PARLAMENTUL ROMÂNIEI

Camera Deputaților **Senatul**

LEGE

privind prevenirea şi combaterea criminalității informatice

Parlamentul României adoptă prezenta lege:

Capitolul I
Dispoziții generale

Art.1 – Prezenta lege reglementează prevenirea şi combaterea criminalității informatice, prin măsuri specifice de prevenire, descoperire şi sancționare a infracțiunilor săvârşite prin intermediul sistemelor informatice, asigurându-se respectarea drepturilor omului şi protecția datelor personale.

Art.2 - (1) În prezenta lege, termenii şi expresiile de mai jos au următorul înțeles:

a) prin „**sistem informatic**" se înțelege orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relație funcțională, dintre care unul sau mai multe asigură prelucrarea automată a datelor, cu ajutorul unui program informatic;

b) prin „**prelucrare automată a datelor**" se înțelege procesul prin care datele dintr-un sistem informatic sunt prelucrate prin intermediul unui program informatic;

c) prin „**program informatic**" se înțelege un ansamblu de instrucțiuni care pot fi executate de un sistem informatic în vederea obținerii unui rezultat determinat;

d) prin „**date informatice**" se înțelege orice reprezentare a unor fapte, informații sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic. În această categorie se include şi orice program informatic care poate determina realizarea unei funcții de către un sistem informatic ;

e) prin „**furnizor de servicii**" se înțelege:

1. orice persoană fizică sau juridică ce oferă utilizatorilor posibilitatea de a comunica prin intermediul sistemelor informatice;
2. orice altă persoană fizică sau juridică ce prelucrează sau stochează date informatice pentru persoanele prevăzute la pct.1 şi pentru utilizatorii serviciilor oferite de acestea;

f) prin „**date referitoare la traficul informațional**" se înțelege orice date informatice referitoare la o comunicare realizată printr-un sistem informatic şi produse de acesta, care reprezintă o parte din lanțul de comunicare, indicând originea, destinația, ruta, ora, data, mărimea, volumul şi durata comunicării, precum şi tipul serviciului utilizat pentru comunicare;

g) prin "**date referitoare la utilizatori**" se înțelege orice informație care poate conduce la identificarea unui utilizator, incluzând tipul de comunicație şi serviciul folosit, adresa poştală, adresa geografică, numere de telefon sau alte numere de acces şi modalitatea de plată a serviciului respectiv, precum şi orice alte date care pot conduce la identificarea utilizatorului;

h) prin „**măsuri de securitate**" se înțelege 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;

i) prin „**materiale pornografice cu minori**" se înțelege orice material care prezintă un minor având un comportament sexual explicit sau o persoană majoră care este prezentată ca un minor având un comportament sexual explicit ori imagini care, deşi nu prezintă o persoană reală, simulează, în mod credibil, un minor având un comportament sexual explicit.

(2) În sensul prezentei legi, acționează fără drept persoana care nu este autorizată, în temeiul legii sau al unui contract, depăşeşte limitele autorizării ori nu are permisiunea, din partea persoanei abilitate, de a folosi, administra sau controla un sistem informatic ori de a desfăşura cercetări ştiințifice sau de a efectua orice altă operațiune într-un sistem informatic.

Capitolul II
Prevenirea criminalității informatice

Art.3 – Pentru asigurarea securității sistemelor informatice şi a protecției datelor personale, autoritățile şi instituțiile publice cu competențe în domeniu, furnizorii de servicii, organizațiile neguvernamentale şi alți reprezentanți ai societății civile desfăşoară activități comune şi programe de prevenire a criminalității informatice.

Art.4 – Autoritățile şi instituțiile publice cu competențe în domeniu, în cooperare cu furnizorii de servicii, organizațiile neguvernamentale şi alți reprezentanți ai societății civile promovează politici, practici, măsuri, proceduri şi standarde minime de securitate a sistemelor informatice.

Art.5 - Autoritățile şi instituțiile publice cu competențe în domeniu, în cooperare cu furnizorii de servicii, organizațiile neguvernamentale şi alți reprezentanți ai societății civile organizează campanii de informare privind criminalitatea informatică şi riscurile la care sunt expuşi utilizatorii de sisteme informatice.

