SINTEZA
obiecțiilor și propunerilor (recomandărilor)
la proiectul legii pentru modificarea Legii nr. 20/2009 privind prevenirea și combaterea criminalității informatice
(număr unic 104/MAI/2023)

Participantul la avizare (expertizare)/consultare publică	Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
Ministerul Economiei	1. 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. 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**.	**Precizare** Art. II a proiectului prevede că Guvernul, până la intrarea în vigoare a prezentei legi, va elabora instrucțiunile privind punerea în aplicare a prevederilor din articolul 4 alineatul (1) și articolul 7 alineatul (1) litera e 1), alineatul (3) și (4) din Legea nr. 20/2009. Concomitent în cadrul proiectului art. 7 a fost completat cu alineatul (3) și (4) cu următorul cuprins : „(3) Reglementarea procedurii de sistare a accesului la pagini web în condițiile prevăzute la articolul 7 alineatul (1) litera e1) se realizează cu respectarea următoarelor principii generale: a) proporționalității; b) aplicării măsurii tehnice de sistare cel mai puțin restrictive; c) informării utilizatorilor privind motivele sistării accesului și căile de atac; d) revizuirii periodice a necesității sistării în continuare a accesului la o anumită pagină web; e) respectării dreptului furnizorilor de servicii de a aplica, din proprie inițiativă, alte

		măsuri pentru prevenirea utilizării abuzive a serviciilor sale. (4) Sistarea accesului la pagina web poate fi contestată în ordine de contencios administrativ."
Ministerul Infrastructurii și Dezvoltării Regionale	2. 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[1]) 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.	**Precizare** alineatul (1) litera e[1]), va avea următorul cuprins: „e[1] să sisteze, în modul stabilit de Guvern, folosind metodele și mijloacele tehnice din posesie, accesul din propriul sistem informatic la pagini web, inclusiv cele găzduite de furnizorul respectiv, destinate și utilizate pentru comiterea infracțiunilor ori conțin/difuzează instrucțiuni privind modul de comitere a acestora;
	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.	**Precizare** Recomandarea se referă la alt tip de servicii – cel de găzduire a conținutului. Respectiv prevederile acesteia sunt transpuse în Legea comerțului electronic.
	4. 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	**Se acceptă** Au fost operate modificările de rigoare.

	concordanță cu prevederile art.16, pct.2 din Convenția Consiliului Europei privind criminalitatea informatică.	
Procuratura Generală	5. Potrivit proiectului, Ministerul Afacerilor Interne şi Serviciul de Informații și Securitate (în continuare MAI şi SIS) vor putea dispune prin intermediul subdiviziunilor sale centrale specializate în prevenirea şi combaterea criminalității informatice sistarea accesului la pagini web în condițiile prevăzute la articolul 7 alineatul (1) litera e[1]) din Legea 20/2009. Potrivit art.7 alineatul (1) litera e[1]) din Legea 20/2009: „Furnizorii de servicii sânt obligați: să sisteze, în condițiile legii, folosind metodele şi mijloacele tehnice din posesie, accesul din propriul sistem informatic la toate adresele IP pe care sunt amplasate pagini web, inclusiv cele găzduite de furnizorul respectiv, ce contribuie la comiterea infracțiunilor sau la încălcarea prevederilor legislației în vigoare ori conțin/difuzează instrucțiuni privind modul de comitere a acestora;" Prin urmare, pentru a preveni eventuale abuzuri şi/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[1]) din Legea 20/2009, considerăm oportună instituirea unui sistem adecvat de garanții şi 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 şi contracararea abuzurilor, fiind asigurate garanții privind respectarea drepturilor şi libertăților fundamentale.	**Nu se acceptă.** 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. Prin analogie, legislația din statul membru UE Franța prevede dispunerea sistării de către o subdiviziune a poliției special desemnată în acest sens.
	6. 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 şi nota informativă a acestuia, se atestă lipsa unor precizări cu privire	**Precizare** Legea nr. 20/2009 deja prevede la art. 7 alin.(1) lit. c) *„conservarea imediată a datelor informatice ori a datelor referitoare la traficul informatic, față de care există pericolul*

	la perioada/termenele pentru care poate fi dispusă conservarea datelor informatice ori a datelor referitoare la traficul informatic şi nici temeiurile/motivele în baza cărora poate fi dispusă conservarea datelor.	*distrugerii ori alterării, pe un termen de până la 120 de zile calendaristice*". Totodată, termenul de conservare este ajustat la prevederile Convenției Budapesta.
	7. Mai mult, conservarea datelor informatice reprezintă o măsură secretă, făcută în condiții de confidențialitate, despre care persoanele vizate nu sunt înștiințate, şi prin care pot fi conservate nu numai datele despre identitatea utilizatorului sau altei persoane, dar şi date privind conexiunile sau chiar conținutul comunicațiilor. În consecință, acestea se află sub protecția art. 8 CEDO - Dreptul la respectarea vieții private şi 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 corespondentei (Campbell împotriva Regatului Unit, pct. 33), realizarea de copii (Foxley împotriva Regatului Unit, pct. 30) sau ştergerea anumitor pasaje (Pfeifer şi Plankl împotriva Austriei, pct. 43); - stocarea datelor interceptate referitoare la utilizarea telefonului, a adresei de e-mail şi 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). Aşadar, statului îi revine obligația pozitivă de a proteja aceste date şi a preveni abuzurile în raport cu ele. Sub aspect comparat indicăm şi practicile altor state (membre UE) în materia vizată.	**Nu se acceptă.** Dispunerea conservării datelor informatice reprezintă una din atribuțiile punctului de contact 24/7 responsabil de realizarea prevederilor articolului 35 din Convenția Budapesta. Totodată, Legea menționată a României prevede că punctul de contact 24/7 este în cadrul procuraturii (parchetului). În legea din Republic Moldova prevederile privind punctul de contact 24/7 sunt diferite de cele din România şi anume Legea nr. 6/2009 pentru ratificarea Convenției Consiliului Europei privind criminalitatea informatică prevede că Ministerul Afacerilor Interne desemnează punctul de contact respectiv (inclusiv sub aspectul dispunerii conservării datelor informatice). Astfel, este necesar a fi prevăzută atribuția MAI de dispunere a conservării datelor informatice. Prin analogie, legislația din statele UE precum Danemarca, Irlanda, Italia, Lituania, Portugalia prevede dispunerea măsurii date de către organele de poliție, măsura fiind prevăzută în lege sectorială.

	Spre exemplu, în România conservarea datelor informatice constituie o acțiune procedurală, prevăzută la art. 154 al Codului de procedură penală al României, 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 şi 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."	
	8. 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 şi ale căror date au fost conservate." În cazul pus în discuție urmează de ținut cont de faptul că obiectivul Legii 20/2009 privind prevenirea şi combaterea criminalității informatice este de a reglementa raporturile juridice privind: a) prevenirea şi combaterea infracțiunilor informatice; b) cadrul de asistență mutuală în prevenirea şi combaterea criminalității informatice, în protecția şi acordarea de ajutor furnizorilor de servicii şi utilizatorilor de sisteme informatice; c) colaborarea autorităților administrației publice cu organizații neguvernamentale şi cu alți reprezentanți ai	**Nu se acceptă.** Măsura conservării datelor informatice nu implică obținerea acestor date, ci doar prelungirea termenului de păstrare, prin implementarea măsurilor de securitate pentru a preveni compromiterea informațiilor. Prin urmare, nu putem face o analogie cu măsurile realizate în secret, precum măsurile speciale de investigații.

	societății civile în activitatea de prevenire şi de combatere a criminalității informatice; d) cooperarea cu alte state, cu organizații internaționale şi regionale având competențe în domeniu. Prin urinare, după adoptarea legii în cauză şi 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 şi al garantării drepturilor protejate ale omului.	
	9. 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.	**Nu se acceptă.** Convenția Budapesta prevede dispunerea conservării datelor informatice pentru orice gen de infracțiune.
	10. Reieşind din cele expuse, se constată că proiectul de lege supus dezbaterilor nu corespunde: principiului echilibrul între reglementările concurente şi principiului respectării drepturilor şi libertăților fundamentale prevăzute la art. 3 din Legea nr. 100 din 22.12.2017 cu privire la actele normative.	**Nu se acceptă.** Cu referire cu cele invocate în aviz, au fost expuse argumentele pentru fiecare obiecție înaintată de către autorul avizului.
Agenția Națională pentru Reglementare în Comunicații Electronice şi Tehnologia Informației	11. Considerăm că modificarea art. 7 alin. (1) lit. e1), prin excluderea textului „în condițiile legii" şi, 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) şi art. 30 alin. (1) lit. c) din Legea nr. 100/2017, autorul	**Nu se acceptă.** Aquis-ului european nu prevede că astfel de prevedere poate fi prevăzute doar în lege. Astfel, Guvernul, va elabora instrucțiunile privind punerea în aplicare a acestor prevederi.

	proiectului urmează să asigure compatibilitatea legislației naționale cu legislația Uniunii Europene, în acest scop, este util de a releva că potrivit aquis-ului european, 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.	
	12. 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 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 reglementează căile de atac ale actelor autorităților publice, respectiv regimul juridic al ordinelor de sistare/ blocare, emise de autorități competente, urmează a fi reglementate de a 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, sa transpus art. 2-5 din Regulamentul (UE) 2015/2120 al Parlamentului European şi 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.	**Nu se acceptă.** Codul administrativ prevede procedura de atac a deciziilor autorităților care realizează aplicarea legii.

