacerilor Interne și/sau Serviciul de Informații și Securitate), furnizorii de servicii și utilizatorii de sisteme informatice.”*.	*de sistare a accesului la o pagină web sau de eliminare a conținutului online la sursă, precum și pentru colaborarea între Ministerul Afacerilor Interne și/sau Serviciul de Informații și Securitate și furnizorii de servicii de acces la Internet, furnizorii de servicii de găzduire a conținutului online și/sau furnizorii de conținut, în vederea implementării măsurilor de sistare a accesului sau eliminare a conținutului la sursă.”*
	2.	2. După punctul 9 din Instrucțiune, propunem completarea cu un punct nou, urmat de renumerotarea corespunzătoare, cu următorul conținut: „10. Ordinul de sistare a accesului la pagini web sau de eliminare a conținutului online la sursă va conține următoarele elemente: 10.1. Informațiile care identifică autoritatea emitentă; 10.2. Temeiul juridic al ordinului; 10.3. Indicarea și motivarea aplicabilității criteriilor de apreciere a informației publicate sau puse la dispoziție prin orice mod pe pagina web, ca fiind destinată și utilizată pentru pregătirea sau comiterea infracțiunilor; 10.4. Informații care să permită furnizorului de servicii să identifice și să localizeze conținutul în cauză, inclusiv unul sau mai multe adrese URL şi, dacă este necesar, informații suplimentare;	**Se acceptă**

		10.5. Informații privind modul şi termenul de contestare.”	
	3.	3. La finalul punctului 14, propunem completarea cu următorul text: „Furnizorii de servicii vor informa autoritatea emitentă a ordinului, fără întârzieri, cu privire la modul în care s-a dat curs acestuia, indicând data la care s-a realizat punerea în aplicare a ordinului.”	**Se acceptă**
Grupului de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător	1.	Prezentul aviz este acordat în temeiul art. 3 alin. (2), art. 271, anexa nr. 1 și art. 32 alin. (22) din Legea nr. 100/2017 cu privire la actele normative, în conformitate cu prevederile Legii nr. 235/2006 cu privire la principiile de bază de reglementare a activității de întreprinzător, Hotărârii Guvernului nr. 1429/2008 privind revizuirea şi optimizarea cadrului normativ de reglementare a activității de întreprinzător și Hotărârii Guvernului nr. 574/2024 cu privire la aprobarea Metodologiei de analiză a impactului de reglementare. **Evaluarea proiectului de act normativ:** ***Concluzia:*** Proiectul conține prevederi discordante cu principiile de reglementare a activității de întreprinzător. ***Comentarii, recomandări:*** Însăși mecanismul de sistare a accesului la pagini web în Legea nr. 20/2009 este plasat într-un context juridic incert și ambiguu. Adică pe de o parte aceasta are cumva scopul luptei și contracarării cu fenomenul infracțional pe pagini web, însă nici în lege și nici în proiectul prezentat nu clarifică ce tip de măsură este această sistare și cum această măsură are legătură cu instrumentarul procedural penal sau cel din urmărirea penală în principiu. Nu este clar din ce cauză aceste ordine de sistare, în contextul legii, nu se regăsesc în rândul măsurilor speciale	**Se acceptă parțial** S-a exclus pct. 6 din proiect care oferea furnizorilor de serviciu de găzduire sau conținut 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. Totodată, se comunică că: Sistarea nu reprezintă o măsură procesual penală, dar un instrument juridic reglementat de Legea nr. 20/2009 ce contribuie la prevenirea și combaterea criminalității informatice. Este important de înțeles că nu orice

		de investigații, dar și în proiectul prezentat nu se face cumva nici o legătură clară cu procesul de urmărire penală. Spre exemplu, dacă în cazul aplicării unei măsuri speciale de investigații aceasta se materializează într-un dosar special cu proces-verbal corespunzător, legalitatea căruia este verificată și care trebuie să contribuie la urmărirea penală ce va urma, în cazul ordinului de sistare a accesului la pagini web, proiectul propus nu prevede nici o finalitate procesuală clară. Din altă perspectivă, încadrarea măsurilor de constrângere în raport cu accesul la pagini web sau informația conținută pe acestea în procesul administrativ nu se racordează cu însăși conceptul și obiectivele Codului administrativ. Ori procedura administrativă în sine este una destul de permisivă, lăsând o marjă foarte mare de discreție pentru autoritatea publică, nu impune unele garanții procedurale în raport cu persoana fizică/juridică, anume din considerentul că nu conține sau nu ar trebui să conțină acțiuni de constrângere și limitări grave de drepturi. Astfel modul de reglementare a acestui concept în unele cazuri poate duce la încălcarea principiului proporționalității în raporturile dintre autoritate publică și întreprinzători, fiind posibilă recurgerea la acțiuni în exces necesităților atingerii scopurilor societății. Proiectul conține prevederi care depășesc conceptual prevederile Legii nr. 20/2009. În special prin stabilirea la pct. 6 a dreptului discreționar pentru furnizori „să ia măsuri pro active proporționale și specifice de sistare a accesului la pagini web sau de eliminare a conținutului online” în lipsa oricăror ordine sau adresări oficiale din partea autorităților de drept, evident în lipsa oricăror funcții legale sau chiar capacități profesionale corespunzătoare în acest sens. Mai mult, acest drept nu este suplinit de nici o restricție sau obligația procesuală ulterioară, adică nu se clarifică de	acțiune/măsură ce se referă la crime trebuie să se regăsească în Codul de procedură penală. Asemenea abordări sunt sortite caducității chiar din momentul nașterii, or fenomenul infracțional este în permanentă schimbare. Scopul sistării accesului la pagina web sau de eliminare a conținutului la sursă este oprirea imediată a propagării conținutului dăunător în mediul online, care a devenit o parte din viața fiecăruia. Prin urmare, teza avizatorului referitoare la finalitatea proiectului în sensul scopului procesului penal nu este relevantă, deoarece această instrucțiune are ca scop, ce poate fi privit ca și finalitate, sistare accesului la o pagină web sau de eliminare a conținutului online la sursă în cazul paginilor web care conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor.

