PARLAMENTUL REPUBLICII MOLDOVA

ПАРЛАМЕНТ РЕСПУБЛИКИ МОЛДОВА

L E G E
privind prevenirea şi combaterea criminalităţii 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

Parlamentul adoptă prezenta lege organică.

Capitolul I
DISPOZIŢII GENERALE

Articolul 1. Obiectul de reglementare

Prezenta lege reglementează raporturile juridice privind:

a) prevenirea şi combaterea infracţiunilor informatice;

b) cadrul de asistenţă mutuală în prevenirea şi combaterea criminalităţii informatice, în protecţia şi acordarea de ajutor furnizorilor de servicii şi utilizatorilor de sisteme informatice;

c) colaborarea autorităţilor administraţiei publice cu organizaţii neguvernamentale şi cu alţi reprezentanţi ai societăţii civile în activitatea de prevenire şi de combatere a criminalităţii informatice;

d) cooperarea cu alte state, cu organizaţii internaţionale şi regionale avînd competenţe în domeniu.

Articolul 2. Noţiuni principale

În sensul prezentei legi, următoarele noţiuni 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, informaţii sau concepte sub o formă adecvată prelucrării într-un sistem informatic, inclusiv un program capabil să determine executarea unei funcţii 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 şi orice altă entitate care prelucrează sau stochează date informatice pentru acest serviciu de comunicaţii 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 lanţului de comunicare, indicînd originea, destinaţia, itinerarul, ora, data, mărimea, durata sau tipul de serviciu subiacent;

date referitoare la utilizatori – orice informaţie, sub formă de date informatice sau sub orice altă formă, deţinută de un furnizor de servicii, referitoare la abonaţii acestor servicii, altele decît datele referitoare la trafic sau conţinut, şi care permit stabilirea: tipului de serviciu de comunicaţii utilizat, dispoziţiilor tehnice luate în această privinţă şi perioadei serviciului; identităţii, adresei poştale sau geografice, numărului de telefon al abonatului şi oricărui alt număr de contact, precum şi a datelor referitoare la facturare şi plată, disponibile în baza unui contract sau a unui aranjament de servicii; oricărei alte informaţii referitoare la locul în care se găsesc echipamentele de comunicaţie, disponibile în baza unui contract sau a unui aranjament de servicii, precum şi 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 restricţionat 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 şi combaterii criminalităţii informatice

Prevenirea şi combaterea criminalităţii informatice se efectuează pe următoarele principii:

a) legalitatea;

b) respectarea drepturilor şi libertăţilor fundamentale ale omului;

c) operativitatea;

d) inevitabilitatea pedepsei;

e) securitatea informatică şi protecţia datelor cu caracter personal;

f) utilizarea complexă a măsurilor de profilaxie: juridice, social-economice şi informatice;

g) parteneriatul social, colaborarea autorităţilor administraţiei publice cu organizaţii internaţionale, cu organizaţii neguvernamentale, cu alţi reprezentanţi ai societăţii civile.

Capitolul II
CADRUL INSTITUŢIONAL

Articolul 4. Funcţiile autorităţilor şi instituţiilor publice competente în domeniul prevenirii şi combaterii criminalităţii informatice

(1) Ministerul Afacerilor Interne şi Serviciul de Informaţii şi Securitate:

a) formează şi actualizează în permanenţă bazele de date privind criminalitatea informatică;

b) dispun, prin ordinul emis de conducătorul subdiviziunii specializate în prevenirea şi combaterea criminalităţii informatice, sistarea accesului la pagini web, în condiţiile prevăzute la art.7 alin.(1) lit.e[1]), precum şi sistarea transmiterii într-o reţea de comunicaţii electronice sau a stocării conţinutului online, găzduit sau furnizat de către furnizorii de servicii de găzduire sau furnizorii de conţinut, prin eliminarea acestuia la sursă, în condiţiile prevăzute la art.7 alin.(1) lit.h).