	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. (23) lit. a) în corelare cu art. 64 alin. (21) a 2-a teză și alin. (3) din Legea nr. 241/2007 (în redacția Legii nr. 245/20020).	
	13. 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.	**Precizare** Norma privind sistarea deja este prevăzută în Legea nr. 20/2009. Proiectul de lege urmărește scopul de îmbunătățire a normei.
Serviciul Tehnologia Informației și Securitate Cibernetică	14. 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.	**Precizare** Art. II a proiectului prevede că Guvernul, până la intrarea în vigoare a acestei legi, va elabora instrucțiunile privind punerea în aplicare a prevederilor
Ministerul Justiției	15. Comunică lipsa obiecțiilor de ordin conceptual. Totodată, la Art. II alin. (1) atrage atenția că este conceptual inacceptabilă folosirea cuvintelor și altor expresii similare inexacte cum ar fi, „intră în vigoare până la", „intră în vigoare în timp de", „intră în vigoare în termen de", care de fapt se referă nu la o dată concretă, ci la o anumită perioadă, deoarece actul normativ nu poate intra în vigoare la diferite momente în interiorul unei perioade. Pentru indicarea exactă a momentului intrării în vigoare a actului normativ	**Se acceptă.** Art. II alin (1) va avea următorul cuprins: „Prezenta lege intră în vigoare.

	recomandăm utilizarea cuvintelor „la expirarea a", urmată de perioada rezervată pentru intrarea în vigoare a actului sau prin indicarea exactă a datei intrării în vigoare.	
	16. Suplimentar, Art. II alin. (2) se va revizui, întru respectarea uzanțelor normative, prin indicarea că Guvernul, până la intrarea în vigoare a prezentei legi, va aduce actele sale normative în concordanță cu prezenta lege. În cazul în care intenția a fost de a stabili competența Guvernului de a aproba acte normative pentru implementarea prevederilor Legii nr. 20/2009, această competență se va indica în conținutul prevederilor din legea dată. Astfel, de exemplu, la art. 7 alin. (1) lit. e1) se va propune nu excluderea cuvintelor „în condițiile legii", dar substituirea cu cuvintele „în modul stabilit de Guvern".	**Se acceptă.** Au fost operate modificări conform propunerii
Agenția de Guvernare Electronică	17. 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.e1) din Legea nr.20/2009 în scopul limitării temeiurilor pentru sistarea accesului la paginile web;	**Precizare** Observațiile și propunerile ATIC sunt incluse în prezenta sinteză.
	18. 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.	**Precizare** Art. II a proiectului prevede că Guvernul, până la intrarea în vigoare a acestei legi, va elabora instrucțiunile privind punerea în aplicare a prevederilor. Totodată, procedura privind conservarea datelor informatice este deja stabilită în Legea nr. 20/2009 și urmează a fi specificată MAI în calitate de autoritate care dispune măsura respectivă.

Serviciul de Informații și Securitate	19. Lipsa de obiecții și propuneri.	
Asociația Națională a Companiilor din Domeniul TIC (ATIC)	20. 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-zise1. Totuși, aceste modificări nu sunt suficiente pentru a aduce această prevedere în conformitate cu normele internaționale și constituționale. Remarcăm că o normă similară cu cea stabilită la art. 7 alin. (1) lit. e[1]) din Legea nr. 20/2009 a fost examinată anterior de Comisia de la Veneția, care a formulat mai multe observații și recomandări față de aceasta. Potrivit Comisiei, în Recomandarea sa către statele membre privind măsurile de promovare a respectării libertății de exprimare și de informare în legătură cu filtrarea conținutului de pe Internet (CM/Rec(2008)6), Comitetul de Miniștri al Consiliului Europei a declarat, inter alia, că statele ar trebui să se abțină de la filtrarea conținutului de pe Internet din alte motive decât cele prevăzute la articolul 10, paragraful 2 Convenția Europeană a Drepturilor Omului (CEDO), astfel cum este interpretat de Curtea Europeană a Drepturilor Omului (CtEDO), și ar trebui să garanteze că măsurile generale de blocare sau filtrare la nivel național sunt introduse numai dacă condițiile de la articolul 10, paragraful 2 CEDO sunt îndeplinite. Articolul 10 CEDO și art. 32, 34 și 54 din Constituția RM garantează că orice persoană are dreptul la libertate de exprimare. Acest drept include libertatea de opinie și libertatea de a primi sau a comunica informații ori idei fără amestecul autorităților publice și fără a ține seama de frontiere. Exercitarea acestor libertăți poate fi supusă unor	**Se acceptă parțial.** Art. II a proiectului prevede că Guvernul, până la intrarea în vigoare a prezentei legi, va elabora instrucțiunile privind punerea în aplicare a prevederilor din articolul 4 alineatul (1) și articolul 7 alineatul (1) litera e 1), alineatul (3) și (4) din Legea nr. 20/2009. Concomitent în cadrul proiectului art. 7 a fost completat cu alineatul (3) și (4) cu următorul cuprins: „(3) Reglementarea procedurii de sistare a accesului la pagini web în condițiile prevăzute la articolul 7 alineatul (1) litera e1) se realizează cu respectarea următoarelor principii generale: a) proporționalității; b) aplicării măsurii tehnice de sistare cel mai puțin restrictive; c) informării utilizatorilor privind motivele sistării accesului și căile de atac; d) revizuirii periodice a necesității sistării în continuare a accesului la o anumită pagină web; e) respectării dreptului furnizorilor de servicii de a aplica, din proprie inițiativă, alte măsuri pentru prevenirea utilizării abuzive a serviciilor sale. (4) Sistarea accesului la pagina web poate fi contestată în ordine de contencios administrativ." Codul administrativ prevede procedura de atac a deciziilor autorităților care realizează aplicarea legii. Pornind de la practica națională deja existentă privind sistarea/blocarea accesului la

	restrângeri sau sancțiuni prevăzute de lege care, într-o societate democratică, constituie măsuri necesare pentru securitatea națională, integritatea teritorială sau siguranța publică, apărarea ordinii şi prevenirea infracțiunilor, protecția sănătății, a moralei, a reputației sau a drepturilor altora, pentru a împiedica divulgarea informațiilor confidențiale sau pentru a garanta autoritatea şi imparțialitatea puterii judecătorești. Potrivit Comisiei, aceasta înseamnă că trebuie prevăzute motive și garanții deosebit de puternice pentru limitarea accesului publicului la Internet, măsură care, făcând cantități mari de informații inaccesibile, restrânge substanțial drepturile utilizatorilor de internet și este probabil să aibă efecte colaterale semnificative. În opinia CtEDO, restricțiile, cum ar fi ordinele de blocare a internetului „nu sunt neapărat incompatibile cu Convenția, ca principiu. Cu toate acestea, este necesar un cadru legal, care să asigure atât un control strict asupra întinderii interdicțiilor, cât și un control judiciar eficient pentru a preveni orice abuz de putere [...]. În această privință, controlul judiciar al unei astfel de măsuri, bazat pe o cântărire a intereselor concurente în joc și menit să stabilească un echilibru între ele, este de neconceput fără un cadru care să stabilească norme precise şi specifice privind aplicarea restricțiilor preventive asupra libertății de exprimare [...]" (Ahmet Yıldırım v. Turkey, Cerere Nr 3111/10, Hotărâre din 18.12.2012, § 67). De asemenea, Recomandarea precizează că „așa acțiuni de către stat ar trebui luate numai dacă filtrarea se referă la conținut specific și clar identificabil, o autoritate națională competentă a luat o decizie privind ilegalitatea acestuia și decizia poate fi revizuită de un tribunal sau de un organism de reglementare independent și imparțial, în conformitate cu cerințele articolului 6 din Convenția Europeană a Drepturilor Omului".	web site-uri ce promovează știri false privind COVID (identificate de SIS și sistarea dispusă de ANRCETI) şi 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. În analogie, legislația din statul-membru UE Franța prevede dispunerea sistării de către o subdiviziune a poliției special desemnată în acest sens.

	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".	
	21. Pentru a asigura respectarea normelor internaționale citate, se impune, în primul rând, limitarea temeiurilor pentru sistarea accesului. Referința la pagini web "ce contribuie la comiterea infracțiunilor sau la încălcarea prevederilor legislației în vigoare ori conține/difuzează instrucțiuni privind modul de comitere a acestora" este prea largă. Ținând cont de faptul că Legea nr. 20/2009 are ca obiect prevenirea și combaterea criminalității informatice 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).	**Se acceptă.** Alineatul (1) litera e^1), va avea următorul cuprins: „e^1 să sisteze, în modul stabilit de Guvern, folosind metodele și mijloacele tehnice din posesie, accesul din propriul sistem informatic la pagini web, inclusiv cele găzduite de furnizorul respectiv, destinate și utilizate pentru comiterea infracțiunilor ori conține/difuzează instrucțiuni privind modul de comitere a acestora.
	22. De asemenea, Comisia de la Veneția recomandă excluderea prevederii potrivit căreia poate servi drept temei pentru sistarea accesului faptul că o pagină web "conține/difuzează instrucțiuni privind modul de comitere a [infracțiunilor]". Totodată, norma respectivă trebuie să prevadă că sistarea accesului poate fi dispusă numai referitor la paginile web care sunt destinate 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.	**Se acceptă.** Alineatul (1) litera e^1), va avea următorul cuprins: „e^1 să sisteze, în modul stabilit de Guvern, folosind metodele și mijloacele tehnice din posesie, accesul din propriul sistem informatic la pagini web, inclusiv cele găzduite de furnizorul respectiv, destinate și utilizate pentru comiterea infracțiunilor ori conține/difuzează instrucțiuni privind modul de comitere a acestora;
	23. În al doilea rând, se impune detalierea condițiilor de aplicare a acestei măsuri. În acest scop, este necesară	**Nu se acceptă.**

