Criminalitatea informatică poate cauza multe probleme în societatea modernă. Prin urmare, România a adoptat legislaţia privind criminalitatea informatică care corespunde pe deplin convenţiilor şi standardelor internaţionale. Totuşi, această legislaţie poate fi complexă din punctul de vedere al aplicării sale pentru autorităţile care o implementează, în special pentru aceia care sunt mai puţin familiarizaţi cu computerele şi serviciile electronice ca parte a vieţii de fiecare zi.

Portalul eFrauda a fost realizat de către Ministerul Comunicaţiilor şi Tehnologiei Informaţiei şi este gestionat împreună cu Serviciul de Combatere a Criminalităţii Informatice din cadrul Ministerului Administraţiei şi Internelor şi secţia specializată din Parchetul de pe lânga Înalta Curte de Casaţie şi Justiţie. Portalul dă oricui posibilitatea de a sesiza autorităţile cu privire la o posibilă fraudă sau alte activităţi ilegale pe Internet.
www.efrauda.ro

Acest *Ghid introductiv pentru aplicarea dispoziţiilor legale referitoare la criminalitatea informatică* a fost elaborat de către proiectul RITI dot-Gov, în cooperare cu Ministerul Comunicaţiilor şi Tehnologiei Informaţiei. *Ghidul* asigură asistenţă pentru autorităţile care aplică legea şi pentru toţi cei care sunt implicaţi în prevenirea criminalităţii informatice.

Proiectul RITI dot-Gov face parte din Iniţiativa pentru Tehnologia Informaţiei în România, RITI, a cărei implementare a fost începută în 2002 de către Misiunea din România a Agenţiei Statelor Unite pentru Dezvoltare Internaţională (USAID), în cooperare cu Ministerul Comunicaţiilor şi Tehnologiei Informaţiei. Proiectul RITI dot-Gov este implementat în România de Internews Network Inc, o organizaţie non-profit cu sediul în Statele Unite.

Pentru informaţii suplimentare:
www.usaid.gov/info_technology/dotcom
www.riti-internews.ro
www.internews.org
www.mcti.ro

GHID
INTRODUCTIV PENTRU APLICAREA DISPOZIŢIILOR LEGALE REFERITOARE LA CRIMINALITATEA INFORMATICĂ

INTERNEWS
RITI dot-Gov

MCTI

Bucureşti,
Mai 2004

Elaborarea acestui ghid a fost posibilă prin asistența asigurată de către Centrul de Servicii Regional Budapesta al Agenției Statelor Unite pentru Dezvoltare Internațională, USAID, în cadrul Acordului nr. CA # 186-A-00-02-00101-00; LA#GDG-A-00-01-00009-00; Internews Network/RITI dot-Gov Project.

Opiniile exprimate în cadrul acestui document aparțin autorilor şi nu reprezintă în mod necesar vederile Agenției Statelor Unite pentru Dezvoltare Internațională.

Anexa I

Legea nr. 161/2003

Titlul III
Prevenirea şi combaterea criminalităţii informatice

Capitolul I – Dispoziţii generale

Art. 34 – Prezentul titlu reglementează prevenirea şi combaterea criminalităţii informatice, prin măsuri specifice de prevenire, descoperire şi sancţionare a infracţiunilor săvârşite prin intermediul sistemelor informatice, asigurându-se respectarea drepturilor omului şi protecţia datelor personale.

Art.35 – (1) În prezentul titlu, termenii şi expresiile de mai jos au următorul înţeles:

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

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

c) prin „program informatic" se înţelege un ansamblu de instrucţiuni care pot fi executate de un sistem informatic în vederea obţinerii unui rezultat determinat;

d) prin „date informatice" se înţelege orice reprezentare a unor fapte, informaţii 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 funcţii de către un sistem informatic ;

e) prin „furnizor de servicii" se înţelege:

   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 informaţional" se înţelege orice date informatice referitoare la o comunicare realizată printr-un sistem informatic şi produse de acesta, care reprezintă o parte din lanţul de comunicare, indicând originea, destinaţia, ruta, ora, data, mărimea, volumul şi durata comunicării, precum şi tipul serviciului utilizat pentru comunicare;

g) prin "date referitoare la utilizatori" se înţelege orice informaţie care poate conduce la identificarea unui utilizator, incluzând tipul de comunicaţie şi serviciul folosit, adresa poştală, adresa geografică, adresa de IP, 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 înţelege 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;

i) prin „materiale pornografice cu minori" se înţelege 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 prezentului titlu, acţionează fără drept persoana care se află în una din următoarele situaţii:

d) nu este autorizată, în temeiul legii sau al unui contract;
e) depăşeşte limitele autorizării;
f) nu are permisiunea, din partea persoanei fizice sau juridice competente, potrivit legii, să o acorde,

de a folosi, administra sau controla un sistem informatic ori de a desfăşura cercetări ştiinţifice sau de a efectua orice altă operaţiune într-un sistem informatic.

Capitolul II – Prevenirea criminalităţii informatice

Art.36 – Pentru asigurarea securităţii sistemelor informatice şi a protecţiei datelor personale, autorităţile şi instituţiile publice cu competenţe în domeniu, furnizorii de servicii, organizaţiile neguvernamentale şi alţi reprezentanţi ai societăţii civile desfăşoară activităţi comune şi programe de prevenire a criminalităţii informatice.

Art.37 – Autorităţile şi instituţiile publice cu competenţe în domeniu, în cooperare cu furnizorii de servicii, organizaţiile neguvernamentale şi alţi reprezentanţi ai societăţii civile promovează politici, practici, măsuri, proceduri şi standarde minime de securitate a sistemelor informatice.

Art.38 – Autorităţile şi instituţiile publice cu competenţe în domeniu, în cooperare cu furnizorii de servicii, organizaţiile neguvernamentale şi alţi reprezentanţi ai societăţii civile organizează campanii de informare privind criminalitatea informatică şi riscurile la care sunt expuşi utilizatorii de sisteme informatice.

Art.39 – (1) Ministerul Justiţiei, Ministerul de Interne şi Ministerul Comunicaţiilor şi Tehnologiei Informaţiei constituie şi actualizează continuu baze de date privind criminalitatea informatică.

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

Art.40 – Ministerul Justiţiei, Ministerul de Interne şi Ministerul Comunicaţiilor şi Tehnologiei Informaţiei desfăşoară programe speciale de pregătire şi perfecţionare a personalului cu atribuţii în prevenirea şi combaterea criminalităţii informatice.

Art.41 – Proprietarii sau administratorii de sisteme informatice la care accesul este interzis sau restricţionat pentru anumite categorii de utilizatori au obligaţia de a avertiza utilizatorii cu privire la condiţiile legale de acces şi utilizare, precum şi cu privire la consecinţele juridice ale accesului fără drept la aceste sisteme informatice.

Capitolul III – Infracţiuni şi contravenţii

Secţiunea 1
Infracţiuni contra confidenţialităţii şi integrităţii datelor şi sistemelor informatice

Art.42 – (1) Accesul, fără drept, la un sistem informatic constituie infracţiune şi se pedepseşte cu închisoare de la 6 luni la 3 ani sau cu amendă.

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

Art.43 – (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 infracţiune şi se pedepseşte cu închisoare de la 2 la 7 ani.

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

Art.44 – (1) Fapta de a modifica, şterge sau deteriora date informatice ori de a restricţiona accesul la aceste date, fără drept, constituie infracţiune şi se pedepseşte cu închisoare de la 2 la 7 ani.

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

(3) Cu pedeapsa prevăzută la alin.(2) se sancţionează şi transferul neautorizat de date dintr-un mijloc de stocare a datelor informatice.

Art.45 – Fapta de a perturba grav, fără drept, funcţionarea unui sistem informatic, prin introducerea, transmiterea, modificarea, ştergerea sau deteriorarea datelor informatice sau prin restricţionarea accesului la aceste date constituie infracţiune şi se pedepseşte cu închisoarea de la 3 la 15 ani.

Art.46 – (1) Constituie infracţiune şi se pedepseşte cu închisoare de la unu la 6 ani:

a) fapta de a produce, vinde, de a importa, distribui sau de a pune la dispoziţie, sub orice altă formă, fără drept, a unui dispozitiv sau

program informatic conceput sau adaptat în scopul săvârşirii uneia din infracţiunile prevăzute în art.42-45;

b) fapta de a produce, vinde, de a importa, distribui sau de a pune la dispoziţie, sub orice altă formă, fără drept, a unei parole, cod de acces sau alte asemenea date informatice care permit accesul total sau parţial la un sistem informatic în scopul săvârşirii uneia din infracţiunile prevăzute în art.42-45.

(2) Cu aceeaşi pedeapsă se sancţionează şi deţinerea, 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 infracţiunile prevăzute în art.42-45.

Art.47 – Tentativa infracţiunilor prevăzute în art.42-46 se pedepseşte.

Secţiunea 2
Infracţiuni informatice

Art.48. – Fapta de a introduce, modifica sau şterge, fără drept, date informatice ori de a restricţiona, fără drept, accesul la aceste date, rezultând date necorespunzătoare adevărului, în scopul de a fi utilizate în vederea producerii unei consecinţe juridice, constituie infracţiune şi se pedepseşte cu închisoare de la 2 la 7 ani.

Art.49 – Fapta de a cauza un prejudiciu patrimonial unei persoane prin introducerea, modificarea sau ştergerea de date informatice, prin restricţionarea accesului la aceste date ori prin împiedicarea în orice mod a funcţionării unui sistem informatic, în scopul de a obţine un beneficiu material pentru sine sau pentru altul, constituie infracţiune şi se pedepseşte cu închisoare de la 3 la 12 ani.

Art.50 – Tentativa infracţiunilor prevăzute în art.48 şi 49 se pedepseşte.

Secţiunea 3
Pornografia infantilă prin sisteme informatice

Art.51 – (1) Constituie infracţiune şi se pedepseşte cu închisoare de la 3 la 12 ani şi interzicerea unor drepturi producerea în vederea răspândirii, oferirea sau punerea la dispoziţie, răspândirea sau transmiterea, procurarea pentru sine sau pentru altul, de materiale pornografice cu minori prin sisteme informatice, ori deţinerea, fără drept, de materiale pornografice cu minori într-un sistem informatic sau un mijloc de stocare a datelor informatice.

(2) Tentativa se pedepseşte.

Secţiunea 4

Contravenţii

Art.52 – Nerespectarea obligaţiei prevăzute în art.41 constituie contravenţie şi se sancţionează cu amendă de la 5.000.000 lei la 50.000.000 lei.

Art.53 – (1) Constatarea contravenţiei prevăzute în art.52 şi aplicarea sancţiunii se fac de către personalul împuternicit în acest scop de către ministrul comunicaţiilor şi tehnologiei informaţiei, precum şi de către personalul special abilitat din cadrul Ministerului de Interne.

(2) Dispoziţiile Ordonanţei Guvernului nr.2/2001 privind regimul juridic al contravenţiilor, aprobată cu modificări prin Legea nr.180/2002 sunt aplicabile.

Capitolul IV – Dispoziţii procedurale

Art.54 – (1) În cazuri urgente şi temeinic justificate, dacă există date sau indicii temeinice cu privire la pregătirea sau săvârşirea unei infracţiuni 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 informaţional, faţă de care există pericolul distrugerii ori alterării.

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

(3) Măsura prevăzută în 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) Ordonanţa procurorului sau încheierea instanţei se transmite, de îndată, oricărui furnizor de servicii sau oricărei persoane în posesia căreia se află datele prevăzute în alin.(1), aceasta fiind obligată să le conserve imediat, în condiţii de confidenţialitate.

(5) În cazul în care datele referitoare la traficul informaţional se află în posesia mai multor furnizori de servicii, furnizorul de servicii prevăzut în alin.(4) are obligaţia de a pune, de îndată, la dispoziţia organului de urmărire penală sau a instanţei informaţiile necesare identificării celorlalţi furnizori de servicii, în vederea cunoaşterii tuturor elementelor din lanţul de comunicare folosit.

(6) Până la terminarea urmăririi penale, procurorul este obligat să încunoştinţeze, în scris, persoanele faţă de care se efectuează urmărirea penală şi ale căror date au fost conservate.

Art.55 – (1) În termenul prevăzut la art.54 alin.(3) procurorul, pe baza autorizaţiei 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 Justiţie, ori instanţa de judecată dispune cu privire la ridicarea obiectelor care conţin date informatice, date referitoare la traficul informaţional sau date referitoare la utilizatori, de la persoana sau furnizorul de servicii care le deţine, în vederea efectuării de copii, care pot servi ca mijloc de probă.

(2) Dacă obiectele care conţin datele informatice sau datele referitoare la traficul informaţional nu sunt puse de bunăvoie la dispoziţia organelor judiciare pentru efectuarea de copii, procurorul prevăzut în alin.(1) sau instanţa de judecată dispune ridicarea silită. În cursul judecăţii, dispoziţia de ridicare silită se comunică procurorului, care ia măsuri de aducere la îndeplinire, prin organul de cercetare penală.

(3) Copiile prevăzute în alin.(1) se realizează cu mijloace tehnice şi proceduri adecvate de natură să asigure integritatea informaţiilor conţinute de acestea.

Art.56 – (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, organul competent prevăzut de lege poate dispune efectuarea unei percheziţii.

(2) Dacă organul de urmărire penală sau instanţa de judecată apreciază că ridicarea obiectelor care conţin datele prevăzute în alin.(1) ar afecta grav desfăşurarea activităţii persoanelor care deţin aceste obiecte, poate dispune efectuarea de copii, care pot servi ca mijloc de probă şi care se realizează potrivit art.55 alin.(3).

(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 iniţial, se poate dispune, de îndată, autorizarea efectuării percheziţiei în vederea cercetării tuturor sistemelor informatice sau suporturilor de stocare a datelor informatice căutate.