(2) Ministerul Afacerilor Interne:

a) efectuează măsuri speciale de investigaţii, de urmărire penală, de cooperare internaţională, de identificare a persoanelor care comit infracţiuni informatice;

b) dispune, prin ordinul emis de conducătorul subdiviziunii specializate în prevenirea şi combaterea criminalităţii informatice, conservarea imediată, de către furnizorii de servicii, a datelor informatice sau a datelor referitoare la traficul informatic faţă de care există pericolul distrugerii sau alterării, în cazul solicitărilor autorităţilor competente străine transmise prin punctul de contact, disponibil 24/7, în conformitate cu art.10.

(3) Serviciul de Informaţii şi Securitate desfăşoară activităţi de prevenire şi combatere a criminalităţii informatice ce prezintă ameninţări la adresa securităţii statului, precum şi de depistare a legăturilor organizaţiilor criminale internaţionale.

(4) Procuratura Generală:

a) coordonează, conduce şi exercită urmărirea penală, în modul prevăzut de lege;

b) dispune, în cadrul desfăşurării urmăririi penale, la solicitarea organului de urmărire penală sau din oficiu, conservarea imediată a datelor informatice ori a datelor referitoare la traficul informatic, faţă de care există pericolul distrugerii ori alterării, în condiţiile legislaţiei de procedură penală;

c) reprezintă învinuirea, în numele statului, în instanţă de judecată în modul prevăzut de lege.

(5) Ministerul Economiei, în comun cu Serviciul de Informaţii şi Securitate, prezintă propuneri privind asigurarea protecţiei şi securităţii informatice.

(6) Institutul Naţional al Justiţiei realizează perfecţionarea profesională a personalului antrenat în înfăptuirea justiţiei în domeniul combaterii criminalităţii 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 4[1]. Emiterea ordinului de sistare a accesului la o pagină web sau de eliminare a conţinutului online la sursă

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

a) proporţionalitatea;

b) aplicarea celei mai puţin restrictive măsuri tehnice de sistare;

c) informarea despre motivele sistării accesului şi despre căile de atac;

d) revizuirea periodică a necesităţii sistării în continuare a accesului la o anumită pagină web;

e) respectarea dreptului furnizorilor de servicii de a aplica, din proprie iniţiativă, alte măsuri pentru prevenirea utilizării abuzive a serviciilor acestora;

f) respectarea prevederilor Legii nr.284/2004 privind serviciile societăţii informaţionale.

(2) Sistarea accesului la o pagină web ce cuprinde informaţii destinate şi utilizate pentru pregătirea sau comiterea infracţiunilor 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 depăşi termenul de 30 de zile.

[Art.4[1] introdus prin Legea nr.200 din 25.07.2024, în vigoare 15.11.2024]

Articolul 4[2]. Criterii privind sistarea accesului la o pagină webce cuprinde informaţii destinate şi utilizate pentru pregătirea sau comiterea infracţiunilor sau privind eliminarea la sursă a conţinutului online ce cuprinde informaţii destinate şi utilizate pentru pregătirea sau comiterea infracţiunilor

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

a) afişarea sau distribuirea informaţiei respective reprezintă în sine o faptă infracţională prevăzută la art.173, 175[1], 177, 178, 186, 189, 190, 208[1], 237, 245[10] sau 259–261[1] din Codul penal nr.985/2002;

b) informaţia respectivă este utilizată pentru determinarea potenţialei victime a infracţiunii să furnizeze anumite date sau să întreprindă alte acţiuni cu scopul de a obţine un beneficiu material pentru sine sau pentru o altă persoană;

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

d) informaţia respectivă este utilizată pentru răspândirea programelor maliţioase utilizate la comiterea infracţiunilor, în special a celor informatice şi din domeniul comunicaţiilor electronice;

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

f) informaţia respectivă este utilizată pentru distribuirea, difuzarea, importarea, procurarea, schimbarea, folosirea sau păstrarea de imagini sau alte reprezentări ale unui sau mai multor copii implicaţi în activităţi 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) informaţia respectivă este utilizată pentru conversaţii online îndreptate spre propagarea pedofiliei (interesului sexual faţă de minori sau actului de abuz sexual asupra copiilor).