		principiu ce trebuie să facă și cum (în ce termene) trebuie să procedeze furnizorul după ce a făcut uz de acest drept. Aceasta nu este doar o normă cu caracter primar care depășește normele legii, dar este și una potențial abuzivă față de beneficiarii de servicii ale furnizorului în cauză. În aceiași ordine de idei, prevederile de la pct.21, 22 și 23 prevăd drepturi care sunt excepție de la mecanismul prevăzut de Legea nr. 20/2009 și aceste excepții nu sunt menționate în lege. Atenționăm că Guvernul nu este în drept decât să pună în aplicare normele deja prevăzute în lege și nu poate veni cu excepții de la aceste norme.	
	2.	**Evaluarea notei de fundamentare (analizei impactului de reglementare)** ***Concluzia:*** Nota de fundamentare conține suficiente informații pentru a stabili oportunitatea intervenției propuse din perspectivă juridică, cu toate că nu conține toată informația și analiza necesară cu privire la impactul asupra agenților economici la nivel național, astfel corespunde parțial cu cerințele metodologice prevăzute de Legea nr.100/2017 cu privire la actele normative. ***Comentarii, recomandări:*** La analiza situației existente nu este clară magnitudinea reală la nivel național a problematicii abordate de proiect și lipsește descrierea persoanelor (întreprinderilor) vizate. Impactul asupra sectorului privat este dezvoltat superficial, fiind înaintate doar concluzii generale că implementarea măsurilor din proiect va implica costuri administrative și operaționale suplimentare pentru unii furnizori. Este necesar ca analiza să prezinte unele estimări de costuri.	**Se acceptă parțial** Proiectul a fost consultat cu reprezentanții ATIC și furnizorii de servicii, precum Orange, Moldtelecom, Star-Net, Moldcell, etc. În plus, în partea ce se referă la impactul financiar, se comunică faptul colaborării și asumării impactului financiar de furnizorii de servicii. Dovada strânsei colaborări poate servi conversația oficială dintre Ministerul Afacerilor Interne și reprezentanții mediului de afaceri reprezentați ATIC și furnizorii de servicii, precum Orange, Moldtelecom, Star-Net, Moldcell, care au comunicat că: ***Stimate dl. Jalba,***

			Prin prezenta, dorim să confirmăm că elaborarea proiectului Hotărârii Guvernului 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 a fost realizată în strânsă colaborare cu Asociația Națională a Companiilor din Domeniul TIC (ATIC) și cu furnizorii de servicii relevante. *ATIC și reprezentanții sectorului privat au participat activ la procesul de consultare și elaborare a acestui proiect normativ, contribuind cu expertiză tehnică și operațională pentru asigurarea fezabilității implementării prevederilor propuse.* ***Totodată, menționăm că nu sunt costuri adiționale de conformare asociate implementării acestui proiect normativ**, având în vedere că*

			mecanismele propuse sunt deja parte din procesele operaționale ale furnizorilor de servicii. *Rămânem la dispoziția dumneavoastră pentru orice clarificări și vă asigurăm de sprijinul nostru în finalizarea acestui demers legislativ.* **Extrasul conversației se anexează la materialele dosarului proiectului.**
Avocatul Poporului	1.	Avocatul Poporului a analizat proiectul 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, plasat pentru consultări publice din perspectiva respectării drepturilor omului1. Temeiul legal al elaborării instrucțiunii a constituit art. II alin. (2) din Legea nr. 200/2024 privind modificarea Legii nr. 20/2009 privind prevenirea și combaterea criminalității informatice. De asemenea, nota de fundamentare explică clar scopul și obiectivele Instrucțiunii. Avocatul Poporului susține necesitatea combaterii criminalității informatice, dar subliniază că acest obiectiv legitim nu trebuie atins în detrimentul drepturilor fundamentale, în special al libertății de exprimare. În context, Ombudsmanul atrage atenția asupra necesității respectării standardelor cu privire la drepturilor omului în domeniul utilizării internetului.	**Se acceptă** Proiectul a fost completat cu un punct nou care reglementează toate cerințele ce trebuie să fie întrunite de Ordinul de sistare a accesului la pagini web sau de eliminare a conținutului online la sursă (*propunerea Procuraturii Generale*) – criterii ce corespund obiecției formulate în privința conținutului Ordinelor și anume: 1) Informațiile care identifică autoritatea emitentă; 2) Temeiul juridic al ordinului; 3) Indicarea și motivarea aplicabilității criteriilor de apreciere a informației publicate sau puse la dispoziție prin orice mod pe pagina web, ca fiind

