

TABEL COMPARATIV

la proiectul de lege pentru modificarea Legii nr. 20/2009 privind prevenirea și combaterea criminalității informatice

Nr. d/o	Reglementarea în vigoare	Modificările propuse	Prevederile după modificare
1.	<p>Articolul 4. Funcțiile autorităților și instituțiilor publice competente în domeniul prevenirii și combaterii criminalității informatice</p> <p>(1) Ministerul Afacerilor Interne, și Serviciul de Informații și Securitate formează și actualizează în permanență bazele de date privind criminalitatea informatică.</p> <p>(2) Ministerul Afacerilor Interne efectuează măsuri speciale de investigație, de urmărire penală, de cooperare internațională, de identificare a persoanelor care comit infracțiuni informatice.</p> <p>(3) Serviciul de Informații și Securitate desfășoară activități de prevenire și combatere a criminalității informatice ce prezintă amenințări la adresa securității naționale, activități operative de investigații, de depistare a legăturilor organizațiilor criminale internaționale, alte activități în limita competenței sale.</p>	<p>alineatul (1) se completează cu textul „ , dispun, prin ordinul emis de conducătorul subdiviziunii specializate în prevenirea și combaterea criminalității informatice, sistarea accesului la pagini web, în condițiile prevăzute la articolul 7 alineatul (1) litera e1), precum și sistarea transmiterii într-o rețea de comunicații electronice ori stocării conținutului online găzduit sau furnizat de către furnizorii de servicii de găzduire sau furnizorii de conținut, prin eliminarea acestuia la sursă, în condițiile prevăzute la articolul 7 alineatul (1) litera h).”</p> <p>alineatul (2) se completează în final cu textul „ , dispune, prin ordinul emis de conducătorul subdiviziunii specializate în prevenirea și combaterea criminalității informatice, conservarea imediată de către furnizorii de servicii a datelor informatice ori a datelor referitoare la traficul informatic, față de care există pericolul distrugerii sau alterării, în cazul</p>	<p>Articolul 4. Funcțiile autorităților și instituțiilor publice competente în domeniul prevenirii și combaterii criminalității informatice</p> <p>(1) Ministerul Afacerilor Interne, și Serviciul de Informații și Securitate formează și actualizează în permanență bazele de date privind criminalitatea informatică, dispun, prin ordinul emis de conducătorul subdiviziunii specializate în prevenirea și combaterea criminalității informatice, sistarea accesului la pagini web în condițiile prevăzute la articolul 7 alineatul (1) litera e1), precum și sistarea transmiterii ori stocării într-o rețea de comunicații electronice a conținutului online găzduit sau furnizat de către furnizorii de servicii de găzduire, prin eliminarea acestuia la sursă în condițiile prevăzute la articolul 7 alineatul (1) litera h).</p> <p>(2) Ministerul Afacerilor Interne efectuează măsuri speciale de investigație, de</p>

