



LEGE

privind prevenirea și combaterea criminalității informatice

nr. 20-XVI din 03.02.2009

Monitorul Oficial nr.11-12/17 din 26.01.2010

* * *

C U P R I N S

Capitolul I

DISPOZIȚII GENERALE

[Articolul 1.](#) Obiectul de reglementare

[Articolul 2.](#) Noțiuni principale

[Articolul 3.](#) Principiile de bază ale prevenirii și combaterii criminalității informatice

Capitolul II

CADRUL INSTITUȚIONAL

[Articolul 4.](#) Funcțiile autorităților și instituțiilor publice competente în domeniul prevenirii și combaterii criminalității informatice

[Articolul 4¹.](#) Emiterea ordinului de sistare a accesului la o pagină web sau de eliminare a conținutului online la sursă

[Articolul 4².](#) Criterii privind sistarea accesului la o pagină web ce cuprinde informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor sau privind eliminarea la sursă a conținutului online ce cuprinde informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor

[Articolul 4³.](#) Contestarea ordinului de sistare a accesului la o pagină web sau de eliminare a conținutului online la sursă

[Articolul 5.](#) Colaborarea autorităților competente în prevenirea și combaterea criminalității informatice

[Articolul 6.](#) Obligațiile proprietarilor de sisteme informatice

[Articolul 7.](#) Obligațiile furnizorilor de servicii

Capitolul III

COOPERAREA INTERNAȚIONALĂ

[Articolul 8.](#) Cooperarea internațională a autorităților competente

[Articolul 9.](#) Activitatea specială de investigații și de urmărire penală desfășurată în comun

[Articolul 10.](#) Solicitățile autorităților competente străine

Capitolul IV

RĂSPUNDEREA

[Articolul 11.](#) Răspunderea pentru încălcarea prezentei legi

Capitolul V

DISPOZIȚII FINALE

[Articolul 12.](#) Intrarea în vigoare. Îndatoririle Guvernului

Parlamentul adoptă prezenta lege organică.

Capitolul I **DISPOZIȚII GENERALE**

Articolul 1. Obiectul de reglementare

Prezenta lege reglementează raporturile juridice privind:

- a) prevenirea și combaterea infracțiunilor informatice;
- b) cadrul de asistență mutuală în prevenirea și combaterea criminalității informatice, în protecția și acordarea de ajutor furnizorilor de servicii și utilizatorilor de sisteme informatice;
- c) colaborarea autorităților administrației publice cu organizații neguvernamentale și cu alți reprezentanți ai societății civile în activitatea de prevenire și de combatere a criminalității informatice;
- d) cooperarea cu alte state, cu organizații internaționale și regionale avînd competențe în domeniu.

Articolul 2. Noțiuni principale

În sensul prezentei legi, următoarele noțiuni principale semnifică:

sistem informatic – orice dispozitiv izolat sau ansamblu de dispozitive interconectate ori aflate în legătură care asigură ori dintre care unul sau mai multe elemente asigură, prin executarea unui program, prelucrarea automată a datelor;

date informatice – orice reprezentare de fapte, informații sau concepte sub o formă adecvată prelucrării într-un sistem informatic, inclusiv un program capabil să determine executarea unei funcții de către un sistem informatic;

furnizor de servicii – orice entitate publică sau privată care oferă utilizatorilor serviciilor sale posibilitatea de a comunica prin intermediul unui sistem informatic, precum și orice altă entitate care prelucrează sau stochează date informatice pentru acest serviciu de comunicații sau pentru utilizatorii săi;

date referitoare la trafic – orice date avînd legătură cu o comunicare transmisă printr-un sistem informatic, produse de acest sistem în calitate de element al lanțului de comunicare, indicînd originea, destinația, itinerarul, ora, data, mărimea, durata sau tipul de serviciu subiacent;

date referitoare la utilizatori – orice informație, sub formă de date informatice sau sub orice altă formă, deținută de un furnizor de servicii, referitoare la abonații acestor servicii, altele decît datele referitoare la trafic sau conținut, și care permit stabilirea: tipului de serviciu de comunicații utilizat, dispozițiilor tehnice luate în această privință și perioadei serviciului; identității, adresei poștale sau geografice, numărului de telefon al abonatului și oricărui alt număr de contact, precum și a datelor referitoare la facturare și plată, disponibile în baza unui contract sau a unui aranjament de servicii; oricărei alte informații referitoare la locul în care se găsesc echipamentele de comunicație, disponibile în baza unui contract sau a unui aranjament de servicii, precum și a oricăror alte date care pot conduce la identificarea utilizatorului;

măsuri de securitate – folosirea unor proceduri, dispozitive sau programe informatice specializate cu ajutorul cărora accesul la un sistem informatic este restricționat sau interzis pentru anumite categorii de utilizatori.