		În particular, standardele internaționale notează că blocarea și filtrarea paginilor web sunt exemple de restricții care pot fi considerate ca încălcări ale libertății de exprimare. Măsurile generale de blocare sau filtrare la nivel național trebuie să fie luate doar de către autoritățile publice, numai dacă filtrajul se referă la un conținut specific și identificabil, în baza unei decizii cu privire la ilegalitatea acestui conținut, luate de către autoritatea națională competentă și care poate fi revizuită de o instanță sau de către o entitate independentă și imparțială de reglementare, în conformitate cu dispozițiile art. 6 al CEDO. Autoritățile publice trebuie să se asigure că toate acțiunile de filtraj sunt evaluate atât înainte, cât și în timpul aplicării acestora, pentru a se asigura că efectele filtrării sunt în conformitate cu obiectivul restricției și, prin urmare, justificate într-o societate democratică, in scopul evitării blocajului nejustificat al conținutului. Măsurile luate pentru a bloca un anumit conținut sau pagină nu trebuie să fie utilizate în mod arbitrar ca un mijloc de a opera o blocare generală a informațiilor pe Internet. Acestea nu trebuie să aibă efecte secundare de a face inaccesibil redarea cantității mari de informații, limitând astfel în mod substanțial drepturile utilizatorilor, și trebuie să fie prevăzute de lege. Mai mult, trebuie să existe o supraveghere strictă a domeniului de aplicare a blocajului și un control jurisdicțional efectiv, pentru a preveni orice abuz de putere. Controlul jurisdicțional al unei astfel de măsuri trebuie să evalueze interesele concurente puse in joc, să asigure un echilibru intre ele și să stabilească dacă o măsură cu un grad de aplicare mai scăzut poate bloca accesul la un conținut specific pe Internet.	destinată și utilizată pentru pregătirea sau comiterea infracțiunilor; 4) Informații care să permită furnizorului de servicii să identifice și să localizeze conținutul în cauză, inclusiv unul sau mai multe adrese URL şi, dacă este necesar, informații suplimentare; 5) Informații privind modul şi termenul de contestare.

		Curtea Europeană s-a pronunțat în repetate rânduri cu privire la compatibilitatea, cu art. 10 din Convenție, a măsurilor luate de autoritățile naționale pentru blocarea accesului la anumite site-uri Internet. În esență, reclamanții s-au plâns de efectul colateral al măsurilor de blocare. În special, Curtea a subliniat necesitatea de a evalua comparativ diferitele interese implicate, examinând, printre altele, necesitatea blocării totale a accesului (Ahmet Yıldırım împotriva Turciei, pct. 66) și a constatat că autoritățile ar fi trebuit să țină seama de faptul că o astfel de măsură, care făcea inaccesibile multe informații, nu putea decât să afecteze în mod semnificativ drepturile utilizatorilor de Internet și să aibă un efect colateral semnificativ (ibid.; Cengiz și alții împotriva Turciei, pct. 64). În ceea ce privește caracterul justificat al măsurii de blocare, Curtea a hotărât că, deși astfel de restrângeri prealabile nu sunt, a priori, incompatibile cu Convenția, ele trebuie totuși să se încadreze într-un cadru legal deosebit de strict în ceea ce privește delimitarea interdicției și eficacitatea controlului judecătoresc în legătură cu eventualele abuzuri, iar controlul judecătoresc al unor astfel de măsuri exercitat de către instanță, care se întemeiază pe o punere în balanță a intereselor aflate în conflict și care urmărește să asigure un echilibru între aceste interese, nu poate fi conceput fără un cadru care să prevadă norme precise și specifice privind aplicarea restricțiilor preventive privind libertatea de exprimare (Ahmet Yıldırırım împotriva Turciei, pct. 64; Cengiz și alții împotriva Turciei, pct. 62, care se referă la primirea sau comunicarea de informații și idei; a se vedea, de asemenea, OOO Flavus și alții împotriva Rusiei, pct. 40-43). Urmare a analizei conținutul proiectului instrucțiunii, Avocatul Poporului intervine cu unele sugestii din	

		perspectiva abordării bazate pe drepturilor omului și prevenirii unor eventuale încălcări: 1. Din perspectiva principiului previzibilității și clarității, în virtutea criteriilor prevăzute la art. 4^2 din Legea nr. 20/2009 care determină eligibilitatea unei pagini și justificarea acțiunii de sistare/eliminare a conținutului, se recomandă reglementarea în cuprinsul Ordinului de sistare și/sau a Actului privind examinarea paginii, a următoarelor aspecte: - Criteriul concret din cuprinsul celor prevăzute la art. 42 din Legea nr. 20/2009, cu relevanță la speța concretă, care constituie temei pentru sistare/eliminarea conținutului; - Informația concretă existentă (cu tangență la pregătirea/comiterea infracțiunii) și cum aceasta se raportează/încadrează în criteriul ce constituie temei legal de sistare/eliminarea conținutului. În pofida faptului că legea prevede expres criteriile în temeiul cărora se determină că o pagină web conține "informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor", proiectul Instrucțiunii nu conține reglementări subsecvente privind reglementarea modului/procedurii în conformitate cu care se califică "pertinența" informațiilor concrete în fiecare speță individual.	
	2.	2. În scopul evitării unor conflicte de competență și/sau unor suprapuneri în exercitarea funcțiilor atribuite, se recomandă reglementarea expresă a atribuțiilor de intervenție a celor două autorități competente, precum și interacțiunea dintre acestea și interacțiunea cu furnizorii de servicii. Deși în art. 4 din Lege nr. 20/2009 sunt menționate funcțiile acestor autorități, instrucțiunea nu vizează detalii referitor la	**Nu se acceptă** Potrivit prevederilor art. 4 al Legii nr. 20/2009, atât Ministerul Afacerilor Interne, cât și Serviciul de Informații și Securitate pot dispune prin Ordinul conducătorul subdiviziunii specializate

		atribuțiile/repartizarea domeniilor de competență a fiecăreia și modul cum vor interacționa.	sistarea accesului la pagina web sau eliminarea conținutului online la sursă în baza criteriilor menționate la art. 4^2 din aceiași lege. Prin urmare, nu există domenii de competență distinctă în partea Ministerului Afacerilor Interne sau Serviciului de Informații și Securitate și nu este clară necesitatea unei asemenea delimitări.
	3.	3. Din punct de vedere al respectării principiului transparenței, considerăm oportun includerea prevederilor privind condiția de publicare în Monitorul Oficial a Ordinului de eliminare a conținutului/sistare a accesului la pagina web.	**Nu se acceptă** Presupune costuri suplimentare ce nu sunt necesare. În plus, principiul transparenței este asigurat prin faptul că, după emiterea Ordinul conducătorul subdiviziunii specializate privind sistarea accesului la pagina web sau eliminarea conținutului online la sursă, accesarea paginii web sistate te redirecționează la pagina web dedicată a autorității respective, unde sunt informații despre autoritatea publică emitentă, circumstanțele de fapt și de drept ce au stat la baza emiterii Ordinului, precum și alte informații.