	completarea Codului de procedură penală (în continuare – CPP). Observăm că art. 2 alin. (4) CPP stabilește că normele juridice cu caracter procesual din alte legi naționale pot fi aplicate numai cu condiția includerii lor în cod. În avizul său, Comisia de la Veneția, de asemenea, recomandă de a include cel puțin o parte din prevederile necesare în CPP. Prin urmare, la art. 7 alin. (1) lit. e^1) din Legea nr. 20/2009 trebuie păstrată sintagma „în condițiile legii".	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. Prin analogie, legislația din statul membru UE Franța prevede dispunerea sistării de către o subdiviziune a poliției special desemnată în acest sens.
	24. Printre detaliile care trebuie să fie reglementate în CPP pot fi evidențiate următoarele: Stabilirea infracțiunilor sau categoriilor de infracțiuni pentru comiterea cărora se permite sistarea accesului la pagina web.	**Precizare** Din punct de vedere practic, poate fi folosită o pagină web pentru contribuire la comiterea oricărui gen de infracțiune. Respectiv, considerăm inoportună indicarea unei liste vaste de articole din codul penal. Procedura urmează a fi detaliată în Hotărâre de Guvern.
	25. Stabilirea procedurii de autorizare a măsurii de sistare a accesului (poate fi similară cu cea stabilită pentru autorizarea măsurilor procesuale de constrângere), inclusiv: a. organului abilitat de a autoriza asemenea măsură, la propunerea cui 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).	**Nu se acceptă.** 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

	b. etapei procesului penal la care este posibilă dispunerea unei asemenea măsuri, de exemplu, doar după pornirea urmăririi penale. c. elementelor pe care trebuie să le conțină actul procesual prin care se autorizează măsură respectivă, de exemplu, conținutul online ilicit sau activitatea ilicită desfășurată prin intermediul paginii web, încadrarea juridică a acestei activități, motivarea necesității aplicării acestei măsuri, precum și adresa URL a paginii web accesul la care trebuie sistat. d. La soluționarea chestiunii privind necesitatea aplicării măsurii respective, procurorul și instanța de judecată trebuie să evalueze și să stabilească dacă măsura este proporțională cu circumstanțele individuale ale cauzei penale, inclusiv dacă sistarea accesului la pagina web este este cea mai puțin restrictivă măsură pentru atingerea scopului legitim, de exemplu, dacă este posibilă eliminarea a conținutului online ilicit la sursă de către furnizorul acestuia sau de către furnizorul serviciilor de găzduire a conținutului online. e. Copia de pe ordonanța procurorului sau prin încheierea instanței de judecată trebuie adusă la cunoștința furnizorului de conținut online ilicit (dacă este posibilă identificarea acestuia), în termenul care să fie stabilit prin lege. Stabilirea actului prin care se dispune măsura respectivă și conținutul acestuia.	respective. Menționăm că poliția este organ de constatare a infracțiunilor, la fel precum SIS și ASP constată ilegalitate altor categorii de informații din internet. Prin analogie, legislația din statul membru UE Franța prevede dispunerea sistării de către o subdiviziune a poliției special desemnată în acest sens.
	26. 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). 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	**Nu se acceptă.** Codul administrativ prevede procedura de atac a deciziilor autorităților care realizează aplicarea legii.

	utilizatorii și/sau autorii de conținut susțin că conținutul a fost blocat nerezonabil".	
	27. Stabilirea procedurii de revocare şi încetare a actelor privind autorizarea şi dispunerea unei asemenea măsuri (poate fi similară cu cea stabilită pentru autorizarea măsurilor procesuale preventive), inclusiv temeiurile revocării şi încetării, organul abilitat să dispună acest lucru, la propunerea cui şi prin care act procesual. De exemplu, măsura se revocă de către organul care a dispus-o dacă temeiurile care au servit la aplicarea acesteia au dispărut şi măsura nu mai este justificată, cu înștiințarea furnizorului de conținut online respectiv.	**Precizare** Art. II a proiectului prevede că Guvernul, până la intrarea în vigoare a prezentei legi, va elabora instrucțiunile privind punerea în aplicare a prevederilor din articolul 4 alineatul (1) și articolul 7 alineatul (1) litera e 1), alineatul (3) și (4) din Legea nr. 20/2009. Concomitent în cadrul proiectului art. 7 a fost completat cu alineatul (3) și (4) cu următorul cuprins : „(3) Reglementarea procedurii de sistare a accesului la pagini web în condițiile prevăzute la articolul 7 alineatul (1) litera e^1) se realizează cu respectarea următoarelor principii generale: a) proporționalității; b) aplicării măsurii tehnice de sistare cel mai puțin restrictive; c) informării utilizatorilor privind motivele sistării accesului și căile de atac; d) revizuirii periodice a necesității sistării în continuare a accesului la o anumită pagină web; e) respectării dreptului furnizorilor de servicii de a aplica, din proprie inițiativă, alte măsuri pentru prevenirea utilizării abuzive a serviciilor sale. (4) Sistarea accesului la pagina web poate fi contestată în ordine de contencios administrativ."
	28. Condițiile sistării accesului la paginile web în afara procesului penal urmează a fi reglementate prin legile speciale (de exemplu, art. 46 din Legea nr. 120/2017 cu privire la prevenirea şi combaterea terorismului, art. 48 din Legea nr. 291/2016 cu privire la organizarea şi desfășurarea jocurilor de	**Precizare** Procedura este deja prevăzută în legea specială Legea nr. 20/2009 privind prevenirea şi combaterea criminalității informatice.

	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 şi drepturile conexe).	
	29. Conservarea datelor informatice şi a datelor privind traficul informatic. Aşa cum am remarcat mai sus, art. 2 alin. (4) CPP stabileşte că normele juridice cu caracter procesual din alte legi naționale pot fi aplicate numai cu condiția includerii lor în cod. Prin urmare, norma prevăzută la art. 4 alin. (2) şi art. 7 alin. (1) lit. c) din Legea nr. 20/2009 trebuie dublată şi detaliată în CPP.	**Nu se acceptă.** Conservarea datelor informatice nu presupune şi obținerea acestor date, ci doar prelungirea termenului de păstrare. Respectiv, norma este reglementată în lege specială, la fel cum obligația furnizorilor de servicii de păstrare a datelor cu privire la utilizatori este prevăzută în legi sectoriale în domeniul TIC.
	30. Procedura şi garanțiile procesuale pentru efectuarea acestei măsuri sunt stabilite la art. 16, 17 şi 29 din Convenția privind criminalitatea informatică. În conformitate cu aceste norme, se propune următoarea redacție a articolului dedicat din CPP: „Articolul [XXX]. Conservarea rapidă a datelor informatice (1) Prin conservarea rapidă a datelor informatice se înțelege păstrarea şi protejarea integrității datelor informatice, inclusiv a datelor referitoare la trafic, stocate prin intermediul unui sistem informatic, efectuată în scopul de a permite autorităților competente să obțină dezvăluirea acestora. (2) Conservarea rapidă a datelor informatice se dispune atunci când există motive de a crede că acestea sunt în mod special susceptibile de pierdere sau de modificare. (3) Conservarea se dispune de procuror, prin ordonanța 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;	**Nu se acceptă.** Conservarea datelor informatice nu presupune şi obținerea acestor date, ci doar prelungirea termenului de păstrare. Respectiv, norma este reglementată în lege specială, la fel cum obligația furnizorilor de servicii de păstrare a datelor cu privire la utilizatori este prevăzută în legi sectoriale în domeniul TIC.

	b) persoana asupra căreia se pune obligație de conservare; c) infracțiunea care face obiectul urmăririi penale şi prezentarea succintă a faptelor care au legătură cu aceasta; d) datele informatice specifice ce urmează a fi conservate, inclusiv numele şi prenumele persoanei sau persoanelor ale căror date trebuie să fie conservate (dacă acestea sunt disponibile), genul de date care trebuie conservate, perioada de 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 şi de a le menține integritatea, cu păstrarea confidențialității cu privire la aplicarea acestei măsuri; şi g) perioada de păstrare a datelor informatice ce urmează a fi conservate. (5) Măsura conservării poate fi prelungită de către procuror o singură dată pentru motive temeinic justificate, pe o durată maximă de 90 de zile. (6) Extrasul din ordonanța procurorului, care trebuie să cuprindă informațiile specificate la literele a), b), d), f) şi g) din alin. (4), se transmite persoanei în posesia sau sub controlul căreia se află datele stocate, aceasta fiind obligată să asigure conservarea lor rapidă, cu păstrarea confidențialității cu privire la aplicarea acestei măsuri. (7) În cazul în care în transmiterea 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 şi a canalelor prin intermediul căruia comunicaţia a fost transmisă. (8) Procurorul este obligat să dispună încetarea conservării, înaintea expirării perioadei pentru care a fost dispusă, de îndată ce au dispărut temeiurile şi motivele care au justificat-o. (9) Procurorul dispune ridicarea datelor conservate de la persoana care le-a conservat în termenul prevăzut în alin. (3) sau (5), după caz. Ridicarea datelor conservate se efectuează în conformitate cu prevederile art. 125-132. Până la terminarea urmăririi penale, procurorul este obligat să anunţe, în scris, utilizatorii ale căror date au fost conservate."	
Agenţia Servicii Publice	31. Lipsa de obiecţii şi propuneri	
SINTEZA obiecţiilor şi propunerilor parvenite repetat la proiectul de lege pentru modificarea Legii nr. 20/2009 privind prevenirea şi combaterea criminalităţii informatice (număr unic 104/MAI/2023)		
Ministerul Justiţiei	32. La Art. II alin. (2), nu este suficient a prevedea competenţa de elaborare, fiind necesar a stabili competenţa de aprobare a actelor normative.	**Se acceptă.** Art. II. – (1) Prezenta lege intră în vigoare în termen de 3 luni de la data publicării în Monitorul Oficial al Republicii Moldova. (2) Guvernul, până la intrarea în vigoare a prezentei legi, va elabora şi aproba instrucţiunile privind punerea în aplicare a prevederilor din articolul 7 alineatul (1) litera e^1) din Legea nr. 20/2009.
Serviciul de Informaţii Şi Securitate	33. La Articolul I: - la pct. 1, articolul 4 propunem a se completa cu următorul conţinut: „la alineatul (3) sintagma „activităţi operative de investigaţii" a se substitui cu sintagma „activităţi	**Nu se acceptă.** Legea nr. 20/2009 prevede la art. 1 ca obiect prevenirea şi combaterea infracţiunilor informatice, respectiv măsurile contrainformative/ informative externe depăşesc sfera de aplicare a legii menţionate.