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

Art.57 – (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 situaţiei de fapt sau identificarea făptuitorilor nu poate fi realizată în baza altor probe.

(2) Măsurile prevăzute în 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 Justiţie ori de procurorul general al Parchetului Naţional Anticorupţie, de către organele de cercetare penală, cu sprijinul unor persoane specializate, care sunt obligate să păstreze secretul operaţiunii efectuate.

(3) Autorizaţia prevăzută în alin.(2) se dă pentru cel mult 30 de zile, cu posibilitatea prelungirii în aceleaşi condiţii, pentru motive temeinic justificate, fiecare prelungire neputând depăşi 30 de zile. Durata maximă a măsurii autorizate nu poate depăşi 4 luni.

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

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

Art.58 - Dispoziţiile prezentului capitol se aplică în urmărirea penală sau judecarea cauzelor privind infracţiunile prevăzute în prezentul titlu şi a oricăror alte infracţiuni săvârşite prin intermediul sistemelor informatice.

Art.59 - În cazul infracţiunilor prevăzute în prezentul titlu şi a oricăror alte infracţiuni 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 internaţională

Art.60 – (1) Autorităţile judiciare române cooperează în mod direct, în condiţiile legii şi cu respectarea obligaţiilor decurgând din instrumentele juridice internaţionale la care România este parte, cu instituţiile având atribuţii similare din alte state, precum şi cu organizaţiile internaţionale specializate în domeniu.

(2) Cooperarea, care se organizează şi se desfăşoară potrivit alin. (1) poate avea ca

obiect, după caz, asistenţa judiciară internaţională în materie penală, extrădarea, identificarea, blocarea, sechestrarea şi confiscarea produselor şi instrumentelor infracţiunii, desfăşurarea anchetelor comune, schimbul de informaţii, asistenţa tehnică sau de altă natură pentru culegerea şi analiza informaţiilor, formarea personalului de specialitate, precum şi alte asemenea activităţi.

Art.61 – (1) La solicitarea autorităţilor competente române sau ale altor state, pe teritoriul României se pot desfăşura anchete comune, în vederea prevenirii şi combaterii criminalităţii informatice.

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

(3) Reprezentanţii autorităţilor competente române pot participa la anchete comune desfăşurate pe teritorii ale altor state, cu respectarea legislaţiilor acestora.

Art.62 – (1) Pentru asigurarea cooperării internaţionale imediate şi permanente în domeniul combaterii criminalităţii informatice, se înfiinţează, în cadrul Secţiei de Combatere a Criminalităţii Organizate şi Antidrog din Parchetul de pe lângă Curtea Supremă de Justiţiei, Serviciul de combatere a criminalităţii informatice, ca punct de contact disponibil permanent.

(2) Serviciul de combatere a criminalităţii informatice are următoarele atribuţii:

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

Art.63 – (1) În cadrul cooperării internaţionale, autorităţile străine competente pot solicita Serviciului de combatere a criminalităţii informatice conservarea imediată a datelor informatice ori a datelor referitoare la traficul informaţional, existente într-un sistem informatic de pe teritoriul României, cu privire la care autoritatea străină urmează să formuleze o cerere de asistenţă judiciară internaţională 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 informaţie disponibilă, necesară pentru identificarea deţinătorului de date informatice şi a localizării sistemului informatic;
e) utilitatea datelor informatice şi necesitatea conservării lor;
f) intenţia autorităţii străine de a formula o cerere de asistenţă judiciară internaţională în materie penală.

(3) Cererea de conservare se execută potrivit art.54 pentru o perioadă care nu poate fi mai mică de 60 de zile şi este valabilă până la luarea unei decizii de către autorităţile române competente cu privire la cererea de asistenţă judiciară internaţională în materie penală.

Art.64 - Dacă, în executarea cererii formulate potrivit art.63 alin.(1), se constată că un furnizor de servicii al altui stat este în posesia unor date referitoare la traficul informaţional, Serviciul de combatere a criminalităţii informatice va informa de îndată despre aceasta autoritatea străină solicitantă, comunicând totodată informaţiile necesare identificării respectivului furnizor de servicii.

Art.65 - (1) O autoritate străină competentă poate avea acces la sursele publice române de date informatice publice, fără a fi necesară formularea unei solicitări în acest sens către autorităţile române.

(2) O autoritate străină competentă poate avea acces sau poate primi, prin intermediul unui sistem informatic existent pe teritoriul său, date informatice stocate în România, dacă are aprobarea persoanei autorizate, potrivit legii, să le pună la dispoziţie prin intermediul acelui sistem informatic, fără a fi necesară formularea unei solicitări în acest sens către autorităţile române.

Art.66 – Autorităţile române competente pot transmite, din oficiu, autorităţilor străine competente, cu respectarea prevederilor legale privind protecţia datelor cu caracter personal, informaţiile şi datele deţinute, necesare pentru descoperirea infracţiunilor săvârşite prin intermediul sistemelor informatice sau pentru soluţionarea, de către autorităţile străine competente, a cauzelor referitoare la aceste infracţiuni.

Art.67 – Art.29 din Legea nr.365/2002 privind comerţul electronic, publicată în Monitorul Oficial al României, Partea I, nr.483 din 7 mai 2002 se abrogă.

Anexa II

Consiliul Europei

Convenţie privind criminalitatea informatică

Seria Tratatelor Europene nr. 185

Aprobată prin Legea 64/2004 şi publicată în Monitorul Oficial, Partea I, nr. 343/2004

Budapesta, 23 noiembrie 2001

PREAMBUL

Statele membre ale Consiliului Europei şi celelalte state semnatare ale prezentei convenţii,

considerând că scopul Consiliului Europei este realizarea unei uniuni cât mai strânse între membrii săi,

recunoscând importanţa promovării cooperării cu celelalte state părţi la prezenta convenţie,

convinse de necesitatea de a urmări, cu prioritate, aplicarea unei politici penale comune, destinată să protejeze societatea împotriva criminalităţii informatice, în special prin adoptarea unei legislaţii adecvate, precum şi prin îmbunătăţirea cooperării internaţionale,

conştiente de profundele schimbări determinate de digitalizarea, convergenţa şi globalizarea continuă a reţelelor de calculatoare,

preocupate de riscul că reţelele de calculatoare şi informaţia electronică ar putea fi utilizate şi pentru comiterea de infracţiuni şi că probele privind asemenea infracţiuni ar putea fi stocate şi transmise prin intermediul acestor reţele,

recunoscând necesitatea cooperării între state şi industria privată în lupta împotriva criminalităţii informatice, precum şi nevoia de a proteja interesele legitime în utilizarea şi dezvoltarea tehnologiilor informaţiei,

considerând că lupta eficientă purtată împotriva criminalităţii informatice impune o cooperare internaţională intensificată, rapidă şi eficace în materie penală,

convinse că prezenta convenţie este necesară pentru a preveni actele îndreptate împotriva confidenţialităţii, integrităţii şi disponibilităţii sistemelor informatice, a reţelelor şi a datelor, precum şi a utilizării frauduloase a unor asemenea sisteme, reţele şi date, prin asigurarea incriminării unor asemenea conduite, aşa cum sunt ele descrise în prezenta convenţie, şi prin adoptarea unor măsuri suficiente pentru a permite combaterea eficace a acestor infracţiuni, menite să faciliteze descoperirea, investigarea şi urmărirea penală a acestora atât la nivel naţional, cât şi internaţional, precum şi prin prevederea unor dispoziţii materiale necesare asigurării unei cooperări internaţionale rapide şi sigure,

conştiente de necesitatea garantării unui echilibru adecvat între interesele acţiunii represive şi respectarea drepturilor fundamentale ale omului, consacrate prin Convenţia Consiliului Europei pentru apărarea drepturilor omului şi a libertăţilor fundamentale (1950), Pactul internaţional privind drepturile civile şi politice al Naţiunilor Unite (1966), precum şi prin alte tratate internaţionale aplicabile în materia drepturilor omului, care reafirmă dreptul fiecăruia la opinie, libertatea de expresie, precum şi libertatea de a căuta, de a obţine şi de a comunica informaţii şi idei de orice natură, fără a ţine seama de frontiere, precum şi drepturile privind respectarea intimităţii şi a vieţii private,

conştiente, de asemenea, de dreptul la protecţia datelor personale, conferit, de exemplu, prin Convenţia Consiliului Europei pentru protejarea persoanelor faţă de prelucrarea automatizată a datelor cu caracter personal (1981),

luând în considerare Convenţia Naţiunilor Unite privind drepturile copilului (1989) şi Convenţia Organizaţiei Internaţionale a Muncii privind interzicerea celor mai grave forme ale muncii copiilor (1999),

ţinând seama de convenţiile în vigoare ale Consiliului Europei privind cooperarea în materie penală, precum şi de celelalte tratate similare încheiate între statele membre ale Consiliului Europei şi alte state şi subliniind că prezenta convenţie are ca scop completarea acestora, în vederea creşterii eficienţei anchetelor şi procedurilor penale având ca obiect infracţiunile în legătură cu sistemele şi datele informatice, precum şi de a permite colectarea probelor electronice ale unei infracţiuni,

salutând recentele iniţiative destinate să îmbunătăţească înţelegerea şi cooperarea internaţională în scopul combaterii criminalităţii în spaţiul informatic, în special acţiunile întreprinse de Naţiunile Unite, Organizaţia pentru Cooperare şi Dezvoltare Economică, Uniunea Europeană şi de Grupul celor 8,

reamintind recomandările Comitetului Miniştrilor nr. R (85) 10 privind aplicarea în practică a Convenţiei europene de asistenţă judiciară în materie penală, referitoare la comisiile rogatorii pentru supravegherea telecomunicaţiilor, nr. R (88) 2 privind măsurile vizând combaterea pirateriei în domeniul

drepturilor de autor şi al drepturilor conexe, nr. R (87) 15 vizând reglementarea utilizării datelor cu caracter personal în sectorul poliţiei, nr. R(95)4 privind protecţia datelor cu caracter personal în domeniul serviciilor de telecomunicaţii, cu referire specială la serviciile de telefonie şi nr. R (89) 9 referitoare la criminalitatea în legătură cu utilizarea calculatorului, care indică structurilor legiuitoare naţionale principiile directoare pentru definirea anumitor infracţiuni, precum şi nr. R (95) 13 privind problemele de procedură penală în legătură cu tehnologia informaţiei,

ţinând seama de Rezoluţia nr. 1, adoptată de miniştrii europeni de justiţie cu ocazia celei de-a XXI-a conferinţe a lor (Praga, 10-11 iunie 1997), care recomandă Comitetului Miniştrilor să sprijine activităţile privind combaterea criminalităţii informatice, desfăşurate de Comitetul European pentru problemele criminalităţii, în scopul de a asigura apropierea între legislaţiile penale naţionale şi de a permite utilizarea unor mijloace eficiente de investigare a infracţiunilor informatice, precum şi de Rezoluţia nr. 3, adoptată la cea de-a XXIII-a Conferinţă a miniştrilor europeni de justiţie (Londra, 8-9 iunie 2000), care încurajează părţile participante la negocieri să îşi continue eforturile pentru găsirea unor soluţii care să permită unui număr cât mai mare de state să devină parte la convenţie şi recunoaşte necesitatea de a dispune de un mecanism rapid şi eficient de cooperare internaţională care să ţină seama de exigenţele specifice luptei împotriva criminalităţii informatice,

ţinând seama, de asemenea, de planul de acţiune adoptat de şefii de stat şi de guvern din Consiliul Europei cu ocazia celei de-a doua întâlniri a lor la nivel înalt (Strasbourg, 10-11 octombrie 1997), în scopul de a găsi răspunsuri comune, bazate pe normele şi valorile Consiliului Europei, la dezvoltarea noilor tehnologii ale informaţiei,

au convenit următoarele:

CAPITOLUL I - Terminologie

ARTICOLUL 1 - Definiţii

În sensul prezentei convenţii:

a) expresia sistem informatic desemnează 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;
b) expresia date informatice desemnează 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;

c) expresia furnizor de servicii desemnează:
   (i) orice entitate publică sau privată care oferă utilizatorilor serviciilor sale posibilitatea de a comunica prin intermediul unui sistem informatic;
   şi
   (ii) orice altă entitate care prelucrează sau stochează date informatice pentru acest serviciu de comunicaţii sau pentru utilizatorii săi;
d) datele referitoare la trafic desemnează orice date având legătură cu o comunicare transmisă printr-un sistem informatic, produse de acest sistem în calitate de element al lanţului de comunicare, indicând originea, destinaţia, itinerarul, ora, data, mărimea, durata sau tipul de serviciu subiacent.

CAPITOLUL II - Măsuri care trebuie luate la nivel naţional

SECŢIUNEA 1 - Drept penal material

TITLUL 1 - Infracţiuni împotriva confidenţialităţii, integrităţii şi disponibilităţii datelor şi sistemelor informatice

ARTICOLUL 2 - Accesarea ilegală

Fiecare parte va adopta măsurile legislative şi alte măsuri considerate necesare pentru a incrimina ca infracţiune, potrivit dreptului său intern, accesarea intenţionată şi fără drept a ansamblului ori a unei părţi a unui sistem informatic. O parte poate condiţiona o astfel de incriminare de comiterea încălcării respective prin violarea măsurilor de securitate, cu intenţia de a obţine date informatice ori cu altă intenţie delictuală, sau de legătura dintre încălcarea respectivă şi un sistem informatic conectat la alt sistem informatic.