		<p>solicitărilor autorităților competente străine parvenite prin punctul de contact, disponibil 24/7, în conformitate cu art. 10.”.</p> <p>alineatul (3) va avea următorul cuprins:</p> <p>„(3) Serviciul de Informații și Securitate desfășoară activități de prevenire și combatere a criminalității informatice ce prezintă amenințări la adresa securității statului, precum și de depistare a legăturilor organizațiilor criminale internaționale.”.</p>	<p>urmărire penală, de cooperare internațională, de identificare a persoanelor care comit infracțiuni informatice, dispune, prin ordinul emis de conducătorul subdiviziunii specializate în prevenirea și combaterea criminalității informatice, conservarea imediată de către furnizorii de servicii a datelor informatice ori a datelor referitoare la traficul informatic, față de care există pericolul distrugerii sau alterării, în cazul solicitărilor autorităților competente străine parvenite prin punctul de contact, disponibil 24/7, în conformitate cu art. 10.</p> <p>(3) Serviciul de Informații și Securitate desfășoară activități de prevenire și combatere a criminalității informatice ce prezintă amenințări la adresa securității statului, precum și de depistare a legăturilor organizațiilor criminale internaționale.</p>
		<p>Se completează cu articolele 4¹, cu următorul cuprins:</p> <p>„Articolul 4¹. Emiterea ordinului de sistare a accesului la pagini web sau de eliminare a conținutului online la sursă</p> <p>(1) Emiterea ordinului de sistare a accesului la pagini web sau de eliminare a conținutului online la sursă, în condițiile prevăzute la articolul 7 alineatul (1) litera e¹) sau h), are loc cu respectarea următoarelor principii:</p> <p>a) proporționalității;</p>	<p>Articolul 4¹. Emiterea ordinului de sistare a accesului la pagini web sau de eliminare a conținutului online la sursă</p> <p>(1) Emiterea ordinului de sistare a accesului la pagini web sau de eliminare a conținutului online la sursă, în condițiile prevăzute la articolul 7 alineatul (1) litera e¹) sau h), are loc cu respectarea următoarelor principii:</p> <p>a) proporționalității;</p> <p>b) aplicării măsurii tehnice de sistare cel mai puțin restrictive;</p>

		<p>b) aplicării măsurii tehnice de sistare cel mai puțin restrictive;</p> <p>c) informării privind motivele sistării accesului și căile de atac;</p> <p>d) revizuirii periodice a necesității sistării în continuare a accesului la o anumită pagină web;</p> <p>e) respectării dreptului furnizorilor de servicii de a aplica, din proprie inițiativă, alte măsuri pentru prevenirea utilizării abuzive a serviciilor sale;</p> <p>f) respectării prevederilor Legii nr. 284/2004 privind serviciile societății informaționale.</p> <p>(2) Sistarea accesului la pagina web, ce conține informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor, poate fi dispusă pe un termen de 30 de zile, cu posibilitatea prelungirii acestuia, dar nu mai mult de 90 de zile. Fiecare prelungire nu poate depăși termenul de 30 de zile.</p>	<p>c) informării privind motivele sistării accesului și căile de atac;</p> <p>d) revizuirii periodice a necesității sistării în continuare a accesului la o anumită pagină web;</p> <p>e) respectării dreptului furnizorilor de servicii de a aplica, din proprie inițiativă, alte măsuri pentru prevenirea utilizării abuzive a serviciilor sale;</p> <p>f) respectării prevederilor Legii nr. 284/2004 privind serviciile societății informaționale.</p> <p>(2) Sistarea accesului la pagina web, ce conține informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor, poate fi dispusă pe un termen de 30 de zile, cu posibilitatea prelungirii acestuia, dar nu mai mult de 90 de zile. Fiecare prelungire nu poate depăși termenul de 30 de zile.</p>
		<p>Se completează cu articolele 4², cu următorul cuprins:</p> <p>Articolul 4². Criterii 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</p> <p>(1) O pagină web poate fi apreciată ca fiind destinată și utilizată pentru pregătirea sau comiterea infracțiunilor în cazul în</p>	<p>Articolul 4². Criterii 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</p> <p>(1) O pagină web poate fi apreciată ca fiind destinată și utilizată pentru pregătirea sau comiterea infracțiunilor în cazul în care, informația publicată sau oferită în orice mod pe aceasta, inclusiv sub formă de link-uri,</p>