	4.	4. Suplimentar, se recomandă specificarea faptului că măsurile de blocare să fie ultima ratio și să se prioritizează pe eliminarea conținutului ilegal și nu la întregul site pentru a evita încălcarea principiului proporționalității.	**Se acceptă** Acest fapt este consacrat în principiile reglementate de prevederile art. 4^1 din Legea nr. 20/2009.
	5.	5. În partea ce vizează procedura de contestare a Ordinului de eliminare a conținutului/sistare a accesului la pagina web, semnalăm asupra neconcordanței dintre prevederile legii și cele ale instrucțiunii. Astfel, art. 4^3 din Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice reglementează expres procedura de contestare a ordinului vizat, specificând la alin. (7) că "Prevederile Codului administrativ se aplică în măsura în care nu contravin prevederilor prezentei legi". Totodată, pct. 11 din proiectul Instrucțiunii stipulează că „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". În contextul în care legea deja reglementează procedura de contestare și face referire la contencios ca excepție, instrucțiunea nu poate institui "regula" procedurii de contencios. Respectiv, pentru asigurarea caracterului clar și previzibil al legii, se propune aducerea în concordanță a prevederilor pct. 11 din proiectul Instrucțiunii cu prevederile art. 42 din lege. În lumina celor expuse, Avocatul Poporului consideră judicios examinarea oportunității includerii propunerilor formulate.	**Se acceptă** Instrucțiunea a fost modificată conform prevederilor Legii nr. 20/2009.
Poziția autorităților avizatoare expusă în virtutea pct. 231 din Regulamentul Guvernului aprobat prin Hotărârea Guvernului nr. 610/2018			

Ministerul Culturii	**1.**	În baza pct. 231 din Regulamentul Guvernului aprobat prin Hotărârea Guvernului nr. 610/2018, lipsă de obiecții și propuneri.	**S-a luat act**
Ministerul Muncii și Protecției Sociale	**1.**	În baza pct. 231 din Regulamentul Guvernului aprobat prin Hotărârea Guvernului nr. 610/2018, lipsă de obiecții și propuneri.	**S-a luat act**
Ministerul Dezvoltării Economice și Digitalizării		În baza pct. 231 din Regulamentul Guvernului aprobat prin Hotărârea Guvernului nr. 610/2018, lipsă de obiecții și propuneri.	**S-a luat act**
Ministerul Educației și Cercetării	**1.**	Ministerul Educației și Cercetării a examinat repetat proiectul de hotărâre pentru aprobarea Instrucțiunii privind procedura de sistare a accesului la pagini web care conțin informații destinate si utilizate pentru pregătirea sau comiterea infracțiunilor si de eliminare a conținutului respectiv la sursă (număr unic 152/MAI/2025) și, în limitele competențelor, comunică lipsă de obiecții și propuneri.	**S-a luat act**
Ministerul Finanțelor	**1.**	În baza pct. 231 din Regulamentul Guvernului aprobat prin Hotărârea Guvernului nr. 610/2018, lipsă de obiecții și propuneri.	**S-a luat act**
Serviciul Tehnologia Informației și Securitate Cibernetică	**1.**	În baza pct. 231 din Regulamentul Guvernului aprobat prin Hotărârea Guvernului nr. 610/2018, lipsă de obiecții și propuneri.	**S-a luat act**
Consiliul Superior al Magistraturii	**1.**	La 11 aprilie 2025 Ministerul Afacerilor Interne al Republicii Moldova a adresat Consiliului Superior al Magistraturii un demers prin care a solicitat avizarea repetată a proiectului 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 (număr unic 152/MAI/2025). Autorul demersului a menționat că proiectul elaborat și definitivat însoțit de nota și sinteza obiecțiilor și	**S-a luat act**

		propunerilor se remite entităților publice, pentru examinare și avizare repetată. Consiliul Superior al Magistraturii reține că, prin Avizul din 18 martie 2025 a avizat proiectul actului normativ elaborat de Ministerul Afacerilor Interne, fiind înaintate unele obiecții pe marginea conținutului lui. Analizând proiectul definitiv al 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, precum și sinteza obiecțiilor și propunerilor, Consiliul Superior al Magistraturii constată că la definitivarea proiectului actului normativ sus-menționat s-a ținut cont de opiniile exprimate prin Avizul din 18 martie 2025 și de alte opinii și propuneri ale entităților publice implicate în procesul decizional, inclusiv de completarea Instrucțiunii cu prevederi ce țin de sistarea accesului la paginile web destinate utilizate pentru pregătirea sau comiterea infracțiunilor din Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice. Din raționamentele expuse supra, Consiliul Superior al Magistraturii avizează repetat 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 (număr unic 152/MAI/2025), fără a înainta careva propuneri și/sau obiecții. Avizul se remite Ministerului Afacerilor Interne al Republicii Moldova, Cancelariei de Stat și se publică pe pagina web a Consiliului Superior al Magistraturii (www.csm.md).	