ARTICOLUL 3 - Interceptarea ilegală

Fiecare parte va adopta măsurile legislative şi alte măsuri considerate necesare pentru a incrimina ca infracţiune, potrivit dreptului său intern, interceptarea intenţionată şi fără drept, efectuată prin mijloace tehnice, a transmisiilor de date informatice care nu sunt publice, destinate, provenite sau aflate în interiorul unui sistem informatic, inclusiv a emisiilor electromagnetice provenind de la un sistem informatic care transportă asemenea date. O parte poate condiţiona o astfel de

incriminare de comiterea încălcării respective cu intenţie delictuală sau de legătura dintre încălcarea respectivă şi un sistem informatic conectat la alt sistem informatic.

ARTICOLUL 4 - Afectarea integrităţii datelor

1. Fiecare parte va adopta măsurile legislative şi alte măsuri considerate necesare pentru a incrimina ca infracţiune, potrivit dreptului său intern, fapta comisă intenţionat şi fără drept de a distruge, şterge, deteriora, modifica sau elimina date informatice.

2. O parte va putea să îşi rezerve dreptul de a condiţiona incriminarea comportamentului descris la paragraful 1 de producerea unor daune grave.

ARTICOLUL 5 - Afectarea integrităţii sistemului

Fiecare parte va adopta măsurile legislative şi alte măsuri care sunt necesare pentru a incrimina ca infracţiune, în conformitate cu dreptul intern, afectarea gravă, intenţionată şi fără drept a funcţionării unui sistem informatic, prin introducerea, transmiterea, periclitarea, ştergerea, deteriorarea, alterarea sau suprimarea datelor informatice.

ARTICOLUL 6 - Abuzurile asupra dispozitivelor

1. Fiecare parte va adopta măsurile legislative şi alte măsuri necesare pentru a incrimina ca infracţiuni, conform dreptului său intern, atunci când se comit în mod intenţionat şi fără drept:

a) producerea, vânzarea, obţinerea pentru utilizare, importarea, difuzarea sau alte forme de punere la dispoziţie:
   (i) a unui dispozitiv, inclusiv un program informatic, conceput special sau adaptat pentru a permite comiterea uneia dintre infracţiunile stabilite în conformitate cu art. 2-5;
   (ii) a unei parole, a unui cod de acces sau a unor date informatice similare care să permită accesarea în tot sau în parte a unui sistem informatic,

   cu intenţia ca acestea să fie utilizate în vederea comiterii uneia dintre infracţiunile vizate la art. 2-5; şi

b) posesia unui element vizat la subparagrafele a) (i) sau a) (ii) sus-menţionate, cu intenţia de a fi utilizat în vederea comiterii uneia dintre infracţiunile vizate la art. 2-5. O parte va putea solicita, în conformitate cu dreptul intern, ca un anumit număr dintre aceste elemente să fie deţinute pentru a fi atrasă răspunderea penală.

2. Prezentul articol nu va fi interpretat în sensul impunerii unei răspunderi penale atunci când producerea, vânzarea, obţinerea pentru utilizare, importarea, difuzarea sau alte forme de punere la dispoziţie, menţionate la paragraful 1 din prezentul articol, nu au ca scop comiterea unei infracţiuni stabilite în conformitate cu art. 2-5, cum ar fi situaţia testării sau protecţiei autorizate a unui sistem informatic.
3. Fiecare parte îşi va putea rezerva dreptul de a nu aplica paragraful 1 al prezentului articol, cu condiţia ca această rezervă să nu privească vânzarea, distribuţia sau orice altă formă de punere la dispoziţie a elementelor menţionate la paragraful 1 subparagraful a) (ii) din prezentul articol.

TITLUL 2 - Infracţiuni informatice

ARTICOLUL 7 - Falsificarea informatică
Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a incrimina ca infracţiune, potrivit dreptului său intern, introducerea, alterarea, ştergerea sau suprimarea intenţionată şi fără drept a datelor informatice, din care să rezulte date neautentice, cu intenţia ca acestea să fie luate în considerare sau utilizate în scopuri legale ca şi cum ar fi autentice, chiar dacă sunt sau nu sunt în mod direct lizibile şi inteligibile. O parte va putea condiţiona răspunderea penală de existenţa unei intenţii frauduloase sau a unei alte intenţii delictuale.

ARTICOLUL 8 - Frauda informatică
Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a incrimina ca infracţiune, potrivit dreptului său intern, fapta intenţionată şi fără drept de a cauza un prejudiciu patrimonial unei alte persoane:

a) prin orice introducere, alterare, ştergere sau suprimare a datelor informatice;
b) prin orice formă care aduce atingere funcţionării unui sistem informatic,

cu intenţia frauduloasă sau delictuală de a obţine fără drept un beneficiu economic pentru el însuşi sau pentru altă persoană.

TITLUL 3 - Infracţiuni referitoare la conţinut

ARTICOLUL 9 - Infracţiuni referitoare la pornografia infantilă

1. Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a incrimina ca infracţiune, potrivit dreptului său intern, următoarele comportamente, atunci când acestea sunt comise în mod intenţionat şi fără drept:
   a) producerea de materiale pornografice având ca subiect copii, în vederea difuzării acestora prin intermediul unui sistem informatic;
   b) oferirea sau punerea la dispoziţie de materiale pornografice având ca subiect copii, prin intermediul unui sistem informatic;
   c) difuzarea sau transmiterea de materiale pornografice având ca subiect copii, prin intermediul unui sistem informatic;
   d) fapta de a-şi procura sau de a procura pentru alte persoane materiale pornografice având ca subiect copii, prin intermediul unui sistem informatic;
   e) posesia de materiale pornografice având ca subiect copii, într-un sistem informatic sau într-un mijloc de stocare de date informatice.
2. În sensul paragrafului 1 sus-menţionat, termenul materiale pornografice având ca subiect copii desemnează orice material pornografic care reprezintă într-un mod vizual:
   a) un minor care se dedă unui comportament sexual explicit;
   b) o persoană majoră, prezentată ca o persoană minoră, care se dedă unui comportament sexual explicit;
   c) imagini realiste reprezentând un minor care se dedă unui comportament sexual explicit.
3. În sensul paragrafului 2 sus-menţionat, termenul minor desemnează orice persoană în vârstă de mai puţin de 18 ani. Totuşi o parte poate solicita o limită de vârstă inferioară, care trebuie să fie de cel puţin 16 ani.
4. O parte îşi va putea rezerva dreptul de a nu aplica, în totalitate sau parţial, paragraful 1 subparagrafele d) şi e) şi paragraful 2 subparagrafele b) şi c).

TITLUL 4 - Infracţiuni referitoare la atingerile aduse proprietăţii intelectuale şi drepturilor conexe

ARTICOLUL 10 - Infracţiuni referitoare la atingerile aduse proprietăţii intelectuale şi drepturilor conexe

1. Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a incrimina ca infracţiune, potrivit dreptului său intern,

atingerile aduse proprietăţii intelectuale, definite de legislaţia acestei părţi, în conformitate cu obligaţiile pe care le-a subscris în aplicarea Actului de la Paris din 24 iulie 1971 care revizuieşte Convenţia de la Berna pentru protecţia operelor literare şi artistice, a Acordului privind aspectele comerciale ale drepturilor de proprietate intelectuală şi a Tratatului OMPI privind proprietatea intelectuală, cu excepţia oricărui drept moral conferit de aceste convenţii, atunci când astfel de acte sunt comise deliberat, la scară comercială şi prin intermediul unui sistem informatic.
2. Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a incrimina ca infracţiune, potrivit dreptului său intern, atingerile aduse drepturilor conexe definite de legislaţia acestei părţi în conformitate cu obligaţiile pe care le-a subscris în aplicarea Convenţiei internaţionale pentru protecţia artiştilor interpreţi sau executanţi, a producătorilor de fonograme şi a organismelor de radiodifuziune (Convenţia de la Roma), a Acordului privind aspecte comerciale ale drepturilor de proprietate intelectuală şi a Tratatului OMPI privind interpretările şi fonogramele, cu excepţia oricărui drept moral conferit de aceste convenţii, atunci când astfel de acte sunt comise deliberat, la scară comercială şi prin intermediul unui sistem informatic.
3. O parte va putea, în circumstanţe bine delimitate, să îşi rezerve dreptul de a nu impune răspunderea penală în baza paragrafelor 1 şi 2 ale prezentului articol, cu condiţia ca alte recursuri eficiente să fie disponibile şi cu condiţia ca o astfel de rezervă să nu aducă atingere obligaţiilor internaţionale care incumbă acestei părţi în aplicarea instrumentelor internaţionale menţionate la paragrafele 1 şi 2 ale prezentului articol.

TITLUL 5 - Alte forme de răspundere şi de sancţionare

ARTICOLUL 11 - Tentativa şi complicitatea
1. Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a incrimina ca infracţiune, potrivit dreptului său intern, orice complicitate intenţionată la comiterea uneia dintre infracţiunile stabilite în aplicarea art. 2-10, săvârşite cu intenţie.
2. Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a incrimina ca infracţiune, potrivit dreptului său intern, orice tentativă săvârşită cu intenţia comiterii uneia dintre infracţiunile stabilite în aplicarea art. 3-5, art. 7, 8 şi a art. 9 paragraful 1 subparagrafele a) şi c).
3. Fiecare parte îşi va putea rezerva dreptul de a nu aplica, în totalitate sau parţial, paragraful 2 al prezentului articol.

ARTICOLUL 12 - Răspunderea persoanelor juridice

1. Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru ca persoanele juridice să poată fi trase la răspundere pentru infracţiunile stabilite în aplicarea prezentei convenţii, atunci când acestea sunt comise pe cont propriu de către orice persoană fizică care acţionează fie individual, fie în calitate de membru al unui organ al persoanei juridice, care exercită o funcţie de conducere în cadrul acesteia, având la bază:
   a) o calitate de reprezentare a persoanei juridice;
   b) puterea de luare a deciziilor în numele persoanei juridice;
   c) puterea de a exercita controlul în cadrul persoanei juridice.

2. Cu excepţia cazurilor deja prevăzute la paragraful 1 al prezentului articol, fiecare parte va adopta măsurile care se dovedesc necesare pentru a se asigura că o persoană juridică poate fi trasă la răspundere atunci când absenţa supravegherii sau a controlului din partea persoanei fizice menţionate la paragraful 1 a permis comiterea infracţiunilor stabilite în aplicarea prezentei convenţii pentru numita persoană juridică de către o persoană fizică care acţionează sub autoritatea acesteia.

3. În funcţie de principiile juridice ale părţii, răspunderea unei persoane juridice poate fi penală, civilă sau administrativă.

4. Această răspundere va fi stabilită fără a prejudicia răspunderea penală a persoanelor fizice care au comis infracţiunea.

ARTICOLUL 13 - Sancţiuni şi măsuri

1. Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru ca infracţiunilor stabilite în aplicarea art. 2-11 să li se poată aplica sancţiuni efective, proporţionale şi convingătoare, care cuprind pedepse privative de libertate.

2. Fiecare parte va veghea ca toate persoanele juridice trase la răspundere în aplicarea art. 12 să facă obiectul sancţiunilor sau măsurilor penale ori nepenale efective, proporţionale şi convingătoare, care cuprind sancţiuni pecuniare.

SECŢIUNEA a 2-a - Drept procedural

TITLUL 1 - Dispoziţii comune

ARTICOLUL 14 - Aria de aplicare a măsurilor procedurale

1. Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a stabili prerogativele şi procedurile prevăzute în prezenta secţiune, în scopul desfăşurării anchetelor sau procedurilor penale specifice.
2. Cu excepţia dispoziţiei contrare care figurează la art. 21, fiecare parte va aplica prerogativele şi procedurile menţionate la paragraful 1 al prezentului articol:
   a) infracţiunilor stabilite în conformitate cu art. 2-11;
   b) tuturor celorlalte infracţiuni comise prin intermediul unui sistem informatic; şi
   c) strângerii dovezilor electronice referitoare la orice infracţiune.
3. a) Fiecare parte îşi va putea rezerva dreptul de a nu aplica măsurile menţionate la art. 20 decât infracţiunilor sau categoriilor de infracţiuni specificate în rezervă, astfel încât sfera acestor infracţiuni sau categorii de infracţiuni să nu fie mai redusă decât cea a infracţiunilor cărora aceasta le aplică măsurile menţionate la art. 21. Fiecare parte va avea în vedere să limiteze o astfel de rezervă încât să permită cea mai largă aplicare posibilă a măsurii menţionate la art. 20.
b) În cazul în care o parte, din cauza restricţiilor impuse de legislaţia sa în vigoare la momentul adoptării prezentei convenţii, nu va fi în măsură să aplice măsurile vizate la art. 20 şi 21 comunicaţiilor transmise într-un sistem informatic al unui furnizor de servicii:
   (i) care este folosit în beneficiul unui grup închis de utilizatori; şi
   (ii) care nu utilizează reţelele publice de telecomunicaţii şi care nu este conectat la un alt sistem informatic, public sau privat,

 această parte îşi va putea rezerva dreptul de a nu aplica aceste măsuri pentru astfel de comunicaţii. Fiecare parte va avea în vedere să limiteze o astfel de rezervă încât să permită cea mai largă aplicare posibilă a măsurilor menţionate la art. 20 şi 21.

ARTICOLUL 15 - Condiţii şi măsuri de protecţie

1. Fiecare parte va veghea ca stabilirea, realizarea şi aplicarea prerogativelor şi a procedurilor prevăzute în prezenta secţiune să fie supuse condiţiilor şi măsurilor de protecţie prevăzute în dreptul său intern, care trebuie să asigure o protecţie adecvată a drepturilor şi a libertăţilor omului, în special a drepturilor stabilite în conformitate cu obligaţiile pe care aceasta le-a subscris în aplicarea Convenţiei Consiliului Europei pentru apărarea drepturilor omului şi a libertăţilor fundamentale (1950), a Pactului internaţional privind drepturile civile şi politice al Naţiunilor Unite (1966), precum şi a altor instrumente internaţionale aplicabile privind drepturile omului, şi care trebuie să integreze principiul proporţionalităţii.

