

INTERNEWS
RITI dot-Gov



MCTI

Bucure⁰ti,
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 și nu reprezintă în mod necesar vederile Agenției Statelor Unite pentru Dezvoltare Internațională.

© Internews Network, Inc., 2004. Acest ghid poate fi utilizat și copiat în scop ne-comercial atâta vreme cât "Internews Network, RITI dot-GOV" este creditat ca sursă și "USAID" menționat ca finanțator.

Anexa I

Legea nr. 161/2003

Titlul III Prevenirea și combaterea criminalității informatice

Capitolul I – Dispoziții generale

Art. 34 – Prezentul titlu reglementează prevenirea și combaterea criminalității informatice, prin măsuri specifice de prevenire, descoperire și sancționare a infracțiunilor săvârșite prin intermediul sistemelor informatice, asigurându-se respectarea drepturilor omului și protecția datelor personale.

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

- a) prin „sistem informatic” se înțelege orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relație funcțională, dintre care unul sau mai multe asigură prelucrarea automată a datelor, cu ajutorul unui program informatic;
- b) prin „prelucrare automată a datelor” se înțelege procesul prin care datele dintr-un sistem informatic sunt prelucrate prin intermediul unui program informatic;
- c) prin „program informatic” se înțelege un ansamblu de instrucțiuni care pot fi executate de un sistem informatic în vederea obținerii unui rezultat determinat;
- d) prin „date informatice” se înțelege orice reprezentare a unor fapte, informații sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic. În această categorie se include și orice program informatic care poate determina realizarea unei funcții de către un sistem informatic ;
- e) prin „furnizor de servicii” se înțelege:
 - 1. orice persoană fizică sau juridică ce oferă utilizatorilor posibilitatea de a comunica prin intermediul sistemelor informatice;

2. orice altă persoană fizică sau juridică ce prelucrează sau stochează date informatice pentru persoanele prevăzute la pct.1 și pentru utilizatorii serviciilor oferite de acestea;

- f) prin „date referitoare la traficul informațional” se înțelege orice date informatice referitoare la o comunicare realizată printr-un sistem informatic și produse de acesta, care reprezintă o parte din lanțul de comunicare, indicând originea, destinația, ruta, ora, data, mărimea, volumul și durata comunicării, precum și tipul serviciului utilizat pentru comunicare;
- g) prin “date referitoare la utilizatori” se înțelege orice informație care poate conduce la identificarea unui utilizator, incluzând tipul de comunicație și serviciul folosit, adresa poștală, adresa geografică, adresa de IP, numere de telefon sau alte numere de acces și modalitatea de plată a serviciului respectiv, precum și orice alte date care pot conduce la identificarea utilizatorului;
- h) prin „măsuri de securitate” se înțelege folosirea unor proceduri, dispozitive sau programe informatice specializate cu ajutorul cărora accesul la un sistem informatic este restricționat sau interzis pentru anumite categorii de utilizatori;
- i) prin „materiale pornografice cu minori” se înțelege orice material care prezintă un minor având un comportament sexual explicit sau o persoană majoră care este prezentată ca un minor având un comportament sexual explicit ori imagini care, deși nu prezintă o persoană reală, simulează, în mod credibil, un minor având un comportament sexual explicit.

(2) În sensul prezentului titlu, acționează fără drept persoana care se află în una din următoarele situații:

- d) nu este autorizată, în temeiul legii sau al unui contract;
- e) depășește 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 desfășura cercetări științifice sau de a efectua orice altă operațiune într-un sistem informatic.

Capitolul II – Prevenirea criminalității informatice

Art.36 – Pentru asigurarea securității sistemelor informatice și a protecției datelor personale, autoritățile și instituțiile publice cu competențe în domeniu, furnizorii de servicii, organizațiile neguvernamentale și alți reprezentanți ai societății civile desfășoară activități comune și programe de prevenire a criminalității informatice.

Art.37 – Autoritățile și instituțiile publice cu competențe în domeniu, în cooperare cu furnizorii de servicii, organizațiile neguvernamentale și alți reprezentanți ai societății civile promovează politici, practici, măsuri, proceduri și standarde minime de securitate a sistemelor informatice.