		<p>care, informația publicată sau oferită în orice mod pe aceasta, inclusiv sub formă de link-uri, corespunde unui sau mai multor din următoarele criterii:</p> <p>a) afișarea sau distribuirea informației respective reprezintă în sine o faptă infracțională;</p> <p>b) determinarea potențialei victime a infracțiunii de a furniza anumite date sau de a întreprinde alte acțiuni ce îi provoacă un prejudiciu;</p> <p>c) determinarea persoanei să intre în contact cu infractorii;</p> <p>d) comercializarea, oferirea sau promovarea în orice mod a obiectelor sau substanțelor interzise prin lege;</p> <p>e) comercializarea sau oferirea ilegală a obiectelor sau substanțelor, circulația căror este limitată prin legea penală;</p> <p>f) răspândirea programelor malițioase, utilizate la comiterea infracțiunilor, în special a celor informatice și din domeniul comunicațiilor electronice;</p> <p>g) determinarea publică la comiterea unei infracțiuni.”.</p> <p>(2) Ordinul de sistare a accesului la paginile web se emite numai dacă conținutul online nu poate fi eliminat la sursă de către furnizorii de servicii de găzduire a conținutului online sau furnizorii de conținut online de pe teritoriul Republicii Moldova.</p>	<p>corespunde unui sau mai multor din următoarele criterii:</p> <p>a)afișarea sau distribuirea informației respective reprezintă în sine o faptă infracțională prevăzută de art. 173, 1751, 177, 178, 186, 189, 190, 2081, 237, 24510, 259–2611 Cod penal;</p> <p>b)determinarea potențialei victime a infracțiunii de a furniza anumite date sau de a întreprinde alte acțiuni, cu scopul de a obține un beneficiu material pentru sine sau pentru o altă persoană;</p> <p>c)recrutarea sau determinarea persoanei pentru favorizarea sau comiterea infracțiunilor prevăzute la lit. a);</p> <p>d)răspândirea programelor malițioase, utilizate la comiterea infracțiunilor, în special a celor informatice și din domeniul comunicațiilor electronice;</p> <p>e)comercializarea, oferirea sau promovarea în orice mod a obiectelor sau substanțelor interzise prin lege sau a căror circulație este limitată prin legea penală;</p> <p>f) distribuirea, difuzarea, importarea, procurarea, schimbarea, folosirea sau păstrarea de imagini sau alte reprezentări ale unui sau mai mulți copii implicați în activități sexuale explicite, reale sau simulate, ori de imagini sau alte reprezentări ale organelor sexuale ale unui copil, reprezentate de manieră lascivă sau obscenă;</p>
--	--	---	---

		<p>(3) Ordinul de sistare a accesului la pagini web sau de eliminare a conținutului online la sursă se publică pe pagina web a autorității competente emitente.</p> <p>(4) Autoritatea competentă, prin intermediul conducătorului subdiviziunii centrale specializate în prevenirea și combaterea criminalității informatice, este obligat să dispună încetarea sistării accesului la paginile web, înaintea expirării perioadei pentru care a fost dispusă, de îndată ce au dispărut temeiurile și motivele care au justificat-o.”.</p>	<p>g) conversații online îndreptate spre propagarea pedofiliei (interesului sexual față de minori sau actului de abuz sexual asupra copiilor).</p> <p>(2) Ordinul de sistare a accesului la paginile web se emite numai dacă conținutul online nu poate fi eliminat la sursă de către furnizorii de servicii de găzduire a conținutului online sau furnizorii de conținut online de pe teritoriul Republicii Moldova.</p> <p>(3) Ordinul de sistare a accesului la pagini web sau de eliminare a conținutului online la sursă se publică pe pagina web a autorității competente emitente.</p> <p>(4) Autoritatea competentă, prin intermediul conducătorului subdiviziunii centrale specializate în prevenirea și combaterea criminalității informatice, este obligat să dispună încetarea sistării accesului la paginile web, înaintea expirării perioadei pentru care a fost dispusă, de îndată ce au dispărut temeiurile și motivele care au justificat-o.”.</p>
		<p>Se completează cu articolele 4³, cu următorul cuprins:</p> <p>Articolul 4³. Contestarea ordinului privind sistarea accesului la pagina web sau eliminarea de la sursă a conținutului online, ce cuprinde informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor</p>	<p>Articolul 4³. Contestarea ordinului privind sistarea accesului la pagina web sau eliminarea de la sursă a conținutului online, ce cuprinde informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor</p> <p>(1) Ordinul privind sistarea accesului la pagina web sau eliminarea la sursă a conținutului online, ce cuprinde informații</p>