2. Ţinând cont de natura procedurii sau a prerogativelor acordate, aceste condiţii şi măsuri de protecţie vor include, între altele, atunci când situaţia o impune, o supervizare judiciară sau alte forme de supervizare independentă a motivelor care justifică aplicarea, precum şi limitarea ariei de aplicare şi a duratei prerogativelor sau procedurii în cauză.
3. În măsura în care acest lucru este în conformitate cu interesul public, în special cu buna administrare a justiţiei, fiecare parte va examina efectul prerogativelor şi al procedurilor în această secţiune privind drepturile, responsabilităţile şi interesele legitime ale terţilor.

TITLUL 2 - Conservarea rapidă a datelor informatice stocate

ARTICOLUL 16 - Conservarea rapidă a datelor informatice stocate
1. Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a permite autorităţilor sale competente să ordone sau să impună într-un alt mod conservarea rapidă a datelor informatice menţionate, inclusiv a datelor referitoare la trafic, stocate prin intermediul unui sistem informatic, cu precădere atunci când există motive de a crede că acestea sunt în mod special susceptibile de pierdere sau de modificare.
2. În cazul în care o parte va aplica prevederile paragrafului anterior, prin intermediul unui ordin adresat unei persoane de a păstra date stocate, precum cele menţionate care se găsesc în posesia sau sub controlul său, această parte va adopta măsurile legislative, precum şi măsurile care se dovedesc necesare pentru a obliga această persoană să păstreze şi să protejeze integritatea datelor pentru atât timp cât este necesar, cel mult 90 de zile, în scopul de a permite autorităţilor competente să obţină dezvăluirea acestora. O parte poate prevedea ca ordinul să fie ulterior reînnoit.
3. Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a obliga persoana care veghează asupra datelor sau o altă persoană însărcinată să le păstreze să păstreze confidenţialitatea cu privire la aplicarea numitelor proceduri pe durata prevăzută în dreptul său intern.
4. Prerogativelor şi procedurilor menţionate în prezentul articol li se aplică prevederile art. 14 şi 15.

ARTICOLUL 17 - Conservarea şi dezvăluirea parţială rapidă a datelor referitoare la trafic
1. În scopul de a asigura conservarea datelor referitoare la trafic, în aplicarea art. 16, fiecare parte va adopta măsurile legislative, precum şi măsurile care se dovedesc necesare:

a) pentru a veghea ca păstrarea rapidă a datelor referitoare la trafic să fie posibilă, indiferent dacă în transmiterea comunicaţiei au fost implicaţi unul sau mai mulţi furnizori de servicii; şi
b) pentru a asigura dezvăluirea rapidă către autoritatea competentă a părţii sau către o persoană desemnată de această autoritate a unei cantităţi de date referitoare la trafic, suficientă pentru a permite părţii identificarea furnizorilor de servicii şi a canalului prin intermediul căruia comunicaţia a fost transmisă.

2. Prerogativelor şi procedurilor menţionate în prezentul articol li se aplică prevederile art. 14 şi 15.

TITLUL 3 - Ordinul de punere la dispoziţie a datelor

ARTICOLUL 18 - Ordinul de punere la dispoziţie a datelor

1. Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a conferi autorităţilor sale competente dreptul de a ordona:
a) unei persoane prezente pe teritoriul său să comunice datele informatice menţionate, aflate în posesia sau sub controlul său, care sunt stocate într-un sistem informatic ori pe un suport de stocare informatic; şi
b) unui furnizor de servicii care oferă prestaţii pe teritoriul părţii să comunice datele din posesia sau de sub controlul său referitoare la abonaţi şi la astfel de servicii.

2. Prerogativelor şi procedurilor menţionate în prezentul articol li se aplică prevederile art. 14 şi 15.

3. În sensul prezentului articol, expresia date referitoare la abonaţi va desemna orice informaţie, sub formă de date informatice sau sub orice altă formă, deţinută de un furnizor de servicii, referitoare la abonaţii acestor servicii, altele decât datele referitoare la trafic sau conţinut, şi care permit stabilirea:
a) tipului de serviciu de comunicaţii utilizat, dispoziţiilor tehnice luate în această privinţă şi perioadei serviciului;
b) 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;
c) oricărei alte informaţii referitoare la locul în care se găsesc echipamentele de comunicaţie, disponibile în baza unui contract sau a unui aranjament de servicii.

TITLUL 4 - Percheziţia şi sechestrarea datelor informatice stocate

ARTICOLUL 19 - Percheziţia şi sechestrarea datelor informatice stocate

1. Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a conferi autorităţilor sale competente dreptul de a percheziţiona sau de a accesa într-un mod similar:
   a) un sistem informatic sau o parte a acestuia, precum şi datele informatice care sunt stocate în acesta; şi
   b) un suport de stocare informatic care permite stocarea datelor informatice pe teritoriul său.
2. În cazul în care autorităţile părţii vor percheziţiona sau vor accesa într-un mod similar un sistem informatic specific ori o parte din acesta, în conformitate cu paragraful 1 subparagraful a), şi vor avea motive de a considera că datele urmărite sunt stocate într-un alt sistem informatic sau într-o parte a acestuia situat pe teritoriul său şi că aceste date sunt în mod legal accesibile de la sistemul iniţial ori sunt disponibile pentru acest sistem iniţial, fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru ca numitele autorităţi să fie în măsură de a extinde rapid percheziţia sau accesarea într-un mod similar a celuilalt sistem.
3. Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a conferi autorităţilor sale competente dreptul de a sechestra sau de a obţine într-un mod similar datele informatice pentru care accesarea a fost realizată în aplicarea paragrafelor 1 sau 2. Aceste măsuri includ următoarele prerogative:
   a) sechestrarea sau obţinerea într-un mod similar a unui sistem informatic ori a unei părţi din acesta sau a unui suport de stocare informatic;
   b) realizarea şi conservarea unei copii a acestor date informatice;
   c) menţinerea integrităţii datelor informatice relevante stocate;
   d) suprimarea accesării sau îndepărtarea acestor date informatice din sistemul informatic accesat.
4. Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a conferi autorităţilor sale competente dreptul de a ordona oricărei persoane care cunoaşte funcţionarea sistemului informatic sau măsurile aplicate pentru protecţia datelor informatice să pună la dispoziţie toate informaţiile considerate necesare pentru a permite aplicarea măsurilor vizate la paragrafele 1 şi 2.
5. Prerogativelor şi procedurilor menţionate în prezentul articol li se aplică prevederile art. 14 şi 15.

TITLUL 5 - Colectarea în timp real a datelor informatice

ARTICOLUL 20 - Colectarea în timp real a datelor referitoare la trafic

1. Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a conferi autorităţilor sale competente următoarele drepturi:
   a) de a culege sau de a înregistra prin aplicarea mijloacelor tehnice care există pe teritoriul său; şi
   b) de a obliga un furnizor de servicii, în limita capacităţilor sale tehnice existente, la:
      (i) strângerea sau înregistrarea prin aplicarea mijloacelor tehnice care există pe teritoriul său;

      sau la

      (ii) acordarea concursului şi asistenţei sale autorităţilor competente, pentru culegerea sau înregistrarea,

      în timp real, a datelor referitoare la trafic, asociate comunicaţiilor respective, transmise pe teritoriul său prin intermediul unui sistem informatic.
2. În cazul în care o parte, datorită principiilor stabilite de legislaţia internă, nu va putea adopta măsurile enunţate la paragraful 1 subparagraful a), aceasta va putea, în schimb, adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a asigura strângerea sau înregistrarea în timp real a datelor referitoare la trafic, asociate comunicaţiilor respective, transmise pe teritoriul său prin aplicarea mijloacelor tehnice existente pe acest teritoriu.
3. Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a obliga un furnizor de servicii să păstreze confidenţialitatea faptului că a fost exercitată oricare dintre prerogativele prevăzute în prezentul articol, precum şi orice informaţie în legătură cu acest subiect.
4. Prerogativelor şi procedurilor menţionate în prezentul articol li se aplică prevederile art. 14 şi 15.

ARTICOLUL 21 - Interceptarea datelor referitoare la conţinut

1. Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a conferi autorităţilor sale competente, cu privire la o serie de infracţiuni grave care să fie definite în legislaţia internă, următoarele drepturi:
   a) de a culege sau de a înregistra prin aplicarea mijloacelor tehnice care există pe teritoriul său; şi
   b) de a obliga un furnizor de servicii, în limita capacităţilor sale tehnice, la:
      (i) strângerea sau înregistrarea prin aplicarea mijloacelor tehnice care există pe teritoriul său;

sau la

(ii) acordarea sprijinului şi asistenţei sale autorităţilor competente, pentru colectarea sau înregistrarea,

în timp real, a datelor referitoare la conţinut, asociate comunicaţiilor respective, transmise pe teritoriul său prin intermediul unui sistem informatic.

2. În cazul în care o parte, datorită principiilor stabilite de legislaţia internă, nu va putea adopta măsurile enunţate la paragraful 1 subparagraful a), aceasta va putea, în schimb, adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a asigura strângerea sau înregistrarea în timp real a datelor referitoare la conţinutul comunicaţiilor respective, transmise pe teritoriul său prin aplicarea mijloacelor tehnice existente pe acest teritoriu.

3. Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a obliga un furnizor de servicii să păstreze confidenţialitatea faptului că oricare dintre prerogativele prevăzute în prezentul articol a fost exercitată, precum şi orice informaţie în legătură cu acest subiect.

4. Prerogativelor şi procedurilor menţionate în prezentul articol li se aplică prevederile art. 14 şi 15.

SECŢIUNEA a 3-a - Competenţa

ARTICOLUL 22 - Competenţa

1. Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a stabili competenţa sa cu privire la orice infracţiune incriminată în conformitate cu art. 2-11, atunci când infracţiunea este comisă:

a) pe teritoriul său; sau
b) la bordul unui vas sub pavilionul acestei părţi; sau
c) la bordul unei aeronave înmatriculate în conformitate cu legislaţia acestei părţi; sau
d) de către unul dintre cetăţenii săi, dacă infracţiunea poate atrage răspunderea penală în locul în care aceasta a fost comisă sau dacă infracţiunea nu este de competenţa teritorială a nici unui stat.

2. Fiecare parte îşi va putea rezerva dreptul de a nu aplica sau de a aplica doar în cazuri ori în condiţii specifice regulile de competenţă definite la paragraful 1 subparagrafele b)-d) al prezentului articol sau în orice parte a acestui paragraf.

3. Fiecare parte va adopta măsurile care se dovedesc necesare pentru a stabili competenţa sa cu privire la orice infracţiune menţionată la art. 24 paragraful 1, în cazul în care autorul prezumat al infracţiunii este prezent pe teritoriul său şi nu

poate fi extrădat spre o altă parte decât în baza naţionalităţii sale, în urma unei cereri de extrădare.
4. Prezenta convenţie nu va exclude nici o competenţă penală exercitată de o parte în conformitate cu dreptul său intern.
5. În cazul în care mai multe părţi îşi revendică jurisdicţia cu privire la o infracţiune stabilită în conformitate cu prezenta convenţie, părţile implicate se vor pune de acord, atunci când acest lucru este oportun, în scopul de a determina partea cea mai potrivită pentru a exercita urmărirea.

CAPITOLUL III - Cooperarea internaţională

SECŢIUNEA 1 - Principii generale

TITLUL 1 - Principii generale referitoare la cooperarea internaţională

ARTICOLUL 23 - Principii generale referitoare la cooperarea internaţională
Părţile vor coopera între ele, în conformitate cu dispoziţiile prezentului capitol şi în aplicarea instrumentelor internaţionale relevante cu privire la cooperarea internaţională în materie penală, a acordurilor încheiate pe baza legislaţiilor uniforme sau reciproce şi a dreptului lor intern, în cea mai largă măsură posibilă, în scopul investigărilor sau al aplicării procedurilor privind infracţiunile în legătură cu sisteme şi date informatice sau pentru a culege dovezile unei infracţiuni în format electronic.

TITLUL 2 - Principii referitoare la extrădare

ARTICOLUL 24 - Extrădarea
1. a) Prezentul articol se va aplica extrădării între părţi pentru infracţiunile stabilite în conformitate cu art. 2-11, cu condiţia ca acestea să poată fi sancţionate, potrivit legislaţiilor ambelor părţi implicate, printr-o pedeapsă privativă de libertate, al cărei maxim special este de cel puţin un an, sau printr-o pedeapsă mai severă.
b) În cazul în care se va impune o pedeapsă minimă diferită, în baza unui tratat de extrădare aplicabil între două sau mai multe părţi, inclusiv Convenţia europeană de extrădare (STE nr. 24), sau a unui acord care are la bază legislaţii uniforme sau reciproce, se va aplica pedeapsa minimă prevăzută prin acest tratat ori aranjament.
2. Infracţiunile descrise la paragraful 1 vor fi considerate incluse în categoria infracţiunilor care pot atrage extrădarea în orice tratat de extrădare care există

între părţi. Părţile se vor angaja să includă astfel de infracţiuni ca infracţiuni care pot atrage extrădarea în orice tratat de extrădare care va fi încheiat între părţi.
3. Dacă o parte care condiţionează extrădarea de existenţa unui tratat primeşte o cerere de extrădare de la altă parte cu care nu a încheiat un tratat de extrădare, aceasta va putea considera prezenta convenţie drept bază juridică pentru extrădarea cu privire la orice infracţiune menţionată la paragraful 1 al prezentului articol.
4. Părţile care nu condiţionează extrădarea de existenţa unui tratat vor recunoaşte infracţiunile menţionate la paragraful 1 al prezentului articol ca infracţiuni care pot atrage extrădarea între acestea.
5. Extrădarea va fi supusă condiţiilor prevăzute de dreptul intern al părţii solicitate sau de tratatele de extrădare în vigoare, inclusiv în ceea ce priveşte motivele pentru care partea solicitată poate refuza extrădarea.
6. Dacă extrădarea pentru o infracţiune menţionată la paragraful 1 al prezentului articol va fi refuzată doar pe motivul cetăţeniei persoanei sau pentru că partea solicitată consideră că este competentă cu privire la această infracţiune, partea solicitată va supune cauza, la cererea părţii solicitante, autorităţilor sale competente, în scopul urmăririi, şi va raporta în timp util, la încheierea cauzei, părţii solicitante. Autorităţile în cauză vor decide şi vor desfăşura ancheta şi procedura în acelaşi mod ca pentru orice altă infracţiune de natură comparabilă, în conformitate cu legislaţia acestei părţi.
7. a) Fiecare parte va comunica secretarului general al Consiliului Europei, în momentul semnării ori depunerii instrumentului său de ratificare, de acceptare, de aprobare sau de aderare, numele şi adresa fiecărei autorităţi responsabile de trimiterea ori de primirea unei cereri de extrădare sau de arestare provizorie, în absenţa unui tratat.
b) Secretarul general al Consiliului Europei va realiza şi va actualiza un registru al autorităţilor astfel desemnate de către părţi. Fiecare parte va trebui să se asigure de faptul că datele care figurează în registru sunt corecte în orice moment.