Procuratura Generală	**1.**	În baza pct. 231 din Regulamentul Guvernului aprobat prin Hotărârea Guvernului nr. 610/2018, lipsă de obiecții și propuneri.	**S-a luat act**
Serviciul Informații și Securitate		Serviciul Informații și Securitate, a examinat repetat proiectul de hotărârii de Guvern pentru aprobarea Instrucțiunii privind procedura de sistare a accesului la pagini web care conțin informații destinate si utilizate pentru pregătirea sau comiterea infracțiunilor si de eliminare a conținutului respectiv la sursă (număr unic 152/MAI/2025) și Vă comunică lipsă de obiecții.	**S-a luat act**
		Expertizare	
Centrul Național Anticorupție	**1.**	**RAPORT DE EXPERTIZĂ ANTICORUPŢIE** Nr. EHG25/10514 din 23.04.2025 la proiectul de hotărâre a Guvernului 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 (număr unic 152/MAI/2025) Prezentul raport de expertiză anticorupție a fost întocmit de Centrul Național Anticorupție al Republicii Moldova în baza Legii nr.100/2017 cu privire la actele normative, a Legii nr.1104/2002 cu privire la Centrul Național Anticorupție, a Legii integrității nr.82/2017 și a Metodologiei de efectuare a expertizei anticorupție a proiectelor de acte legislative și normative, aprobată prin Hotărârea Colegiului Centrului nr.6 din 20 octombrie 2017. **I. Analiza riscurilor de corupere a procesului de promovare a proiectului**	**S-a luat act** de partea introductivă a Raportului de expertiză. Detalii suplimentare sunt oferite la compartimentul III din Raportul de expertiză, unde s-a abordat fiecare obiecție formulată de Centrul Național Anticorupție.

		I.1. Pertinența autorului, categoriei propuse a actului și a procedurii de promovare a proiectului Autor al proiectului de act normativ este Guvernul, iar autor nemijlocit este Ministerul Afacerilor Interne, ceea ce corespunde art.102 din Constituție, art.14 din Legea nr.100/2017 cu privire la actele normative. Categoria actului normativ propus este Hotărâre a Guvernului, ceea ce corespunde art.102 din Constituție, art.6 și art.14 din Legea nr.100/2017 cu privire la actele normative. *I.2. Respectarea rigorilor de transparență în procesul decizional la promovarea proiectului* Potrivit art.8 al Legii nr.239/2008 privind transparența în procesul decizional „etapele asigurării transparenței procesului de elaborare a deciziilor sunt: a) informarea publicului referitor la inițierea elaborării deciziei; b) punerea la dispoziția părților interesate a proiectului de decizie și a materialelor aferente acestuia; c) consultarea cetățenilor, asociațiilor constituite în corespundere cu legea, altor părți interesate; d) examinarea recomandărilor cetățenilor, asociațiilor constituite în corespundere cu legea, altor părți interesate în procesul de elaborare a proiectelor de decizii; e) informarea publicului referitor la deciziile adoptate". Totodată, art.10 din Legea nr.239/2008 stabilește expres că: „(1) Autoritatea publică asigură accesul la proiectele de decizii și la materialele aferente acestora prin publicarea obligatorie a lor pe pagina web oficială a autorității publice, prin asigurarea accesului la sediul autorității, precum și prin	

		expediere prin poştă sau prin alte mijloace disponibile, la solicitarea persoanei interesate. (2) Proiectul de decizie şi materialele aferente acestuia se plasează pe pagina web oficială a autorităţii publice responsabile cel puţin pentru perioada recepţionării şi examinării recomandărilor". În contextul normei de la art. 9 al Legii nr. 239 din 13 noiembrie 2008 privind transparența în procesul decizional, potrivit căreia: „După inițierea procesului de elaborare a deciziei, autoritatea publică va plasa, în termen de cel mult 15 zile lucrătoare, anunțul respectiv pe pagina web oficială [...]”, menționăm că autorul proiectului a asigurat informarea publicului referitor la inițierea elaborării prezentului proiect de hotărâre. În acest sens, autorul a publicat un anunț pe portalul guvernamental www.particip.gov.md, la 14 noiembrie 2024 și, repetat, la 18 martie 2025. Totodată, proiectul supus expertizei anticorupție lipsește atât pe pagina web oficială a ministerului, cât și pe portalul guvernamental www.particip.gov.md. Prin urmare, în procesul de promovare a proiectului, n-au fost respectate rigorile de asigurare a transparenței decizionale prevăzute la art. 11 alin. (22) și art. 12 alin. (2) al Legii nr. 239/2008 privind transparența în procesul decizional. *I.3. Scopul anunţat şi scopul real al proiectului* În nota de fundamentare autorul a menționat că proiectul are drept 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.	

		Analizând normele elaborate s-a constatat că prin proiect se propune aprobarea procedurilor pentru identificarea paginilor web care conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor, în vederea implementării măsurilor de sistare a accesului sau eliminare a conținutului la sursă. Prin urmare, conchidem că scopul declarat de către autor în nota de fundamentare corespunde scopului real al proiectului. *I.4. Interesul public şi interesele private promovate prin proiect* Prevederile proiectului promovează interesele Guvernului, în ceea ce privește apropierea Republicii Moldova de standardele Uniunii Europene de prevenire și combatere a criminalității informatice/cibernetice, prin perfecționarea mecanismului de sistare a accesului la paginile web destinate și utilizate pentru pregătirea sau comiterea infracțiunilor. Prin urmare, promovarea intereselor menționate supra nu este în detrimentul interesului public în cazul în care prevederile proiectului vor fi aplicate cu respectarea strictă a cadrului legal, adică evitarea unor eventuale abuzuri din partea entităților responsabile de sistarea accesului la paginile web. *I.5. Justificarea soluțiilor proiectului* *I.5.1. Suficienţa argumentării din nota informativă.* În conformitate cu art.30 al Legii nr.100/2017 cu privire la actele normative, proiectele de acte normative sunt însoțite de „nota de fundamentare care cuprinde:	