[Art.2 completat prin [Legea nr.45 din 22.03.2013](#), în vigoare 12.04.2013]

Articolul 3. Principiile de bază ale prevenirii și combaterii criminalității informatice

Prevenirea și combaterea criminalității informatice se efectuează pe următoarele principii:

- a) legalitatea;
- b) respectarea drepturilor și libertăților fundamentale ale omului;
- c) operativitatea;
- d) inevitabilitatea pedepsei;

- e) securitatea informatică și protecția datelor cu caracter personal;
- f) utilizarea complexă a măsurilor de profilaxie: juridice, social-economice și informatice;
- g) parteneriatul social, colaborarea autorităților administrației publice cu organizații internaționale, cu organizații neguvernamentale, cu alți reprezentanți ai societății civile.

Capitolul II

CADRUL INSTITUȚIONAL

Articolul 4. Funcțiile autorităților și instituțiilor publice competente în domeniul prevenirii și combaterii criminalității informatice

(1) Ministerul Afacerilor Interne și Serviciul de Informații și Securitate:

- a) formează și actualizează în permanență bazele de date privind criminalitatea informatică;
- b) dispun, prin ordinul emis de conducătorul subdiviziunii specializate în prevenirea și combaterea criminalității informatice, sistarea accesului la pagini web, în condițiile prevăzute la art.7 alin.(1) lit.e¹), precum și sistarea transmiterii într-o rețea de comunicații electronice sau a 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 art.7 alin.(1) lit.h).

(2) Ministerul Afacerilor Interne:

- a) efectuează măsuri speciale de investigații, de urmărire penală, de cooperare internațională, de identificare a persoanelor care comit infracțiuni informatice;
- b) dispune, prin ordinul emis de conducătorul subdiviziunii specializate în prevenirea și combaterea criminalității informatice, conservarea imediată, de către furnizorii de servicii, a datelor informatice sau a datelor referitoare la traficul informatic față de care există pericolul distrugerii sau alterării, în cazul solicitărilor autorităților competente străine transmise prin punctul de contact, disponibil 24/7, în conformitate cu art.10.

(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.

(4) Procuratura Generală:

- a) coordonează, conduce și exercită urmărirea penală, în modul prevăzut de lege;
- b) dispune, în cadrul desfășurării urmăririi penale, la solicitarea organului de urmărire penală sau din oficiu, conservarea imediată a datelor informatice ori a datelor referitoare la traficul informatic, față de care există pericolul distrugerii ori alterării, în condițiile legislației de procedură penală;
- c) reprezintă învinuirea, în numele statului, în instanță de judecată în modul prevăzut de lege.

(5) Ministerul Economiei, în comun cu Serviciul de Informații și Securitate, prezintă propuneri privind asigurarea protecției și securității informatice.

(6) Institutul Național al Justiției realizează perfecționarea profesională a personalului antrenat în îndeplinirea justiției în domeniul combaterii criminalității informatice.

[Art.4 modificat prin Legea nr.200 din 25.07.2024, în vigoare 15.11.2024]

[Art.4 modificat prin Legea nr.156 din 09.06.2022, în vigoare 01.07.2022]

[Art.4 modificat prin [Legea nr.79 din 24.05.2018](#), în vigoare 15.06.2018]

[Art.4 modificat prin [Legea nr.45 din 22.03.2013](#), în vigoare 12.04.2013]

[Art.4 modificat prin [Legea nr.120 din 25.05.2012](#), în vigoare 01.10.2012]

Articolul 4¹. Emiterea ordinului de sistare a accesului la o pagină web sau de eliminare a conținutului online la sursă

(1) Emiterea ordinului de sistare a accesului la o pagină web sau de eliminare a conținutului online la sursă, în condițiile prevăzute la art.7 alin.(1) lit.e¹) sau h), se face cu respectarea următoarelor principii:

- a) proporționalitatea;
- b) aplicarea celei mai puțin restrictive măsuri tehnice de sistare;
- c) informarea despre motivele sistării accesului și despre căile de atac;

- d) revizuirea periodică a necesității sistării în continuare a accesului la o anumită pagină web;
- e) respectarea dreptului furnizorilor de servicii de a aplica, din proprie inițiativă, alte măsuri pentru prevenirea utilizării abuzive a serviciilor acestora;
- f) respectarea prevederilor [Legii nr.284/2004](#) privind serviciile societății informaționale.