Art.6 – **(1)** Ministerul Justiției, Ministerul de Interne şi Ministerul Comunicațiilor şi Tehnologiei Informației constituie şi actualizează o bază de date privind criminalitatea informatică.

(2) Institutul Național de Criminologie din subordinea Ministerului Justiției efectuează studii periodice în scopul identificării cauzelor care determină şi a condițiilor ce favorizează criminalitatea informatică.

Art.7 - Ministerul Justiției, Ministerul de Interne şi Ministerul Comunicațiilor şi Tehnologiei Informației desfăşoară programe speciale de pregătire şi perfecționare a personalului cu atribuții în prevenirea şi combaterea criminalității informatice.

Art.8 – Proprietarii sau administratorii de sisteme informatice la care accesul este interzis sau restricționat pentru anumite categorii de utilizatori au obligația de a avertiza utilizatorii cu privire la condițiile legale de acces şi utilizare, precum şi cu privire la consecințele juridice ale accesului fără drept la aceste sisteme informatice.

Capitolul III
Infracțiuni şi contravenții

Secțiunea 1
Infracțiuni contra confidențialității şi integrității datelor şi sistemelor informatice

Art.9 – **(1)** Accesul, fără drept, la un sistem informatic constituie infracțiune şi se pedepseşte cu închisoare de la 6 luni la 5 ani.

(2) Dacă fapta prevăzută la alin.(1) este săvârşită prin încălcarea măsurilor de securitate, pedeapsa este închisoarea de la 3 la 12 ani.

Art.10 – **(1)** Interceptarea, fără drept, a unei transmisii de date informatice care nu este publică şi care este destinată unui sistem informatic, provine dintr-un asemenea sistem sau se efectuează în cadrul unui sistem informatic constituie infracțiune şi se pedepseşte cu închisoare de la unu la 7 ani.

(2) Cu aceeaşi pedeapsă se sancționează şi interceptarea, fără drept, a unei emisii electromagnetice provenite dintr-un sistem informatic ce conține date informatice care nu sunt publice.

Art.11 – **(1)** Fapta de a modifica, şterge sau deteriora date informatice ori de a restricționa accesul la aceste date, fără drept, constituie infracțiune şi se pedepseşte cu închisoare de la unu la 7 ani.

(2) Transferul neautorizat de date dintr-un sistem informatic se pedepseşte cu închisoare de la 3 la 12 ani.

Art.12 – Fapta de a perturba grav, fără drept, funcționarea unui sistem informatic, prin introducerea, transmiterea, modificarea, ştergerea sau deteriorarea datelor informatice sau prin restricționarea accesului la aceste date constituie infracțiune şi se pedepseşte cu închisoarea de la 3 la 15 ani.

Art.13 – **(1)** Constituie infracțiune şi se pedepseşte cu închisoare de la 6 luni la 5 ani:

a) fapta de a produce, vinde, de a importa, distribui sau de a pune la dispoziție, sub orice altă formă, fără drept, a unui dispozitiv sau program informatic conceput sau adaptat în scopul săvârşirii uneia din infracțiunile prevăzute la art.9-12;

b) fapta de a produce, vinde, de a importa, distribui sau de a pune la dispoziție, sub orice altă formă, fără drept, a unei parole, cod de acces sau alte asemenea date informatice care permit accesul total sau parțial la un sistem informatic în scopul săvârşirii uneia din infracțiunile prevăzute în art.9-12.

(2) Cu aceeaşi pedeapsă se sancționează şi deținerea, fără drept, a unui dispozitiv, program informatic, parolă, cod de acces sau dată informatică dintre cele prevăzute în alin.(1) în scopul săvârşirii uneia din infracțiunile prevăzute în art.9-12.

Art.14 – Tentativa infracțiunilor prevăzute în art.9-13 se pedepseşte.

Secțiunea a 2 - a
Infracțiuni informatice

Art.15. – Fapta de a introduce, modifica sau şterge, fără drept, date informatice ori de a restricționa, fără drept, accesul la aceste date, dacă fapta are ca rezultat date necorespunzătoare adevărului, în scopul de a fi utilizate în vederea producerii unei consecințe juridice, constituie infracțiune şi se pedepseşte cu închisoare de la 2 la 7 ani.