TITLUL 3 - Principii generale referitoare la asistenţa mutuală

ARTICOLUL 25 - Principii generale referitoare la asistenţa mutuală
1. Părţile îşi vor acorda asistenţă mutuală într-o măsură cât mai largă posibil, în scopul investigărilor sau al aplicării procedurilor privind infracţiunile în legătură cu sisteme şi date informatice sau pentru a culege dovezile unei infracţiuni în format electronic.

2. De asemenea, fiecare parte va adopta măsurile legislative, precum şi măsurile care se dovedesc necesare pentru a-şi îndeplini obligaţiile stabilite în cuprinsul art. 27-35.
3. În caz de urgenţă fiecare parte va putea formula o cerere de asistenţă mutuală sau comunicările care se raportează acesteia prin mijloace rapide de comunicare, precum faxul sau poşta electronică, cu condiţia ca aceste mijloace să ofere condiţii suficiente de securitate şi de autentificare (inclusiv folosirea codării, atunci când este necesar), cu o confirmare oficială ulterioară dacă partea solicitată va revendica acest lucru. Partea solicitată va accepta cererea şi va răspunde prin oricare dintre mijloacele sale rapide de comunicare.
4. Cu excepţia unei dispoziţii contrare expres prevăzute în prezentul capitol, asistenţa mutuală va fi supusă condiţiilor fixate de dreptul intern al părţii solicitate sau de tratatele de asistenţă mutuală aplicabile, inclusiv în ceea ce priveşte motivele pe baza cărora partea solicitată poate refuza cooperarea. Partea solicitată nu îşi va exercita dreptul de a refuza asistenţa mutuală privind infracţiunile vizate la art. 2-11 doar din motivul că cererea vizează o infracţiune pe care aceasta o consideră de natură fiscală.
5. În cazul în care, în conformitate cu dispoziţiile prezentului capitol, părţii solicitate îi este permis să condiţioneze asistenţa mutuală de existenţa dublei incriminări, această condiţie va fi considerată îndeplinită dacă fapta care constituie infracţiunea pentru care asistenţa mutuală este solicitată este calificată drept infracţiune de dreptul său intern, indiferent dacă dreptul intern include sau nu infracţiunea în cadrul aceleiaşi categorii de infracţiuni ori dacă o defineşte sau nu prin aceeaşi terminologie ca dreptul părţii solicitante.

ARTICOLUL 26 - Informarea spontană
1. O parte va putea, în limitele dreptului său intern şi în absenţa unei cereri prealabile, să comunice unei alte părţi informaţii obţinute în cadrul propriilor anchete, în cazul în care consideră că acest lucru ar putea ajuta partea destinatară la începerea sau finalizarea cu succes a anchetelor ori a procedurilor având ca obiect infracţiuni stabilite în conformitate cu prezenta convenţie sau în cazul în care aceste informaţii ar putea conduce la o cerere de cooperare formulată de această parte în virtutea prezentului capitol.
2. Înainte de a comunica astfel de informaţii, partea care le furnizează va putea solicita ca acestea să rămână confidenţiale sau să nu fie utilizate decât în anumite condiţii. Dacă partea destinatară nu va putea îndeplini această cerinţă, va informa cealaltă parte, care va stabili în acest caz dacă informaţiile în cauză ar trebui totuşi furnizate. Dacă partea destinatară va accepta informaţiile cu condiţiile prescrise, partea destinatară va fi legată de acestea din urmă.

TITLUL 4 - Procedurile referitoare la cererile de asistenţă mutuală în absenţa acordurilor internaţionale aplicabile

ARTICOLUL 27 - Procedurile referitoare la cererile de asistenţă mutuală în absenţa acordurilor internaţionale aplicabile

1. În absenţa unui tratat de asistenţă mutuală ori a unui acord care are la bază legislaţii uniforme sau reciproce în vigoare între partea solicitantă şi partea solicitată, se vor aplica dispoziţiile paragrafelor 2-9 din prezentul articol. Acestea nu se vor aplica atunci când există un tratat, un acord sau o legislaţie de acest tip, în afară de cazul în care părţile implicate nu convin să aplice în locul lor totul sau o parte din restul acestui articol.

2.

a) Fiecare parte va desemna una sau mai multe autorităţi centrale însărcinate să trimită cererile de asistenţă mutuală sau să răspundă, să le execute ori să le transmită autorităţilor competente pentru executarea lor.
b) Autorităţile centrale vor comunica direct una cu cealaltă.
c) Fiecare parte, în momentul semnării sau depunerii instrumentelor sale de ratificare, de acceptare, de aprobare sau de aderare, va comunica secretarului general al Consiliului Europei numele şi adresele autorităţilor desemnate în aplicarea prezentului paragraf.
d) Secretarul general al Consiliului Europei va stabili şi va actualiza un registru al autorităţilor centrale desemnate de către părţi. Fiecare parte va veghea în permanenţă asupra exactitudinii datelor care figurează în registru.

3. Cererile de asistenţă mutuală adresate în baza prezentului articol vor fi executate în conformitate cu procedura menţionată de partea solicitantă, cu excepţia cazului în care aceasta este incompatibilă cu legislaţia părţii solicitate.

4. Pe lângă condiţiile sau motivele de refuz prevăzute la art. 25 paragraful 4, asistenţa mutuală va putea fi refuzată de partea solicitată, dacă:

a) cererea vizează o infracţiune pe care partea solicitată o consideră de natură politică ori legată de o infracţiune de natură politică; sau
b) partea solicitată va considera că faptul de a da curs cererii ar risca să aducă atingere suveranităţii, securităţii, ordinii sale publice sau altor interese esenţiale.

5. Partea solicitată va putea suspenda executarea cererii dacă aceasta ar risca să aducă prejudicii anchetelor sau procedurilor desfăşurate de autorităţile sale.

6. Înainte de a refuza sau de a suspenda cooperarea, partea solicitată va examina, ulterior consultării părţii solicitante, dacă poate da curs parţial cererii ori cu rezerva condiţiilor pe care le consideră necesare.
7. Partea solicitată va informa rapid partea solicitantă asupra răspunsului pe care intenţionează să îl dea cererii de asistenţă mutuală.
Aceasta va trebui să motiveze eventualul său refuz sau eventuala întârziere a cererii. De asemenea, partea solicitată va informa partea solicitantă asupra oricărui motiv care ar face imposibilă executarea cererii de asistenţă mutuală sau care ar fi susceptibil de a o întârzia în mod semnificativ.
8. Partea solicitantă va putea cere ca partea solicitată să păstreze confidenţialitatea faptului că a fost formulată o cerere în baza prezentului capitol, precum şi a obiectului acesteia, cu excepţia măsurilor necesare executării cererii în cauză. Dacă partea solicitată nu va putea da curs acestei cereri de confidenţialitate, aceasta va trebui să informeze rapid partea solicitantă, care va trebui în acest caz să determine dacă cererea trebuie totuşi executată.
9.

a) În caz de urgenţă, cererile de asistenţă mutuală sau comunicările care se raportează acestora vor putea fi transmise direct de către autorităţile judiciare ale părţii solicitante autorităţilor similare ale părţii solicitate. Într-un asemenea caz, o copie va fi adresată simultan autorităţilor centrale ale părţii solicitate prin intermediul autorităţii centrale a părţii solicitante.
b) Orice cerere sau comunicare formulată în baza prezentului paragraf va putea fi avansată prin intermediul Organizaţiei Internaţionale de Poliţie Criminală (Interpol).
c) În cazul în care o cerere a fost formulată în aplicarea subparagrafului a) al prezentului paragraf şi în cazul în care autoritatea nu va fi competentă pentru a o analiza, aceasta o va transmite autorităţii naţionale competente şi va informa direct partea solicitantă.
d) Cererile sau comunicările efectuate în aplicarea prezentului paragraf, care nu presupun măsuri coercitive, vor putea fi direct transmise de către autorităţile competente ale părţii solicitante la autorităţile competente ale părţii solicitate.
e) Fiecare parte îl va putea informa pe secretarul general al Consiliului Europei, în momentul semnării sau depunerii instrumentului său de ratificare, de acceptare, de aprobare sau de aderare, că, pentru motive de eficienţă, cererile formulate în baza acestui paragraf vor trebui adresate autorităţilor sale centrale.

ARTICOLUL 28 - Confidenţialitatea şi restricţia de utilizare
1. În absenţa unui tratat de asistenţă mutuală sau a unui aranjament care să aibă la bază legislaţii uniforme ori reciproce în vigoare între partea solicitantă şi partea solicitată, se vor aplica dispoziţiile prezentului articol. Acestea nu se vor aplica în cazul în care există un tratat, un aranjament sau o legislaţie de acest tip, cu excepţia cazului în care părţile implicate decid să aplice în locul acestora totul sau o parte din acest articol.
2. Partea solicitată va putea condiţiona comunicarea de informaţii sau de materiale, reprezentând răspunsul la cerere, de:
a) păstrarea confidenţialităţii acestora, în cazul în care cererea de asistenţă mutuală nu ar putea fi respectată în absenţa acestei condiţii; sau
b) neutilizarea acestora pentru alte anchete sau proceduri decât cele indicate în cerere.
3. Dacă partea solicitantă nu va putea îndeplini una dintre condiţiile enunţate la paragraful 2, aceasta va informa rapid partea solicitată, care va determina în acest caz dacă informaţia trebuie totuşi furnizată. Dacă partea solicitantă va accepta această condiţie, aceasta va fi legată de condiţia menţionată.
4. Orice parte care va furniza informaţii sau materiale ce se supun uneia dintre condiţiile enunţate la paragraful 2 va putea solicita celeilalte părţi să-i ofere explicaţii în legătură cu această condiţie privind utilizarea acestor informaţii sau a acestui material.

SECŢIUNEA a 2-a - Dispoziţii speciale

TITLUL 1 - Asistenţa mutuală în materie de măsuri provizorii

ARTICOLUL 29 - Conservarea rapidă a datelor informatice stocate
1. O parte va putea solicita unei alte părţi să ordone sau să impună printr-un alt mijloc conservarea rapidă a datelor stocate prin intermediul unui sistem informatic care se găseşte pe teritoriul acestei alte părţi şi la adresa cărora partea solicitantă are intenţia de a formula o cerere de asistenţă mutuală în vederea percheziţiei ori accesării printr-un mijloc similar, sechestrului sau obţinerii printr-un mijloc similar ori divulgării datelor în cauză.
2. O cerere de conservare formulată în aplicarea paragrafului 1 va trebui să precizeze:
a) autoritatea care solicită conservarea;
b) infracţiunea care va face obiectul anchetei sau procedurilor penale, precum şi o scurtă expunere a faptelor care au legătură cu aceasta;

c) datele informatice stocate care vor trebui conservate şi natura legăturii lor cu infracţiunea;
d) toate informaţiile disponibile care vor permite identificarea posesorului datelor informatice stocate sau locaţia sistemului informatic;
e) necesitatea măsurii conservării; şi
f) faptul că partea are intenţia de a formula o cerere de asistenţă mutuală în vederea percheziţiei ori accesării printr-un mijloc similar, sechestrului sau obţinerii printr-un mijloc similar, ori divulgării datelor informatice în cauză.

3. După primirea cererii unei alte părţi, partea solicitată va trebui să ia toate măsurile care se impun pentru a proceda fără întârziere la conservarea datelor menţionate, în conformitate cu dreptul său intern. Pentru a putea răspunde unei astfel de solicitări, dubla incriminare nu va fi solicitată ca o condiţie prealabilă a conservării.

4. O parte care va solicita dubla incriminare ca o condiţie pentru a răspunde unei cereri de asistenţă mutuală în vederea percheziţiei ori accesării printr-un mijloc similar, sechestrului sau obţinerii printr-un mijloc similar ori divulgării datelor stocate, va putea, pentru alte infracţiuni decât cele stabilite în conformitate cu art. 2-11 să-şi rezerve dreptul de a refuza cererea de conservare în baza prezentului articol, în cazul în care aceasta va avea motive de a considera că, în momentul divulgării, condiţia dublei incriminări nu va putea fi îndeplinită.

5. Pe de altă parte, o cerere de conservare va putea fi refuzată doar dacă:
a) cererea vizează o infracţiune pe care partea solicitată o consideră ca fiind de natură politică ori legată de o infracţiune politică; sau
b) partea solicitată consideră că faptul de a da curs cererii ar risca de a aduce atingere suveranităţii sale, securităţii, ordinii publice sau altor interese esenţiale.

