



Republic of Moldova, Chișinău, MD-2012, 134, Ștefan cel Mare și Sfânt Ave.  
Phone: +373 22 820 026, email: [office@egov.md](mailto:office@egov.md), web: <http://www.egov.md>

Nr. 3007 – 32 din 22.02.2023  
La nr. \_\_\_\_\_ din \_\_\_\_\_

Ministerul Afacerilor Interne

*copie: Cancelaria de Stat*

La indicația Cancelariei de Stat nr. 18-69-1458 din 10.02.2023, Instituția publică „Agenția de Guvernare Electronică” a examinat **proiectul de hotărâre a Guvernului cu privire la aprobarea proiectului de lege pentru modificarea Legii nr.20/2009 privind prevenirea și combaterea criminalității informatice (număr unic 104/MAI/2023), autor – Ministerul Afacerilor Interne, remis spre avizare, și, în limitele competențelor Agenției comunicăm că îl susținem în principiu.**

Totodată, propunem ca, la definitivarea proiectului, autorul să ia în considerare observațiile și propunerile Asociației Naționale a Companiilor din sectorul TIC (ATIC) față de intervenția propusă, expuse în documentul de analiză a impactului de reglementare la proiectul de lege, în partea ce ține de oportunitatea completării proiectului cu amendamente:

- la art.7 alin.(1) lit.e<sup>1</sup>) din Legea nr.20/2009 în scopul limitării temeiurilor pentru sistarea accesului la paginile web;

- la Codul de procedură penală al Republicii Moldova nr.122/2003 pentru detalierea condițiilor de aplicare de către autoritățile competente a măsurii de sistare a accesului la paginile web și pentru reglementarea procedurii și garanțiilor procesuale pentru conservarea rapidă a datelor informatice.

Directoare

Digitally signed by Tumuruc Olga  
Date: 2023.02.22 13:48:22 EET  
Reason: MoldSign Signature  
Location: Moldova



Olga TUMURUC

Ex.: Eduard Fricatel,  
e-mail: [eduard.fricatel@egov.md](mailto:eduard.fricatel@egov.md),  
tel.: 0794 38 138



Nr. 02 - DCAJ / 278

23 februarie 2023

la Nr. \_\_\_\_\_

**Ministerul Afacerilor Interne**  
[secretariat@mai.gov.md](mailto:secretariat@mai.gov.md)

*Spre informare:*  
**Cancelaria de Stat**  
[cancelaria@gov.md](mailto:cancelaria@gov.md)

Referitor la solicitarea Cancelariei de Stat nr. 18-69-1458 din 10 februarie 2023<sup>1</sup> de avizare la proiectul de *Lege pentru modificarea Legii nr. 20/2009 privind prevenirea și combaterea criminalității informatice (număr unic 104/MAI/2023)*, Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației (ANRCETI), ținând cont de domeniile de competență date prin lege, în conformitate cu dispozițiile art. 33 din Legea cu privire la actele normative nr. 100/2017, susține proiectul cu următoarele propuneri.

Considerăm că modificarea art. 7 alin. (1) lit. e<sup>1</sup>), prin excluderea textului „în condițiile legii” și, în consecință, propunerea autorului proiectului de a sista (bloca) accesul la paginile *web* conform unei instrucțiuni, aprobate de Guvern [art. II alin. (2) din proiect], nu reflectă exigențele privind calitatea legii, prescrisă de prevederile Legii nr. 100/2017.

În această ordine de idei, conform cerințelor art. 3 alin. (3) și art. 30 alin. (1) lit. c) din Legea nr. 100/2017, autorul proiectului urmează să asigure *compatibilitatea* legislației naționale cu *legislația Uniunii Europene*, în acest scop, este util de a releva că potrivit *aquis*-ului european<sup>2</sup>, în special, ar trebui să se asigure faptul că sarcinile impuse furnizorilor de servicii de acces la internet în cauză nu sunt nerezonabile, că necesitatea și proporționalitatea ordinelor de sistare/ blocare sunt evaluate în mod riguros și după emiterea lor și că atât furnizorii, cât și utilizatorii afectați dispun de o cale de atac și de mecanisme extrajudiciare de contestare, prescris prin act normativ la *nivel de lege*.

Mai mult decât atât, având în vedere că potrivit art. 26 alin. (2) în corelare cu art. 37 alin. (3) lit. a) din Legea nr. 100/2017, autorul proiectului trebuie să asigure

<sup>1</sup> înregistrată la ANRCETI cu nr. 248-e din 10.02.2023.

<sup>2</sup> (i) Directiva 2011/93/UE a Parlamentului European și a Consiliului din 13 decembrie 2011 privind combaterea abuzului sexual; (ii) Regulamentul (UE) 2021/784 al Parlamentului European și al Consiliului din 29 aprilie 2021 privind prevenirea diseminării conținutului online cu caracter terorist și (iii) Regulamentul (UE) 2021/1232 al Parlamentului European și al Consiliului din 14 iulie 2021 privind o derogare temporară de la anumite dispoziții ale Directivei 2002/58/CE în ceea ce privește utilizarea tehnologiilor de către furnizorii de servicii de comunicații interpersonale care nu se bazează pe numere pentru prelucrarea datelor cu caracter personal și a altor date în scopul combaterii abuzului sexual online asupra copiilor.

concordanța între proiectul actului normativ cu prevederile Constituției, dar și cu jurisprudența Curții Constituționale, este relevant că potrivit art. 72 din Constituție, prin lege organică se reglementază căile de atac ale actelor autorităților publice, respectiv regimul juridic al *ordinelor de sistare/ blocare*, emise de autorități competente, urmează a fi reglementate de acte normative de nivel legislativ.

Nu în ultimul rând, având în vedere dispozițiile art. 3 alin. (1) lit. c) și alin. (4) lit. a) din Legea nr. 100/2017, care dispun că întru asigurarea echilibrului între reglementările concurente, proiectul legislativ trebuie să se integreze organic în cadrul normativ în vigoare, scop în care, urmează să fie corelat cu prevederile actelor normative cu care se află în *conexiune*, reprezintă relevanță că prin Legea nr. 245/2020, s-a transpus art. 2-5 din Regulamentul (UE) 2015/2120 al Parlamentului European și al Consiliului din 25 noiembrie 2015 de stabilire a unor măsuri privind accesul la Internetul deschis.

Or, conform obiectivului Regulamentului (UE) 2015/2120, acesta urmărește garantarea drepturilor utilizatorilor finali de a accesa Internetul *fără restricții*.

Aceasta nu înseamnă că furnizorii de servicii de acces la Internet nu vor avea obligația de a bloca accesul la Internet la un anumit conținut, anumite aplicații sau servicii ori anumite categorii ale acestora, pentru a respecta *legislația în vigoare* sau măsurile menite să pună în aplicare legislația *în vigoare*, inclusiv hotărârile judecătorești sau actele autorităților publice competente – art. 20 alin. (2<sup>3</sup>) lit. a) în corelare cu art. 64 alin. (2<sup>1</sup>) a 2-a teză și alin. (3) din Legea nr. 241/2007 (în redacția Legii nr. 245/20020).

Așa fiind, autorul proiectului urmează a ține cont că, organele de urmărire penală și subiecții care efectuează activitatea specială de investigații, pot interveni în activitatea furnizorilor de servicii de acces la Internet *exclusiv* dacă aceștia se găsesc sub incidența actelor *legislative speciale* (sectoriale) referitoare la *legalitatea* conținutului, a aplicațiilor sau a serviciilor, sau referitoare la siguranța publică, *în special a dreptului penal*, care prevăd **expres**, blocarea anumitor conținuturi, aplicații sau servicii.

**Director adjunct**

Digitally signed by Bojoga Silvia  
Date: 2023.02.23 15:17:53 EET  
Reason: MoldSign Signature  
Location: Moldova



**Silvia BOJOGA**



**AGENȚIA SERVICII PUBLICE A REPUBLICII MOLDOVA**  
**PUBLIC SERVICES AGENCY OF THE REPUBLIC OF MOLDOVA**

MD-2012, mun. Chișinău, str. Aleksandr Pușkin, nr. 42

42 Aleksandr Pushkin str., MD-2012 Chisinau

tel.: +373 22 50 46 54, fax: +373 22 21 22 59, e-mail: asp@asp.gov.md, web: asp.gov.md

06.03.2023

Nr. 01/0327

18-69-1458

10.02.2023

**Cancelaria de Stat**

**Ministerul Afacerilor Interne**

Agencia Servicii Publice a examinat, în limita atribuțiilor funcționale, proiectul de hotărâre a Guvernului *cu privire la aprobarea proiectului de lege pentru modificarea Legii nr.20/2009 privind prevenirea și combaterea criminalității informatice* (număr unic 104/MAI/2023) și vă comunică despre susținerea proiectului enunțat în lipsa obiecțiilor și propunerilor.

**Director adjunct**

Digitally signed by Talmaci Francisco  
Date: 2023.03.06 16:09:55 EET  
Reason: MoldSign Signature  
Location: Moldova



**Francisco TALMACI**



**ASOCIAȚIA NAȚIONALĂ  
A COMPANIILOR DIN  
DOMENIUL TIC**

str. Studenților, 9/11  
MD 2045, mun. Chișinău,  
Republica Moldova

Nr. de înregistrare:  
MD 0056763  
IDNO: 1006600034927

**BC Moldindconbank SA**  
fil. Centru, Chișinău  
MOLDMD2X309  
Cont: 222440923

Nr.440

Data 14.12.2022

**Ministerul Afacerilor Interne**

Republica Moldova,

MD-2012, mun. Chișinău, Bd. Ștefan cel Mare și Sfânt 75

***Ref: modificarea Legii nr. 20/2009 privind prevenirea și combaterea criminalității informatice***

Din numele Asociației Naționale a Companiilor din sectorul TIC (ATIC) Vă adresăm cele mai înalte considerațiuni.