Art.16 – Fapta de a cauza un prejudiciu patrimonial unei persoane prin introducerea, modificarea sau ştergerea de date informatice, prin restricționarea accesului la aceste date ori prin împiedicarea în orice mod a funcționării unui sistem informatic, în scopul de a obține un beneficiu material pentru sine sau pentru altul, constituie infracțiune şi se pedepseşte cu închisoare de la 3 la 12 ani.

Art.17 – Tentativa infracțiunilor prevăzute la art.15 şi 16 se pedepseşte.

Secțiunea a 3 - a
Pornografia infantilă prin sisteme informatice

Art.18 – **(1)** Constituie infracțiune şi se pedepseşte cu închisoare de la 3 la 12 ani şi interzicerea unor drepturi, producerea în vederea răspândirii, oferirea sau punerea la dispoziție, răspândirea sau transmiterea, procurarea pentru sine sau pentru altul, de materiale pornografice cu minori prin sisteme informatice, ori deținerea, fără drept, de materiale pornografice cu minori într-un sistem informatic sau un mijloc de stocare a datelor informatice.

(2) Tentativa se pedepseşte.

Secțiunea a 4 - a
Contravenții

Art.19 – Nerespectarea obligației prevăzute în art.8 constituie contravenție şi se sancționează cu amendă de la 5.000.000 lei la 50.000.000 lei.

Art.20 – (1) Constatarea contravenției prevăzute la art.19 şi aplicarea sancțiunii se fac de către personalul împuternicit în acest scop de către ministrul comunicațiilor şi tehnologiei informației, precum şi de către personalul special abilitat din cadrul Ministerului de Interne.

(2) Contravenției prevăzute la art.19 i se aplică prevederile Ordonanței Guvernului nr.2/2001 privind regimul juridic al contravențiilor, aprobată cu modificări şi completări prin Legea nr.180/2002.

Capitolul IV
Dispoziții procedurale

Art.21 - (1) În cazuri urgente şi temeinic justificate, dacă există date sau indicii temeinice cu privire la pregătirea sau săvârşirea unei infracțiuni prin intermediul sistemelor informatice, în scopul strângerii de probe sau al identificării făptuitorilor, se poate dispune conservarea imediată a datelor informatice ori a datelor referitoare la traficul informațional, față de care există pericolul distrugerii ori alterării.

(2) În cursul urmăririi penale conservarea se dispune de procuror, prin ordonanță motivată, la cererea organului de cercetare penală sau din oficiu, iar în cursul judecății, de instanță prin încheiere.

(3) Măsura prevăzută la alin.(1) se dispune pe o durată ce nu poate depăşi 90 de zile şi poate fi prelungită, o singură dată, cu o perioadă ce nu poate depăşi 30 de zile.

(4) Ordonanța procurorului sau încheierea instanței se transmite, de îndată, oricărui furnizor de servicii sau oricărei persoane în posesia căreia se află datele prevăzute la alin.(1), aceasta fiind obligată să le conserve imediat, în condiții de confidențialitate.

(5) În cazul în care datele referitoare la traficul informațional se află în posesia mai multor furnizori de servicii, furnizorul de servicii prevăzut la alin.(4) are obligația de a pune, de îndată, la dispoziția organului de urmărire penală sau a instanței informațiile necesare identificării celorlalți furnizori de servicii, în vederea cunoaşterii tuturor elementelor din lanțul de comunicare folosit.

(6) Până la terminarea urmăririi penale, procurorul este obligat să încunoştințeze, în scris, persoanele ale căror date au fost conservate.

Art.22 – (1) În termenul prevăzut la art.21 alin.(3) procurorul, pe baza autorizației motivate a procurorului anume desemnat de procurorul general al parchetului de pe lângă curtea de apel sau, după caz, de procurorul general al Parchetului de pe lângă Curtea Supremă de Justiție, ori instanța de judecată dispune ridicarea obiectelor care conțin date informatice, date referitoare la traficul informațional sau date referitoare la utilizatori, de la persoana sau furnizorul de servicii care le deține, în vederea efectuării unei copii, care poate servi ca mijloc de probă.