	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.	
	34. - 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.).	**Nu se acceptă.** Furnizarea serviciilor de închiriere a sistemelor informaționale, cum ar fi cele de hosting poate fi realizată și în regim online către clienții din alte state. Totodată, în condițiile în care aceeași furnizori de servicii prestează și servicii de telefonie mobilă cu internet în baza cartelelor prepay fără identificare în baza actelor de identitate, la moment nu este oportună limitarea serviciilor doar la utilizatorii identificați. De asemenea, plata serviciilor se realizează nu numai prin transfer bancar, dar și prin alte servicii de plăți electronice. Astfel, identificare utilizatorilor de către furnizori de astfel de servicii ar putea fi ca obiect al unui alt proiect de lege.
	35. 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 şi Codul de procedură penală nr. 122/2003. Astfel, operarea modificării propuse este necesară în vederea utilizării unei terminologii constante,	**Se acceptă.** La articolul 9 și pe tot parcursul textului legii cuvintele „activitatea operativă de investigații" se substituie cu cuvintele „activitatea specială de investigații", la forma gramaticală corespunzătoare.

	uniforme şi 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).	
Agenția Națională pentru Reglementare în Comunicații Electronice şi Tehnologia Informației	36. Considerăm că modificarea art. 7, în special a alin. (1) lit. e^1) şi completarea acestuia cu alineate noi, respectiv (3) şi (4), urmează să reflecte mecanismul de sistare/blocare, similar celui în dreptul Uniunii europene, care este conform cu cerințele art. 3 alin. (3) şi art. 30 alin. (1) lit. c) din Legea nr. 100/2017.	**Nu se acceptă.** Reieşind din faptul că procedura de sistare este una tehnică, considerăm inoportună îngreunare legii cu astfel de prevederi detaliate.
	37. Aşa 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 şi (ii) contestare cu aquis-ului european, în special conform Directivei 2011/93/UE a Parlamentului European şi a Consiliului din 13 decembrie 2011 privind combaterea abuzului sexual; (ii) Regulamentul (UE) 2021/784 al Parlamentului European şi al Consiliului din 29 aprilie 2021 privind prevenirea diseminării conținutului online cu caracter terorist şi (iii) Regulamentul (UE) 2021/1232 al Parlamentului European şi al Consiliului din 14 iulie 2021 privind o derogare temporară de la anumite dispoziții ale Directivei 2002/58/CE în ceea ce priveşte utilizarea tehnologiilor de către furnizorii de servicii de comunicații interpersonale care nu se bazează pe numere pentru prelucrarea datelor cu caracter personal şi a altor date în scopul combaterii abuzului sexual online asupra copiilor şi a (iv) Regulamentului (UE) 2022/2065 al Parlamentului European şi al Consiliului din 19 octombrie 2022 privind o piață unică pentru serviciile digitale (Regulamentul privind serviciile digitale).	**Precizare.** În procesul de elaborare a proiectului, au fost luate în considerație actele normative ale UE la care se face referință în avizul ANRCETI. De menționat că actele respective nu detaliază procedura de sistare a accesului.
	38. Conform dreptului UE, sistarea este admisibilă în cazurile de prevenire, investigare, detectare şi urmărire în justiție a unor infracțiuni grave, deosebit de grave şi	**Precizare.** Dreptul UE în procedura de sistare nu pune accent pe categoria de infracțiuni (grave ş.a.) dar

	excepțional de grave, respectiv, nu este proporțional ca sistarea să se realizeze pentru orice faptă.	pe pericolul social al acestei fapte. Spre exemplu, Directiva 2011/93/UE a Parlamentului European și a Consiliului din 13 decembrie 2011 privind combaterea abuzului sexual face referire la infracțiunea de pornografie infantilă, care conform CP al RM (art. 208/1) este o infracțiune mai puțin gravă.
	39. 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. 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^1) din același act legislativ.	**Nu se acceptă.** Procedura de sistare urmează a fi aplicată și până la etapa procesului penal, având un aspect de prevenire a posibilității de accesare prin intermediul serviciilor furnizorilor din Republica Moldova a conținutului respectiv, precum și prevenirii răspândirii infracțiunii în spațiul internet. Spre exemplu, în cazul în care este răspândită adresa URL a unui web site cu conținut de pornografie infantilă, unui web site care promovează terorismul, sau este un web site de phising, este posibil ca site-ul respectiv să fie creat de către o persoană din alt stat și în lipsa unor victime din Republica Moldova, fapta dată deși este infracțională, nu cade sub incidența legii penale naționale după principiul acțiunii legii în spațiu. Totodată, legea procesual penală prevede contestarea acțiunilor organului de urmărire penală ce se reflectă asupra unei persoane concrete, în timp ce sistarea accesului presupune interzicerea accesării unei resurse din internet de către publicul larg.
	40. Așa fiind, urmează a se consacra un mecanism prin lege și nu prin acte normative subordonate legii - potrivit art. 72	**Precizare.** Procedura de atac a deciziilor autorităților executive printr-o acțiune în contencios

	din Constituție, prin lege organică se reglementează căile de atac ale actelor autorităților publice.	administrativ este prevăzută în Codul administrativ.
Asociația Națională a Companiilor sectorul TIC (ATIC)	41. 1. Sistarea accesului la paginile web O normă similară cu cea stabilită la art. 7 lit. (1) lit. e[1]) din Legea nr. 20/20092 a fost examinată anterior de Comisia de la Veneția, care a formulat mai multe observații şi recomandări față de aceasta. Potrivit Comisiei, în Recomandarea sa către statele membre privind măsurile de promovare a respectării libertății de exprimare şi de informare în legătură cu filtrarea conținutului de pe Internet (CM/Rec(2008)6)4, Comitetul de Miniștri al Consiliului Europei a declarat, inter alia, că statele ar trebui să se abțină de la filtrarea conținutului de pe Internet din alte motive decât cele prevăzute la articolul 10, paragraful 2 Convenția Europeană a Drepturilor Omului (CEDO), astfel cum este interpretat de Curtea Europeană a Drepturilor Omului (CtEDO), şi ar trebui să garanteze că măsurile generale de blocare sau filtrare la nivel național sunt introduse numai dacă condițiile de la articolul 10, paragraful 2 CEDO sunt îndeplinite. Articolul 10 CEDO şi art. 32, 34 şi 54 din Constituția RM garantează că orice persoană are dreptul la libertate de exprimare. Acest drept include libertatea de opinie şi libertatea de a primi sau a comunica informații ori idei fără amestecul autorităților publice şi fără a ţine 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 şi prevenirea infracțiunilor, protecţia sănătății, a moralei, a reputației sau a drepturilor altora, pentru a împiedica divulgarea informațiilor confidențiale sau pentru a garanta autoritatea şi imparțialitatea puterii judecătorești.	**Precizare.** În procesul de elaborare a proiectului, a fost studiată practica statelor UE, iar un exemplu este Franța în care procedura de sistare a accesului este prevăzută în legea specială şi nu în cea procesual-penală şi anume în Legea nr. 2004-575 pentru încredere în economia digitală. Totodată, procedura de atac a deciziilor autorităților executive printr-o acțiune în contencios administrativ este prevăzută în Codul administrativ.

	Potrivit Comisiei, aceasta înseamnă că trebuie prevăzute motive și garanții deosebit de puternice pentru limitarea accesului publicului la Internet, măsură care, făcând cantități mari de informații inaccesibile, restrânge substanțial drepturile utilizatorilor de internet și este probabil să aibă efecte colaterale semnificative. În opinia CtEDO, restricțiile, cum ar fi ordinele de blocare a internetului „nu sunt neapărat incompatibile cu Convenția, ca principiu. Cu toate acestea, este necesar un cadru legal, care să asigure atât un control strict asupra întinderii interdicțiilor, cât și un control judiciar eficient pentru a preveni orice abuz de putere [...]. În această privință, controlul judiciar al unei astfel de măsuri, bazat pe o cântărire a intereselor concurente în joc și menit să stabilească un echilibru între ele, este de neconceput fără un cadru care să stabilească norme precise și specifice privind aplicarea restricțiilor preventive asupra libertății de exprimare [...]" (Ahmet Yildirim v. Turkey, Cerere Nr 3111/10, Hotărâre din 18.12.2012, § 67). De asemenea, Recomandarea precizează că „așa acțiuni de către stat ar trebui luate numai dacă filtrarea se referă la conținut specific și clar identificabil, o autoritate națională competentă a luat o decizie privind ilegalitatea acestuia și decizia poate fi revizuită de un tribunal sau de un organism de reglementare independent și imparțial, în conformitate cu cerințele articolului 6 din Convenția Europeană a Drepturilor Omului". Totodată, în Recomandarea sa CM/Rec(2016)5 privind 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".	