6. În cazul în care partea solicitată va considera că simpla conservare nu va fi suficientă pentru garantarea disponibilităţii viitoare a datelor, va compromite confidenţialitatea anchetei părţii solicitante sau o va afecta într-un alt mod, aceasta va informa rapid partea solicitantă, care va decide în acel caz dacă cererea va trebui totuşi executată.

7. Orice conservare efectuată ca răspuns la o cerere menţionată la paragraful 1 va fi valabilă pentru o perioadă de cel puţin 60 de zile, în scopul de a permite părţii solicitante de a formula o cerere în vederea percheziţiei ori accesării printr-un mijloc similar, sechestrului sau obţinerii printr-un mijloc similar ori divulgării datelor. După primirea unei astfel de cereri, datele vor trebui în continuare conservate în aşteptarea adoptării unei decizii referitoare la cerere.

ARTICOLUL 30 - Dezvăluirea rapidă a datelor conservate
1. În cazul în care, în timpul executării unei cereri de conservare a datelor referitoare la trafic în legătură cu o comunicare specifică formulată în aplicarea art. 29, partea solicitată va descoperi că un furnizor de servicii a participat într-un alt stat la transmiterea acestei comunicări, aceasta va dezvălui rapid părţii solicitante o cantitate suficientă de date referitoare la trafic, pentru identificarea acestui furnizor de servicii şi a canalului prin care comunicarea a fost transmisă.
2. Dezvăluirea datelor referitoare la trafic în aplicarea paragrafului 1 va putea fi refuzată doar dacă:
a) cererea vizează o infracţiune pe care partea solicitată o consideră de natură politică ori legată de o infracţiune de natură politică; sau
b) partea solicitată consideră că faptul de a da curs cererii ar risca să aducă atingere suveranităţii sale, securităţii, ordinii publice sau altor interese esenţiale.

TITLUL 2 - Asistenţa mutuală privind prerogativele de investigare

ARTICOLUL 31 - Asistenţa mutuală privind accesarea datelor stocate
1. O parte va putea solicita unei alte părţi să percheziţioneze sau să acceseze într-un mod similar, să sechestreze sau să obţină într-un mod similar, să dezvăluie date stocate prin intermediul unui sistem informatic care se găseşte pe teritoriul acestei alte părţi, inclusiv date conservate în conformitate cu art. 29.
2. Partea solicitată va răspunde cererii cu aplicarea instrumentelor internaţionale, a aranjamentelor şi a legislaţiilor menţionate la art. 23 şi conformându-se dispoziţiilor relevante ale prezentului capitol.
3. Cererea va trebui satisfăcută cât mai repede posibil, dacă:
a) există motive de a considera că datele concludente sunt expuse în mod special riscurilor de pierdere ori de modificare; sau
b) instrumentele, aranjamentele şi legislaţiile vizate la paragraful 2 prevăd o cooperare rapidă.

ARTICOLUL 32 - Accesarea transfrontalieră a datelor stocate, cu consimţământ sau în cazul în care acestea sunt accesibile publicului
O parte va putea, fără autorizaţia unei alte părţi:
a) să acceseze date informatice stocate accesibile publicului (sursă deschisă), oricare ar fi localizarea geografică a acestor date; sau
b) să acceseze ori să primească prin intermediul unui sistem informatic situat pe teritoriul său date informatice stocate situate într-un alt stat, dacă

partea va obţine consimţământul persoanei legal autorizate să-i dezvăluie aceste date prin intermediul acestui sistem informatic.

ARTICOLUL 33 - Asistenţa mutuală pentru strângerea în timp real a datelor referitoare la trafic

1. Părţile îşi vor acorda asistenţă mutuală pentru strângerea în timp real a datelor referitoare la trafic, asociate comunicărilor menţionate pe teritoriul acestora, transmise prin intermediul unui sistem informatic. Cu rezerva dispoziţiilor paragrafului 2, asistenţa mutuală este guvernată de condiţiile şi procedurile prevăzute în dreptul intern.

2. Fiecare parte va acorda această asistenţă mutuală cel puţin cu privire la infracţiunile pentru care strângerea în timp real a datelor privitoare la trafic ar fi disponibilă într-o cauză internă echivalentă.

ARTICOLUL 34 - Asistenţa mutuală în domeniul interceptării datelor referitoare la conţinut

Părţile îşi vor acorda asistenţă mutuală, în măsura permisă de tratatele şi legislaţia internă aplicabile, pentru strângerea sau înregistrarea în timp real a datelor referitoare la conţinutul comunicaţiilor specifice, transmise prin intermediul unui sistem informatic.

TITLUL 3 - Reţeaua 24/7

ARTICOLUL 35 - Reţeaua 24/7

1. Fiecare parte va desemna un punct de contact disponibil 24 de ore din 24, 7 zile din 7, în scopul asigurării unei asistenţe imediate pentru investigaţiile referitoare la infracţiunile privind sisteme sau date informatice, sau pentru a strânge dovezile unei infracţiuni în format electronic. Această asistenţă va cuprinde facilitarea sau, dacă dreptul şi practica internă o permit, aplicarea directă a următoarelor măsuri:

a) asistenţa tehnică;
b) conservarea datelor, în conformitate cu art. 29 şi 30;
c) strângerea dovezilor, furnizarea de informaţii cu caracter juridic şi localizarea suspecţilor.

2. a) Punctul de contact al unei părţi va avea mijloacele de a coresponda cu punctul de contact al unei alte părţi potrivit unei proceduri accelerate.

b) Dacă punctul de contact desemnat de către o parte nu va depinde de autoritatea sau de autorităţile acestei părţi responsabile de asistenţa mutuală

internaţională sau de extrădare, punctul de contact va veghea să poată acţiona în coordonare cu această sau aceste autorităţi, potrivit unei proceduri accelerate.
3. Fiecare parte va întreprinde măsurile necesare pentru a dispune de un personal specializat şi echipat corespunzător pentru facilitarea funcţionării reţelei.

CAPITOLUL IV - Clauze finale

ARTICOLUL 36 - Semnarea şi intrarea în vigoare
1. Prezenta convenţie va fi deschisă spre semnare statelor membre ale Consiliului Europei şi statelor membre care au participat la elaborarea sa.
2. Prezenta convenţie va fi supusă ratificării, acceptării sau aprobării. Instrumentele de ratificare, de acceptare sau de aprobare vor fi depuse la secretarul general al Consiliului Europei.
3. Prezenta convenţie va intra în vigoare în prima zi a lunii care urmează expirării unei perioade de 3 luni după data la care 5 state, cuprinzând cel puţin 3 state membre ale Consiliului Europei, îşi vor fi exprimat consimţământul de a fi legate prin convenţie, în conformitate cu dispoziţiile paragrafelor 1 şi 2.
4. Pentru oricare stat semnatar care îşi va exprima ulterior consimţământul de a fi legat prin prezenta convenţie, aceasta va intra în vigoare în prima zi a lunii care urmează expirării unei perioade de 3 luni după data exprimării consimţământului său de a fi legat prin prezenta convenţie, în conformitate cu dispoziţiile paragrafelor 1 şi 2.

ARTICOLUL 37 - Aderarea la convenţie
1. După intrarea în vigoare a prezentei convenţii, Comitetul de Miniştri al Consiliului Europei, după consultarea statelor contractante la convenţie şi după obţinerea asentimentului unanim, vor putea invita orice stat nemembru al Consiliului Europei, care nu a participat la elaborarea sa, să adere la prezenta convenţie. Decizia va fi luată cu majoritatea prevăzută la art. 20 d) din Statutul Consiliului Europei şi cu unanimitatea reprezentanţilor statelor contractante care au dreptul să facă parte din Comitetul de Miniştri.
2. Pentru orice stat care a aderat la prezenta convenţie, în conformitate cu paragraful 1 sus-menţionat, convenţia va intra în vigoare în prima zi a lunii care urmează expirării unei perioade de 3 luni după data depunerii instrumentului de aderare la secretarul general al Consiliului Europei.

ARTICOLUL 38 - Aplicarea teritorială
1. În momentul semnării sau în momentul depunerii instrumentului său de ratificare, de acceptare, de aprobare sau de aderare, oricare stat va putea desemna teritoriul sau teritoriile cărora li se va aplica prezenta convenţie.
2. În orice moment următor, prin declaraţie adresată secretarului general al Consiliului Europei, oricare stat va putea lărgi aplicarea prezentei la convenţii la oricare alt teritoriu desemnat în declaraţie. Convenţia va intra în vigoare cu privire la acest teritoriu în prima zi a lunii care urmează expirării unei perioade de 3 luni de la data primirii declaraţiei de către secretarul general.
3. Orice declaraţie formulată cu aplicarea celor două paragrafe precedente va putea fi retrasă, cu privire la orice teritoriu desemnat în această declaraţie, prin notificare adresată secretarului general al Consiliului Europei. Retragerea va intra în vigoare în prima zi a lunii care urmează expirării unei perioade de 3 luni după data primirii notificării menţionate de către Secretarul general.

ARTICOLUL 39 - Efectele convenţiei
1. Scopul prezentei convenţii este de a completa tratatele sau acordurile multilaterale ori bilaterale aplicabile, existente între părţi, inclusiv dispoziţiile:

- Convenţiei europene de extrădare, deschisă spre semnare la 13 decembrie 1957 la Paris (STE nr. 24);
- Convenţiei europene de asistenţă judiciară în materie penală, deschisă spre semnare la 20 aprilie 1959 la Strasbourg (STE nr. 30);
- Protocolului adiţional la Convenţia europeană de asistenţă judiciară în materie penală, deschis spre semnare la 17 martie 1978 la Strasbourg (STE nr. 99).

2. Dacă două sau mai multe părţi au încheiat deja un acord ori un tratat referitor la domeniile cuprinse în prezenta convenţie sau dacă şi-au stabilit în alt mod relaţiile privind aceste subiecte ori dacă o vor face în viitor, acestea vor avea, de asemenea, dreptul de a aplica acordul sau tratatul menţionat ori de a-şi stabili relaţiile în consecinţă, în locul prezentei convenţii. Totuşi, în cazul în care părţile îşi vor stabili relaţiile privind domeniile care fac obiectul prezentei convenţii într-un mod diferit decât cel prevăzut, acestea o vor face într-un mod care să nu fie incompatibil cu obiectivele şi principiile convenţiei.
3. Nici o prevedere a prezentei convenţii nu va afecta alte drepturi, restricţii, obligaţii şi responsabilităţi ale unei părţi.

ARTICOLUL 40 - Declaraţii
Prin declaraţie scrisă adresată secretarului general al Consiliului Europei în momentul semnării sau depunerii instrumentului său de ratificare, de acceptare,

de aprobare sau de aderare, orice stat va putea să declare că se foloseşte de dreptul de a solicita unul sau mai multe elemente suplimentare, precum cele prevăzute la art. 2, 3, art. 6 paragraful 1 subparagraful b), art. 7, art. 9 paragraful 3 şi art. 27 paragraful 9 subparagraful e).

ARTICOLUL 41 - Clauza federală
1. Un stat federal îşi va putea rezerva dreptul de a onora obligaţiile cuprinse în cap. II în măsura în care acestea vor fi compatibile cu principiile fundamentale care guvernează relaţiile dintre guvernul său central şi statele constitutive sau alte entităţi teritoriale analoage, cu condiţia ca acesta să fie în măsură de a coopera în baza cap. III.
2. Atunci când acesta va formula o rezervă prevăzută la paragraful 1, un stat federal nu se va putea folosi de termenii unei astfel de rezerve pentru a elimina sau a diminua substanţial obligaţiile sale în baza cap. II. În orice caz, acesta va folosi mijloace lărgite şi efective care vor permite aplicarea măsurilor prevăzute în capitolul menţionat.
3. În ceea ce priveşte dispoziţiile acestei convenţii, a căror aplicare ţine de competenţa legislativă a fiecărui stat constitutiv sau a altor entităţi teritoriale analoage care, în baza sistemului constituţional al federaţiei, nu sunt obligate să ia măsuri legislative, guvernul federal va aduce la cunoştinţă autorităţilor competente ale statelor constitutive dispoziţiile menţionate, împreună cu avizul său favorabil, încurajându-le să adopte măsurile potrivite pentru aplicarea lor.

ARTICOLUL 42 - Rezervele
Prin notificare scrisă adresată secretarului general al Consiliului Europei, în momentul semnării sau depunerii instrumentului său de ratificare, de acceptare, de aprobare sau de aderare, orice stat va putea declara că se foloseşte de rezerva sau rezervele prevăzute la art. 4 paragraful 2, art. 6 paragraful 3, art. 9 paragraful 4, art. 10 paragraful 3, art. 11 paragraful 3, art. 14 paragraful 3, art. 22 paragraful 2, art. 29 paragraful 4 şi la art. 41 paragraful 1. Nici o altă rezervă nu va putea fi formulată.

ARTICOLUL 43 - Statutul şi retragerea rezervelor
1. O parte care a formulat o rezervă în conformitate cu art. 42 o va putea retrage în totalitate sau în parte prin notificare adresată secretarului general al Consiliului Europei. Această retragere va intra în vigoare la data primirii de către secretarul general a notificării menţionate. Dacă notificarea va indica faptul că retragerea unei rezerve trebuie să intre în vigoare la o dată precisă şi dacă această

dată va fi ulterioară celei la care secretarul general va primi notificarea, retragerea va intra în vigoare la această dată ulterioară.
2. O parte care a formulat o rezervă, precum cele menţionate la art. 42, va retrage această rezervă, în totalitate sau în parte, de îndată ce împrejurările o permit.
3. Secretarul general al Consiliului Europei va putea solicita periodic părţilor care au formulat una sau mai multe rezerve dintre cele menţionate la art. 42 informaţii cu privire la aspectele retragerii lor.