(2) Sistarea accesului la o pagină web ce cuprinde informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor poate fi dispusă pe un termen de 30 de zile, cu posibilitatea prelungirii acestuia, dar nu mai mult de 90 de zile. Fiecare prelungire nu poate depăși termenul de 30 de zile.

[Art.4¹ introdus prin Legea nr.200 din 25.07.2024, în vigoare 15.11.2024]

Articolul 4². Criterii privind sistarea accesului la o pagină web ce cuprinde informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor sau privind eliminarea la sursă a conținutului online ce cuprinde informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor

(1) O pagină web poate fi considerată ca fiind destinată și utilizată pentru pregătirea sau comiterea infracțiunilor în cazul în care informația publicată sau oferită în orice mod pe aceasta, inclusiv sub formă de linkuri, corespunde unuia sau mai multor dintre următoarele criterii:

a) afișarea sau distribuirea informației respective reprezintă în sine o faptă infracțională prevăzută la art.173, 175¹, 177, 178, 186, 189, 190, 208¹, 237, 245¹⁰ sau 259–261¹ din [Codul penal nr.985/2002](#);

b) informația respectivă este utilizată pentru determinarea potențialei victime a infracțiunii să furnizeze anumite date sau să întreprindă alte acțiuni cu scopul de a obține un beneficiu material pentru sine sau pentru o altă persoană;

c) informația respectivă este utilizată pentru recrutarea sau determinarea persoanei în vederea favorizării sau comiterii infracțiunilor prevăzute la lit.a);

d) informația respectivă este utilizată pentru răspândirea programelor malițioase utilizate la comiterea infracțiunilor, în special a celor informatice și din domeniul comunicațiilor electronice;

e) informația respectivă este utilizată pentru comercializarea, oferirea sau promovarea în orice mod a obiectelor sau substanțelor interzise prin lege sau a căror circulație este limitată prin legea penală;

f) informația respectivă este utilizată pentru distribuirea, difuzarea, importarea, procurarea, schimbarea, folosirea sau păstrarea de imagini sau alte reprezentări ale unui sau mai multor copii implicați în activități sexuale explicite, reale sau simulate, ori de imagini sau alte reprezentări ale organelor sexuale ale unui copil, reprezentate într-o manieră lascivă sau obscenă;

g) informația respectivă este utilizată pentru conversații online îndreptate spre propagarea pedofiliei (interesului sexual față de minori sau actului de abuz sexual asupra copiilor).

(2) Ordinul de sistare a accesului la o pagină web se emite numai dacă conținutul online nu poate fi eliminat la sursă de către furnizorii de servicii de găzduire a conținutului online sau de către furnizorii de conținut online de pe teritoriul Republicii Moldova.

(3) Ordinul de sistare a accesului la o pagină web sau de eliminare a conținutului online la sursă se publică pe pagina web oficială a autorității competente emitente.

(4) Autoritatea competentă, prin intermediul conducătorului subdiviziunii specializate în prevenirea și combaterea criminalității informatice, este obligată să dispună încetarea sistării accesului la pagina web înainte de expirarea perioadei pentru care a fost dispusă sistarea imediat ce au dispărut temeiurile și motivele care au justificat-o.

[Art.4² introdus prin Legea nr.200 din 25.07.2024, în vigoare 15.11.2024]

Articolul 4³. Contestarea ordinului de sistare a accesului la o pagină web sau de eliminare a conținutului online la sursă

(1) Ordinul de sistare a accesului la o pagină web sau de eliminare a conținutului online la sursă poate fi contestat direct în instanța de judecată în a cărei rază teritorială este amplasat sediul autorității care a emis ordinul.