Art.38 – Autoritățile și instituțiile publice cu competențe în domeniu, în cooperare cu furnizorii de servicii, organizațiile neguvernamentale și alți reprezentanți ai societății civile organizează campanii de informare privind criminalitatea informatică și riscurile la care sunt expuși utilizatorii de sisteme informatice.

Art.39 – (1) Ministerul Justiției, Ministerul de Interne și Ministerul Comunicațiilor și Tehnologiei Informației constituie și actualizează continuu baze de date privind criminalitatea informatică.

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

Art.40 – Ministerul Justiției, Ministerul de Interne și Ministerul Comunicațiilor și Tehnologiei Informației desfășoară programe speciale de pregătire și perfecționare a personalului cu atribuții în prevenirea și combaterea criminalității informatice.

Art.41 – Proprietarii sau administratorii de sisteme informatice la care accesul este interzis sau restricționat pentru anumite categorii de utilizatori au obligația de a avertiza utilizatorii cu privire la condițiile legale de acces și utilizare, precum și cu privire la consecințele juridice ale accesului fără drept la aceste sisteme informatice.

Capitolul III – Infrațiuni și contravenții

Secțiunea 1

Infrațiuni contra confidențialității și integrității datelor și sistemelor informatice

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

(2) Dacă fapta prevăzută în alin.(1) este săvârșită 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 și care este destinată unui sistem informatic, provine dintr-un asemenea sistem sau se efectuează în cadrul unui sistem informatic constituie infracțiune și se pedepsește cu închisoare de la 2 la 7 ani.

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

Art.44 – (1) Fapta de a modifica, șterge sau deteriora date informatice ori de a restricționa accesul la aceste date, fără drept, constituie infracțiune și se pedepsește cu închisoare de la 2 la 7 ani.

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

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

Art.45 – Fapta de a perturba grav, fără drept, funcționarea unui sistem informatic, prin introducerea, transmiterea, modificarea, ștergerea sau deteriorarea datelor informatice sau prin restricționarea accesului la aceste date constituie infracțiune și se pedepsește cu închisoarea de la 3 la 15 ani.

Art.46 – (1) Constituie infracțiune și se pedepsește cu închisoare de la unu la 6 ani:

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

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

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

(2) Cu aceeași pedeapsă se sancționează și deținerea, fără drept, a unui dispozitiv, program informatic, parolă, cod de acces sau dată informatică dintre cele prevăzute în alin.(1) în scopul săvârșirii uneia din infracțiunile prevăzute în art.42-45.

Art.47 – Tentativa infracțiunilor prevăzute în art.42-46 se pedepsește.

Secțiunea 2

Infracțiuni informatice

Art.48. – Fapta de a introduce, modifica sau șterge, fără drept, date informatice ori de a restricționa, fără drept, accesul la aceste date, rezultând date necorespunzătoare adevărului, în scopul de a fi utilizate în vederea producerii unei consecințe juridice, constituie infracțiune și se pedepsește cu închisoare de la 2 la 7 ani.

Art.49 – Fapta de a cauza un prejudiciu patrimonial unei persoane prin introducerea, modificarea sau ștergerea de date informatice, prin restricționarea accesului la aceste date ori prin împiedicarea în orice mod a funcționării unui sistem informatic, în scopul de a obține un beneficiu material pentru sine sau pentru altul, constituie infracțiune și se pedepsește cu închisoare de la 3 la 12 ani.

Art.50 – Tentativa infracțiunilor prevăzute în art.48 și 49 se pedepsește.

Secțiunea 3

Pornografia infantilă prin sisteme informatice

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

(2) Tentativa se pedepsește.

Secțiunea 4

Contravenții

Art.52 – Nerespectarea obligației prevăzute în art.41 constituie contravenție și se sancționează cu amendă de la 5.000.000 lei la 50.000.000 lei.

Art.53 – (1) Constatarea contravenției prevăzute în art.52 și aplicarea sancțiunii se fac de către personalul împuternicit în acest scop de către ministrul comunicațiilor și tehnologiei informației, precum și de către personalul special abilitat din cadrul Ministerului de Interne.