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

### **1. Sistarea accesului la paginile web**

ATIC susține, de principiu, stabilirea autorităților abilitate să dispună sistarea accesului la paginile web, precum și înlocuirea obligației de sistare a accesului la adresele IP pe care sunt amplasate paginile web contestate cu obligația de sistare a accesului la paginile web propriu-zise<sup>1</sup>. Totuși, aceste modificări nu sunt suficiente pentru a aduce această prevedere în conformitate cu normele internaționale și constituționale. Remarcăm că o normă similară cu cea stabilită la art. 7 alit. (1) lit. e<sup>1</sup>) din Legea nr. 20/2009<sup>2</sup> a fost examinată anterior de Comisia de la Veneția<sup>3</sup>, care a formulat mai multe observații și recomandări față de aceasta.

<sup>1</sup> A se vedea pct. 98 din avizul menționat mai jos.

<sup>2</sup> Potrivit art. 7 alit. (1) lit. e<sup>1</sup>) din Legea nominalizată, „furnizorii de servicii sînt obligați ... să sisteze, în condițiile legii, folosind metodele și mijloacele tehnice din posesie, accesul din propriul sistem informatic la toate adresele IP pe care sunt amplasate pagini web, inclusiv cele găzduite de furnizorul respectiv, ce contribuie la comiterea infracțiunilor sau la încălcarea prevederilor legislației în vigoare ori conțin/difuzează instrucțiuni privind modul de comitere a acestora”.

<sup>3</sup> Republica Moldova - Aviz comun al Comisiei de la Veneția și al Direcției Generale pentru Drepturile Omului și Statul de Drept (DGI) al Consiliului Europei cu privire la Proiectul de lege nr.161 de modificare și completare a legislației moldovenești în domeniul criminalității cibernetice, adoptat de Comisia de la Veneția la cea de-a 109-a sesiune plenară (Veneția, 9-10 decembrie 2016), pct. 74-75, 90-109 [www.venice.coe.int/webforms/documents/default.aspx?opinion=859&year=all&lang=EN](http://www.venice.coe.int/webforms/documents/default.aspx?opinion=859&year=all&lang=EN)

Notă: document semnat electronic în baza Legii Nr. 91 din 29.05.2014 privind semnătura electronică și documentul electronic. Verificarea semnăturii poate fi realizată la adresa: <https://msign.gov.md>

Potrivit Comisiei, în Recomandarea sa către statele membre privind măsurile de promovare a respectării libertății de exprimare și de informare în legătură cu filtrarea conținutului de pe Internet (CM/Rec(2008)6)<sup>4</sup>, Comitetul de Miniștri al Consiliului Europei a declarat, inter alia, că statele ar trebui să se abțină de la filtrarea conținutului de pe Internet din alte motive decât cele prevăzute la articolul 10, paragraful 2 Convenția Europeană a Drepturilor Omului (CEDO), astfel cum este interpretat de Curtea Europeană a Drepturilor Omului (CtEDO), și ar trebui să garanteze că măsurile generale de blocare sau filtrare la nivel național sunt introduse numai dacă condițiile de la articolul 10, paragraful 2 CEDO sunt îndeplinite<sup>5</sup>.

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

Potrivit Comisiei, aceasta înseamnă că trebuie prevăzute motive și garanții deosebit de puternice pentru limitarea accesului publicului la Internet, măsură care, făcând cantități mari de informații inaccesibile, restrânge substanțial drepturile utilizatorilor de internet și este probabil să aibă efecte colaterale semnificative<sup>6</sup>.

În opinia CtEDO, restricțiile, cum ar fi ordinele de blocare a internetului „*nu sunt neapărat incompatibile cu Convenția, ca principiu. Cu toate acestea, este necesar un cadru legal, care să asigure atât un control strict asupra întinderii interdicțiilor, cât și un control judiciar eficient pentru a preveni orice abuz de putere [...]. În această privință, controlul judiciar al unei astfel de măsuri, bazat pe o cântărire a intereselor concurente în joc și menit să stabilească un echilibru între ele, este de neconceput fără un cadru care să stabilească norme precise și specifice privind aplicarea restricțiilor preventive asupra libertății de exprimare [...]*” (Ahmet Yıldırım v. Turkey, Cerere Nr 3111/10, Hotărâre din 18.12.2012, § 67)<sup>7</sup>.

De asemenea, Recomandarea precizează că „*asa acțiuni de către stat ar trebui luate numai dacă filtrarea se referă la conținut specific și clar identificabil, o autoritate națională competentă a luat o decizie privind ilegalitatea acestuia și decizia poate fi revizuită de un tribunal sau de un organism de reglementare independent și imparțial, în conformitate cu cerințele articolului 6 din Convenția Europeană a Drepturilor Omului*”<sup>8</sup>.

---

<sup>4</sup> Result details (coe.int).

<sup>5</sup> A se vedea pct. 91 și 94 din aviz.

<sup>6</sup> A se vedea pct. 95 din aviz.

<sup>7</sup> A se vedea pct. 96 din aviz.

<sup>8</sup> A se vedea pct. 91 din aviz.

Totodată, în Recomandarea sa CM/Rec(2016)5 privind libertatea Internetului, Comitetul Miniștrilor subliniază că „înainte de a se aplica măsuri restrictive privind accesul la Internet, o instanță sau autoritate administrativă independentă stabilește că deconectarea de la Internet este cea mai puțin restrictivă măsură pentru atingerea scopului legitim”.<sup>9</sup>

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

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

De asemenea, Comisia de la Veneția recomandă excluderea prevederii potrivit căreia poate servi drept temei pentru sistarea accesului faptul că o pagină web “conține/difuzează instrucțiuni privind modul de comitere a [infracțiunilor]”.<sup>10</sup>

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

În al doilea rând, se impune detalierea condițiilor de aplicare a acestei măsuri. În acest scop, este necesară completarea Codului de procedură penală (în continuare – CPP). Observăm că art. 2 alin. (4) CPP stabilește că normele juridice cu caracter procesual din alte legi naționale pot fi aplicate numai cu condiția includerii lor în cod. În avizul său, Comisia de la Veneția, de asemenea, recomandă de a include cel puțin o parte din prevederile necesare în CPP<sup>11</sup>. Prin urmare, la art. 7 alit. (1) lit. e<sup>1</sup>) din Legea nr. 20/2009 trebuie păstrată sintagma „în condițiile legii”.

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

1. Stabilirea infracțiunilor sau categoriilor de infracțiuni pentru comiterea cărora se permite sistarea accesului la pagina web<sup>12</sup>.
2. Stabilirea procedurii de autorizare a măsurii de sistare a accesului (poate fi similară cu cea stabilită pentru autorizarea măsurilor procesuale de constrângere), inclusiv:

---

<sup>9</sup> A se vedea pct. 92 din aviz.

<sup>10</sup> A se vedea pct. 100 din aviz.

<sup>11</sup> A se vedea pct. 75 din aviz.

<sup>12</sup> A se vedea pct. 104 din aviz.

- a. organului abilitat de a autoriza asemenea măsură, la propunerea cui și prin care act procesual, de exemplu, ordonanța procurorului, emisă din oficiu sau la propunerea organului de urmărire penală, sau încheierea instanței de judecată, emisă la demersul procurorului)<sup>13</sup>.
  - b. etapei procesului penal la care este posibilă dispunerea unei asemenea măsuri, de exemplu, doar după pornirea urmăririi penale<sup>14</sup>.
  - c. elementelor pe care trebuie să le conțină actul procesual prin care se autorizează măsură respectivă, de exemplu, conținutul online ilicit sau activitatea ilicită desfășurată prin intermediul paginii web, încadrarea juridică a acestei activități, motivarea necesității aplicării acestei măsuri, precum și adresa URL a paginii web accesul la care trebuie sistat.
  - d. La soluționarea chestiunii privind necesitatea aplicării măsurii respective, procurorul și instanța de judecată trebuie să evalueze și să stabilească dacă măsura este proporțională cu circumstanțele individuale ale cauzei penale, inclusiv dacă sistarea accesului la pagina web este cea mai puțin restrictivă măsură pentru atingerea scopului legitim, de exemplu, dacă este posibilă eliminarea a conținutului online ilicit la sursă de către furnizorul acestuia sau de către furnizorul serviciilor de găzduire a conținutului online<sup>15</sup>.
  - e. Copia de pe ordonanța procurorului sau prin încheierea instanței de judecată trebuie adusă la cunoștința furnizorului de conținut online ilicit (dacă este posibilă identificarea acestuia), în termenul care să fie stabilit prin lege.
3. Stabilirea actului prin care se dispune măsura respectivă și conținutul acestuia.
  4. Stabilirea procedurii de atac a actelor privind autorizarea și dispunerea unei asemenea măsuri (poate fi similară cu cea stabilită pentru autorizarea măsurilor procesuale de constrângere)<sup>16</sup>. Recomandarea CM/Rec(2008)6 clarifică faptul că prevederea privind „mijloacele eficiente și ușor accesibile de recurs și remediere, inclusiv suspendarea filtrelor” este crucială pentru a răspunde „cazurilor în care utilizatorii și/sau autorii de conținut susțin că conținutul a fost blocat nerezonabil”.

<sup>13</sup> A se vedea pct. 99 și 108 din aviz.

<sup>14</sup> A se vedea pct. 99 din aviz.

<sup>15</sup> A se vedea pct. 99 și 105 din aviz.

<sup>16</sup> A se vedea pct. 107 din aviz.



5. Stabilirea procedurii de revocare și încetare a actelor privind autorizarea și dispunerea unei asemenea măsuri (poate fi similară cu cea stabilită pentru autorizarea măsurilor procesuale preventive), inclusiv temeiurile revocării și încetării, organul abilitat să dispună acest lucru, la propunerea cui și prin care act procesual. De exemplu, măsura se revocă de către organul care a dispus-o dacă temeiurile care au servit la aplicarea acesteia au dispărut și măsura nu mai este justificată, cu înștiințarea furnizorului de conținut online respectiv.