		a) denumirea sau numele autorului și, după caz, a/al participanților la elaborarea proiectului actului normativ; b) condițiile ce au impus elaborarea proiectului actului normativ; c) obiectivele urmărite și soluțiile propuse; d) analiza impactului de reglementare; e) compatibilitatea proiectului actului normativ cu legislația UE; f) avizarea și consultarea publică a proiectului actului normativ; h) modul de încorporare a actului în cadrul normativ existent; i) măsurile necesare pentru implementarea prevederilor proiectului actului normativ." În nota de fundamentare sunt specificate: denumirea autorului, condițiile care au impus elaborarea proiectului actului normativ, obiectivele urmărite și soluțiile propuse, analiza impactului de reglementare, avizarea și consultarea publică a proiectului actului normativ. Astfel, considerăm că nota de fundamentare conține o justificare suficientă a necesității promovării proiectului de act normativ. *I.5.2. Argumentarea economică-financiară.* Conform art.30 lit.d) al Legii nr.100/2017 cu privire la actele normative, nota de fundamentare trebuie să conțină „d) analiza impactului de reglementare". În nota de fundamentare autorul a menționat că implementarea în practică a normelor proiectului nu necesită alocarea mijloacelor financiare suplimentare din bugetul de stat. *II. Analiza generală a factorilor de risc ale proiectului* *II.1. Limbajul proiectului*	

		Potrivit art.54 al Legii nr.100/2017 cu privire la actele normative „textul proiectului actului normativ se elaborează [...] cu respectarea următoarelor reguli: [...] a) se expune într-un limbaj simplu, clar şi concis [...] c) terminologia utilizată este constantă, uniformă și corespunde celei utilizate în alte acte normative, în legislația Uniunii Europene și în alte instrumente internaționale la care Republica Moldova este parte, cu respectarea prevederilor prezentei legi; [...] e) se interzice folosirea neologismelor dacă există sinonime de largă răspândire, [...] f) se evită folosirea [...] a cuvintelor și expresiilor [...] care nu sînt utilizate sau cu sens ambiguu; g) se evită tautologiile juridice; h) se utilizează, pe cât este posibil, noțiuni monosemantice, [...]". În textul proiectului a fost fost identificată a formulare ambiguă care la aplicare va admite interpretări abuzive. Mai detaliat la acest aspect ne vom referi la compartimentul III din prezentul raport de expertiză anticorupție. *II.2. Coerența legislativă a proiectului* În textul proiectului au fost identificată o neconcordanță între normele acestuia. Mai detaliat la acest aspect ne vom referi la compartimentul III din prezentul raport de expertiză anticorupție. *II.3. Activitatea agenţilor publici şi a entităților publice reglementată în proiect* Prevederile proiectului reglementează activitatea subdiviziunilor specializate în prevenirea și combaterea criminalității informatice, din cadrul Ministerului Afacerilor Interne și Serviciului de Informații și Securitate, responsabile de identificarea și sistarea accesului la paginile web ce conțin	

		informații destinate și utilizate pentru comiterea infracțiunilor, precum și de eliminare a conținutului respectiv la sursă. *II.4. Atingeri ale drepturilor omului care pot fi cauzate la aplicarea proiectului* Prevederile proiectului nu aduc atingere drepturilor fundamentale ale omului consacrate de Constituţia Republicii Moldova, Declaraţia Universală a Drepturilor Omului şi Convenţia Europeană a Drepturilor Omului.	
		III. Analiza detaliată a factorilor de risc și a riscurilor de corupție ale proiectului *Ca obiecție generală* *Obiecții:* Punctul 2 din proiectul Instrucțiunii, referindu-se la subiecții cărora se aplică prevederile acesteia, definește următoarele noțiuni: „furnizor de servicii de acces la Internet”, „furnizor de servicii de găzduire a conținutului”, „furnizor de conținut” și „furnizor de servicii/conținut”, ultima înglobînd furnizorii de servicii de acces la Internet, furnizorii de servicii de găzduire a conținutului online cât și furnizorii de conținut. Prin urmare, în cazul normelor generale, care se aplică tuturor furnizorilor enumerați supra, urmează să se utilizeze noțiunea „furnizor de servicii/conținut”. Însă, în textul proiectului autorul utilizează noțiuni diferite, inclusiv noțiuni eronate (nedefinite), fapt care face dificilă înțelegerea corectă a sensului normelor în ceea ce privește subiecții vizați și, în rezultat, aplicarea neuniformă a reglementărilor Instrucțiunii. Astfel, în proiect sunt utilizați în mod eronat/inoportun următorii termeni:	**Se acceptă** 1) la pct. 8, subpct. 8.6 – s-a utilizat noțiunea *furnizorii de servicii/ conținut*; 2) la pct. 9 subpct. 9.4 – s-a modificat cu *furnizorilor de servicii de acces la Internet și furnizorilor de servicii de găzduire a conținutului*; 3) la pct. 14 – modificat prin completarea normei că noțiunea corespunzătoare.

		-) „furnizorilor de servicii” – pct. 8, subpct. 8.6, pct. 9 subpct. 9.4, pct. 14 din proiectul Instrucțiunii; -) „furnizorilor de servicii de acces la Internet” – pct. 20 din proiectul Instrucțiunii; -) „furnizorului de servicii de găzduire a paginii web” – pct. 3 din anexa la proiectul Instrucțiunii. Utilizarea neuniformă a termenilor poate duce la apariția abuzurilor din partea exponenților atît din sectorul public, cît și a celui privat. *Recomandări:* Redactarea prevederilor proiectului prin prisma utilizării uniforme a noțiunilor. *Factori de risc:* ● Utilizarea neuniformă a termenilor *Riscuri de corupție:* ● Generale	
	2.	*La pct. 3 din proiectul Instrucțiunii* „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. 42 alin. (1) literele a)-g) din Legea nr. 20/2009 cu privire la prevenirea și combaterea criminalității informatice.” *Obiecții:* Articolul 54 alin. (1) lit. a) din Legea nr.100/2017 stabilește că la elaborarea textului proiectului de act normativ „conținutul proiectului se expune într-un limbaj simplu, clar și concis, pentru a se exclude orice echivoc [...]”.	**Se acceptă** Norma a fost modificată conform propunerii.