(2) Ordinul de sistare a accesului la o pagină web sau de eliminare a conținutului online la sursă poate fi contestat de către furnizorul de servicii, inclusiv furnizorul serviciilor de găzduire a conținutului online, și/sau de către titularul paginii web (furnizorul de conținut online).

(3) Depunerea contestației nu suspendă acțiunea ordinului de sistare a accesului la o pagină web sau de eliminare a conținutului online la sursă. Contestația se examinează de către instanța de judecată în termen de 15 zile, cu sau fără prezența părților, cărora li se comunică locul, data și ora examinării contestației.

(4) Autoritatea care a emis ordinul de sistare a accesului la pagina web sau de eliminare a conținutului online la sursă este obligată să prezinte în instanța de judecată, în termen de 3 zile de la primirea înștiințării, materialele care au servit la emiterea ordinului.

(5) Instanța de judecată, în urma examinării contestației, emite o încheiere care va conține una dintre următoarele soluții:

a) admiterea contestației și anularea ordinului prin care s-a dispus sistarea accesului la pagina web sau eliminarea conținutului online la sursă;

b) admiterea parțială a contestației și modificarea ordinului prin care s-a dispus sistarea accesului la pagina web sau eliminarea conținutului online la sursă;

c) respingerea contestației ca fiind neîntemeiată.

(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.

(7) Prevederile [Codului administrativ](#) se aplică în măsura în care nu contravin prevederilor prezentei legi.

[Art.4³ introdus prin Legea nr.200 din 25.07.2024, în vigoare 15.11.2024]

Articolul 5. Colaborarea autorităților competente în prevenirea și combaterea criminalității informatice

În cadrul activităților de prevenire și combatere a criminalității informatice, autoritățile competente, furnizorii de servicii, organizațiile neguvernamentale, alți reprezentanți ai societății civile colaborează prin schimb de informații, de experți, prin activități comune de cercetare a cazurilor și de identificare a infractorilor, de instruire a personalului, prin realizarea de inițiative în scopul promovării unor programe, practici, măsuri, proceduri și standarde minime de securitate a sistemelor informatice, prin campanii de informare privind criminalitatea informatică și riscurile la care sînt expuși utilizatorii de sisteme informatice, prin alte activități în domeniu.

Articolul 6. Obligațiile proprietarilor de sisteme informatice

Proprietarii de sisteme informatice accesul la care este interzis sau restricționat pentru anumite categorii de utilizatori au obligația de a avertiza utilizatorii referitor la condițiile legale de acces și de utilizare, precum și la consecințele juridice ale accesului nesancționat la aceste sisteme informatice. Avertizarea trebuie să fie accesibilă oricărui utilizator.

Articolul 7. Obligațiile furnizorilor de servicii

(1) Furnizorii de servicii sînt obligați:

a) să țină evidența utilizatorilor de servicii;

b) să comunice autorităților competente datele despre traficul informatic, inclusiv datele despre accesul ilegal la informația din sistemul informatic, despre tentativele de introducere a unor programe ilegale, despre încălcarea de către persoane responsabile a regulilor de colectare, prelucrare, păstrare, difuzare, repartizare a informației ori a regulilor de protecție a sistemului informatic prevăzute în conformitate cu statutul informației sau cu gradul ei de protecție, dacă acestea au contribuit la însușirea, la denaturarea sau la distrugerea informației ori au provocat alte urmări grave, perturbarea funcționării sistemelor informatice, alte delict informatice;

c) să execute, în condiții de confidențialitate, solicitarea autorității competente privind conservarea imediată a datelor informatice ori a datelor referitoare la traficul informatic, față de care există pericolul distrugerii ori alterării, pe un termen de pînă la 120 de zile calendaristice, în condițiile legislației naționale;

d) să prezinte autorităților competente, în temeiul unei solicitări efectuate în condițiile legii, date

referitoare la utilizatori, inclusiv la tipul de comunicație și la serviciul de care a beneficiat utilizatorul, la modalitatea de plată a serviciului;

e) să întreprindă măsuri de securitate prin utilizarea unor proceduri, dispozitive sau programe informatice specializate cu al căror ajutor accesul la un sistem informatic să fie restricționat sau interzis utilizatorilor neautorizați;

e¹) să sisteze, la solicitarea autorităților competente, folosind metodele și mijloacele tehnice din posesie, accesul din propriul sistem informatic la paginile web ce cuprind informații destinate și utilizate pentru pregătirea sau comiterea infracțiunilor;

f) să asigure monitorizarea, supravegherea și păstrarea datelor referitoare la trafic, pe o perioadă de 180 de zile calendaristice, pentru identificarea furnizorilor de servicii, utilizatorilor de servicii și a canalului prin al cărui intermediu comunicația a fost transmisă;

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;

h) să sisteze, la solicitarea autorităților competente, transmiterea într-o rețea de comunicații electronice sau 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.