	42. 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]".	**Se acceptă** Art. 7 alineatul (1) litera e^1) va avea următorul cuprins : *„să sisteze, în modul stabilit de Guvern, folosind metodele şi mijloacele tehnice din posesie, accesul din propriul sistem informatic la pagini web, inclusiv cele găzduite de furnizorul respectiv, destinate şi utilizate pentru comiterea infracțiunilor".*
	43. 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. Printre detaliile care trebuie să fie reglementate în CPP pot fi evidențiate următoarele: 1. Stabilirea infracțiunilor sau categoriilor de infracțiuni pentru comiterea cărora se permite sistarea accesului la pagina web. 2. Stabilirea procedurii de autorizare a măsurii de sistare a accesului (poate fi similară cu cea stabilită pentru autorizarea măsurilor procesuale de constrângere), inclusiv: a. organului abilitat de a autoriza asemenea măsură, la propunerea cui şi prin care act procesual, de exemplu, ordonanța procurorului, emisă din oficiu sau la propunerea organului de urmărire penală, sau încheierea instanței de judecată, emisă la demersul procurorului). Subdiviziunile centrale specializate în prevenirea şi combaterea criminalității	**Nu se acceptă.** Procedura de sistare urmează a fi aplicată și până la etapa procesului penal, având un aspect de prevenire a posibilității de accesare prin intermediul serviciilor furnizorilor din Republica Moldova a conținutului respectiv, precum și prevenirii răspândirii infracțiunii în spațiul internet. Spre exemplu, în cazul în care este răspândită adresa URL a unui web site cu conținut de pornografie infantilă, unui web site care promovează terorismul, sau este un web site de phising, este posibil ca site-ul respectiv să fie creat de către o persoană din alt stat și în lipsa unor victime din Republica Moldova, fapta dată deși este infracțională, nu cade sub incidența legii penale naționale după principiul acțiunii legii în spațiu. Totodată, sistarea accesului nu este neapărat o normă juridică cu caracter procesual penal, întrucât măsurile procesual-penale din CPP se reflectă asupra unei persoane concrete urmărite penal, în timp ce sistarea accesului presupune interzicerea accesării unei resurse din internet de către publicul larg.

	informatice ale Ministerului Afacerilor Interne şi Serviciului de Informaţii şi Securitate (SIS) şi Informaţii nu pot fi calificate drept autoritate administrativă independentă şi imparţială. b. etapei procesului penal la care este posibilă dispunerea unei asemenea măsuri, de exemplu, doar după pornirea urmăririi penale. O pagină web nu poate fi calificată drept destinată şi utilizată în scopul comiterii infracţiunilor, dacă nu este pornită urmărirea penală pe faptul comiterii sau tentativei de comitere a infracţiunii. c. elementelor pe care trebuie să le conţină actul procesual prin care se autorizează măsură respectivă, de exemplu, conţinutul online ilicit sau activitatea ilicită desfăşurată prin intermediul paginii web, încadrarea juridică a acestei activităţi, motivarea necesităţii aplicării acestei măsuri, precum şi adresa URL a paginii web accesul la care trebuie sistat. Aceste elemente trebuie să permită persoanelor vizate să înţeleagă 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, ţinând cont de faptul că, potrivit art. 14 alin. (3) din Legea nr. 284/2004, furnizorii de servicii nu au obligaţia de a supraveghea informaţiile pe care le transmit sau le stochează atunci când furnizează serviciile şi nici obligaţia de a căuta în mod activ fapte sau circumstanţe din care rezultă că activităţile sunt ilicite. d. cerinţei, potrivit căreia, la soluţionarea chestiunii privind necesitatea aplicării măsurii respective, procurorul şi instanţa de judecată trebuie să evalueze şi să stabilească dacă măsura este proporţională cu circumstanţele individuale ale cauzei penale, inclusiv dacă sistarea accesului la pagina web este este cea mai puţin restrictivă măsură pentru atingerea scopului	

	legitim, de exemplu, dacă este posibilă eliminarea a conținutului online ilicit la sursă de către furnizorul acestuia sau de către furnizorul serviciilor de găzduire a conținutului online. e. 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. 3. Stabilirea actului prin care se dispune măsura respectivă şi conținutul acestuia. 4. Stabilirea procedurii de atac a actelor privind autorizarea şi dispunerea unei asemenea măsuri (poate fi similară cu cea stabilită în CPP pentru autorizarea măsurilor procesuale de constrângere). Recomandarea CM/Rec(2008)6 clarifică faptul că prevederea privind „mijloacele eficiente şi uşor accesibile de recurs şi remediere, inclusiv suspendarea filtrelor" este crucială pentru a răspunde „cazurilor în care utilizatorii şi/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 şi combaterii criminalității. 5. Stabilirea procedurii de revocare şi încetare a actelor privind autorizarea şi dispunerea unei asemenea măsuri (poate fi similară cu cea stabilită pentru autorizarea măsurilor procesuale preventive), inclusiv temeiurile revocării şi încetării, organul abilitat să să dispună acest lucru, la propunerea cui şi prin care act procesual. De exemplu, măsura se revocă de către organul care a dispus-o dacă temeiurile care au servit la aplicarea acesteia au dispărut şi măsura nu mai este justificată, cu înștiințarea furnizorului de conținut online respectiv.	

	44. Conservarea datelor informatice şi a datelor privind traficul informatic: Aşa cum am remarcat mai sus, art. 2 alin. (4) CPP stabileşte că normele juridice cu caracter procesual din alte legi naţionale pot fi aplicate numai cu condiţia includerii lor în cod. Prin urmare, norma prevăzută la art. 4 alin. (2) şi art. 7 alin. (1) lit. c) din Legea nr. 20/2009 trebuie dublată şi detaliată în CPP. Procedura şi garanţiile procesuale pentru efectuarea acestei măsuri sunt stabilite la art. 16, 17 şi 29 din Convenţia privind criminalitatea informatică. În conformitate cu aceste norme, se propune următoarea redacţie a articolului dedicat din CPP: „Articolul [XXX]. Conservarea rapidă a datelor informatice (1) Prin conservarea rapidă a datelor informatice se înţelege păstrarea şi protejarea integrităţii datelor informatice, inclusiv a datelor referitoare la trafic, stocate prin intermediul unui sistem informatic, efectuată în scopul de a permite autorităţilor competente să obţină 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 ordonanţă 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 ordonanţa de conservare trebuie să fie indicate: a) autoritatea care solicită conservarea; b) persoana asupra căreia se pune obligaţia de conservare; c) infracţiunea care face obiectul urmăririi penale şi prezentarea succintă a faptelor care au legătură cu aceasta; d) datele informatice specifice ce urmează a fi conservate, inclusiv numele şi prenumele persoanei sau persoanelor ale	**Nu se acceptă.** Conservarea datelor informatice nu presupune şi obţinerea acestor date, ci doar prelungirea termenului de păstrare. Respectiv, norma este reglementată în lege specială, la fel cum obligaţia furnizorilor de servicii de păstrare a datelor cu privire la utilizatori este prevăzută în legi sectoriale în domeniul TIC. Dispunerea conservării datelor informatice reprezintă una din atribuţiile punctului de contact 24/7 responsabil de realizarea prevederilor articolului 35 din Convenţia Budapesta. Observăm că textul propus al normei privind conservarea datelor informatice este inspirat din legea României. Subliniem faptul că legea menţionată a României prevede că punctul de contact 24/7 este în cadrul procuraturii (parchetului). În acelaşi timp, în legea din Republic Moldova prevederile privind punctul de contact 24/7 sunt diferite de cele din România şi anume Legea nr. 6/2009 pentru ratificarea Convenţiei Consiliului Europei privind criminalitatea informatică prevede că Ministerul Afacerilor Interne desemnează punctul de contact respectiv (inclusiv sub aspectul dispunerii conservării datelor informatice). Astfel, este necesar a fi prevăzută atribuţia MAI de dispunere a conservării datelor informatice. Prin analogie, legislaţia din statele UE precum Danemarca, Irlanda, Italia, Lituania, Portugalia prevede dispunerea măsurii date de către organele de poliţie, măsura fiind prevăzută în lege sectorială.

	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 şi de a le menține integritatea, cu păstrarea confidențialității cu privire la aplicarea acestei măsuri; şi g) perioada de păstrare a datelor informatice ce urmează a fi conservate. (5) Măsura conservării poate fi prelungită de către procuror o singură dată pentru motive temeinic justificate, pe o durată maximă de 90 de zile. (6) Extrasul din ordonanța procurorului, care trebuie să cuprindă informațiile specificate la literele a), b), d), f) şi g) din alin. (4), se transmite persoanei în posesia sau sub controlul căreia se află datele stocate, aceasta fiind obligată să asigure conservarea lor rapidă, cu păstrarea confidențialității cu privire la aplicarea acestei măsuri. (7) În cazul în care în transmiterea 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 şi 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 şi motivele care au justificat-o.	