(2) Dacă obiectele care conțin datele informatice sau datele referitoare la traficul informațional nu sunt puse de bunăvoie la dispoziția organelor judiciare pentru efectuarea unei copii, procurorul sau instanța de judecată dispune ridicarea silită. În cursul judecății, dispoziția de ridicare silită se comunică procurorului, care ia măsuri de aducere la îndeplinire, prin organul de cercetare penală.

Art.23 – (1) Ori de câte ori pentru descoperirea şi strângerea probelor este necesară cercetarea unui sistem informatic sau a unui suport de stocare a datelor informatice, procurorul sau instanța de judecată poate dispune efectuarea unei percheziții.

(2) Dacă organul de urmărire penală sau instanța de judecată apreciază că ridicarea obiectelor care conțin datele prevăzute la alin.(1) ar afecta grav desfăşurarea activității persoanelor care dețin aceste obiecte, poate dispune efectuarea unei copii, care poate servi ca mijloc de probă

(3) În cazul în care, cu ocazia cercetării unui sistem informatic sau a unui suport de stocare a datelor informatice se constată că datele informatice căutate sunt cuprinse într-un alt sistem informatic sau suport de stocare a datelor informatice şi sunt accesibile din sistemul sau suportul inițial, se poate dispune, de îndată, autorizarea efectuării percheziției în vederea cercetării tuturor sistemelor informatice sau suporturilor de stocare a datelor informatice căutate.

(4) Dispozițiile din Codul de procedură penală referitoare la efectuarea percheziției domiciliare se aplică în mod corespunzător.

Art.24 – (1) Accesul într-un sistem informatic, precum şi interceptarea şi înregistrarea comunicărilor desfăşurate prin intermediul sistemelor informatice se efectuează când sunt utile pentru aflarea adevărului, iar stabilirea situației de fapt sau identificarea făptuitorilor nu poate fi realizată în baza altor probe.

(2) Măsurile prevăzute la alin.(1) se realizează cu autorizarea motivată a procurorului anume desemnat de procurorul general al parchetului de pe lângă curtea de apel sau, după caz, de procurorul general al Parchetului de pe lângă Curtea Supremă de Justiție, iar pentru infracțiunile de corupție, a procurorului general al Parchetului Național Anticorupție, de către organele de cercetare penală, cu sprijinul unor persoane specializate, care sunt obligate să păstreze secretul operațiunii efectuate.

(3) Autorizația prevăzută la alin.(2) se dă pentru cel mult 30 de zile, cu posibilitatea prelungirii în aceleaşi condiții, pentru motive temeinic justificate, fiecare prelungire neputând depăşi 30 de zile. Durata maximă a acestor măsuri nu poate depăşi 4 luni.

(4) Până la terminarea urmăririi penale, procurorul este obligat să încunoştințeze în scris persoanele față de care s-au dispus măsurile prevăzute la alin.(1).

(5) Dispozițiile Codului de procedură penală referitoare la înregistrările audio sau video se aplică în mod corespunzător.

Art.25 - Dispozițiile prezentului capitol se aplică în urmărirea penală sau judecarea cauzelor privind infracțiunile prevăzute în prezenta lege şi a oricăror alte infracțiuni săvârşite prin intermediul sistemelor informatice.

Art.26 - În cazul infracțiunilor prevăzute în prezenta lege şi a oricăror alte infracțiuni săvârşite prin intermediul sistemelor informatice, pentru a garanta aducerea la îndeplinire a confiscării speciale prevăzute în art.118 din Codul penal se pot lua măsurile asigurătorii prevăzute de Codul de procedură penală.

Capitolul V
Cooperare internațională

Art.27 – (1) Autoritățile judiciare române cooperează în mod direct, în condițiile legii şi cu respectarea obligațiilor decurgând din instrumentele juridice internaționale la care România este parte, cu instituțiile având atribuții similare din alte state, precum şi cu organizațiile internaționale specializate în domeniu.

(2) Cooperarea, care se organizează şi se desfăşoară potrivit alin. (1) poate avea ca obiect, după caz, asistența judiciară internațională în materie penală, extrădarea, identificarea, blocarea, sechestrarea şi confiscarea produselor şi instrumentelor infracțiunii, desfăşurarea anchetelor comune, schimbul de informații, asistența tehnică sau de altă natură pentru culegerea şi analiza informațiilor, formarea personalului de specialitate, precum şi alte asemenea activități.