		<p>(1) Ordinul privind sistarea accesului la pagina web sau eliminarea la sursă a conținutului online, ce cuprinde informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor, poate fi contestat direct în instanța de judecată în raza teritorială a căreia este amplasat sediul autorității ce a emis ordinul.</p> <p>(2) Pot contesta ordinul privind sistarea accesului la pagina web sau eliminarea la sursă a conținutului online, ce cuprinde informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor, furnizorul de servicii, inclusiv a serviciilor de găzduire a conținutului online și/sau titularul paginii web (furnizorul de conținut online).</p> <p>(3) Depunerea contestației nu suspendă acțiunea ordinului privind sistarea accesului la pagina web sau eliminarea la sursă a conținutului online. Contestația se examinează de instanța de judecată în termen de 15 de zile, cu sau fără prezența părților, cărora li se comunică locul, data și ora examinării contestației.</p> <p>(4) Autoritatea care a emis ordinul privind sistarea accesului la pagina web sau eliminarea la sursă a conținutului online, ce cuprinde informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor, este obligată să prezinte în instanța de judecată materialele ce au servit</p>	<p>destinate și utilizate pentru pregătirea sau comiterea infracțiunilor, poate fi contestat direct în instanța de judecată în raza teritorială a căreia este amplasat sediul autorității ce a emis ordinul.</p> <p>(2) Pot contesta ordinul privind sistarea accesului la pagina web sau eliminarea la sursă a conținutului online, ce cuprinde informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor, furnizorul de servicii, inclusiv a serviciilor de găzduire a conținutului online și/sau titularul paginii web (furnizorul de conținut online).</p> <p>(3) Depunerea contestației nu suspendă acțiunea ordinului privind sistarea accesului la pagina web sau eliminarea la sursă a conținutului online. Contestația se examinează de instanța de judecată în termen de 15 de zile, cu sau fără prezența părților, cărora li se comunică locul, data și ora examinării contestației.</p> <p>(4) Autoritatea care a emis ordinul privind sistarea accesului la pagina web sau eliminarea la sursă a conținutului online, ce cuprinde informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor, este obligată să prezinte în instanța de judecată materialele ce au servit la emiterea ordinului de sistare, în termen de 3 zile de la primirea înștiințării.</p>
--	--	---	---

		<p>la emiterea ordinului de sistare, în termen de 3 zile de la primirea înștiințării.</p> <p>(5) Instanța de judecată, urmare a examinării contestației, emite o încheiere, care va conține una dintre următoarele soluții:</p> <p>a) admite contestația, anulează integral ordinul prin care s-a dispus sistarea accesului la pagina web sau eliminarea la sursă a conținutului online;</p> <p>b) admite parțial contestația, modifică ordinul prin care s-a dispus sistarea accesului la pagina web sau eliminarea la sursă a conținutului online;</p> <p>c) respinge contestația ca fiind neîntemeiată.</p> <p>(6) Copia de pe încheiere se expediază părților în termen de 3 zile lucrătoare de la data emiterii, iar autoritatea care a emis ordinul anulat înștiințează furnizorul de servicii despre anularea acestuia în termen de 3 zile lucrătoare de la data recepționării încheierii de anulare.</p> <p>(7) În măsura în care nu contravine prevederilor prezentei legi, se aplică prevederile Codului administrativ nr. 116/2018.</p>	<p>(5) Instanța de judecată, urmare a examinării contestației, emite o încheiere, care va conține una dintre următoarele soluții:</p> <p>a) admite contestația, anulează integral ordinul prin care s-a dispus sistarea accesului la pagina web sau eliminarea la sursă a conținutului online;</p> <p>b) admite parțial contestația, modifică ordinul prin care s-a dispus sistarea accesului la pagina web sau eliminarea la sursă a conținutului online;</p> <p>c) respinge contestația ca fiind neîntemeiată.</p> <p>(6) Copia de pe încheiere se expediază părților în termen de 3 zile lucrătoare de la data emiterii, iar autoritatea care a emis ordinul anulat înștiințează furnizorul de servicii despre anularea acestuia în termen de 3 zile lucrătoare de la data recepționării încheierii de anulare.</p> <p>(7) În măsura în care nu contravine prevederilor prezentei legi, se aplică prevederile Codului administrativ nr. 116/2018.</p>
	<p>Articolul 7. Obligațiile furnizorilor de servicii</p> <p>(1) Furnizorii de servicii sînt obligați:</p>	<p>litera e¹) va avea următorul cuprins:</p> <p>„e¹) la solicitarea autorităților competente, să sisteze, folosind metodele și mijloacele tehnice din posesie, accesul din propriul sistem informatic la pagini web, ce</p>	<p>Articolul 7. Obligațiile furnizorilor de servicii</p> <p>(1) Furnizorii de servicii sînt obligați:</p> <p>e¹) la solicitarea autorităților competente, să sisteze, folosind metodele și</p>