	(9) Procurorul dispune ridicarea datelor conservate de la persoana care le-a conservat în termenul prevăzut în alin. (3) sau (5), după caz. Ridicarea datelor conservate se efectuează în conformitate cu prevederile art. 125-132. (10) Până la terminarea urmăririi penale, procurorul este obligat să anunțe, în scris, utilizatorii ale căror date au fost conservate."	
Procuratura Generală	45. Potrivit proiectului, Ministerul Afacerilor Interne şi Serviciul de Informații şi Securitate (în continuare MAI şi SIS) vor putea dispune prin intermediul subdiviziunilor sale centrale specializate în prevenirea şi combaterea criminalității informatice sistarea accesului la pagini web în condițiile prevăzute la articolul 7 alineatul (1) litera e[1]) din Legea 20/2009 privind prevenirea şi combaterea criminalității informatice (în continuare Legea 20/2009). Astfel, conform art. 7 alineatul (1) litera e[1]) din Legea 20/2009: „Furnizorii de servicii sânt obligați: să sisteze, în condițiile legii, folosind metodele şi mijloacele tehnice din posesie, accesul din propriul sistem informatic la toate adresele IP pe care sunt amplasate pagini web, inclusiv cele găzduite de furnizorul respectiv, ce contribuie la comiterea infracțiunilor sau la încălcarea prevederilor legislației în vigoare ori conțin/difuzează instrucțiuni privind modul de comitere a acestora". Procuratura Generală în avizul nr.4-ld/23-197,198 din 28.02.2023 a invocat că, pentru a preveni eventuale abuzuri şi/sau aprecieri arbitrare ale subdiviziunilor MAI şi 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[1]) din Legea 20/2009, consideră oportună instituirea unui sistem adecvat de garanții şi control asupra realizării acestei activități. Autorizarea de către un procuror desemnat din cadrul	**Precizare.** Urmare a consultărilor publice art. 7 alineatul (1) litera e[1]) va avea următorul cuprins : „*să sisteze, în modul stabilit de Guvern, folosind metodele şi mijloacele tehnice din posesie, accesul din propriul sistem informatic la pagini web, inclusiv cele găzduite de furnizorul respectiv, destinate şi utilizate pentru comiterea infracțiunilor*" , concomitent art. 7 se propune de completat cu alineatele (3) şi (4), cu următorul cuprins: „(3) Reglementarea procedurii de sistare a accesului la pagini web în condițiile prevăzute la articolul 7 alineatul (1) litera e[1]) se realizează cu respectarea următoarelor principii generale: a) proporționalității; b) aplicării măsurii tehnice de sistare cel mai puțin restrictive; c) informării utilizatorilor privind motivele sistării accesului şi căile de atac; d) revizuirii periodice a necesității sistării în continuare a accesului la o anumită pagină web; e) respectării dreptului furnizorilor de servicii de a aplica, din proprie inițiativă, alte măsuri pentru prevenirea utilizării abuzive a serviciilor sale.

	Procuraturii Generale a măsurii de sistare a accesului la pagini web, va contribui la prevenirea şi contracararea abuzurilor, fiind asigurate garanţii privind respectarea drepturilor şi libertăţilor fundamentale. Conform sintezei obiecţiilor şi propunerilor la proiectul de Lege, propunerea menţionată nu a fost acceptată de către autorul proiectului din motiv că, "Pornind de la practica naţională deja existentă privind sistarea/blocarea accesului la web site-uri ce promovează ştiri false privind COVID (identificate de SIS şi sistarea dispusă de ANRCETI şi privind web site-urile de jocuri de noroc nelicenţiate (identificate de ASP şi sistarea dispusă de ANRCETI), considerăm inoportună intervenţia procuraturii prin autorizarea măsurii respective. Menţionăm că poliţia este organ de constatare a infracţiunilor, la fel precum SIS şi ASP constată ilegalitate altor categorii de informaţii din internet". Considerăm că, argumentele invocate de către autorul proiectului cu referire la propunerile/obiecţiile ale Procuraturii Generale indicate supra sunt neîntemeiate. În considerarea acestor raţionamente, menţionăm că, practica naţională invocată de către autorul proiectului de Lege nu poate servi ca temei juridic pentru operarea modificărilor legislative. Totodată, efectuând un studiu al cazurilor de sistare/blocare a accesului la web site-uri, ce promovează ştiri false, constatăm că, majoritatea Ordinelor Directorului Serviciului de Informaţii şi Securitate al Republicii Moldova cu privire la blocarea accesului utilizatorilor din Republica Moldova la sursele cu conţinut on-line, care promovează informaţii false, sunt emise în temeiul art. 26-28 din Dispoziţia nr. 1 din 24.02.2022 a Comisiei pentru Situaţii Excepţionale a Republicii Moldova.	(4) Sistarea accesului la pagina web poate fi contestată în ordine de contencios administrativ. Astfel fiind instituite garanţii privind respectarea drepturilor omului şi căile de atac. Un exemplu elocvent de sistarea accesului la conţinutul infracţional este împiedicarea utilizatorilor să acceseze site-uri web care prezintă materiale de abuz sexual asupra copiilor, reprezentând o parte importantă a luptei împotriva acestei infracţiuni. Prin sistarea accesului la acest conţinut, se va diminua re-victimizarea copiilor abuzaţi, dar şi un efect de prevenire, care ar reduce riscul de săvârşire a unor infracţiuni grave în raport cu utilizatorii care vizualizează sau descărcă astfel de conţinut. În acest context, rolul de prevenire şi combaterea acestui fenomen este în competenţa subdiviziunii specializate a Ministerului Afacerilor Interne, care nu este indicată în lista autorităţilor cu dreptul de a dispune această măsură, astfel dispunând de capacităţi limitate în domeniul prevenirii acestui fenomen, comparativ cu Franţa de exemplu, în care procedura de sistare a accesului este prevăzută în legea specială şi nu în cea procesual-penală şi anume în Legea nr. 2004-575 pentru încredere în economia digitală.

	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.4-1 d/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 încălcărilor la acest capitol, fiind asigurate garanții privind respectarea drepturilor și libertăților fundamentale ale cetățenilor.	
	46. Reiterăm poziția instituțională redată în avizul precedent, precum că, 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	**Nu se acceptă.** Articolul 35 din Convenția Consiliului Europei privind criminalitatea informatică, prevede desemnarea punctelor de contact ale părților semnatare, sunt disponibile 24/7 în

	despre identitatea utilizatorului sau altei persoane, dar şi date privind conexiunile sau chiar conținutul comunicațiilor. Cu toate că autorul proiectului de Lege în Nota informativă a indicat că, conservarea datelor informatice nu prezintă în sine o ingerință în viaţa privată, deoarece nu presupune oferirea datelor respective către autoritățile abilitate, ci este o măsură de asigurare a integrității datelor pentru ulterioară obţinere în condițiile legii, considerăm că modificările propuse aduc atingerea vieții private şi de familie (art.8 din CEDO). E de menţionat că, Ghidul privitor la art.8 din CEDO presupune mai multe cerințe în raport cu respectarea drepturilor protejate şi în special: "Noile tehnologii intră, de asemenea, sub incidenţa art. 8, în special mesajele electronice (emailurile) [Copland împotriva Regatului Unit, pct. 41; Bărbulescu împotriva României (MC), pct. 72], utilizarea Internatului (Copland împotriva Regatului Unit, pct. 41-42). şi datele stocate pe servere informatice (Wieser şi Bicos Beteiligungen GmbH împotriva Austriei, pct. 45), inclusiv pe hard-diskuri (Petri Sallinen şi alţii împotriva Finlandei, pct. 71) şi dischete (Iliyct Stefanov împotriva Bulgariei, pct. 42)." Tot aici, considerăm oportun de menţionat că, conform jurisprudenţei Curții Europene a Drepturilor Omului, în calitate de ingerinţă în dreptul la respectarea corespondenţei se includ şi următoarele acte imputabile autorităților publice: - controlul corespondenţei (Campbell împotriva Regatului Unit, pct. 33), realizarea de copii (Foxley împotriva Regatului Unit, pct. 30) sau ştergerea anumitor pasaje (Pfeifer şi Plankl împotriva Austriei, pct. 43); - stocarea datelor interceptate referitoare la utilizarea telefonului, a adresei de e-mail şi a internetului (Copland împotriva Regatului Unit, pct. 44). Simplul fapt că astfel de date pot fi obținute în mod legitim, de exemplu din facturile	vederea asigurării asistenței imediate în anchete sau proceduri, care permite înghețarea datelor, și, în consecință, păstrarea probelor electronice. Punctele de contact sunt un instrument important, întrucât creează o posibilitate rapidă de conservare a probelor electronice înainte de a trimite o cerere de asistență judiciară reciprocă. Conservarea datelor informatice nu presupune și obținerea acestor date, aceste date rămân la furnizorul de servicii electronice, obligația acestuia este de păstrare. Respectiv, norma este reglementată în lege specială, la fel cum obligația furnizorilor de servicii de păstrare a datelor cu privire la utilizatori este prevăzută în legi sectoriale în domeniul TIC. (art. 20 alin. (3) lit. c) din Legea nr. 241/2007 comunicațiilor electronice*). Cu referire la practicile CEDO prezentate în aviz, aceste țin de domeniul secretului corespondenței, controlul corespondenței, realizarea de copii, ștergerea anumitor pasaje, iar stocarea datelor interceptate referitor la utilizarea telefonului, a adresei de e-mail și a internetului de către o instituție de învățământ Colegiu, ceea ce este diferit de conservarea datelor informatice de către furnizorul de servicii electronice, care conform legii sectoriale are obligația de păstrare a datelor. Prin analogie, legislația din statele UE precum Danemarca, Irlanda, Italia, Lituania, Portugalia prevede dispunerea măsurii date de către organele de poliție, măsura fiind prevăzută în lege sectorială.