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

## **2. Conservarea datelor informatice și a datelor privind traficul informatic**

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

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

„Articolul [XXX]. Conservarea rapidă a datelor informatice

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

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

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

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

- a) autoritatea care solicită conservarea;
- b) persoana asupra căreia se pune obligația de conservare;
- c) infracțiunea care face obiectul urmăririi penale și prezentarea succintă a faptelor care au legătură cu aceasta;
- d) datele informatice specifice ce urmează a fi conservate, inclusiv numele și prenumele persoanei sau persoanelor ale căror date trebuie să fie conservate (dacă acestea sunt disponibile), genul de date care trebuie conservate, perioada de referință pentru care trebuie conservate datele;
- e) motivele dispunerii conservării: natura legăturii acestor date cu infracțiunea, motivarea îndeplinirii condițiilor prevăzute în alin. (2);

Notă: document semnat electronic în baza Legii Nr. 91 din 29.05.2014 privind semnătura electronică și documentul electronic. Verificarea semnăturii poate fi realizată la adresa: <https://msign.gov.md>

- f) obligația persoanei asupra căreia se pune obligația de conservare de a păstra datele informatice și de a le menține integritatea, cu păstrarea confidențialității cu privire la aplicarea acestei măsuri; și
  - g) perioada de păstrare a datelor informatice ce urmează a fi conservate.
- (5) Măsura conservării poate fi prelungită de către procuror o singură dată pentru motive temeinic justificate, pe o durată maximă de 90 de zile.
- (6) Extrasul din ordonanța procurorului, care trebuie să cuprindă informațiile specificate la literele a), b), d), f) și g) din alin. (4), se transmite persoanei în posesia sau sub controlul căreia se află datele stocate, aceasta fiind obligată să asigure conservarea lor rapidă, cu păstrarea confidențialității cu privire la aplicarea acestei măsuri.
- (7) În cazul în care în transmiterea comunicației au fost implicați mai mulți furnizori de servicii, procurorul, prin ordonanța de conservare sau o altă ordonanță, poate dispune dezvăluirea rapidă de către persoana în posesia sau sub controlul căruia se află datele referitoare la trafic a unei cantități de date referitoare la trafic, suficiente pentru a permite identificarea furnizorilor de servicii și a canalelor prin intermediul căruia comunicația a fost transmisă.
- (8) Procurorul este obligat să dispună încetarea conservării, înaintea expirării perioadei pentru care a fost dispusă, de îndată ce au dispărut temeiurile și motivele care au justificat-o.
- (9) Procurorul dispune ridicarea datelor conservate de la persoana care le-a conservat în termenul prevăzut în alin. (3) sau (5), după caz. Ridicarea datelor conservate se efectuează în conformitate cu prevederile art. 125-132.
- (10) Până la terminarea urmăririi penale, procurorul este obligat să anunțe, în scris, utilizatorii ale căror date au fost conservate.”

Rămânem la dispoziția autorităților pentru definitivarea proiectului în cauză, în concordanță cu rigorile internaționale și constituționale.

Cu respect,  
**Marina Bzovii**  
Director Executiv  
Asociația Națională Companiilor din Domeniul TIC

*Persoane de contact:*

*Marina Bzovii, email: mbzovii@ict.md*  
*Oxana Barbaros, email: obarbaros@ict.md*

Notă: document semnat electronic în baza Legii Nr. 91 din 29.05.2014 privind semnătura electronică și documentul electronic. Verificarea semnăturii poate fi realizată la adresa: <https://msign.gov.md>



Ministerul Economiei  
al Republicii Moldova

nr.07-508 din 24.02.2023

la nr. 18-69-1458 din 10.02.2023

**Ministerul Afacerilor Interne**

*copie: Cancelaria de Stat*

Cu referire la proiectul de hotărâre a Guvernului cu privire la aprobarea proiectului de lege pentru modificarea Legii nr. 20/2009 privind prevenirea și combaterea criminalității informatice (număr unic 104/MAI/2023), în limita competențelor funcționale, comunicăm despre susținerea obiectivului de reglementare a procedurii de sistare a accesului la conținut web cu caracter infracțional și a procedurii de dispunere a conservării datelor informatice.

În același timp, este imperativ ca modificările propuse să fie conformate cu normele internaționale și constituționale, în vederea garantării aplicării măsurilor generale de blocare sau filtrare a conținutului web la nivel național, cu condiția îndeplinirii prevederilor art. 10, paragraful 2 din Convenția Europeană a drepturilor Omului (CEDO), cât și prevederilor art. 32, 34 și 54 din Constituția Republicii Moldova.

În acest sens, exercitarea libertății de exprimare, libertății de opinie și libertatea de a primi sau a comunica informații pot fi supuse unor restrângeri sau sancțiuni stabilite de lege, prin măsuri necesare pentru asigurarea securității naționale, integrității teritoriale sau siguranței publice, apărării ordinii și prevenirii infracțiunilor, protecției sănătății, a moralei, a reputației sau a drepturilor altora, pentru a împiedica divulgarea informațiilor confidențiale sau pentru a garanta autoritatea și imparțialitatea puterii judecătorești.

În acest context, proiectul de lege urmează să detalieze condițiile de aplicare a normei propuse prin stabilirea infracțiunilor sau categoriilor de infracțiuni pentru comiterea cărora se va sista accesul la pagina web, cât și să stabilească cu claritate procedura de autorizare a măsurii de sistare a accesului.

**Secretar de stat**

Digitally signed by Gumene Vadim  
Date: 2023.02.24 17:16:27 EET  
Reason: MoldSign Signature  
Location: Moldova



**Vadim GUMENE**

Victoria Iorga,  
022 250 556



Ministerul Infrastructurii  
și Dezvoltării Regionale  
al Republicii Moldova

Nr. 09-1306 din 03.03.2023

La nr. 18-69-1458 din 10.02.2023

**Ministerului Afacerilor Interne**  
secretariat@mai.gov.md

**Copie: Cancelaria de Stat**  
cancelaria@gov.md

Cu referire la proiectul de hotărâre a Guvernului cu privire la aprobarea proiectului de lege pentru modificarea Legii nr.20/2009 privind prevenirea și combaterea criminalității informatice (**număr unic 104/MAI/2023**), comunicăm susținerea efortului de reglementare a procedurii de sistare a conținutului web cu caracter infracțional și a activităților de conservare a datelor informatice.

Totodată, considerăm că modificările propuse în proiectul de lege urmează să fie corelate cu normele internaționale și europene privind drepturile omului la libertatea de exprimare, garantată inclusiv de Constituția Republicii Moldova.

Astfel, se propune păstrarea la art.7 alin.(1) lit.e<sup>1</sup>) a textului „în condițiile legii”, deoarece Legea nr.20/2009 trebuie să conțină norme clare privind:

- stabilirea infracțiunilor și categoriile de infracțiuni pentru comiterea cărora se poate dispune sistarea accesului la paginile web;
- stabilirea procedurii de autorizare a activității de sistare a accesului la aceste pagini web.

Subsecvent, în contextul procesului de modificare a Anexei XXVIII B la Acordul de Asociere Republica Moldova - Uniunea Europeană în vederea ajustării legislației naționale în domeniul comunicațiilor electronice la acquis-ul european actualizat, este oportună transpunerea în cadrul normativ național a prevederilor Recomandării (UE) 2018/334 a Comisiei Europene din 1 martie 2018 privind măsuri de combatere eficace a conținutului ilegal online <https://is.gd/CaJpL0>.

Suplimentar, se propune modificarea art.7 alin.(1) lit.g) al Legii nr.20/2009, prin substituirea textului „de 90 de zile” prin textul „de cel mult 90 de zile”, pentru a aduce în concordanță cu prevederile art.16, pct.2 din Convenția Consiliului Europei privind criminalitatea informatică.

**Ministru**

Digitally signed by Dabija Lilia  
Date: 2023.03.07 21:43:03 EET  
Reason: MoldSign Signature  
Location: Moldova



**Lilia DABIJA**

Valeriu Gribincea, 022 250630



# Procuratura Republicii Moldova

Republica Moldova, MD-2001, mun. Chișinău, bd. Ștefan cel Mare și Sfânt, 73,  
tel.: (+373) 22-828-373, (+373) 22-828-375; e-mail: proc-gen@procuratura.md

28 februarie 2023 nr.4-1d/23-

169 Ministerul Afacerilor Interne

168 Copie: Cancelaria de Stat  
(la nr.18-69-1458)

Procuratura Generală a examinat *proiectul de hotărâre a Guvernului cu privire la aprobarea proiectului de lege pentru modificarea Legii nr.20/2009 privind prevenirea și combaterea criminalității informatice (număr unic 104/MAI/2023)*, remis spre avizare.

Apreciind conținutul proiectului prin prisma principiilor activității de legiferare prevăzute de art.3 din Legea nr.100/2017 cu privire la actele normative, în limita competențelor legale, expunem obiecțiile și propunerile indicate *infra*:

1. Potrivit proiectului, Ministerul Afacerilor Interne și Serviciul de Informații și Securitate (în continuare MAI și SIS) vor putea dispune prin intermediul subdiviziunilor sale centrale specializate în prevenirea și combaterea criminalității informatice sistarea accesului la pagini web în condițiile prevăzute la articolul 7 alineatul (1) litera e<sup>1</sup>) din Legea 20/2009.

Potrivit art.7 alineatul (1) litera e<sup>1</sup>) din Legea 20/2009:

„Furnizorii de servicii sînt obligați: să sisteze, în condițiile legii, folosind metodele și mijloacele tehnice din posesie, accesul din propriul sistem informatic la toate adresele IP pe care sunt amplasate pagini web, inclusiv cele găzduite de furnizorul respectiv, **ce contribuie la comiterea infracțiunilor sau la încălcarea prevederilor legislației în vigoare ori conțin/difuzează instrucțiuni privind modul de comitere a acestora;**”

Prin urmare, pentru a preveni eventuale abuzuri și/sau aprecieri arbitrare ale subdiviziunilor MAI și SIS în cazurile de sistare a accesului la anumite adresele IP pe care sunt amplasate pagini web, pentru alte motive decât cele prevăzute de art.7 alineatul (1) litera e<sup>1</sup>) din Legea 20/2009, considerăm oportună instituirea unui sistem adecvat de garanții și control asupra realizării acestei activități. Autorizarea de către un procuror desemnat din cadrul Procuraturii Generale a măsurii de sistare a accesului la pagini web, va contribui la prevenirea și contracararea abuzurilor, fiind asigurate garanții privind respectarea drepturilor și libertăților fundamentale.