	<p>e¹) să sisteze, în condițiile legii, folosind metodele și mijloacele tehnice din posesie, accesul din propriul sistem informatic la toate adresele IP pe care sunt amplasate pagini web, inclusiv cele găzduite de furnizorul respectiv, ce contribuie la comiterea infracțiunilor sau la încălcarea prevederilor legislației în vigoare ori conțin/difuzează instrucțiuni privind modul de comitere a acestora;</p> <p>g) să asigure descifrarea datelor informatice care se conțin în pachetele protocoalelor de rețea cu conservarea acestor date pe o perioadă de 90 de zile calendaristice.</p>	<p>conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor;”;</p> <p>la litera g), textul „de 90 de zile” se substituie cu textul „de cel mult 90 de zile”;</p> <p>se completează cu litera h), cu următorul cuprins:</p> <p>„h) la solicitarea autorităților competente, să sisteze transmiterea într-o rețea de comunicații electronice ori stocarea conținutului online, ce cuprinde informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor, furnizat sau găzduit de aceștia, prin eliminarea conținutului respectiv la sursă.”.</p>	<p>mijloacele tehnice din posesie, accesul din propriul sistem informatic la pagini web, ce conțin informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor;</p> <p>g) să asigure descifrarea datelor informatice care se conțin în pachetele protocoalelor de rețea cu conservarea acestor date pe o perioadă de cel mult 90 de zile calendaristice.</p> <p>h) la solicitarea autorităților competente, să sisteze transmiterea într-o rețea de comunicații electronice ori stocarea conținutului online, ce cuprinde informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor, furnizat sau găzduit de aceștia, prin eliminarea conținutului respectiv la sursă.</p>
--	--	---	--

<p>Articolul 9. Activitatea operativă de investigații și de urmărire penală desfășurată în comun</p> <p>(1) La solicitarea autorităților naționale competente sau ale altor state, pe teritoriul Republicii Moldova se pot desfășura, în condițiile legii, activități operative de investigații în cadrul urmăririi penale comune în vederea prevenirii și combaterii criminalității informatice.</p> <p>(2) Anchetele comune se vor desfășura și în bază de acorduri bilaterale sau multilaterale încheiate de autoritățile competente.</p> <p>(3) Reprezentanții autorităților competente din Republica Moldova pot participa la anchete comune desfășurate pe teritoriul unor alte state, cu respectarea legislației lor.</p>	<p>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.</p>	<p>Articolul 9. Activitatea specială de investigații și de urmărire penală desfășurată în comun</p> <p>(1) La solicitarea autorităților naționale competente sau ale altor state, pe teritoriul Republicii Moldova se pot desfășura, în condițiile legii, activități speciale de investigații în cadrul urmăririi penale comune în vederea prevenirii și combaterii criminalității informatice.</p> <p>(2) Anchetele comune se vor desfășura și în bază de acorduri bilaterale sau multilaterale încheiate de autoritățile competente.</p> <p>(3) Reprezentanții autorităților competente din Republica Moldova pot participa la anchete comune desfășurate pe teritoriul unor alte state, cu respectarea legislației lor.</p>
---	---	---