	telefonice, nu constituie o piedică în calea constatării unei „ingerinţe"; de asemenea, este irelevant faptul că informaţiile nu au fost dezvăluite unor părţi terţe sau nu au fost utilizate în cadrul unor proceduri disciplinare sau de altă natură împotriva persoanei în cauză (ibidem, pct. 43). Aşadar, pentru asigurarea respectării garanţiilor fundamentale, prevăzute de art.8 al Convenţiei Europene a Drepturilor Omului, statului îi revine obligaţia pozitivă de a proteja aceste date şi a preveni abuzurile în raport cu ele. E de menţionat că, normele prevăzute la art. 4 alin. (2) şi art. 7 alin. (l) lit. e[1]) din proiectul de Lege supus avizării, poartă un caracter procesual, dar conform art.2 alin.(4) Codul de procedură penală, normele juridice cu caracter procesual din alte legi naţionale pot fi aplicate numai cu condiţia includerii lor în Cod. Prin urmare, după adoptarea Legii 20/2009 şi odată cu ratificarea de către Republica Moldova a Convenţiei Consiliului Europei privind criminalitatea informativă adoptată la Budapesta la 23.11.2001, prin Legea nr.6/2009, urma ca activul normativ naţional, 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 şi al garantării drepturilor protejate ale omului. Reieşind din cele expuse, reiterăm opinia instituţională că, proiectul de lege supus avizării nu corespunde: principiului echilibrului între reglementările concurente şi principiului respectării drepturilor şi libertăţilor fundamentale prevăzute la art. 3 din Legea nr. 100 din 22.12.2017 cu privire la actele normative.	

Ministerul Dezvoltării Economice şi Digitalizării	Lipsă de obiecţii şi propuneri.	
Ministerul Infrastructurii şi Dezvoltării Regionale	Lipsă de obiecţii şi propuneri.	
Agenţia Servicii Publice	Lipsă de obiecţii şi propuneri.	
Serviciul Tehnologia Informaţiei şi Securitate Cibernetică	Lipsă de obiecţii şi propuneri.	
Agenţia de Guvernare Electronică	Lipsă de obiecţii şi propuneri.	
Şedinţe interministeriale organizate în temeiul punctului 204 din Regulamentul Guvernului, aprobat prin Hotărârea Guvernului nr. 610/2018		
Procuratura Generală Proces-verbal nr. 1 din 11.08.2023	Conform art. 7 alineatul (1) litera e[1]) din Legea 20/2009: „Furnizorii de servicii sânt obligaţi: să sisteze, în condiţiile legii, folosind metodele şi mijloacele tehnice din posesie, accesul din propriul sistem informatic la toate adresele IP pe care sunt amplasate pagini web, inclusiv cele găzduite de furnizorul respectiv, ce contribuie la comiterea infracţiunilor sau la încălcarea prevederilor legislaţiei în vigoare ori conţin/difuzează instrucţiuni 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 şi/sau aprecieri arbitrare ale subdiviziunilor MAI şi 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[1]) din Legea 20/2009, consideră oportună instituirea unui sistem adecvat de garanţii şi control asupra realizării	**Nu se acceptă.** Având în vedere obiectul de reglementare al Legii nr. 20/2009 privind prevenirea şi combaterea criminalităţii informatice, *sistarea accesului la pagini web* se va realiza doar în condiţiile şi limitele prevenirii şi combaterii infracţiunilor informatice, în modul stabilit de Guvern şi cu respectarea strictă a unor principii stabilite la alin. (3) din proiect, precum şi cu oferirea posibilităţii de a contesta decizia în contencios administrativ. Astfel fiind instituite garanţii privind respectarea drepturilor omului şi căile de atac.

	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.	
	De asemenea, reprezentantul Procuraturii Generale a reiterat opinia potrivit căreia sintagma *„în condițiile legii”*, care este în Legea nr. 20/2009 în redacția actuală corespunde criteriilor de claritate și previzibilitate și nu urmează a fi înlocuită cu sintagma *„în modul stabilit de Guvern”*. Curtea Constituțională a Republicii Moldova anterior s-a expus în privința acestei probleme de interpretare, ridicate în sesizările adresate Curții, concluzionând că, nu poate fi reținut argumentul că, sintagma „prevăzut de lege” sau „în condițiile legii” presupune că, ar trebui să existe o normă de drept echivalentă cu Legea cu excepția cazurilor în care Constituția reclamă în mod expres ca un domeniu să fie reglementat prin lege (în sens restrâns), ea interpretează conceptele „prevăzut de lege” sau „în condițiile legii” astfel cum acestea sunt interpretate de Curtea Europeană. Prevederile legale naționale pot include nu doar legile, ci și anumite reglementări interne bazate pe lege (a se vedea De Wilde, Ooms și Versyp v. Belgia, 18 noiembrie 1970). În rezultatul discuțiilor în cadrul ședinței privind sistarea accesului la paginile web de către Ministerul Afacerilor Interne, dar și obiecția cu privire la completarea art. 4 alin. (2) din Legea nr. 20/2009 în partea ce ține de conservarea imediată a datelor informatice ori a datelor referitoare la traficul informatic și reieșind din	**Nu se acceptă.** Cât privește sintagma „în modul stabilit de Guvern”, care nu este susținută de către Procuratura Generală, în favoarea textului „în condițiile legii”, se menționează că, în conformitate cu art. 14 alin. (1) lit. a) din Legea nr. 100/2017 cu privire la actele normative, Hotărârea Guvernului este un act care se adoptă de către Guvern pentru exercitarea atribuțiilor Guvernului și pentru organizarea executării legilor.

	argumentele înaintate de către autorul proiectului, s-a decis: - Se acceptă argumentele invocate de către autorul proiectului de la Obiecția nr. 45; - Se acceptă argumentele invocate de către autorul proiectului de la Obiecția nr. 46, iar în scopul concretizării că datele conservate sunt păstrate la furnizor și nu la organul de urmărire penală, cum ar putea fi interpretat eronat, Procuratura Generală a înaintat propunerea de completare a alin. (2) din proiect, în următoarea redacție: *„ , dispune conservarea imediată de către furnizorii de servicii a datelor informatice ori a datelor referitoare la traficul informatic".*	
Serviciul de Informații și Securitate Proces-verbal nr. 2 din 11.08.2023	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".* Astfel, autorul proiectului a menționat că obiectul de reglementare a proiectului de lege este îngust și se limitează doar la prevenirea şi combaterea infracțiunilor informatice, respectiv are un efect de prevenire și nicidecum nu se extinde asupra a factorilor de risc și a amenințărilor externe sau de proveniență externă la adresa securității naționale, care au un spectru cu mult mai larg, încadrându-se în sfera securității cibernetice şi nu neapărat reprezintă infracțiuni informatice. Prin urmare, SIS a acceptat argumentele invocate de către autorul proiectului, cu următoarea formulare: Art. 4 alin. (3) va avea următorul cuprins: *„Serviciul de Informații și Securitate desfășoară activități de prevenire și combatere a criminalității informatice ce prezintă amenințări*	**Se acceptă.**

	la adresa securității statului, precum și de depistare a legăturilor organizațiilor criminale internaționale."	
	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".* De către autor au fost aduse argumente că unele servicii sunt furnizate în internet de la distanță, prin contractare online. Totodată, în practica UE furnizarea serviciilor fără identitate, precum PrePay nu este interzisă. Prin urmare, SIS a acceptat argumentele invocate de către autorul proiectului de excludere a propunerii și ca fiind neacceptată.	
	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).	**Se acceptă.** De către autorul proiectului propunerea de completare a proiectului cu un punct nou, prin care să fie operate modificări la art. 9 al Legii nr. 20/2009, astfel încât, textul *„activitatea operativă de investigații"* să fie substituită cu textul *„activitate specială de investigații"*.
Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației	Se comunică despre susținerea de principiu a proiectului, iar procedura de sistare a accesului la paginile web să fie cât mai clară și transparentă. De asemenea, s-a propus de elaborat o listă exhaustivă ale elementelor constitutive a condițiilor pentru blocarea accesului la paginile web, de precizat sensul termenului de infracțiuni informatică pentru a fi clar pe ce	**Se acceptă.**

	genuri de infracțiuni este posibilă aplicarea măsurii de sistare a accesului, cine va constata infracțiunile și la ce etapă și reieșind din argumentele înaintate de către autorul proiectului, s-a decis: *Toate sugestiile menționate în cadrul ședinței urmează a fi sistematizate și incluse în hotărârea de Guvern, conform celor menționate la art. 7 alin. (1) lit. e1) din proiect.*	
Asociația Națională a Companiilor din sectorul TIC (ATIC)	În linii generale ATIC susține proiectul. Totodată, având în vedere că Legea nr. 20/2009 face parte din sistemul legislației procesual penale, a fost recomandat ca sistarea accesului la paginile web, să fie posibil doar în cadrul procesului penal, pe motiv că: - potrivit art. 7 alin. (1) lit. e1), furnizorii sunt obligați *„să sisteze, în modul stabilit de Guvern, folosind metodele și mijloacele tehnice din posesie, accesul din propriul sistem informatic la pagini web, inclusiv cele găzduite de furnizorul respectiv,* ***destinate și utilizate pentru comiterea infracțiunilor".*** Respectiv stabilirea existenței/inexistenței elementelor constitutive ale unei infracțiuni se poate realiza doar în cadrul procesului penal de către organul de urmărire penală/procuror. - procedura de sistare, categoriile de infracțiunii pentru care pot fi solicitate sistările, organele care urmează să autorizeze sistarea necesită să fie regăsite în Codul de procedură penală (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). - sistarea accesului la paginile web, necesită să fie autorizate de către instanța de judecată sau procuror, în scopul evitării abuzurilor din cauza lipsei unui control judiciar (este	**Nu se acceptă.** Această procedură urmează să se realizeze până la etapa procesului penal, având un aspect de prevenire a posibilității de accesare prin intermediul serviciilor furnizorilor din Republica Moldova a conținutului respectiv, precum și prevenirii răspândirii infracțiunii în spațiul internet.