2. Potrivit proiectului, art.4 alineatul (2) din Legea 20/2009 se completează cu textul „ , *dispune conservarea imediată a datelor informatice ori a datelor referitoare la traficul informatic* ”.

Analizând proiectul de lege cât și nota informativă a acestuia, se atestă lipsa unor precizări cu privire la perioada/termenele pentru care poate fi dispusă conservarea datelor informatice ori a datelor referitoare la traficul informatic și nici temeiurile/motivele în baza cărora poate fi dispusă conservarea datelor.

Mai mult, conservarea datelor informatice reprezintă o măsură secretă, făcută în condiții de confidențialitate, despre care persoanele vizate nu sunt înștiințate, și prin care pot fi conservate nu numai datele despre identitatea utilizatorului sau altei persoane, dar și date privind conexiunile sau chiar conținutul comunicațiilor. În consecință, acestea se află sub protecția art. 8 CEDO - Dreptul la respectarea vieții private și de familie.

În acest context, reținem jurisprudența Curții europene a drepturilor omului potrivit căreia în calitate de ingerință în dreptul la respectarea corespondenței pot include următoarele acte imputabile autorităților publice:

- controlul corespondenței (Campbell împotriva Regatului Unit, pct. 33), realizarea de copii (Foxley împotriva Regatului Unit, pct. 30) sau ștergerea anumitor pasaje (Pfeifer și Plankl împotriva Austriei, pct. 43);

- stocarea datelor interceptate referitoare la utilizarea telefonului, a adresei de e-mail și a internetului (Copland împotriva Regatului Unit, pct. 44). Simplul fapt că astfel de date pot fi obținute în mod legitim, de exemplu din facturile telefonice, nu constituie o piedică în calea constatării unei „ingerințe”; de asemenea, este irelevant faptul că informațiile nu au fost dezvăluite unor părți terțe sau nu au fost utilizate în cadrul unor proceduri disciplinare sau de altă natură împotriva persoanei în cauză (ibidem, pct. 43).

Așadar, statului îi revine obligația pozitivă de a proteja aceste date și a preveni abuzurile în raport cu ele.

Sub aspect comparat indicăm și practicile altor state (membre UE) în materia vizată.

Spre exemplu, în România conservarea datelor informatice constituie o acțiune procedurală, prevăzută la art. 154 al Codului de procedură penală al României<sup>1</sup>, care prevede:

„Dacă există o suspiciune rezonabilă cu privire la pregătirea sau săvârșirea unei infracțiuni, în scopul strângerii de probe ori identificării făptuitorului, suspectului sau a inculpatului, procurorul care supraveghează sau efectuează urmărirea penală poate dispune conservarea imediată a anumitor date informatice, inclusiv a datelor referitoare la traficul informațional, care au fost stocate prin intermediul unui sistem informatic și care se află în posesia sau sub controlul unui furnizor de rețele publice de comunicații electronice ori unui furnizor de servicii de comunicații electronice destinate publicului, în cazul în care există pericolul pierderii sau modificării acestora.”

Subsecvent, pentru a asigura respectarea garanțiilor prevăzute de art. 8 CEDO, legea procesuală a României prevede:

„Până la terminarea urmăririi penale, procurorul este obligat să încunoștințeze, în scris, persoanele față de care se efectuează urmărirea penală și ale căror date au fost conservate.”

În cazul pus în discuție urmează de ținut cont de faptul că obiectivul Legii 20/2009 privind prevenirea și combaterea criminalității informatice este de a reglementa raporturile juridice privind:

- a) prevenirea și combaterea infracțiunilor informatice;*
- b) cadrul de asistență mutuală în prevenirea și combaterea criminalității informatice, în protecția și acordarea de ajutor furnizorilor de servicii și utilizatorilor de sisteme informatice;*
- c) colaborarea autorităților administrației publice cu organizații neguvernamentale și cu alți reprezentanți ai societății civile în activitatea de prevenire și de combatere a criminalității informatice;*

---

<sup>1</sup> <https://legislatie.just.ro/Public/DetaliiDocument/120611>

*d) cooperarea cu alte state, cu organizații internaționale și regionale având competențe în domeniu.*

Prin urmare, după adoptarea legii în cauză și odată cu ratificarea de către Republica Moldova a Convenției Consiliului Europei privind criminalitatea informativă adoptată la Budapesta la 23.11.2001, prin Legea nr.6 din 02.02.2009, urma ca activul normativ național, în principal Codul de procedură penală să fie completat cu măsura de conservare în corespundere cu angajamentele externe ale Republicii Moldova atât la compartimentul combaterii crimei cibernetice, cât și al garantării drepturilor protejate ale omului.

Totodată, pentru reglementarea în Codul de procedură penală trebuie de luat în considerație necesitatea precizării tipurilor de infracțiuni pentru care poate fi dispusă conservarea datelor informatice ori a datelor referitoare la traficul informatic, subiectul autorizării (procurorul sau instanța de judecată), etc.

Reieșind din cele expuse, se constată că proiectul de lege supus dezbaterilor nu corespunde: principiului echilibrul între reglementările concurente; și principiului respectării drepturilor și libertăților fundamentale; prevăzute la art. 3 din Legea nr. 100 din 22.12.2017 cu privire la actele normative.

Procurorul General interimar



Ion MUNTEANU



**SERVICIUL DE INFORMAȚII ȘI SECURITATE  
AL REPUBLICII MOLDOVA**

---

MD-2004, Chișinău, bd. Ștefan cel Mare și Sfânt, 166 tel. 022-239-625, fax 022-234-068, e-mail: sis@sis.md

24 februarie 2023

Nr. E/1958

La scrisoarea Cancelariei de Stat

Nr. 18-69-1458 din 10.02.2023

**Ministerul Afacerilor Interne**  
Copie: **Cancelaria de Stat**

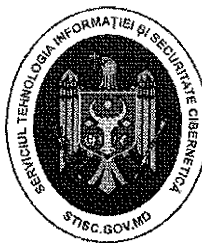
Serviciul de Informații și Securitate al Republicii Moldova a examinat proiectul de hotărâre a Guvernului *cu privire la aprobarea proiectului de lege pentru modificarea Legii nr. 20/2009 privind prevenirea și combaterea criminalității informatice (număr unic 104/MAI/2023)* și, în limita competenței funcționale, comunică lipsa de obiecții și propuneri.

**Alexandru MUSTEAȚA**  
**Director**

Digitally signed by Musteața Alexandru  
Date: 2023.02.24 14:03:55 EET  
Reason: MoldSign Signature  
Location: Moldova







## SERVICIUL TEHNOLOGIA INFORMAȚIEI ȘI SECURITATE CIBERNETICĂ

MD-2012 mun. Chișinău, Piața Marii Adunări Naționale, 1 IDNO 1003600096694  
tel.: + 373 22 820 900, fax: + 373 22 250 522 e-mail: [stisc@stisc.gov.md](mailto:stisc@stisc.gov.md), [itsec@itsec.gov.md](mailto:itsec@itsec.gov.md)

20.02.2023

1.4/315/23

La nr. 18-69-1458 din 10.02.2023

**Ministerul Afacerilor Interne**

*Copie: Cancelaria de Stat*

Prin prezenta, în ordinea examinării proiectului de hotărâre a Guvernului cu privire la aprobarea proiectului de lege pentru modificarea Legii nr. 20/2009 *privind prevenirea și combaterea criminalității informatice (număr unic 104/MAI/2023)*, I.P. „Serviciul Tehnologia Informației și Securitate Cibernetică”, în limitele competenței funcționale, Vă comunică despre susținerea acestuia în limita următoarei obiecții.

În scopul eficientizării și implementării imediate a dispoziției MAI și/sau SIS, precum și asigurării unui mecanism de transparență, se impune necesitatea creării unei baze unice de date, care va fi publică, și prin intermediul căreia, întru aplicarea măsurii, va fi asigurat schimbul securizat de date cu furnizorii de servicii.

**Cu respect**

Digitally signed by Pantaz Gheorghe  
Date: 2023.02.20 18:05:20 EET  
Reason: MoldSign Signature  
Location: Moldova



**Director**

**Gheorghe PANTAZ**



**AGENȚIA SERVICII PUBLICE A REPUBLICII MOLDOVA**  
**PUBLIC SERVICES AGENCY OF THE REPUBLIC OF MOLDOVA**

MD-2012, mun. Chișinău, str. Aleksandr Pușkin, nr. 42

42 Aleksandr Pushkin str., MD-2012 Chisinau

tel.: +373 22 50 46 54, fax: +373 22 21 22 59, e-mail: asp@asp.gov.md, web: asp.gov.md

12.07.2023  
38/2998

Nr. 01/1088  
04.07.2023

**Ministerul Afacerilor Interne**

Agencia Servicii Publice a examinat repetat, în limita atribuțiilor funcționale, proiectul de hotărâre a Guvernului *cu privire la aprobarea proiectului de lege pentru modificarea Legii nr.20/2009 privind prevenirea și combaterea criminalității informatice (număr unic 104/MAI/2023)* și vă comunică despre lipsa obiecțiilor și propunerilor.

**Director**

**Mircea EȘANU**

Digitally signed by Eșanu Mircea  
Date: 2023.07.12 15:29:45 EEST  
Reason: MoldSign Signature  
Location: Moldova





**ASOCIAȚIA NAȚIONALĂ  
A COMPANIILOR DIN  
DOMENIUL TIC**

str. Studenților, 9/11  
MD 2045, mun. Chișinău,  
Republica Moldova

Nr. de înregistrare:  
MD 0056763  
IDNO: 1006600034927

Tel: +373 22 887000  
Fax: +373 22 887001  
info@ict.md

**BC Moldindconbank SA**  
fil. Centru, Chișinău  
MOLDMD2X309  
Cont: 222440923

Nr. 587  
Data 19.07.2023

**Domnul Sergiu Gaibu  
Director ANRCETI**

**COPIE: Ministerul Afacerilor Interne  
Republica Moldova,  
MD-2012, mun. Chișinău, Bd. Ștefan cel Mare și Sfânt 75**

***Ref: proiectul actualizat al Legii pentru modificarea Legii nr. 20/2009 privind prevenirea și combaterea criminalității informatice***

Din numele Asociației Naționale a Companiilor din sectorul TIC (ATIC) Vă adresăm cele mai înalte considerațiuni.