(2) Dispozițiile Ordonanței Guvernului nr.2/2001 privind regimul juridic al contravențiilor, aprobată cu modificări prin Legea nr.180/2002 sunt aplicabile.

Capitolul IV – Dispoziții procedurale

Art.54 – (1) În cazuri urgente și temeinic justificate, dacă există date sau indicii temeinice cu privire la pregătirea sau săvârșirea unei infracțiuni prin intermediul sistemelor informatice, în scopul strângerii de probe sau al identificării făptuitorilor, se poate dispune conservarea imediată a datelor informatice ori a datelor referitoare la traficul informațional, față de care există pericolul distrugerii ori alterării.

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

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

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

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

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

Art.55 – (1) În termenul prevăzut la art.54 alin.(3) procurorul, pe baza autorizației motivate a procurorului anume desemnat de procurorul general al parchetului de pe lângă curtea de apel sau, după caz, de procurorul general al Parchetului de pe lângă Curtea Supremă de Justiție, ori instanța de judecată dispune cu privire la ridicarea obiectelor care conțin date informatice, date referitoare la traficul informațional sau date referitoare la utilizatori, de la persoana sau furnizorul de servicii care le deține, în vederea efectuării de copii, care pot servi ca mijloc de probă.

(2) Dacă obiectele care conțin datele informatice sau datele referitoare la traficul informațional nu sunt puse de bunăvoie la dispoziția organelor judiciare pentru efectuarea de copii, procurorul prevăzut în alin.(1) sau instanța de judecată dispune ridicarea silită. În cursul judecării, dispoziția 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 și proceduri adecvate de natură să asigure integritatea informațiilor conținute de acestea.

Art.56 – (1) Ori de câte ori pentru descoperirea și 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 percheziții.

(2) Dacă organul de urmărire penală sau instanța de judecată apreciază că ridicarea obiectelor care conțin datele prevăzute în alin.(1) ar afecta grav desfășurarea activității persoanelor care dețin aceste obiecte, poate dispune efectuarea de copii, care pot servi ca mijloc de probă și 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 și sunt accesibile din sistemul sau suportul inițial, se poate dispune, de îndată, autorizarea efectuării percheziției în vederea cercetării tuturor sistemelor informatice sau suporturilor de stocare a datelor informatice căutate.

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

Art.57 – (1) Accesul într-un sistem informatic, precum și interceptarea și înregistrarea comunicărilor desfășurate prin intermediul sistemelor informatice se efectuează când sunt utile pentru aflarea adevărului, iar stabilirea situației de fapt sau identificarea făptuitorilor nu poate fi realizată în baza altor probe.

(2) Măsurile prevăzute 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 Justiție ori de procurorul general al Parchetului Național Anticorupție, de către organele de cercetare penală, cu sprijinul unor persoane specializate, care sunt obligate să păstreze secretul operațiunii efectuate.

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

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

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

Art.58 - Dispozițiile prezentului capitol se aplică în urmărirea penală sau judecarea cauzelor privind infracțiunile prevăzute în prezentul titlu și a oricăror alte infracțiuni săvârșite prin intermediul sistemelor informatice.

Art.59 - În cazul infracțiunilor prevăzute în prezentul titlu și a oricăror alte infracțiuni săvârșite prin intermediul sistemelor informatice, pentru a garanta aducerea la îndeplinire a confiscării speciale prevăzute în art.118 din Codul penal se pot lua măsurile asigurătorii prevăzute de Codul de procedură penală.

Capitolul V – Cooperare internațională

Art.60 – (1) Autoritățile judiciare române cooperează în mod direct, în condițiile legii și cu respectarea obligațiilor decurgând din instrumentele juridice internaționale la care România este parte, cu instituțiile având atribuții similare din alte state, precum și cu organizațiile internaționale specializate în domeniu.

(2) Cooperarea, care se organizează și se desfășoară potrivit alin. (1) poate avea ca

obiect, după caz, asistența judiciară internațională în materie penală, extrădarea, identificarea, blocarea, sechestrarea și confiscarea produselor și instrumentelor infracțiunii, desfășurarea anchetelor comune, schimbul de informații, asistența tehnică sau de altă natură pentru culegerea și analiza informațiilor, formarea personalului de specialitate, precum și alte asemenea activități.