	recomandat şi de Comisia de la Veneţia care a examinat anterior o normă similară cu cea stabilită la art. 7 alin. (1) lit. e1) din Legea nr. 20/2009) /de văzut recomandările ATIC/. La fel pentru protecţia copiilor împotriva impactului negativ al informaţiei, în afara procesului penal a fost propusă completarea cu un nou art. 51 al Legii nr. 30 din 07.03.2013 cu privire la protecţia copiilor împotriva impactului negativ al informaţiei cu următoarele alienate noi: Articolul 5^1. Blocarea paginilor web ce conţin pornografie infantilă, promovează abuzul sexual sau exploatarea sexuală a copiilor Furnizorii de servicii de acces la Internet, la decizia Agenţiei Naţionale pentru Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei, bazată pe lista de pagini web elaborată de Organizaţia Internaţională a Poliţiei Criminale (The INTERPOL "Worst of" List) şi comunicată de Inspectoratul General al Poliţiei, au obligaţia de a sista, fără întârzieri nejustificate, folosind metodele şi mijloacele tehnice din posesie, accesul din propriile reţele publice de comunicaţii electronice la paginile web respective. Reieşind din argumentele înaintate de către autorul proiectului, s-a decis: *Asociaţia Naţională a Companiilor din sectorul TIC îşi menţine obiecţia în legătură cu procedura de sistare accesului la pagini web, prin care aceasta urmează a fi aplicată doar în cadrul unui proces penal şi în baza Codului de procedură penală sau cu supravegherea/autorizarea fie a procurorului, fie a instanţei de judecată.*	
Şedinţa de lucru organizată pentru definitivarea proiectului de lege pentru modificarea Legii nr. 20/2009 privind prevenirea şi combaterea criminalităţii informatice (număr unic 104/MAI/2023)		
1. Procuratura Generală **2. Ministerul Justiţiei**	La 8 mai 2024, în cadrul şedinţei de lucru a fost definitivat proiectul de lege menţionat, conform propunerilor	**Se acceptă,** proiectul de lege a fost modificat conform propunerilor şi obiecţiilor formulate.

3. Serviciul de Informații și Securitate **4. Asociația națională a companiilor din sectorul tehnologii informaționale și comunicare**	autorităților publice vizate, care au fost acceptate și inserate în proiectul de lege. Proces-verbal se anexează.	Dovada atingerii consensului este Proces-verbal din 8 mai 2024.
Ședința de lucru a Grupului de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător în temeiul Hotărârii Guvernului nr. 23/2019 cu privire la aprobarea Metodologiei de analiză a impactului în procesul de fundamentare a proiectelor de acte normative		
Grupului de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător	**I. Aspecte introductive** Proiectul de act normativ a fost analizat prin prisma principiilor de reglementare ale activității de întreprinzător stabilite în Legea nr. 235 din 20.07.2006 cu privire la principiile de bază de reglementare a activității de întreprinzător, alte legi care conțin principii de reglementare a activității de întreprinzător (Legea nr.160/2011, Legea nr.131/2012, Legea 161/2011 ș.a.) și altor acte legislative aferente. **II. Analiza proiectului de act normativ** Însăși conceptul propus în proiect și modul de reglementare a acestui concept într-o varietate foarte mare de cazuri poate duce la încălcarea principiului proporționalității în raporturile dintre autoritate publică și întreprinzători, fiind posibilă și foarte probabilă recurgerea la acțiuni în exces necesităților atingerii scopurilor societății. Încadrarea măsurilor de constrângere în raport cu accesul la pagini web sau informația conținută pe acestea în procesul administrativ („dispunerea" în temeiul unui ordin al unui funcționar) nu se racordează cu însăși conceptul și obiectivele Codului administrativ. Luând în calcul că obiectivul măsurilor este de a combate activitatea infracțională și temeiul măsurilor sunt indici de infracțiune, nu este clar și nu este argumentat din ce cauză măsurile propuse nu sunt încadrate în activitatea	**Poziția reprezentanților MAI** **Se acceptă obiecțiile** Grupului de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător în partea ce se referă la interpretabilitatea criteriilor privind sistarea accesului la pagina web sau eliminarea de la sursă a conținutului online, ce conține informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor, cu modificarea acestora într-un sens mai restrictiv și exhaustiv. Totodată, se menționează despre atingerea consensului în privința celorlalte obiecții, fapt realizat în cadrul ședinței Grupului de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător.

	specială de investigații (în rândul măsurilor speciale de investigații conform Legii nr.59/2012). Ori procedura administrativă în sine este una destul de permisivă, lăsînd 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. Ceea ce este și mai grav, în proiect se propune ca și contestarea actului administrativ individual să fie realizată în procedura de contencios administrativ. Ori spre deosebire de procedura penală, unde povara probațiunii stă pe autoritatea publică, în contencios administrativ, povara probațiunii este totdeauna pe reclamant, adică pe persoana care contestă aplicarea măsurilor de constrângere. În circumstanțele din proiectul de lege, luând în calcul că temeiul care stă la baza aplicării măsurilor de constrângere țin în mod direct sau indirect de comiterea unei infracțiuni, de facto se propune încălcarea principiului prezumției nevinovăției (art.21 din Constituție) și obligă persoana să-și dovedească nevinovăția (contrar art.8 din Codul de Procedură Penală). Odată ce în practică, factorul de decizie din cadrul autorității publice are o libertate destul de mare de a decide aplicarea măsurii coercitive (nefiind restrâns de rigorile penale ale probatoriului ș.a. necesități de argumentare suplimentară), iar în cadrul contestării, reclamantul va fi obligat să demonstreze că măsura i-a fost aplicată eronat sau disproporționat, ceea ce în esență, în majoritatea cazurilor va presupune că reclamantul trebuie deja să dovedească că nu a comis infracțiuni sau nu a avut legătură cu comiterea acestora. Chiar dacă autorii încearcă să prevadă la alin.(4) art.4/3 că autoritatea trebuie să prezinte în instanță „materiale" ce au stat la baza emiterii ordinului, acesta nu schimbă sarcina probei de pe reclamant,	

	în limitele contenciosului, neprezentarea acestor „materiale" nu poate să influențeze procesul, nu este temei valid pentru judecător să dea câștig de cauză reclamantului. Dar și în principiu termenul „materiale" este unul foarte vag și nu presupune nicicum probe, mijloace de probă adecvate procedurii penale, obținute în modul stabilit de lege. Nu este clar ce concret poate fi sistat, fiind utilizat doar termenul „pagină web", adică tot spectrul de conținut transmis prin internet, indiferent de volumul și categoria acestuia. Ceea ce presupune că poate fi sistate portaluri întregi, platforme (marketplace), acces la baze de date și aplicații importante. În multe cazuri (cum sunt pagini de gen 999 sau facebook) un număr nelimitat de persoane are posibilitatea să creeze conținut public și monitorizarea acestuia de către deținătorul platformei este foarte complicat. Astfel fără o claritate în privința obiectului măsurii totdeauna există riscul să fie aplicată măsurile propuse în lege în mod disproporționat, abuziv și nejustificat. Temeiurile din art.4/2 alin.(1) care stau la baza emiterii ordinului, în mare parte sunt expuse foarte general, fără trimiteri la componente clare de infracțiune, corespunzător funcționarul are o marjă extrem de mare de discreție, ceea ce, chiar și involuntar, poate aduce la abuzuri. În special temeiurile prevăzute la lit. d)-g) sunt extrem de discutabile și de facto extind aria legii penale. Spre exemplu, se prevede că orice „determinare" la comiterea oricărei infracțiuni este temei de a aplica măsura coercitivă, însă Codul penal prevede un număr restrîns de infracțiuni în raport cu care se pedepsește nu doar fapta în sine dar și instigarea sau determinarea la o infracțiune. Nicidecum determinarea sau instigarea la toate infracțiunile din Cod sunt pasibile de pedeapsă penală. Sau „răspîndirea programelor utilizate la comiterea infracțiunilor", luînd în calcul că infracțiunile pot fi comise	

	practic cu orice program (depinde modul în care e folosit programul) și în lipsa clarificării termenului „maliții̦os", iese că răsîndirea majorității programelor poate fi temei pentru aplicarea măsurii. La fel, apare un șir de întrebări în privința temeiului de „promovarea substanțelor interzise prin lege" ș.a.m.d. Nu este clar și argumentat nici termenul de 30 de zile propus pentru valabilitatea ordinului. Este cel puțin contrar principiului „proporționalității" prevăzut în același articol, odată ce, conform acestui principiu, termenul trebuie să fie raportat la necesitățile procesului ce va urma (de urmărire, investigare și colectare de probe) și nu e clar din ce cauză se prevede fix sau minim 30 de zile dar nu „pînă la 30 de zile". La fel nu e clar prin ce se justifică și argumentează limitarea la 90 de zile. **III. Concluzie** Proiectul se susține condiționat.	

Secretar de Stat **Andrei CECOLTAN**