ATIC a examinat proiectul actualizat al Legii pentru modificarea Legii nr. 20/2009 privind prevenirea și combaterea criminalității informatice, transmis cu scrisoarea ANRCETI nr. 01-DRA/876 din 17.07.2023, și prezintă următoarele observații și propuneri privind acest subiect:

### **1. Sistarea accesului la paginile web**

Așa cum a remarcat în primul său aviz la proiectul în cauză, ATIC susține, de principiu, stabilirea autorităților abilitate să dispună sistarea accesului la paginile web, precum și înlocuirea obligației de sistare a accesului la adresele IP pe care sunt amplasate paginile web contestate cu obligația de sistare a accesului la paginile web propriu-zise<sup>1</sup>. De asemenea, ATIC apreciază faptul că autorii au acceptat unele dintre recomandările sale la proiectul inițial, în special excluderea obligației de sistare a accesului la paginile web care contribuie “la încălcarea prevederilor legislației în vigoare”, care nu constituie infracțiune și nu trebuie să servească temei pentru sistarea accesului în baza Legii nr. 20/2009 sau Codului de procedură penală, precum și sistarea accesului la paginile web care sunt destinate și utilizate în scopul comiterii infracțiunilor, și nu doar contribuie la comiterea acestora.

---

<sup>1</sup> A se vedea pct. 98 din avizul menționat mai jos.

Notă: document semnat electronic în baza Legii Nr. 91 din 29.05.2014 privind semnătura electronică și documentul electronic. Verificarea semnăturii poate fi realizată la adresa: <https://msign.gov.md>

Totuși, aceste modificări nu sunt suficiente pentru a aduce această prevedere în conformitate cu normele internaționale și constituționale.

Amintim că o normă similară cu cea stabilită la art. 7 alit. (1) lit. e<sup>1)</sup> din Legea nr. 20/2009<sup>2</sup> a fost examinată anterior de Comisia de la Veneția<sup>3</sup>, care a formulat mai multe observații și recomandări față de aceasta.

Potrivit Comisiei, în Recomandarea sa către statele membre privind măsurile de promovare a respectării libertății de exprimare și de informare în legătură cu filtrarea conținutului de pe Internet (CM/Rec(2008)6)<sup>4</sup>, Comitetul de Miniștri al Consiliului Europei a declarat, inter alia, că statele ar trebui să se abțină de la filtrarea conținutului de pe Internet din alte motive decât cele prevăzute la articolul 10, paragraful 2 Convenția Europeană a Drepturilor Omului (CEDO), astfel cum este interpretat de Curtea Europeană a Drepturilor Omului (CtEDO), și ar trebui să garanteze că măsurile generale de blocare sau filtrare la nivel național sunt introduse numai dacă condițiile de la articolul 10, paragraful 2 CEDO sunt îndeplinite<sup>5</sup>.

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

Potrivit Comisiei, aceasta înseamnă că trebuie prevăzute motive și garanții deosebit de puternice pentru limitarea accesului publicului la Internet, măsură care, făcând cantități mari de informații inaccesibile, restrânge substanțial drepturile utilizatorilor de internet și este probabil să aibă efecte colaterale semnificative<sup>6</sup>.

În opinia CtEDO, restricțiile, cum ar fi ordinele de blocare a internetului „*nu sunt neapărat incompatibile cu Convenția, ca principiu. Cu toate acestea, este necesar un cadru legal, care să asigure atât un control strict asupra întinderii interdicțiilor, cât și un control judiciar eficient pentru a preveni orice abuz de putere [...] În această privință, controlul judiciar al unei astfel de*

---

<sup>2</sup> Potrivit art. 7 alit. (1) lit. e<sup>1)</sup> din Legea nominalizată, „furnizorii de servicii sînt obligați ... să sisteze, în condițiile legii, folosind metodele și mijloacele tehnice din posesie, accesul din propriul sistem informatic la toate adresele IP pe care sunt amplasate pagini web, inclusiv cele găzduite de furnizorul respectiv, ce contribuie la comiterea infracțiunilor sau la încălcarea prevederilor legislației în vigoare ori conțin/difuzează instrucțiuni privind modul de comitere a acestora”.

<sup>3</sup> Republica Moldova - Aviz comun al Comisiei de la Veneția și al Direcției Generale pentru Drepturile Omului și Statul de Drept (DGI) al Consiliului Europei cu privire la Proiectul de lege nr.161 de modificare și completare a legislației moldovenești în domeniul criminalității cibernetice, adoptat de Comisia de la Veneția la cea de-a 109-a sesiune plenară (Veneția, 9-10 decembrie 2016), pct. 74-75, 90-109 [www.vcnice.coe.int/webforms/documents/default.aspx?opinion=859&year=all&lang=EN](http://www.vcnice.coe.int/webforms/documents/default.aspx?opinion=859&year=all&lang=EN)

<sup>4</sup> Result details (coe.int).

<sup>5</sup> A se vedea pct. 91 și 94 din aviz.

<sup>6</sup> A se vedea pct. 95 din aviz.

Notă: document semnat electronic în baza Legii Nr. 91 din 29.05.2014 privind semnătura electronică și documentul electronic. Verificarea semnăturii poate fi realizată la adresa: <https://msign.gov.md>

*măsură, bazat pe o cântărire a intereselor concurente în joc și menit să stabilească un echilibru între ele, este de neconceput fără un cadru care să stabilească norme precise și specifice privind aplicarea restricțiilor preventive asupra libertății de exprimare [...]*" (Ahmet Yıldırım v. Turkey, Cerere Nr 3111/10, Hotărâre din 18.12.2012, § 67)<sup>7</sup>.

De asemenea, Recomandarea precizează că „*asa acțiuni de către stat ar trebui luate numai dacă filtrarea se referă la conținut specific și clar identificabil, o autoritate națională competentă a luat o decizie privind ilegalitatea acestuia și decizia poate fi revizuită de un tribunal sau de un organism de reglementare independent și imparțial, în conformitate cu cerințele articolului 6 din Convenția Europeană a Drepturilor Omului*”<sup>8</sup>.

Totodată, în Recomandarea sa CM/Rec(2016)5 privind libertatea Internetului, Comitetul Miniștrilor subliniază că „*înainte de a se aplica măsuri restrictive privind accesul la Internet, o instanță sau autoritate administrativă independentă stabilește că deconectarea de la Internet este cea mai puțin restrictivă măsură pentru atingerea scopului legitim*”<sup>9</sup>.

Pentru a asigura respectarea normelor internaționale citate, se impune, în primul rând, limitarea temeiurilor pentru sistarea accesului. Astfel, Comisia de la Veneția recomandă excluderea prevederii potrivit căreia poate servi drept temei pentru sistarea accesului faptul că o pagină web „conține/difuzează instrucțiuni privind modul de comitere a [infracțiunilor]”<sup>10</sup>.

În al doilea rând, se impune detalierea condițiilor de aplicare a acestei măsuri. În acest scop, este necesară completarea Codului de procedură penală (în continuare – CPP). Includerea cerinței de reglementare a modului de aplicare a acestei măsuri prin Hotărâre de Guvern, dar nu prin CPP, ar intra în contradicție cu prevederile art. 2 alin. (4) CPP, care stabilește că normele juridice cu caracter procesual din alte legi naționale pot fi aplicate numai cu condiția includerii lor în cod. În avizul său, Comisia de la Veneția, de asemenea, recomandă de a include cel puțin o parte din prevederile necesare în CPP<sup>11</sup>.

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

1. Stabilirea infracțiunilor sau categoriilor de infracțiuni pentru comiterea cărora se permite sistarea accesului la pagina web<sup>12</sup>.
2. Stabilirea procedurii de autorizare a măsurii de sistare a accesului (poate fi similară cu cea stabilită pentru autorizarea măsurilor procesuale de constrângere), inclusiv:

---

<sup>7</sup> A se vedea pct. 96 din aviz.

<sup>8</sup> A se vedea pct. 91 din aviz.

<sup>9</sup> A se vedea pct. 92 din aviz.

<sup>10</sup> A se vedea pct. 100 din aviz.

<sup>11</sup> A se vedea pct. 75 din aviz.

<sup>12</sup> A se vedea pct. 104 din aviz.