Art.61 – (1) La solicitarea autorităților competente române sau ale altor state, pe teritoriul României se pot desfășura anchete comune, în vederea prevenirii și combaterii criminalității informatice.

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

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

Art.62 – (1) Pentru asigurarea cooperării internaționale imediate și permanente în domeniul combaterii criminalității informatice, se înființează, în cadrul Secției de Combatere a Criminalității Organizate și Antidrog din Parchetul de pe lângă Curtea Supremă de Justiție, Serviciul de combatere a criminalității informatice, ca punct de contact disponibil permanent.

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

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

Art.63 – (1) În cadrul cooperării internaționale, autoritățile străine competente pot solicita Serviciului de combatere a criminalității informatice conservarea imediată a datelor informatice ori a datelor referitoare la traficul informațional, existente într-un sistem informatic de pe teritoriul României, cu privire la care autoritatea străină urmează să formuleze o cerere de asistență judiciară internațională în materie penală.

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

- a) autoritatea care solicită conservarea;

- b) o scurtă prezentare a faptelor care fac obiectul urmăririi penale și încadrarea juridică a acestora;
- c) datele informatice care se solicită a fi conservate;
- d) orice informație disponibilă, necesară pentru identificarea deținătorului de date informatice și a localizării sistemului informatic;
- e) utilitatea datelor informatice și necesitatea conservării lor;
- f) intenția autorității străine de a formula o cerere de asistență judiciară internațională în materie penală.

(3) Cererea de conservare se execută potrivit art.54 pentru o perioadă care nu poate fi mai mică de 60 de zile și este valabilă până la luarea unei decizii de către autoritățile române competente cu privire la cererea de asistență judiciară internațională 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 informațional, Serviciul de combatere a criminalității informatice va informa de îndată despre aceasta autoritatea străină solicitantă, comunicând totodată informațiile necesare identificării respectivului furnizor de servicii.

Art.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 autoritățile 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 dispoziție prin intermediul aceluși sistem informatic, fără a fi necesară formularea unei solicitări în acest sens către autoritățile române.

Art.66 – Autoritățile române competente pot transmite, din oficiu, autorităților străine competente, cu respectarea prevederilor legale privind protecția datelor cu caracter personal, informațiile și datele deținute, necesare pentru descoperirea infracțiunilor săvârșite prin intermediul sistemelor informatice sau pentru soluționarea, de către autoritățile străine competente, a cauzelor referitoare la aceste infracțiuni.

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

Anexa II

Consiliul Europei

Convenție privind criminalitatea informatică

Seria Tratatelor Europene nr. 185

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

Budapesta, 23 noiembrie 2001

PREAMBUL

Statele membre ale Consiliului Europei și celelalte state semnatare ale prezentei convenții,

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

recunoscând importanța promovării cooperării cu celelalte state părți la prezenta convenție,

convinse de necesitatea de a urmări, cu prioritate, aplicarea unei politici penale comune, destinată să protejeze societatea împotriva criminalității informatice, în special prin adoptarea unei legislații adecvate, precum și prin îmbunătățirea cooperării internaționale,

conștiente de profunde schimbări determinate de digitalizarea, convergența și globalizarea continuă a rețelelor de calculatoare,

preocupate de riscul că rețelele de calculatoare și informația electronică ar putea fi utilizate și pentru comiterea de infracțiuni și că probele privind asemenea infracțiuni ar putea fi stocate și transmise prin intermediul acestor rețele,

recunoscând necesitatea cooperării între state și industria privată în lupta împotriva criminalității informatice, precum și nevoia de a proteja interesele legitime în utilizarea și dezvoltarea tehnologiilor informației,

considerând că lupta eficientă purtată împotriva criminalității informatice impune o cooperare internațională intensificată, rapidă și eficace în materie penală,