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

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

(4) Autoritatea competentă, prin intermediul conducătorului subdiviziunii specializate în prevenirea şi combaterea criminalităţii 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 şi motivele care au justificat-o.

[Art.4[2] introdus prin Legea nr.200 din 25.07.2024, în vigoare 15.11.2024]

Articolul 4[3]. Contestarea ordinului de sistare a accesului la o pagină web sau de eliminare a conţinutului online la sursă

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

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

(3) Depunerea contestaţiei nu suspendă acţiunea ordinului de sistare a accesului la o pagină web sau de eliminare a conţinutului online la sursă. Contestaţia se examinează de către instanţa de judecată în termen de 15 zile, cu sau fără prezenţa părţilor, cărora li se comunică locul, data şi ora examinării contestaţiei.

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

(5) Instanţa de judecată, în urma examinării contestaţiei, emite o încheiere care va conţine una dintre următoarele soluţii:

a) admiterea contestaţiei şi anularea ordinului prin care s-a dispus sistarea accesului la pagina web sau eliminarea conţinutului online la sursă;

b) admiterea parţială a contestaţiei şi modificarea ordinului prin care s-a dispus sistarea accesului la pagina web sau eliminarea conţinutului online la sursă;

c) respingerea contestaţiei ca fiind neîntemeiată.

(6) Copia de pe încheiere se expediază părţilor în termen de 3 zile lucrătoare de la data emiterii, iar autoritatea care a emis ordinul anulat înştiinţează furnizorul de servicii despre anularea acestuia în termen de 3 zile lucrătoare de la data recepţionării încheierii de anulare.

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

[Art.4^3 introdus prin Legea nr.200 din 25.07.2024, în vigoare 15.11.2024]

Articolul 5. Colaborarea autorităţilor competente în prevenirea şi combaterea criminalităţii informatice

În cadrul activităţilor de prevenire şi combatere a criminalităţii informatice, autorităţile competente, furnizorii de servicii, organizaţiile neguvernamentale, alţi reprezentanţi ai societăţii civile colaborează prin schimb de informaţii, de experţi, prin activităţi comune de cercetare a cazurilor şi de identificare a infractorilor, de instruire a personalului, prin realizarea de iniţiative în scopul promovării unor programe, practici, măsuri, proceduri şi standarde minime de securitate a sistemelor informatice, prin campanii de informare privind criminalitatea informatică şi riscurile la care sînt expuşi utilizatorii de sisteme informatice, prin alte activităţi în domeniu.

Articolul 6. Obligaţiile proprietarilor de sisteme informatice

Proprietarii de sisteme informatice accesul la care este interzis sau restricţionat pentru anumite categorii de utilizatori au obligaţia de a avertiza utilizatorii referitor la condiţiile legale de acces şi de utilizare, precum şi la consecinţele juridice ale accesului nesancţionat la aceste sisteme informatice. Avertizarea trebuie să fie accesibilă oricărui utilizator.

Articolul 7. Obligaţiile furnizorilor de servicii

(1) Furnizorii de servicii sînt obligaţi:

a) să ţină evidenţa utilizatorilor de servicii;

b) să comunice autorităţilor competente datele despre traficul informatic, inclusiv datele despre accesul ilegal la informaţia 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 informaţiei ori a regulilor de protecţie a sistemului informatic prevăzute în conformitate cu statutul informaţiei sau cu gradul ei de protecţie, dacă acestea au contribuit la însuşirea, la denaturarea sau la distrugerea informaţiei ori au provocat alte urmări grave, perturbarea funcţionării sistemelor informatice, alte delicte informatice;

c) să execute, în condiţii de confidenţialitate, solicitarea autorităţii competente privind conservarea imediată a datelor informatice ori a datelor referitoare la traficul informatic, faţă de care există pericolul distrugerii ori alterării, pe un termen de pînă la 120 de zile calendaristice, în condiţiile legislaţiei naţionale;

d) să prezinte autorităţilor competente, în temeiul unei solicitări efectuate în condiţiile legii, date

referitoare la utilizatori, inclusiv la tipul de comunicaţie şi 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 restricţionat sau interzis utilizatorilor neautorizaţi;

e[1]) să sisteze, la solicitarea autorităţilor competente, folosind metodele şi mijloacele tehnice din posesie, accesul din propriul sistem informatic la paginile web ce cuprind informaţii destinate şi utilizate pentru pregătirea sau comiterea infracţiunilor;