- a. organului abilitat de a autoriza asemenea măsură, la propunerea cui și prin care act procesual, de exemplu, ordonanța procurorului, emisă din oficiu sau la propunerea organului de urmărire penală, sau încheierea instanței de judecată, emisă la demersul procurorului)<sup>13</sup>. Subdiviziunile centrale specializate în prevenirea și combaterea criminalității informatice ale Ministerului Afacerilor Interne și Serviciului de Informații și Securitate (SIS) și Informații nu pot fi calificate drept autoritate administrativă independentă și imparțială.
- b. etapei procesului penal la care este posibilă dispunerea unei asemenea măsuri, de exemplu, doar după pornirea urmăririi penale<sup>14</sup>. O pagină web nu poate fi calificată drept destinată și utilizată în scopul comiterii infracțiunilor, dacă nu este pornită urmărirea penală pe faptul comiterii sau tentativei de comitere a infracțiunii.
- c. elementelor pe care trebuie să le conțină actul procesual prin care se autorizează măsură respectivă, de exemplu, conținutul online ilicit sau activitatea ilicită desfășurată prin intermediul paginii web, încadrarea juridică a acestei activități, motivarea necesității aplicării acestei măsuri, precum și adresa URL a paginii web accesul la care trebuie sistat. Aceste elemente trebuie să permită persoanelor vizate să înțeleagă motivele pentru care este sistat accesul la pagina web, pentru a putea întreprinde măsuri de remediere sau exercita dreptul la apărare prin contestarea măsurii, iar furnizorilor de servicii să determine pagina web specifică la care trebuie sistat accesul, ținând cont de faptul că, potrivit art. 14 alin. (3) din Legea nr. 284/2004, furnizorii de servicii nu au obligația de a supraveghea informațiile pe care le transmit sau le stochează atunci când furnizează serviciile și nici obligația de a căuta în mod activ fapte sau circumstanțe din care rezultă că activitățile sunt ilicite.
- d. cerinței, potrivit căreia, la soluționarea chestiunii privind necesitatea aplicării măsurii respective, procurorul și instanța de judecată trebuie să evalueze și să stabilească dacă măsura este proporțională cu circumstanțele individuale ale cauzei penale, inclusiv dacă sistarea accesului la pagina web este cea mai puțin restrictivă măsură pentru atingerea scopului legitim, de exemplu, dacă este posibilă eliminarea a conținutului online ilicit la sursă de către furnizorul acestuia sau de către furnizorul serviciilor de găzduire a conținutului online<sup>15</sup>.
- e. cerinței, potrivit căreia, copia de pe ordonanța procurorului sau prin încheierea instanței de judecată trebuie adusă la cunoștința furnizorului de conținut online ilicit (dacă este posibilă identificarea acestuia), în termenul care să fie stabilit prin lege.

<sup>13</sup> A se vedea pct. 99 și 108 din aviz.

<sup>14</sup> A se vedea pct. 99 din aviz.

<sup>15</sup> A se vedea pct. 99 și 105 din aviz.

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

## **2. Conservarea datelor informatice și a datelor privind traficul informatic**

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

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

„Articolul [XXX]. Conservarea rapidă a datelor informatice

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

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

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

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

---

<sup>16</sup> A se vedea pct. 107 din aviz.

- a) autoritatea care solicită conservarea;
- b) persoana asupra căreia se pune obligația de conservare;
- c) infracțiunea care face obiectul urmăririi penale și prezentarea succintă a faptelor care au legătură cu aceasta;
- d) datele informatice specifice ce urmează a fi conservate, inclusiv numele și prenumele persoanei sau persoanelor ale căror date trebuie să fie conservate (dacă acestea sunt disponibile), genul de date care trebuie conservate, perioada de referință pentru care trebuie conservate datele;
- e) motivele dispunerii conservării: natura legăturii acestor date cu infracțiunea, motivarea îndeplinirii condițiilor prevăzute în alin. (2);
- f) obligația persoanei asupra căreia se pune obligația de conservare de a păstra datele informatice și de a le menține integritatea, cu păstrarea confidențialității cu privire la aplicarea acestei măsuri; și
- g) perioada de păstrare a datelor informatice ce urmează a fi conservate.

(5) Măsura conservării poate fi prelungită de către procuror o singură dată pentru motive temeinic justificate, pe o durată maximă de 90 de zile.

(6) Extrasul din ordonanța procurorului, care trebuie să cuprindă informațiile specificate la literele a), b), d), f) și g) din alin. (4), se transmite persoanei în posesia sau sub controlul căreia se află datele stocate, aceasta fiind obligată să asigure conservarea lor rapidă, cu păstrarea confidențialității cu privire la aplicarea acestei măsuri.

(7) În cazul în care în transmiterea comunicației au fost implicați mai mulți furnizori de servicii, procurorul, prin ordonanța de conservare sau o altă ordonanță, poate dispune dezvăluirea rapidă de către persoana în posesia sau sub controlul căreia se află datele referitoare la trafic a unei cantități de date referitoare la trafic, suficiente pentru a permite identificarea furnizorilor de servicii și a canalelor prin intermediul căruia comunicația a fost transmisă.

(8) Procurorul este obligat să dispună încetarea conservării, înaintea expirării perioadei pentru care a fost dispusă, de îndată ce au dispărut temeiurile și motivele care au justificat-o.

(9) Procurorul dispune ridicarea datelor conservate de la persoana care le-a conservat în termenul prevăzut în alin. (3) sau (5), după caz. Ridicarea datelor conservate se efectuează în conformitate cu prevederile art. 125-132.

(10) Până la terminarea urmăririi penale, procurorul este obligat să anunțe, în scris, utilizatorii ale căror date au fost conservate.”

Rămânem la dispoziția autorităților pentru definitivarea proiectului în cauză, în concordanță cu rigorile internaționale și constituționale.

Cu respect,

**Marina Bzovî**

Director Executiv

Asociația Națională Companiilor din Domeniul TIC

Notă: document semnat electronic în baza Legii Nr. 91 din 29.05.2014 privind semnătura electronică și documentul electronic. Verificarea semnăturii poate fi realizată la adresa: <https://msign.gov.md>





Ministerul Dezvoltării  
Economice și Digitalizării  
al Republicii Moldova

nr. 11/2 –2058 din 12.07.2023

la nr. 38/2998 din 04.07.2023

## Ministerul Afacerilor Interne

Ministerul Dezvoltării Economice și Digitalizării a examinat proiectul de hotărâre a Guvernului cu privire la aprobarea proiectului de lege pentru modificarea Legii nr. 20/2009 privind prevenirea și combaterea criminalității informatice (**număr unic 104/MAI/2023**) prezentat spre avizare repetată și reieșind din competențele funcționale comunică despre lipsa de obiecții și propuneri.

**Secretar de stat**

**Mihai LUPAȘCU**

Digitally signed by Lupașcu Mihai  
Date: 2023.07.12 10:13:23 EEST  
Reason: MoldSign Signature  
Location: Moldova



Victoria Iorga, tel 022 250 556



Ministerul Infrastructurii  
și Dezvoltării Regionale  
al Republicii Moldova

Nr.21-3478 din 05.07.2023

**Ministerul Afacerilor Interne**

*e-mail: [mai@mai.gov.md](mailto:mai@mai.gov.md)*

Ca urmare a examinării versiunii definitive a proiectului de lege pentru modificarea Legii nr. 20/2009 privind prevenirea și combaterea criminalității informatice (**număr unic 104/MAI/2023**), remis în procedură regulamentară de avizare repetată, precum și în contextul în care au fost acceptate de principiu propunerile exprimate prin avizul nr. 09-1306 din 03 martie 2023, comunicăm lipsa de obiecții și propuneri.

**Secretar general**

Digitally signed by Țurcanu Angela  
Date: 2023.07.05 23:33:57 BEST  
Reason: MoldSign Signature  
Location: Moldova



**Angela ȚURCANU**

*Ex.: Sergiu Melega*

*Tel.: 022-250-620*

*E-mail: [sergiu.melega@midr.gov.md](mailto:sergiu.melega@midr.gov.md)*



Nr. 01-DRA/910

24 iulie 2023

la Nr. \_\_\_\_\_

**Ministerul Afacerilor Interne  
al Republicii Moldova**

Cu referință la proiectul hotărârii de Guvern *cu privire la aprobarea proiectului de lege pentru modificarea Legii nr. 20/2009 privind prevenirea și combaterea criminalității informatice (număr unic 104/MAI/2023)*, remis spre avizare repetată, Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației (ANRCETI), ținând cont de domeniile de competență date prin lege, în conformitate cu dispozițiile art. 33 din Legea cu privire la actele normative nr. 100/2017, susține proiectul cu următoarele propuneri.

Considerăm că modificarea art. 7, în special a alin. (1) lit. e<sup>1</sup>) și completarea acestuia cu alineate *noi*, respectiv (3) și (4), urmează să reflecte mecanismul de sistare/blocare, similar celui în dreptul Uniunii europene, care este conform cu cerințelor art. 3 alin. (3) și art. 30 alin. (1) lit. c) din Legea nr. 100/2017.

Așa fiind, autorul proiectului urmează să asigure *compatibilitatea* legislației naționale cu *legislația Uniunii Europene*, în acest scop, este util de a armoniza mecanismul de (i) sistare/blocare și (ii) contestare cu *aquis*-ului european, în special conform Directivei 2011/93/UE a Parlamentului European și a Consiliului din 13 decembrie 2011 privind combaterea abuzului sexual; (ii) Regulamentul (UE) 2021/784 al Parlamentului European și al Consiliului din 29 aprilie 2021 privind prevenirea diseminării conținutului online cu caracter terorist și (iii) Regulamentul (UE) 2021/1232 al Parlamentului European și al Consiliului din 14 iulie 2021 privind o derogare temporară de la anumite dispoziții ale Directivei 2002/58/CE în ceea ce privește utilizarea tehnologiilor de către furnizorii de servicii de comunicații interpersonale care nu se bazează pe numere pentru prelucrarea datelor cu caracter personal și a altor date în scopul combaterii abuzului sexual online asupra copiilor și a (iv) Regulamentului (UE) 2022/2065 al Parlamentului European și al Consiliului din 19 octombrie 2022 privind o piață unică pentru serviciile digitale (Regulamentul privind serviciile digitale).

Conform dreptului UE, sistarea este admisibilă în cazurile de prevenire, investigare, detectare și urmărire în justiție a unor *infrațiuni grave, deosebit de grave și excepțional de grave*, respectiv, nu este proporțional ca sistarea să se realizeze pentru *orice faptă*<sup>1</sup>.

Având în vedere că Legea nr. 20/2009 face parte din sistemul legislației procesual *penale*, este inadecvat ca contestarea actelor ce rezultă din aplicarea acesteia să se realizeze conform legislației *contenciosului administrativ* (a se vedea alin. 4 din art. 7 din proiect), respectiv, se propune ca acțiunile organelor de urmărire penală (inclusiv ordonanțele de blocare/sistare emise pe acest subiect) să fie contestate potrivit legislației procesual *penale*.

<sup>1</sup> similar art. 5 alin. (7) din Legea nr. 241/2007.

ANRCETI reiterează că Legea nr. 20/2009 *sau* Codul de procedură penală urmează să reglementeze mecanismul de blocare și contestare a ordonanțelor emise de organe abilitate cu aplicarea art. 7 alin. (1) lit. e<sup>1</sup>) din același act legislativ.