Art.28 – (1) La solicitarea autorităților competente române sau ale altor state, pe teritoriul României se pot desfăşura anchete comune, în vederea prevenirii şi combaterii criminalității informatice.

(2) Anchetele comune prevăzute la alin. (1) se desfăşoară în baza acordurilor bilaterale sau multilaterale încheiate de autoritățile competente.

(3) Reprezentanții autorităților competente române pot participa la anchete comune desfăşurate pe teritorii ale altor state, cu respectarea legislațiilor acestora.

Art.29 - (1) Pentru asigurarea cooperării internaționale imediate şi permanente în domeniul combaterii criminalității informatice, se înființează, în cadrul Secției de Combatere a Criminalității Organizate şi Antidrog din cadrul Parchetului de pe lângă Curtea Supremă de Justiție, Serviciul de combatere a criminalității informatice, ca punct de contact disponibil cu activitate neîntreruptă.

(2) Serviciul de combatere a criminalității informatice are următoarele atribuții:

a) acordă asistență de specialitate şi oferă date despre legislația română în materie, punctelor de contact similare din alte state;
b) dispune conservarea imediată a datelor, precum şi ridicarea obiectelor care conțin datele informatice sau datele referitoare la traficul informațional solicitate de o autoritate străină competentă;
c) execută sau facilitează executarea, potrivit legii, a comisiilor rogatorii solicitate în cauze privind combaterea criminalității informatice, cooperând cu toate autoritățile române competente.

Art.30 - (1) În cadrul cooperării internaționale, autoritățile străine competente pot solicita Serviciului de combatere a criminalității informatice conservarea imediată a datelor informatice ori a datelor referitoare la traficul informațional, existente într-un sistem informatic de pe teritoriul României, cu privire la care autoritatea străină urmează să formuleze o cerere de asistență judiciară internațională în materie penală.

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

a) autoritatea care solicită conservarea;

b) o scurtă prezentare a faptelor care fac obiectul urmăririi penale şi încadrarea juridică a acestora;

c) datele informatice care se solicită a fi conservate;

d) orice informație disponibilă, necesară pentru identificarea deținătorului de date informatice şi a localizării sistemului informatic;

e) relevanța datelor informatice şi necesitatea conservării lor;

f) intenția autorității străine de a formula o cerere de asistență judiciară internațională în materie penală.

(3) Cererea de conservare se execută potrivit art.21 pentru o perioadă care nu poate fi mai mică de 60 de zile şi este valabilă până la luarea unei decizii de către autoritățile române competente cu privire la cererea de asistență judiciară internațională în materie penală.

Art.31 - Dacă, în executarea cererii formulate potrivit art.30 alin.(1), se constată că un furnizor de servicii al altui stat este în posesia unor date referitoare la traficul informațional, Serviciul de combatere a criminalității informatice va informa de îndată despre aceasta autoritatea străină solicitantă, comunicând totodată informațiile necesare identificării respectivului furnizor de servicii.

Art.32 - **(1)** O autoritate străină competentă poate avea acces la sursele publice române de date informatice şi poate primi, în condițiile legii, prin intermediul unui sistem informatic existent pe teritoriul său, date informatice stocate în România, dacă are aprobarea persoanei care le deține, fără a fi necesară formularea unei solicitări în acest sens către autoritățile române.

(2) Autoritățile române competente pot transmite, din oficiu, autorităților străine competente, cu respectarea prevederilor legale privind protecția datelor cu caracter personal, informațiile şi datele deținute, necesare pentru descoperirea infracțiunilor săvârşite prin intermediul sistemelor informatice sau pentru soluționarea, de către autoritățile străine competente, a cauzelor referitoare la aceste infracțiuni.

Capitolul VI
Dispoziții finale

Art.33 – Pe data intrării în vigoare a prezentei legi, art.29 din Legea nr.365/2002 privind comerțul electronic, publicată în Monitorul Oficial al României, Partea I, nr.483 din 5 iulie 2002 se abrogă.