convinse că prezenta convenție este necesară pentru a preveni actele îndreptate împotriva confidențialității, integrității și disponibilității sistemelor informatice, a rețelelor și a datelor, precum și a utilizării frauduloase a unor asemenea sisteme, rețele și date, prin asigurarea incriminării unor asemenea conduite, așa cum sunt ele descrise în prezenta convenție, și prin adoptarea unor măsuri suficiente pentru a permite combaterea eficace a acestor infracțiuni, menite să faciliteze descoperirea, investigarea și urmărirea penală a acestora atât la nivel național, cât și internațional, precum și prin prevederea unor dispoziții materiale necesare asigurării unei cooperări internaționale rapide și sigure,

conștiente de necesitatea garantării unui echilibru adecvat între interesele acțiunii represive și respectarea drepturilor fundamentale ale omului, consacrate prin Convenția Consiliului Europei pentru apărarea drepturilor omului și a libertăților fundamentale (1950), Pactul internațional privind drepturile civile și politice al Națiunilor Unite (1966), precum și prin alte tratate internaționale aplicabile în materia drepturilor omului, care reafirmă dreptul fiecăruia la opinie, libertatea de expresie, precum și libertatea de a căuta, de a obține și de a comunica informații și idei de orice natură, fără a ține seama de frontiere, precum și drepturile privind respectarea intimității și a vieții private,

conștiente, de asemenea, de dreptul la protecția datelor personale, conferit, de exemplu, prin Convenția Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (1981),

luând în considerare Convenția Națiunilor Unite privind drepturile copilului (1989) și Convenția Organizației Internaționale a Muncii privind interzicerea celor mai grave forme ale muncii copiilor (1999),

ținând seama de convențiile în vigoare ale Consiliului Europei privind cooperarea în materie penală, precum și de celelalte tratate similare încheiate între statele membre ale Consiliului Europei și alte state și subliniind că prezenta convenție are ca scop completarea acestora, în vederea creșterii eficienței anchetelor și procedurilor penale având ca obiect infracțiunile în legătură cu sistemele și datele informatice, precum și de a permite colectarea probelor electronice ale unei infracțiuni,

salutând recentele inițiative destinate să îmbunătățească înțelegerea și cooperarea internațională în scopul combaterii criminalității în spațiul informatic, în special acțiunile întreprinse de Națiunile Unite, Organizația pentru Cooperare și Dezvoltare Economică, Uniunea Europeană și de Grupul celor 8,

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

drepturilor de autor și al drepturilor conexe, nr. R (87) 15 vizând reglementarea utilizării datelor cu caracter personal în sectorul poliției, nr. R(95)4 privind protecția datelor cu caracter personal în domeniul serviciilor de telecomunicații, cu referire specială la serviciile de telefonie și nr. R (89) 9 referitoare la criminalitatea în legătură cu utilizarea calculatorului, care indică structurilor legiuitoare naționale principiile directoare pentru definirea anumitor infracțiuni, precum și nr. R (95) 13 privind problemele de procedură penală în legătură cu tehnologia informației,

ținând seama de Rezoluția nr. 1, adoptată de miniștrii europeni de justiție cu ocazia celei de-a XXI-a conferințe a lor (Praga, 10-11 iunie 1997), care recomandă Comitetului Miniștrilor să sprijine activitățile privind combaterea criminalității informatice, desfășurate de Comitetul European pentru problemele criminalității, în scopul de a asigura apropierea între legislațiile penale naționale și de a permite utilizarea unor mijloace eficiente de investigare a infracțiunilor informatice, precum și de Rezoluția nr. 3, adoptată la cea de-a XXIII-a Conferință a miniștrilor europeni de justiție (Londra, 8-9 iunie 2000), care încurajează părțile participante la negocieri să își continue eforturile pentru găsirea unor soluții care să permită unui număr cât mai mare de state să devină parte la convenție și recunoaște necesitatea de a dispune de un mecanism rapid și eficient de cooperare internațională care să țină seama de exigențele specifice luptei împotriva criminalității informatice,

ținând seama, de asemenea, de planul de acțiune adoptat de șefii de stat și 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 și valorile Consiliului Europei, la dezvoltarea noilor tehnologii ale informației,

au convenit următoarele:

CAPITOLUL I - Terminologie

ARTICOLUL 1 - Definiții

În sensul prezentei convenții:

- 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, informații sau concepte sub o formă adecvată prelucrării într-un sistem

- informatic, inclusiv un program capabil să determine executarea unei funcții de către un sistem informatic;
- 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;
 - și
 - (ii) orice altă entitate care prelucrează sau stochează date informatice pentru acest serviciu de comunicații 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 lanțului de comunicare, indicând originea, destinația, itinerarul, ora, data, mărimea, durata sau tipul de serviciu subiacent.