Așa fiind, urmează a se consacra un mecanism prin lege și nu prin acte normative subordonate legii - potrivit art. 72 din Constituție, prin lege organică se reglementează căile de atac ale actelor autorităților publice.

**Cu respect,**

**Director**

Digitally signed by Gaibu Sergiu  
Date: 2023.07.24 14:04:56 EEST  
Reason: MoldSign Signature  
Location: Moldova



**Sergiu GAIBU**



---

Republic of Moldova, Chișinău, MD-2012, 134, Ștefan cel Mare și Sfânt Ave.  
Phone: +373 22 820 026, email: [office@egov.md](mailto:office@egov.md), web: <http://www.egov.md>

---

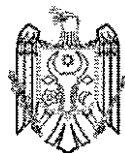
Nr. 3007 – 115 din 05.07.2023  
La nr. 38/2998 din 04.07.2023

**Ministerul Afacerilor Interne**

Instituția publică „Agenția de Guvernare Electronică” a examinat *proiectul definitivat de hotărâre a Guvernului cu privire la aprobarea proiectului de lege pentru modificarea Legii nr.20/2009 privind prevenirea și combaterea criminalității informatice (număr unic 104/MAI/2023)*, autor – **Ministerul Afacerilor Interne**, remis spre avizare repetată, și, în limitele competențelor Agenției comunicăm că îl avizăm favorabil, susținându-l în principiu.

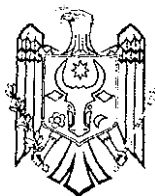
**Directoare**

Digitally signed by Tumoruc Olga  
Date: 2023.07.05 13:31:26 EEST  
Reason: MoldSign Signature  
Location: Moldova



**Olga TUMURUC**

Ex.: Eduard Fricățel,  
e-mail: [eduard.fricatel@egov.md](mailto:eduard.fricatel@egov.md),  
tel.: 0794 38 138



# PROCURATURA REPUBLICII MOLDOVA

PROCURATURA GENERALĂ

mun. Chișinău, bd. Ștefan cel Mare și Sfânt, 73, MD-2001, Tel.: /373 22/ 828 373

www.procuratura.md / e-mail: proc-gen@procuratura.md

17 iulie 2023 nr.4-ld/23- ~~197,198~~

L.a nr. 38/2998 din 04.07.2023

**Ministerul Afacerilor Interne**

Procuratura Generală a examinat *proiectul de hotărâre a Guvernului cu privire la aprobarea proiectului de Lege pentru modificarea Legii nr.20/2009 privind prevenirea și combaterea criminalității informatice (număr unic 104/MAI/2023)* remis spre avizare repetată.

Opinia instituțională pe marginea proiectului de hotărâre menționat *supra* a fost redată în scrisoarea nr.4-ld/23-197,198 din 28.02.2023, iar obiecțiile și propunerile înaintate în mare parte nu au fost acceptate de către autor.

Pe cale de consecință, verificând și apreciind conținutul proiectului înaintat spre avizare repetată și argumentarea autorului proiectului a obiecțiilor și propunerilor înaintate de către Procuratura Generală din sinteza obiecțiilor și propunerilor la proiectul de hotărâre, expunem *infra* următoarele:

I. Cu referire la *proiectul de Lege pentru modificarea Legii nr.20/2009 privind prevenirea și combaterea criminalității informatice (în continuare - proiectul de Lege)*:

1.1. Potrivit proiectului, Ministerul Afacerilor Interne și Serviciul de Informații și Securitate (în continuare MAI și SIS) vor putea dispune prin intermediul subdiviziunilor sale centrale specializate în prevenirea și combaterea criminalității informatice sistarea accesului la pagini web în condițiile prevăzute la articolul 7 alineatul (1) litera e<sup>1</sup>) din *Legea 20/2009 privind prevenirea și combaterea criminalității informatice (în continuare Legea 20/2009)*.

Astfel, conform art.7 alineatul (1) litera e<sup>1</sup>) din *Legea 20/2009*:

*„Furnizorii de servicii sînt obligați: să sisteze, în condițiile legii, folosind metodele și mijloacele tehnice din posesie, accesul din propriul sistem informatic la toate adresele IP pe care sunt amplasate pagini web, inclusiv cele găzduite de furnizorul respectiv, ce contribuie la comiterea infracțiunilor sau la încălcarea prevederilor legislației în vigoare ori conțin/difuzează instrucțiuni privind modul de comitere a acestora;”*

Procuratura Generală în avizul nr.4-ld/23-197,198 din 28.02.2023 a invocat că, pentru a preveni eventuale abuzuri și/sau aprecieri arbitrare ale subdiviziunilor MAI și SIS în cazurile de sistare a accesului la anumite adrese IP pe care sunt amplasate pagini web, pentru alte motive decât cele prevăzute/limitate de art.7 alineatul (1) litera e<sup>1</sup>) din *Legea 20/2009*, consideră oportună instituirea unui sistem adecvat de garanții și control asupra realizării acestei activități. Autorizarea de către un procuror desemnat din cadrul Procuraturii Generale a măsurii de sistare

a accesului la pagini web, va contribui la prevenirea și contracararea abuzurilor, fiind asigurate garanții privind respectarea drepturilor și libertăților fundamentale.

Conform sintezei obiecțiilor și propunerilor la proiectul de Lege, propunerea menționată nu a fost acceptată de către autorul proiectului din motiv că, *"Pornind de la practica națională deja existentă privind sistarea/blocarea accesului la web site-uri ce promovează știri false privind COVID (identificate de SIS și sistarea dispusă de ANRCETI) și privind web site-urile de jocuri de noroc nelicențiate (identificate de ASP și sistarea dispusă de ANRCETI), considerăm inoportună intervenția procuraturii prin autorizarea măsurii respective. Menționăm că poliția este organ de constatare a infracțiunilor, la fel precum SIS și ASP constată ilegalitate altor categorii de informații din internet"*.

Considerăm că, argumentele invocate de către autorul proiectului cu referire la propunerile/obiecțiile ale Procuraturii Generale indicate *supra* sunt neîntemeiate.

În considerarea acestor raționamente, menționăm că, practica națională invocată de către autorul proiectului de Lege nu poate servi ca temelie juridică pentru operarea modificărilor legislative.

Totodată, efectuând un studiu al cazurilor de sistare/blocare a accesului la web site-uri, ce promovează știri false, constatăm că, majoritatea Ordinelor Directorului Serviciului de Informații și Securitate al Republicii Moldova cu privire la blocarea accesului utilizatorilor din Republica Moldova la sursele cu conținut on-line, care promovează informații false, sunt emise în temeiul art.26-28 din Dispoziția nr.1 din 24.02.2022 a Comisiei pentru Situații Excepționale a Republicii Moldova<sup>1</sup>.

E de menționat că, în conformitate cu art.27 din Dispoziția nr.1 din 24.02.2022 a Comisiei pentru Situații Excepționale a Republicii Moldova *"Serviciul de Informații și Securitate al Republicii Moldova va aproba prin ordin și va face publică lista surselor cu conținut Online care promovează informații false ce afectează securitatea națională în condițiile stării de urgență aprobate de către Parlament"*.

Subsidiar, consemnăm că, conform art.1 din *Legea nr. 212/2004 privind regimul stării de urgență, de asediu și de război - "stare de urgență - ansamblu de măsuri cu caracter politic, economic, social și de menținere a ordinii publice, care se instituie provizoriu în unele localități sau pe întreg teritoriul țării ..."*.

În această ordine de idei, se deduce că, sistarea/blocarea accesului la web site-uri, ce promovează știri false, efectuată prin Ordinele Directorului Serviciului de Informații și Securitate al Republicii Moldova este o excepție stabilită pentru o perioadă determinată și nu poate fi atribuită la practica națională.

Pe calea de consecință, reiterăm propunerea înaintată de către Procuratura Generală în avizul nr.4-1d/23-197,198 din 28.02.2023 privind instituirea unui sistem adecvat de garanții și control asupra realizării activității de sistare a accesului la anumite adrese IP pe care sunt amplasate pagini web, în vederea excluderii situației de abuz din partea MAI și SIS, prevenirii și contracarării

<sup>1</sup> [https://sis.md/sites/default/files/comunicate/fisiere/Ordin%20nr.5%20din%2019.01.2023\\_0.pdf](https://sis.md/sites/default/files/comunicate/fisiere/Ordin%20nr.5%20din%2019.01.2023_0.pdf)  
https://sis.md/sites/default/files/comunicate/fisiere/Ordin%20nr.5%20din%2019.01.2023\_0.pdf

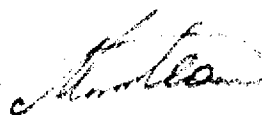




informativă adoptată la Budapesta la 23.11.2001, prin *Legea nr.6/2009*, urma ca activul normativ național, în principal Codul de procedură penală să fie completat cu măsura de conservare în corespundere cu angajamentele externe ale Republicii Moldova, atât la compartimentul combaterii crimei cibernetice, cât și al garantării drepturilor protejate ale omului.

Reieșind din cele expuse, reiterăm opinia instituțională că, proiectul de lege supus avizării nu corespunde: principiului echilibrului între reglementările concurente și principiului respectării drepturilor și libertăților fundamentale prevăzute la art. 3 din *Legea nr. 100 din 22.12.2017 cu privire la actele normative*.

**Procuror General interimar**



**Ion MUNTEANU**



## SERVICIUL TEHNOLOGIA INFORMAȚIEI ȘI SECURITATE CIBERNETICĂ

---

MD-2012 mun. Chișinău, Piața Marii Adunări Naționale, 1 IDNO 1003600096694  
tel.: + 373 22 820 900, fax: + 373 22 250 522 e-mail: [stisc@stisc.gov.md](mailto:stisc@stisc.gov.md), [itsec@itsec.gov.md](mailto:itsec@itsec.gov.md)

17.07.2023

1.4/913/23

La nr. 38/2998 din 04.07.2023

**Ministerul Afacerilor Interne**

Prin prezenta, în ordinea examinării repetate a proiectului de hotărâre a Guvernului cu privire la aprobarea proiectului de lege pentru modificarea Legii nr. 20/2009 *privind prevenirea și combaterea criminalității informatice* (**număr unic 104/MAI/2023**), I.P. „Serviciul Tehnologia Informației și Securitate Cibernetică”, în limitele competenței funcționale, comunică despre lipsa de obiecții și propuneri.