ARTICOLUL 44 - Amendamente
1. La prezenta convenţie vor putea fi propuse amendamente de către fiecare parte, iar acestea vor fi comunicate de către secretarul general al Consiliului Europei statelor membre ale Consiliului Europei, statelor nemembre care au participat la elaborarea prezentei convenţii, precum şi oricărui stat care a aderat sau care a fost invitat să adere, în conformitate cu dispoziţiile art. 37.
2. Orice amendament propus de către o parte va fi comunicat Comitetului European pentru Probleme Criminale (CDPC), care va prezenta avizul său Comitetului de Miniştri cu privire la amendamentul menţionat.
3. Comitetul de Miniştri va examina amendamentul propus şi avizul prezentat de către CDPC şi, după consultarea statelor nemembre care sunt părţi la prezenta convenţie, va putea adopta amendamentul.
4. Textul oricărui amendament adoptat de către Comitetul de Miniştri în conformitate cu paragraful 3 al prezentului articol va fi comunicat părţilor pentru acceptare.
5. Orice amendament adoptat în conformitate cu paragraful 3 al prezentului articol va intra în vigoare în a treizecea zi după ce toate părţile l-au informat pe secretarul general cu privire la acceptarea lor.

ARTICOLUL 45 - Rezolvarea dezacordurilor
1. CDPC va fi informat permanent cu privire la interpretarea şi aplicarea prezentei convenţii.
2. În cazul dezacordului între părţi cu privire la interpretarea şi aplicarea prezentei convenţii, părţile se vor strădui să ajungă la o rezolvare a acestuia prin negociere sau prin orice alt mijloc paşnic pe care îl vor alege, inclusiv prin prezentarea dezacordului CDPC, unui tribunal arbitrar care va lua decizii ce vor lega părţile sau Curţii Internaţionale de Justiţie, potrivit unui acord între părţile implicate.

ARTICOLUL 46 - Reuniunea părţilor
1. Părţile se vor reuni periodic, dacă va fi nevoie, în vederea facilitării:

a) utilizării şi aplicării efective a prezentei convenţii, inclusiv identificării oricărei probleme în domeniu, precum şi efectelor oricărei declaraţii sau rezerve făcute în conformitate cu prezenta convenţie;
b) schimbului de informaţii cu privire la noutăţile juridice, politice sau tehnice importante în domeniul criminalităţii informatice şi strângerii dovezilor în formă electronică;
c) examinării eventualităţii de a completa sau de a amenda convenţia.

2. CDPC va fi ţinut periodic la curent cu privire la rezultatul reuniunilor internaţionale menţionate la paragraful 1.
3. CDPC va facilita, dacă va fi nevoie, întâlnirile menţionate la paragraful 1 şi va adopta măsurile necesare pentru a ajuta părţile în efortul lor care vizează completarea sau amendarea convenţiei. La expirarea unui termen de 3 ani începând de la data intrării în vigoare a prezentei convenţii, cel mai târziu, CDPC va proceda, în cooperare cu părţile, la reexaminarea tuturor dispoziţiilor convenţiei şi va propune, dacă este cazul, amendamentele potrivite.
4. Cu excepţia cazului în care Consiliul Europei le va suporta, cheltuielile ocazionate de aplicarea dispoziţiilor paragrafului 1 vor fi suportate de către părţi în maniera pe care acestea o vor alege.
5. Părţile vor fi asistate în exercitarea funcţiilor care decurg din prezentul articol de către Secretariatul Consiliului Europei.

ARTICOLUL 47 - Denunţarea
1. Orice parte va putea, în orice moment, să denunţe prezenta convenţie printr-o notificare adresată secretarului general al Consiliului Europei.
2. Denunţarea va intra în vigoare în prima zi a lunii care urmează expirării unei perioade de 3 luni după data primirii notificării de către secretarul general.

ARTICOLUL 48 - Notificarea
Secretarul general al Consiliului Europei va notifica statelor membre ale Consiliului Europei, statelor nemembre care au participat la elaborarea prezentei convenţii, precum şi oricărui stat care a aderat sau care a fost invitat să adere, cu privire la:

a) orice semnare;
b) depunerea oricărui instrument de ratificare, de acceptare, de aprobare sau de aderare;
c) orice dată de intrare în vigoare a prezentei convenţii, în conformitate cu art. 36 şi 37;
d) orice declaraţie făcută în aplicarea art. 40 sau orice rezervă făcută în aplicarea art. 42;

e) orice alt act, notificare sau comunicare ce are legătură cu prezenta convenţie.

În acest sens, subsemnaţii, autorizaţi pe deplin în acest scop, au semnat prezenta convenţie.

Adoptată la Budapesta la 23 noiembrie 2001, în limbile franceză şi engleză, ambele texte fiind egal autentice, într-un singur exemplar care va fi depus în Arhivele Consiliului Europei. Secretarul general al Consiliului Europei va transmite fiecăruia dintre statele membre ale Consiliului Europei, statelor nemembre care au participat la elaborarea convenţiei, precum şi oricărui stat invitat să adere o copie certificată conformă cu originalul.

Anexa III

Rec(1995)013

CONSILIUL EUROPEI

COMITETUL DE MINIŞTRI

Recomandarea nr. R (95) 13

a Comitetului de Miniştri către statele membre cu privire la problemele de procedură penală legate de tehnologiile informaţionale

(adoptată de Comitetul de Miniştri la 11 septembrie 1995, în cadrul celei de-a 543-a reuniuni a Delegaţilor Miniştrilor)

Comitetul de Miniştri, în temeiul articolului 15.b din Statutul Consiliului Europei,

Reamintind că scopul Consiliului Europei este de a realiza o uniune mai strânsă între membrii săi;

Având în vedere dezvoltarea fără precedent a tehnologiilor informaţionale şi aplicarea lor în toate sectoarele societăţii contemporane;

Realizând că dezvoltarea sistemelor electronice de informare va accelera transformarea societăţii tradiţionale într-o societate a informaţiei şi va crea un nou spaţiu pentru orice tip de comunicare şi de relaţii;

Conştient de impactul tehnologiilor informaţionale asupra modului în care este organizată societatea şi asupra felului în care indivizii comunică şi interacţionează;

Conştient de faptul că o parte tot mai mare a relaţiilor economice şi sociale va avea loc prin intermediul sau cu ajutorul sistemelor informaţionale electronice;

Preocupat de riscul ca sistemele electronice informaţionale şi informaţia electronice să poată fi de asemenea utilizate pentru comiterea de infracţiuni criminale;

Preocupat de faptul că dovezi ale infracţiunilor penale pot fi stocate şi transmise prin intermediul acestor sisteme;

Constatând faptul că legile de procedură penală ale Statelor membre adeseori încă nu prevăd drepturi corespunzătoare pentru percheziţionarea acestor sisteme şi pentru colectarea de probe în cursul anchetelor penale;

Amintind faptul că, în faţa dezvoltării tehnologiilor informaţionale, lipsa unor puteri speciale corespunzătoare poate aduce atingere bunei executări, de către autorităţile însărcinate cu ancheta, a funcţiilor proprii;

Recunoscând necesitatea de a adapta mijloacele legale de care dispun autorităţile însărcinate cu ancheta în temeiul legilor de procedură penală la caracterul specific al anchetelor în sistemele informaţionale electronice;

Preocupat de riscul potenţial ca Statele membre să nu fie în măsură să îşi acorde asistenţă judiciară într-un mod adecvat, atunci când li se cere să colecteze probe electronice, pe teritoriul lor, în sisteme informaţionale electronice;

Convins de necesitatea de a întări cooperarea internaţională şi de a realiza o mai bună compatibilitate a legilor de procedură penală în domeniu;

Amintind Recomandarea nr. R (81) 20 cu privire la armonizarea legislaţiilor în materie de exigenţă a dovezilor scrise şi în materie de admisibilitate a reproducerilor de documente şi a înregistrărilor informatice, Recomandarea nr. R (85) 10 cu privire la comisiile rogatorii pentru supravegherea telecomunicaţiilor, Recomandarea nr. (87) 15 cu privire la reglementarea utilizării datelor cu caracter personal în domeniul poliţiei şi Recomandarea nr. R (89) 9 cu privire la crima informatică,

Recomandă guvernelor Statelor membre:

i. de a se inspira din principiile aflate în anexa la această recomandare, atunci când îşi revizuiesc legislaţia şi practicile lor interne; şi

ii. de a aduce aceste dispoziţii la cunoştinţa autorităţilor însărcinate cu ancheta şi a altor servicii profesionale, în special a celor din sectorul tehnologiilor informaţionale, care pot fi implicate în punerea lor în aplicare.

Anexa la Recomandarea nr. R (95) 13

cu privire la problemele de procedură penală legate de tehnologiile informaţionale

I. Percheziţie şi sechestru

1. Distincţia făcută prin lege între percheziţia sistemelor informaţionale precum şi sechestrarea datelor pe care le conţin, pe de o parte, şi interceptarea datelor în timpul transmisiunii, pe de altă parte, ar trebui să fie clar stabilită şi aplicată.

2. Legile de procedură penală ar trebui să permită autorităţilor însărcinate cu ancheta să facă percheziţii în sistemele informaţionale şi să sechestreze datele găsite, în condiţii similare celor utilizate în cadrul drepturilor tradiţionale de percheziţie şi sechestru. Persoana care are responsabilitatea sistemului ar trebui să fie informată despre faptul că sistemul a făcut obiectul unei percheziţii şi despre natura datelor sechestrate. Recursurile juridice prevăzute de legislaţie în general împotriva percheziţiei şi a sechestrului ar trebui să fie aplicabile în egală măsură în cazul percheziţiei unui sistem informaţional şi în cel al sechestrării datelor pe care acesta le conţine.

3. În timpul executării percheziţiei, autorităţile însărcinate cu ancheta ar trebui să aibă dreptul, sub rezerva garanţiilor corespunzătoare, de a extinde percheziţia asupra altor sisteme informaţionale din jurisdicţia lor care sunt conectate prin intermediul unei reţele şi de a sechestra datele conţinute în ele, cu condiţia ca o acţiune imediată să fie necesară.

4. În cazul în care există o echivalenţă funcţională între datele care constituie obiectul prelucrării automatizate şi un document tradiţional, dispoziţiile dreptului de procedură penală referitoare la documente ar trebui să se aplice, de asemenea, la date.

II. Supraveghere tehnică

5. Având în vedere convergenţa tehnologiilor informaţionale şi a telecomunicaţiilor, legile cu privire la supravegherea tehnică utilizată în scopuri de anchete penale, cum ar fi interceptarea telecomunicaţiilor, ar trebui să fie revăzute şi modificate, acolo unde este necesar, pentru a asigura aplicabilitatea acestora.

6. Legea ar trebui să permită autorităţilor însărcinate cu ancheta să aplice, în investigarea infracţiunilor penale, orice măsuri tehnice care permit colectarea datelor de trafic.

7. Atunci când sunt colectate în cursul unei anchete penale şi în special când sunt obţinute prin mijloace de interceptare a telecomunicaţiilor, datele protejate prin lege şi prelucrate de un sistem informaţional ar trebui să fie protejate în mod corespunzător.

8. Legile de procedură penală ar trebui să fie revizuite pentru a permite interceptarea telecomunicaţiilor şi colectarea datelor de trafic în cadrul anchetelor privind infracţiuni grave împotriva confidenţialităţii, integrităţii şi disponibilităţii sistemelor de telecomunicaţii sau informatice.

III. Obligaţii de cooperare cu autorităţile însărcinate cu ancheta

9. Sub rezerva privilegiilor sau protecţiei prevăzute de lege, majoritatea legislaţiilor permit autorităţilor însărcinate cu ancheta să dispună unor persoane predarea obiectelor care se află sub controlul lor şi care sunt necesare în calitate de probe. În acelaşi mod, dreptul de procedură penală ar trebui să stipuleze dreptul autorităţilor însărcinate cu ancheta de a dispune unor persoane să prezinte orice date specifice aflate sub controlul lor, într-un sistem informaţional, în forma cerută de către aceste autorităţi.

10. Sub rezerva privilegiilor sau protecţiei prevăzute de lege, autorităţile însărcinate cu ancheta ar trebui să aibă dreptul de a dispune persoanelor care deţin, sub controlul lor, date specifice, de a furniza toate informaţiile necesare pentru a permite accesul la sistemul informaţional şi la datele pe care acesta le conţine. Legile de procedură penală ar trebui să asigure dreptul autorităţilor însărcinate cu ancheta de a da o dispoziţie similară altor persoane care cunosc funcţionarea sistemului informaţional sau orice altă măsură utilizată pentru a proteja datele pe care acesta le conţine.

11. Ar trebui să fie stabilite obligaţii specifice pentru operatorii de reţele publice şi private ca, atunci când oferă servicii de telecomunicaţii publicului, să aplice orice măsură tehnică necesară de natură să permită interceptarea telecomunicaţiilor de către autorităţile însărcinate cu ancheta.

12. Ar trebui să fie stabilite obligaţii specifice pentru furnizorii de servicii care oferă servicii de telecomunicaţii publicului prin intermediul reţelelor de telecomunicaţii publice sau private, pentru a elibera informaţia necesară, atunci

când autorităţile însărcinate cu ancheta dispun acest lucru, în scopul identificării utilizatorului.

IV. Proba electronică

13. Interesul comun de a aduna, de a proteja şi de a prezenta dovezi electronice într-o modalitate care să garanteze cât mai bine caracterul lor irefutabil şi integritatea lor, ar trebui să fie recunoscut atât pentru scopurile anchetelor naţionale cât şi pentru cele ale cooperării internaţionale. În acest scop, ar trebui să fie dezvoltate mai mult proceduri şi metode tehnice de prelucrare a dovezilor electronice astfel încât să se asigure compatibilitatea lor între state. Dispoziţiile dreptului de procedură penală cu privire la probe şi care se referă la documentele tradiţionale ar trebui să se aplice de asemenea la datele stocate într-un sistem informaţional.