CAPITOLUL II - Măsuri care trebuie luate la nivel național

SECȚIUNEA 1 - Drept penal material

TITLUL 1 - Infrațiuni împotriva confidențialității, integrității și disponibilității datelor și sistemelor informatice

ARTICOLUL 2 - Accesarea ilegală

Fiecare parte va adopta măsurile legislative și alte măsuri considerate necesare pentru a incrimina ca infracțiune, potrivit dreptului său intern, accesarea intenționată și fără drept a ansamblului ori a unei părți a unui sistem informatic. O parte poate condiționa o astfel de incriminare de comiterea încălcării respective prin violarea măsurilor de securitate, cu intenția de a obține date informatice ori cu altă intenție delictuală, sau de legătura dintre încălcarea respectivă și un sistem informatic conectat la alt sistem informatic.

ARTICOLUL 3 - Interceptarea ilegală

Fiecare parte va adopta măsurile legislative și alte măsuri considerate necesare pentru a incrimina ca infracțiune, potrivit dreptului său intern, interceptarea intenționată și 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 condiționa o astfel de

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

ARTICOLUL 4 - Afectarea integrității datelor

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

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

ARTICOLUL 5 - Afectarea integrității sistemului

Fiecare parte va adopta măsurile legislative și alte măsuri care sunt necesare pentru a incrimina ca infracțiune, în conformitate cu dreptul intern, afectarea gravă, intenționată și fără drept a funcționării unui sistem informatic, prin introducerea, transmiterea, periclitarea, ștergerea, deteriorarea, alterarea sau suprimarea datelor informatice.

ARTICOLUL 6 - Abuzurile asupra dispozitivelor

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

- a) producerea, vânzarea, obținerea pentru utilizare, importarea, difuzarea sau alte forme de punere la dispoziție:
 - (i) a unui dispozitiv, inclusiv un program informatic, conceput special sau adaptat pentru a permite comiterea uneia dintre infracțiunile 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 intenția ca acestea să fie utilizate în vederea comiterii uneia dintre infracțiunile vizate la art. 2-5; și
- b) posesia unui element vizat la subparagrafele a) (i) sau a) (ii) susmenționate, cu intenția de a fi utilizat în vederea comiterii uneia dintre infracțiunile vizate la art. 2-5. O parte va putea solicita, în conformitate cu dreptul intern, ca un anumit număr dintre aceste elemente să fie deținute pentru a fi atrasă răspunderea penală.

2. Prezentul articol nu va fi interpretat în sensul impunerii unei răspunderi penale atunci când producerea, vânzarea, obținerea pentru utilizare, importarea, difuzarea sau alte forme de punere la dispoziție, menționate la paragraful 1 din prezentul articol, nu au ca scop comiterea unei infracțiuni stabilite în conformitate cu art. 2-5, cum ar fi situația testării sau protecției autorizate a unui sistem informatic.

3. Fiecare parte își va putea rezerva dreptul de a nu aplica paragraful 1 al prezentului articol, cu condiția ca această rezervă să nu privească vânzarea, distribuția sau orice altă formă de punere la dispoziție a elementelor menționate la paragraful 1 subparagraful a) (ii) din prezentul articol.

TITLUL 2 - Infracțiuni informatice

ARTICOLUL 7 - Falsificarea informatică

Fiecare parte va adopta măsurile legislative și alte măsuri care se dovedesc necesare pentru a incrimina ca infracțiune, potrivit dreptului său intern, introducerea, alterarea, ștergerea sau suprimarea intenționată și fără drept a datelor informatice, din care să rezulte date neautentice, cu intenția ca acestea să fie luate în considerare sau utilizate în scopuri legale ca și cum ar fi autentice, chiar dacă sunt sau nu sunt în mod direct lizibile și inteligibile. O parte va putea condiționa răspunderea penală de existența unei intenții frauduloase sau a unei alte intenții delictuale.