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

g) să asigure descifrarea datelor informatice care se conţin în pachetele protocoalelor de reţea cu conservarea acestor date pe o perioadă de cel mult 90 de zile;

h) să sisteze, la solicitarea autorităţilor competente, transmiterea într-o reţea de comunicaţii electronice sau stocarea conţinutului online ce cuprinde informaţii destinate şi utilizate pentru pregătirea sau comiterea infracţiunilor, furnizat sau găzduit de aceştia, prin eliminarea conţinutului 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 dispoziţia autorităţii competente informaţia necesară identificării celorlalţi 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 INTERNAŢIONALĂ

Articolul 8. Cooperarea internaţională a autorităţilor competente

(1) Autorităţile competente colaborează, în condiţiile legii, respectînd obligaţiile prevăzute de tratatele internaţionale la care Republica Moldova este parte, cu instituţiile care au atribuţii similare din alte state, precum şi cu organizaţiile internaţionale specializate în domeniu.

(2) Colaborarea prevede: asistenţa juridică internaţională în materie penală; extrădarea; identificarea; blocarea, sechestrarea şi confiscarea produselor şi a instrumentelor infracţiunii; desfăşurarea anchetelor comune; schimbul de informaţii; formarea personalului de specialitate; alte activităţi similare.

Articolul 9. Activitatea specială de investigaţii şi de urmărire penală desfăşurată în comun

(1) La solicitarea autorităţilor naţionale competente sau ale altor state, pe teritoriul Republicii Moldova se pot desfăşura, în condiţiile legii, activităţi operative de investigaţii în cadrul urmăririi penale comune în vederea prevenirii şi combaterii criminalităţii informatice.

(2) Anchetele comune se vor desfăşura şi în bază de acorduri bilaterale sau multilaterale încheiate de autorităţile competente.

(3) Reprezentanţii autorităţilor competente din Republica Moldova pot participa la anchete comune desfăşurate pe teritoriul unor alte state, cu respectarea legislaţiei lor.

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

Articolul 10. Solicitările autorităţilor competente străine

(1) În cadrul cooperării internaţionale, autoritatea competentă străină poate solicita autorităţii 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 asistenţă juridică internaţională în materie penală.

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

a) denumirea autorităţii care solicită conservarea;

b) prezentarea succintă a faptelor care fac obiectul urmăririi penale şi argumentarea lor juridică;

c) datele informatice care se solicită a fi conservate;

d) orice informaţie disponibilă, necesară identificării deţinătorului de date informatice, localizarea sistemului informatic;

e) utilitatea datelor informatice, necesitatea conservării lor;

f) intenţia autorităţii competente străine de a formula o cerere de asistenţă juridică internaţională în materie penală.

(3) Termenul de conservare a datelor consemnate la alin.(1) nu poate fi mai mic de 60 de zile calendaristice şi este valabil pînă cînd autorităţile competente naţionale decid asupra cererii de asistenţă juridică internaţională în materie penală.

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

Capitolul IV
RĂSPUNDEREA

Articolul 11. Răspunderea pentru încălcarea prezentei legi

Încălcarea prezentei legi atrage răspundere disciplinară, civilă, contravenţională sau penală, în condiţiile legii.

Capitolul V
DISPOZIŢII FINALE

Articolul 12.

(1) Dispoziţiile 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 legislaţiei în vigoare în concordanţă cu prezenta lege.

PREŞEDINTELE PARLAMENTULUI **Mihai GHIMPU**

Chişinău, 3 februarie 2009.

Nr.20-XVI.