V. Folosirea cifrărilor

14. Ar trebui să fie examinate măsuri cu scopul de a minimiza efectele negative ale utilizării cifrării asupra anchetelor privind infracţiunile penale, fără ca acestea să aibă însă consecinţe mai mult decât cele strict necesare asupra utilizării sale legale.

VI. Cercetare, statistici şi instruire

15. Riscul pe care îl implică dezvoltarea şi utilizarea tehnologiilor informaţionale în privinţa săvârşirii infracţiunilor penale ar trebui să facă obiectul unei evaluări permanente. Pentru a permite autorităţilor competente să se familiarizeze cu noile fenomene în materie de crimă informaţională şi pentru a putea dezvolta contramăsuri adecvate, ar trebui să fie favorizate colectarea şi analiza datelor referitoare la infracţiuni, inclusiv *modus operandi* şi aspectele tehnice.

16. Ar trebui să fie examinată crearea de unităţi specializate pentru reprimarea infracţiunilor a căror urmărire cere o experienţă specială în domeniul tehnologiilor informaţionale. Ar trebui să fie promovate programe de instruire care să permită personalului justiţiei penale aprofundarea cunoştinţelor în domeniu.

VII. Cooperare internaţională

17. Ar trebui să fie de asemenea aplicabil dreptul de a extinde percheziţia la alte sisteme informaţionale atunci când sistemul se află sub o jurisdicţie străină, cu condiţia ca o acţiune imediată să fie necesară. În scopul de a evita eventuale

violări ale suveranităţii Statelor sau ale dreptului internaţional, ar trebui creată o bază legală explicită pentru astfel de percheziţii sau sechestre extinse. În consecinţă, există o necesitate urgentă de negociere a unor instrumente internaţionale pentru a stabili cum, când şi în ce măsură astfel de percheziţii sau sechestre pot fi permise.

18. Ar trebui să fie disponibile proceduri accelerate şi corespunzătoare precum şi un sistem de legături care să permită autorităţilor însărcinate cu ancheta să ceară autorităţilor străine să colecteze cu promptitudine dovezi. În acest scop, autorităţile solicitate ar trebui să fie autorizate să percheziţioneze un sistem informaţional şi să sechestreze date în scopul transferării lor ulterioare. Autorităţile solicitate ar trebui de asemenea să fie autorizate să comunice datele de trafic care se referă la o telecomunicaţie specifică, să intercepteze o astfel de telecomunicaţie sau să-i identifice sursa. În acest scop instrumentele de asistenţă judiciară existente ar trebui să fie completate.

Anexa IV

Reguli de bază pentru obţinerea de probe digitale de către ofiţerii de poliţie

(Sursa: Australasian Centre for Policing Research)

- SIGURANŢA OFIŢERULUI ESTE PE PRIMUL PLAN!
- Caută orice cablu vizibil sau rupt. Dacă ai îndoieli referitoare la siguranţa în manipulare, întreabă un expert.
- Asigură-te că ai dreptul să percheziţionezi şi să ridici probe.
- **NU** folosi tastatura sau *mouse*-ul.
- **NU** încerca să examinezi conţinutul calculatorului, ai putea altera probele.
- Înregistrează toate acţiunile de ridicare a probelor.
- Dacă sistemul informatic este închis, **NU** îl deschide.
- Dacă sistemul informatic este deschis, fotografiază ecranul înainte de a merge mai departe.
- **NU** închide sistemul informatic după procedura normală. Scoate direct cablul de alimentare din calculator, nu din priză. Asigură-te că faci acest lucru în deplină siguranţă.
- **NU** ignora celelalte tipuri de probe, cum ar fi amprentele de pe echipamente.

Anexa V

Standarde în domeniul probelor digitale

(Sursa: Scientific Working Group on Digital Evidence)

Principiul 1

Pentru a se asigura că probele digitale sunt strânse, asigurate, examinate sau transferate de o manieră să asigure păstrarea acurateţei şi a încrederii în acestea, organizaţiile vor stabili şi respecta un sistem eficient de control al calităţii. Procedurile Operaţionale Standard (POS) vor constitui baza sistemului de control al calităţii ce trebuie să fie sprijinite de înregistrări corespunzătoare şi să facă apel la proceduri, echipamente şi materiale acceptate pe scară largă.

Standarde şi criterii 1.1.

Toate organizaţiile care realizează investigaţii asupra probelor digitale vor respecta un document de tip POS. Toate aspectele legate de politicile şi procedurile referitoare la probele digitale vor fi evidenţiate în mod clar în POS, document emis de conducerea organizaţiei.

Standarde şi criterii 1.2.

Conducerea organizaţiei va reevalua POS anual în scopul asigurării eficienţei acestora.

Standarde şi criterii 1.3.

Procedurile folosite trebuie să fie acceptate pe scară largă în domeniu sau sprijinite de date obţinute şi înregistrate corect din punct de vedere ştiinţific.

Standarde şi criterii 1.4.

Organizaţia va deţine copii scrise ale procedurilor tehnice.

Standarde şi criterii 1.5.

Organizaţia va folosi hardware şi programe informatice corespunzătoare şi eficiente pentru îndeplinirea procedurilor de investigare şi examinare.

Standarde şi criterii 1.6.

Toate acţiunile în legătură cu investigaţia, depozitarea, examinare sau transferul probelor digitale trebuie să fie înregistrate în scris şi să fie disponibile pentru evaluare şi pentru prezentare în instanţă.

Standarde şi criterii 1.7.

Orice acţiune care poate să altereze, producă pagube sau să distrugă orice aspect al probelor originale trebuie să fie realizată doar de persoane calificate, conform procedurilor investigaţiilor informatice.

Anexa VI

Principii în domeniul probelor digitale

(Sursa: International Organization on Computer Evidence)

1. În procesul de obţinere a probelor digitale, acţiunile întreprinse nu trebuie să modifice probele.
2. Atunci când este necesar ca o persoană să aibă acces la probele digitale originale, această persoană trebuie să fie competentă din punct de vedere criminalistic.
3. Toate activităţile în legătură cu investigaţia, depozitarea, examinare sau transferul probelor digitale trebuie să fie în întregime înregistrate în scris, păstrate şi să fie disponibile pentru evaluare.
4. O persoană este responsabilă pentru toate activităţile în legătură cu probele digitale atâta timp cât ele se află în posesia acesteia.
5. Orice organizaţie, responsabilă cu investigarea, accesarea, depozitarea sau transferarea probelor digitale este responsabilă de respectarea acestor principii.

Anexa VII

Proceduri model de examinare criminalistică a sistemelor informatice

(Sursa: International Association of Computer Investigation Specialists)

Examinarea hard-disk-ului

1. Sunt stabilite condiţii sterile din punct de vedere criminalistic. Toate mediile de stocare folosite în timpul procesului de examinare sunt pregătite recent, curăţite de date neesenţiale, verificate anti-virus şi testate înainte de utilizare;

2. Toate programele informatice folosite au licenţă şi pot fi folosite de instituţia respectivă;

3. Sistemul informatic original este examinat fizic. Se realizează o descriere a hardware-ului care este înregistrată. Se comentează orice element ieşit din comun întâlnit în timpul examinării fizice a sistemului informatic.

4. Sunt luate toate precauţiunile în timpul copierii sau accesului la mediile de stocare originale în scopul de a preveni transferul de viruşi, programe distructive sau orice alte conţinuturi inadvertente de pe/pe mediile de stocare originale. Se recunoaşte faptul că datorită limitărilor hardware şi ale sistemelor de operare acest lucru nu este tot timpul posibil;

5. Sunt verificate conţinutul CMOS şi ceasul intern, iar corectitudinea datei şi orei este înregistrată. Data şi ora ceasului intern este în mod frecvent importantă în stabilirea datei şi orei creării sau modificării unor fişiere.

6. În mod normal, mediile de stocare originale nu sunt folosite în investigare. O copie identică sau o imagine fidelă a mediului de stocare original va fi realizată. Această copie sau imagine va fi folosită pentru

examinarea propriu-zisă. Va fi înregistrată o descriere detaliată a procesului de creare a copiei sau imaginii.

7. Copia sau imaginea hard-disk-ului original va fi examinată şi o descriere a ceea ce s-a observat va fi înregistrată.

8. Datele de *boot*-are precum şi fişierele de comandă operaţionale şi de configurare a sistemului, definite de utilizator (cum ar fi CONFIG. SYS sau AUTOEXEC.BAT) sunt examinate şi o descriere a ceea ce s-a observat va fi înregistrată.

9. Toate fişierele şterse care mai pot fi recuperate vor fi salvate. Atunci când este util sau posibil, primul caracter al fişierelor recuperate va fi modificat din HEX E5 în „-„ sau în alt caracter unic, în scop de identificare.

10. Se realizează, în mod normal, o listare a tuturor fişierelor conţinute de mediul de stocare examinat, indiferent dacă acestea conţin sau nu potenţiale probe.

11. Dacă este cazul, spaţiul nealocat este examinat pentru identificarea de date ascunse sau pierdute.

12. Dacă este cazul, spaţiul inactiv corespunzător fiecărui fişier este examinat pentru identificarea de date ascunse sau pierdute.

13. Se examinează conţinutul fiecărui fişier de date din directoarele rădăcină şi fiecare sub-director (dacă este cazul).

14. Fişierele protejate cu parolă sunt deblocate şi examinate.

15. Se realizează o imprimare sau o copie a tot ceea ce aparent constituie probe. Fişierul sau locaţia de unde aceste posibile probe au fost obţinute este notat(ă) pe fiecare foaie imprimată. Toate probele sunt marcate, numerotate în ordine şi asigurate şi transmise în mod corespunzător.

16. Programele executabile de interes specific vor fi examinate. Fişierele de date ale utilizatorului care nu au putut fi accesate prin alte mijloace vor fi examinate folosind aplicaţia implicită.

17. Comentariile şi concluziile vor fi documentate în mod corespunzător.

Examinarea dischetelor

1. Sunt stabilite condiţii sterile din punct de vedere criminalistic. Toate mediile de stocare folosite în timpul procesului de examinare sunt pregătite recent, curăţite de date neesenţiale, verificate anti-virus şi testate înainte de utilizare;

2. Toate programele informatice folosite au licenţă şi pot fi folosite de instituţia respectivă;

3. Mediul de stocare original este examinat fizic. Se realizează o descriere a dischetei care este înregistrată. Se marchează discheta în scop de identificare.

4. Sunt luate toate precauţiunile în timpul copierii sau accesului la mediile de stocare originale în scopul de a preveni transferul de viruşi, programe distructive sau orice alte conţinuturi inadvertente de pe/pe discheta originală. Se recunoaşte faptul că datorită limitărilor hardware şi ale sistemelor de operare acest lucru nu este tot timpul posibil;

5. Este testată capacitatea de protejare la scriere a drive-ului de dischetă.

6. O copie a dischetei originale protejată la scriere este realizată pe altă dischetă. Această copie va fi folosită pentru examinarea propriu-zisă. Va fi înregistrată o descriere detaliată a procesului de creare a copiei.

7. Copia dischetei originale va fi examinată şi o descriere a ceea ce s-a găsit va fi înregistrată. Orice aspect ieşit din comun va fi notat.

8. Datele de *boot*-are precum şi fişierele de comandă operaţionale şi de configurare a sistemului, definite de utilizator (dacă sunt prezente) sunt examinate şi o descriere a ceea ce s-a observat va fi înregistrată.

9. Toate fişierele şterse care mai pot fi recuperate vor fi salvate. Atunci când este util sau posibil, primul caracter al fişierelor recuperate va fi modificat din HEX E5 în „-„ sau în alt caracter unic, în scop de identificare.

10. Spaţiul nealocat este examinat pentru date ascunse sau pierdute.

11. Spaţiul inactiv corespunzător fiecărui fişier este pentru date ascunse sau pierdute.

12. Se examinează conţinutul fiecărui fişier de date din directoarele rădăcină şi fiecare sub-director (dacă este cazul).

13. Fişierele protejate cu parolă sunt deblocate şi examinate.

14. Dacă discheta conţine aparent probe ce pot fi folosite, re realizează o listare a tuturor fişierelor conţinute pe dischetă, indiferent dacă acestea conţin sau nu potenţiale probe. Listarea va indica ce fişiere au fost imprimate, copiate sau în orice alt mod recuperate.

15. Se realizează o imprimare sau o copie a tot ceea ce aparent constituie probe. Fişierul sau locaţia de unde aceste posibile probe au fost obţinute este notat(ă) pe fiecare foaie imprimată. Toate probele sunt marcate, numerotate în ordine şi asigurate şi transmise în mod corespunzător.

16. Programele executabile de interes specific vor fi examinate. Fişierele de date ale utilizatorului care nu au putut fi accesate prin alte mijloace vor fi examinate folosind aplicaţia implicită.

17. Comentariile şi concluziile vor fi documentate în mod corespunzător.

Anexa VIII

Codul etic al IACIS

(Sursa: International Association of Computer Investigation Specialists)

1. Menţine cel mai ridicat nivel de obiectivitate în toate investigaţiile criminalistice şi prezintă în mod corect faptele;
2. Examinează şi analizează în cele mai mici detalii probele;
3. Realizează examinarea respectând principii consacrate şi validate de practică;
4. Emite opinii pe baze ce pot fi demonstrate în mod rezonabil;
5. Nu ascunde nici un fapt, încriminator sau de natură a înlătura răspunderea penală, care ar putea distorsiona elementele unei investigaţii;
6. Nu îţi prezenta în mod fals educaţia, experienţa şi calitatea de membru în organizaţii profesionale;
7. Ajută şi consiliază pe oricare investigator membru IACIS, indiferent de instituţia pentru care lucrează.