**Cu respect,**

Digitally signed by Corețchi Alexandru  
Date: 2023.07.17 16:12:46 EEST  
Reason: MoldSign Signature  
Location: Moldova



**Director**

**Alexandru COREȚCHI**



## SERVICIUL DE INFORMAȚII ȘI SECURITATE AL REPUBLICII MOLDOVA

MD-2004, Chișinău, bd. Ștefan cel Mare și Sfânt, 166 tel. 022-239-625, fax 022-234-068, e-mail: sis@sis.md

20 iulie 2023

Nr. E/7338

La scr. nr. 38/2998 din 04.07.2023

### Ministerul Afacerilor Interne

Serviciul de Informații și Securitate al Republicii Moldova (în continuare – Serviciul) a examinat repetat *proiectul de hotărâre a Guvernului cu privire la aprobarea proiectului de lege pentru modificarea Legii nr.20/2009 privind prevenirea și combaterea criminalității informatice (număr unic 104/MAI/2023)* și, în limita competenței funcționale, comunică următoarele obiecții și propuneri.

*Cu referire la proiectul de lege:*

1. La Articolul I:

- la pct. 1, articolul 4 propunem a se completa cu următorul conținut:

*„la alineatul (3) sintagma „activități operative de investigații” a se substitui cu sintagma „activități contrainformative și informative externe și măsuri speciale de investigații”.*

Raționamentul propunerii rezidă din faptul adoptării Legii nr.179/2023 privind activitatea contrainformativă și activitatea informativă externă, prin care Serviciului i-a fost atribuită competența de a desfășura măsuri contrainformative/informative externe întru prevenirea și combaterea amenințărilor la adresa securității statului.

- la pct. 2, articolul 7 alineatul (1) propunem a se completa cu o literă nouă cu următorul cuprins:

*„să identifice, până la oferirea serviciilor, utilizatorii care iau în chirie sisteme informaționale, cu ajutorul actelor de identitate valide și/sau rechizite bancare confirmate de emitenți”.*

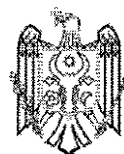
Propunerea dată se argumentează prin faptul că, până la oferirea serviciilor, furnizorii sunt obligați să solicite utilizatorilor indicarea, în mod obligatoriu, a unui set de date care permit stabilirea identității acestora, fapt care ar facilita identificarea în termeni oportuni a infractorilor, inclusiv reducerea și descurajarea comiterii faptelor infracționale (*evaziunea fiscală, spălarea banilor, etc.*).

2. Suplimentar, se propune completarea proiectului cu un punct nou, prin care să fie operate modificări la art. 9 al Legii nr. 20/2009, astfel încât, sintagma „*activitatea operativă de investigații*” să fie substituită cu sintagma „*activitate specială de investigații*”, or, necesitatea ajustării noțiunii respective survine urmare a utilizării noțiunii de activitate specială de investigații în Legea nr. 59/2012 și Codul de procedură penală nr. 122/2003. Astfel, operarea modificării propuse este necesară în vederea utilizării unei terminologii constante, uniforme și care să corespundă celei utilizate în alte acte normative (în corespundere cu art. 54 alin. (1) lit. c) din Legea cu privire la actele normative nr. 100/2017).

În vederea celor expuse supra, considerăm fundamentală ajustarea proiectului de lege ținând cont de propunerile menționate.

**Alexandru MUSTEȚA**  
**Director**

Digitally signed by Musteța Alexandru  
Date: 2023.07.20 12:08:36 EEST  
Reason: MoldSign Signature  
Location: Moldova





# PROCURATURA REPUBLICII MOLDOVA

## PROCURATURA GENERALĂ

mun. Chișinău, bd. Ștefan cel Mare și Sfânt, 73, MD-2001, Tel.: /373 22/ 828 373  
www.procuratura.md / e-mail: proc-gen@procuratura.md

16.11.2023 nr.4-1d/23-~~660~~

La nr.38/4950 din 01.11.2023

**Ministerul Afacerilor Interne**

✓  
Copie: **Cancelaria de Stat**

Procuratura Generală a examinat proiectul de hotărâre a Guvernului pentru aprobarea Regulamentului privind procedura de sistare a accesului la paginile web care conțin informații destinate pentru comiterea infracțiunilor (în continuare – Regulament) expediat pentru expunerea opiniei instituționale.

În urma examinării proiectului de hotărâre a Guvernului privind aprobarea Regulamentului, se atestă că acesta depășește cadrul normativ al Legii Nr. 20/2009 în redacția actuală, în condițiile în care stabilește competența subdiviziunilor specializate din cadrul Ministerului Afacerilor Interne (în continuare – MAI) și a Serviciului de Informații și Securitate (în continuare - SIS) de a emite Ordine de sistare a accesului la paginile web ce conțin informații destinate și utilizate pentru comiterea infracțiunilor (pct.6 sub.2) din Regulament).

Or, potrivit art.14 alin.(1) lit.a) din Legea 100/2017 cu privire la actele normative, „Hotărârea Guvernului este un act care se adoptă de către Guvern pentru: a) exercitarea atribuțiilor Guvernului și pentru organizarea executării legilor;”

În această ordine de idei, este de reținut că, viziunea conceptuală asupra reglementărilor ce vizează posibilitatea dispunerii de către MAI și SIS de a dispune, prin intermediul subdiviziunilor sale centrale specializate în prevenirea și combaterea criminalității informatice, sistarea accesului la pagini web a fost expusă în avizele nr. 4-1d/23-197 din 28 februarie 2023 și nr.4-1d/23-384 din 17 iulie 2023 formulate la proiectul de Lege nr.104/MAI/2023

Prin urmare, reieșind din lipsa unor reglementări legale care să acorde posibilitatea subdiviziunilor menționate *supra* de a dispune sistarea paginilor web, opinia instituțională asupra proiectului, se va rezuma la o analiza textuală tehnico-juridică.

Așadar, referitor la prevederile pct. 3 și 4 din proiectul Regulamentului, urmează a se menționa că nu este clar mecanismul de apreciere a conținutului difuzat/prezentat publicului, or, în cazul respectiv, subdiviziunile din cadrul MAI și SIS ar trebui să fie specializate și în aprecierea conținutului publicat/difuzat pe paginile web, în cadrul normativ actual neexistând un organ public de specialitate menit să asigure aprecierea conținutului afișat ca fiind contrar anumitor prevederi legale (spre exemplu: Agenția de Stat pentru Protecția Moralității a fost un organ public de specialitate pe lângă Ministerul Culturii, care asigura protejarea culturii și moralității prin contracararea tendințelor de propagare a pornografiei, sadismului

și cultului violenței în lucrările de artă, literatură și mass-media, conform pct. 2 din Regulamentul Agenției de Stat pentru Protecția Moralității pe lângă Ministerul Culturii, aprobat prin Hotărârea Guvernului nr. 1400 din 17.12.2001 (abrogată la 10.08.2022).

Astfel, blocarea conținutului de pe Internet este o ingerință clară și în dreptul la libertatea de exprimare, garantat de art. 10 din Convenția Europeană a Drepturilor Omului.

Jurisprudența Curții Europene a Drepturilor Omului privind blocarea Internetului, care s-a dezvoltat în ultimii ani, se bazează pe o abordare în trei etape:

- necesitatea unui temei juridic clar pentru orice măsură de blocare;
- măsura trebuie să urmărească un scop legitim, astfel cum este enumerat la art. 10, paragr. 2 (de exemplu, securitatea națională, prevenirea dezordinii sau a criminalității, protecția sănătății sau a moralei, protecția reputației sau a drepturilor altora);
- măsura trebuie să fie proporțională cu scopul legitim urmărit.

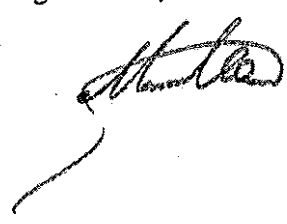
Pe această bază, statele membre ar trebui să se asigure că orice restricții privind accesul la conținutul de Internet care afectează utilizatorii aflați sub jurisdicția lor se bazează pe un cadru juridic strict și previzibil care reglementează domeniul de aplicare al oricăror astfel de restricții și să ofere garanția supravegherii judiciare pentru a preveni eventualele abuzuri.

În plus, instanțele naționale trebuie să examineze dacă orice măsură de blocare este necesară și proporțională și, în special, dacă este suficient de direcționată pentru a avea un impact numai asupra conținutului specific care necesită blocare.

De asemenea, considerăm necesar de a fi exclus subpct.8) din pct. 3 al Regulamentului care conține următoare formulare „alte acțiuni ce reprezintă o infracțiune”. Această formulare este una generală fapt care lasă o marjă prea largă de apreciere a instituțiilor de aplicare a legii. Asupra previzibilității legii, Curtea Constituțională s-a expus în Decizia nr.38 din 08.07.2016 de inadmisibilitate a sesizării nr. 65g/2016 privind excepția de neconstituționalitate a unor prevederi din art. 2 și art. 9 alin. (1) din Legea nr. 16/2008 cu privire la conflictul de interese, statuând următoarele:

„Urmând principiile Curții Europene de examinare a calității legii, în jurisprudența sa Curtea a reținut că o lege (prevedere legală) trebuie să fie suficient de accesibilă, clară și previzibilă. O normă este clară, accesibilă și previzibilă numai atunci când este redactată cu suficientă precizie, în așa fel încât să permită oricărei persoane să își corecteze conduita și să fie capabilă, cu consiliere adecvată, să prevadă, într-o măsură rezonabilă, consecințele care pot apărea dintr-o normă (cauza Silver s.a. vs. Regatul Unit, 25 martie 1983).”.

Procurorul General interimar



Ion MUNTEANU