		Textul „poate fi considerată” oferă posibilitatea interpretării subiective a sensului normei, precum și aplicării discreționare a acesteia de către reprezentanții subdiviziunilor specializate în prevenirea și combaterea criminalității informatice din cadrul Ministerului Afacerilor Interne și Serviciului de Informații și Securitate. Astfel, în lipsa unor reglementări clare, legiuitorul lasă la latitudinea agentului public responsabil să decidă dacă o pagină web este sau nu considerată ca fiind destinată și utilizată pentru pregătirea sau comiterea infracțiunilor, ceea ce implică riscul aplicării neuniforme a prevederilor Instrucțiunii, în dependență de interese, și luării unor decizii diferite în situații identice. *Recomandări:* Substituirea textului „poate fi considerată” cu textul „se consideră”. *Factori de risc:* ● Formulare ambiguă care admite interpretări abuzive *Riscuri de corupţie:* ● Încurajarea sau facilitarea actelor de: - corupere pasivă - trafic de influență - abuz de serviciu - conflict de interese și/sau favoritism - îmbogăţire ilicită - influențare necorespunzătoare - nerespectare a regimului cadourilor - escrocherie	

		- corupere activă	
	3.	*La pct. 13 din proiectul Instrucțiunii* „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.” *Obiecții:* Norma analizată nu este în concordanță cu prevederile pct. 6 din proiectul Instrucțiunii, care reglementează acțiunile subdiviziunii specializate întreprinse după identificarea uneia sau mai multor pagini web ce conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor. În acest context, menționăm că printre acțiunile enumerate la pct. 6 din proiect lipsește refuzul subdiviziunii specializate de a emite Ordinul de sistare a accesului sau de eliminare a conținutului la sursă, de unde rezultă că fiecare caz de identificare a unei pagini web ce conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor automat se finalizează cu emiterea Ordinului de eliminare a conținutului online la sursă și/sau Ordinului de sistare a accesului la paginile web ce conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor, ceea ce nu corespunde realității. Conflictul este un impediment în aplicarea corectă a prevederilor normative și creează premise pentru alegerea subiectivă și abuzivă a normei „convenabile” care se va aplica într-o situație concretă. *Recomandări:* Completarea pct. 6 din proiectul Instrucțiunii în vederea specificării refuzului subdiviziunii specializate de a	**Se acceptă** pct. 6 a fost completat conform obiecției: „*6.2.3. dispune refuzul emiterii Ordinului de eliminare a conținutului la sursă sau Ordinului de sistare a accesului*.”

		emite Ordinul de sistare a accesului sau de eliminare a conținutului la sursă, ca acțiune întreprinsă de aceasta după identificarea uneia sau mai multor pagini web ce conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor. *Factori de risc:* ● Concurenţa normelor de drept *Riscuri de corupţie:* ● Încurajarea sau facilitarea actelor de: - abuz de serviciu - influențare necorespunzătoare	
		IV. Concluzia expertizei Proiectul hotărârii Guvernului 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 scopul creării 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. Proiectul corespunde normelor de tehnică legislativă și respectă parțial rigorile de transparență impuse de Legea nr.239/2008 privind transparența în procesul decizional. Proiectul corespunde interesului public general, în cazul în care prevederile acestuia vor fi aplicate cu respectarea strictă a cadrului legal, adică evitarea unor eventuale abuzuri din partea entităților responsabile de sistarea accesului la paginile web.	**Se acceptă** proiectul a fost modificat conform propunerilor formulate de Centrul Național Anticorupție, a se vedea a compartimentul nr. III din Raportul de expertiză.

		În normele proiectului supus expertizei anticorupție au fost identificați următorii factori de corupție: – utilizarea neuniformă a termenilor; – formulare ambiguă care admite interpretări abuzive; – concurența normelor de drept. În scopul preîntâmpinării apariției manifestărilor de corupție la aplicarea în practică a prevederilor proiectului, considerăm oportună redactarea acestuia în contextul obiecțiilor și recomandărilor din prezentul raport de expertiză anticorupție.	
Ministerul Justiției	**1.**	Urmare examinării proiectului hotărârii Guvernului 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 (număr unic 152/MAI/2025), comunicăm următoarele. Potrivit notei de fundamentare ce însoțește proiectul de act normativ, elaborarea proiectului de hotărâre, este necesară în vederea reglementării detaliate a procedurii 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 context, potrivit prevederilor din Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice, 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	**Nu se acceptă** proiectul Instrucțiunii nu excedă temei juridic menționat la Art. II alin. (2) din Legea nr. 200/2024 pentru modificarea Legii nr. 20/2009 privind prevenirea și combaterea criminalității informatice, conform căruia „*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.*”. Există o continuitate logică care nu poate fi negată și care pornește de la identificarea

		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 acestui proiect de hotărâre a Guvernului, 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, proiectul de hotărâre are ca scop definitivarea și 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. În contextul examinării proiectului, la definitivarea acestuia se vor lua în considerare următoarele obiecții și recomandări: Inițial, se remarcă faptul că în calitate de temei juridic este invocat Art. II alin. (2) din Legea nr. 200/2024 pentru modificarea Legii nr. 20/2009 privind prevenirea și combaterea criminalității informatice, conform căruia „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.”. Raportat la obiectul proiectului de act normativ reglementat la pct. 1, aspectul ce vizează „procedurile pentru identificarea paginilor web care conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor” excedă obligația impusă Guvernului de aprobare a	paginilor web compromise și culminează cu emiterea Ordinului de eliminare a conținutului la sursă sau a Ordinului de sistare a accesului. Literalmente, nici nu se poate de conceput o procedură de emitere a Ordinului de eliminare a conținutului la sursă sau a Ordinului de sistare a accesului fără existența unei pagini web compromise. Avizatorul este chemat să admită faptul că la elaborarea Legii nr. 200/2024 pentru modificarea Legii nr. 20/2009 – proiect expertizat de Ministerul Justiției, s-a admis neintenționat această formulare a temeiului juridic, care, doar interpretată extensiv, poate duce la concluziile exprimate de avizator. Mai mult ca atât, în Nota informativă a Legii nr. 200/2024, precum și în discuțiile interinstituționale desfășurate s-a abordat în repetate rânduri viitoarea Instrucțiune, adică prezentul proiect.