(2) În cazul în care datele referitoare la traficul informatic se află în posesia mai multor furnizori de servicii, furnizorul de servicii solicitat este obligat să pună de îndată la dispoziția autorității competente informația necesară identificării celorlalți furnizori de servicii.

[Art.7 modificat prin Legea nr.200 din 25.07.2024, în vigoare 15.11.2024]

[Art.7 completat prin Legea nr.257 din 16.12.2020, în vigoare 01.01.2021]

[Art.7 modificat prin [Legea nr.45 din 22.03.2013](#), în vigoare 12.04.2013]

Capitolul III

COOPERAREA INTERNAȚIONALĂ

Articolul 8. Cooperarea internațională a autorităților competente

(1) Autoritățile competente colaborează, în condițiile legii, respectând obligațiile prevăzute de tratatele internaționale la care Republica Moldova este parte, cu instituțiile care au atribuții similare din alte state, precum și cu organizațiile internaționale specializate în domeniu.

(2) Colaborarea prevede: asistența juridică internațională în materie penală; extrădarea; identificarea; blocarea, sechestrarea și confiscarea produselor și a instrumentelor infracțiunii; desfășurarea anchetelor comune; schimbul de informații; formarea personalului de specialitate; alte activități similare.

Articolul 9. Activitatea specială de investigații și de urmărire penală desfășurată în comun

(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.

(2) Anchetele comune se vor desfășura și în bază de acorduri bilaterale sau multilaterale încheiate de autoritățile competente.

(3) Reprezentanții autorităților competente din Republica Moldova pot participa la anchete comune desfășurate pe teritoriul unor alte state, cu respectarea legislației lor.

[Art.9 modificat prin Legea nr.200 din 25.07.2024, în vigoare 15.11.2024]

Articolul 10. Solicitățile autorităților competente străine

(1) În cadrul cooperării internaționale, autoritatea competentă străină poate solicita autorității competente din Republica Moldova conservarea imediată a datelor informatice sau a datelor privind traficul informatic, existente într-un sistem informatic de pe teritoriul Republicii Moldova, referitor la care autoritatea competentă străină urmează să formuleze o cerere, argumentată, de asistență juridică internațională în materie penală.

(2) Cererea de conservare imediată prevăzută la alin.(1) cuprinde:

- a) denumirea autorității care solicită conservarea;
- b) prezentarea succintă a faptelor care fac obiectul urmăririi penale și argumentarea lor juridică;
- c) datele informatice care se solicită a fi conservate;
- d) orice informație disponibilă, necesară identificării deținătorului de date informatice, localizarea sistemului informatic;
- e) utilitatea datelor informatice, necesitatea conservării lor;
- f) intenția autorității competente străine de a formula o cerere de asistență juridică internațională în materie penală.

(3) Termenul de conservare a datelor consemnate la alin.(1) nu poate fi mai mic de 60 de zile calendaristice și este valabil pînă cînd autoritățile competente naționale decid asupra cererii de asistență juridică internațională în materie penală.

(4) Transmiterea datelor informatice se va efectua doar în urma acceptării cererii de asistență juridică internațională în materie penală.

Capitolul IV RĂSPUNDEREA

Articolul 11. Răspunderea pentru încălcarea prezentei legi

Încălcarea prezentei legi atrage răspundere disciplinară, civilă, contravențională sau penală, în condițiile legii.

Capitolul V DISPOZIȚII FINALE

Articolul 12.

(1) Dispozițiile art.7 alin.(1) lit.a) vor fi puse în aplicare după 6 luni de la intrarea în vigoare a prezentei legi.

(2) Guvernul, în termen de 3 luni, va prezenta Parlamentului propuneri privind aducerea legislației în vigoare în concordanță cu prezenta lege.

PREȘEDINTELE PARLAMENTULUI

Mihai GHIMPU

Chișinău, 3 februarie 2009.

Nr.20-XVI.