		Instrucțiunii 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. Or, ordinele sunt emise ulterior identificării paginilor web care conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor, iar executate - după emiterea acestora.	
	2.	La proiectul hotărârii, cuvintele „cu modificările ulterioare” se vor exclude din clauza de adoptare.	**Se acceptă**
	3.	Suplimentar, având în vedere pct. 3 din proiectul hotărârii și în temeiul art. 50 alin. (4) din Legea nr. 100/2017 cu privire la actele normative, din lista miniștrilor contrasemnatari se va exclude ministrul justiției.	**Se acceptă**
	4.	La proiectul 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: La pct. 3 cuvântul „literele” se va substitui cu abrevierea „lit.”, pentru a uniformiza trimiterile.	**Se acceptă**
	5.	La pct. 9, se recomandă completarea cu subpct. 9.6 cu următorul cuprins: „9.6. perioada sistării accesului la pagina web.” Necesitatea completării indicate supra, derivă din prevederile art. 41 alin. (2) din Legea nr. 20/2009 privind prevenirea și combaterea criminalității informative.	**Se acceptă**
	6.	Totodată, enumerările de la subpct. 9.1-9.5 vor începe cu literă mică.	**Se acceptă**
	7.	La pct. 12, se impune concretizarea actelor normative conform cărora va avea loc păstrarea actelor ce țin de punerea în aplicare a prevederilor Instrucțiunii.	**Nu se acceptă** proiectul Instrucțiunii se refera la subdiviziunile specializate în prevenirea și combaterea criminalității informatice ce sunt

			în subordinea a două autorități publice distincte: Ministerul Afacerilor Interne și Serviciul de Informații și Securitate. Aceste autorități publice păstrează actele în baza unor prevederi normative distincte. În plus, trimiterile generale sunt binevenite datorită caracterului lor general, adică o eventuală abrogare a acestora nu va impune modificarea prezentului proiect. De asemenea, norma examinată are un caracter simbolic, or prezența sau absența acesteia nu exclude obligativitatea reprezentanților autorităților publice menționate de la păstrarea documentelor pe care le emit.
	8.	La pct. 14, cuvintele „fără întârzieri” se apreciază ca fiind vagi în contextul obligației furnizorilor de servicii de a informa autoritatea emitentă a ordinului cu privire la modul în care s-a dat curs acestuia. Astfel, se impune precizarea perioadei în vederea informării autorității emitente a ordinului de sistare a accesului sau de eliminare a conținutului la sursă.	**Se acceptă**
	9.	La pct. 18 alineatul doi abrevierea „pct.” se va substitui cu abrevierea „subpct.”.	**Se acceptă**
	10.	Potrivit pct. 21 din Instrucțiune, „Prin derogare de la prevederile pct. 6 și 17, eliminarea conținutului online la sursă sau sistarea accesului la pagini web concepute în	**Se acceptă** pct. 21 de Instrucțiune a fost modificat prin eliminarea

		întregime pentru distribuirea materialelor privind abuzul sexual asupra copilului (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." Privitor la acest aspect, se atenționează că norma indicată contravine prevederilor art. 4^1 alin. (2) din Legea nr. 20/2009 privind prevenirea și combaterea criminalității informative. Astfel, potrivit normei nominalizate, „Sistarea accesului la o pagină web ce cuprinde informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor poate fi dispusă pe un termen de 30 de zile, cu posibilitatea prelungirii acestuia, dar nu mai mult de 90 de zile. Fiecare prelungire nu poate depăși termenul de 30 de zile." În acest sens, se notează că, potrivit art. 3 alin. (4) din Legea nr. 100/2017 cu privire la actele normative, „Actul normativ trebuie să se integreze organic în cadrul normativ în vigoare, scop în care: a) proiectul actului normativ trebuie corelat cu prevederile actelor normative de nivel superior sau de acelaşi nivel cu care se află în conexiune; b) proiectul actului normativ întocmit în temeiul unui act normativ de nivel superior nu poate depăşi limitele competenţei instituite prin actul de nivel superior şi nici nu poate contraveni scopului, principiilor şi dispoziţiilor acestuia.". Or, în eventualitatea în care un act normativ inferior (hotărârea de Guvern) contrazice un act normativ superior (o lege), actul normativ inferior nu poate prevala asupra	textului „ *, pe o perioadă nelimitată de timp*". În acest mod, termenul de sistare va fi cel prevăzut de art. 4^1 alin. (2) din Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice.

		dispozițiilor actului superior. În astfel de situații, actul inferior este considerat ineficient în raport cu actul superior. Prin urmare, având în vedere cele menționate supra, se impune a fi revizuită norma de la pct. 21 din 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, în vederea neadmiterii unor contradicții dintre prevederile Instrucțiunii și Legea nr. 20/2009 privind prevenirea și combaterea criminalității informative.	
	11.	La Anexa 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 vederea trimiterii corecte la prevederile Instrucțiunii, textul „pct. 7” se va substitui cu textul „pct. 6”.	**Se acceptă**

Ministru afacerilor interne **Daniella MISAIL-NICHITIN**