ARTICOLUL 8 - Frauda informatică

Fiecare parte va adopta măsurile legislative și alte măsuri care se dovedesc necesare pentru a incrimina ca infracțiune, potrivit dreptului său intern, fapta intenționată și fără drept de a cauza un prejudiciu patrimonial unei alte persoane:

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

cu intenția frauduloasă sau delictuală de a obține fără drept un beneficiu economic pentru el însuși sau pentru altă persoană.

TITLUL 3 - Infrațiuni referitoare la conținut

ARTICOLUL 9 - Infrațiuni referitoare la pornografia infantilă

1. Fiecare parte va adopta măsurile legislative și alte măsuri care se dovedesc necesare pentru a incrimina ca infrațiune, potrivit dreptului său intern, următoarele comportamente, atunci când acestea sunt comise în mod intenționat și 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 dispoziție 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-și 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-menționat, 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-menționat, termenul minor desemnează orice persoană în vârstă de mai puțin de 18 ani. Totuși o parte poate solicita o limită de vârstă inferioară, care trebuie să fie de cel puțin 16 ani.

4. O parte își va putea rezerva dreptul de a nu aplica, în totalitate sau parțial, paragraful 1 subparagrafele d) și e) și paragraful 2 subparagrafele b) și c).

TITLUL 4 - Infrațiuni referitoare la atingerile aduse proprietății intelectuale și drepturilor conexe

ARTICOLUL 10 - Infrațiuni referitoare la atingerile aduse proprietății intelectuale și drepturilor conexe

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

atingerile aduse proprietății intelectuale, definite de legislația acestei părți, în conformitate cu obligațiile pe care le-a subscris în aplicarea Actului de la Paris din 24 iulie 1971 care revizuieste Convenția de la Berna pentru protecția operelor literare și artistice, a Acordului privind aspectele comerciale ale drepturilor de proprietate intelectuală și a Tratatului OMPI privind proprietatea intelectuală, cu excepția oricărui drept moral conferit de aceste convenții, atunci când astfel de acte sunt comise deliberat, la scară comercială și prin intermediul unui sistem informatic.

2. Fiecare parte va adopta măsurile legislative și alte măsuri care se dovedesc necesare pentru a incrimina ca infracțiune, potrivit dreptului său intern, atingerile aduse drepturilor conexe definite de legislația acestei părți în conformitate cu obligațiile pe care le-a subscris în aplicarea Convenției internaționale pentru protecția artiștilor interpreți sau executanți, a producătorilor de fonograme și a organismelor de radiodifuziune (Convenția de la Roma), a Acordului privind aspecte comerciale ale drepturilor de proprietate intelectuală și a Tratatului OMPI privind interpretările și fonogramele, cu excepția oricărui drept moral conferit de aceste convenții, atunci când astfel de acte sunt comise deliberat, la scară comercială și prin intermediul unui sistem informatic.

3. O parte va putea, în circumstanțe bine delimitate, să își rezerve dreptul de a nu impune răspunderea penală în baza paragrafelor 1 și 2 ale prezentului articol, cu condiția ca alte recursuri eficiente să fie disponibile și cu condiția ca o astfel de rezervă să nu aducă atingere obligațiilor internaționale care incumbă acestei părți în aplicarea instrumentelor internaționale menționate la paragrafele 1 și 2 ale prezentului articol.

TITLUL 5 - Alte forme de răspundere și de sancționare

ARTICOLUL 11 - Tentativa și complicitatea

1. Fiecare parte va adopta măsurile legislative și alte măsuri care se dovedesc necesare pentru a incrimina ca infracțiune, potrivit dreptului său intern, orice complicitate intenționată la comiterea uneia dintre infracțiunile stabilite în aplicarea art. 2-10, săvârșite cu intenție.

2. Fiecare parte va adopta măsurile legislative și alte măsuri care se dovedesc necesare pentru a incrimina ca infracțiune, potrivit dreptului său intern, orice tentativă săvârșită cu intenția comiterii uneia dintre infracțiunile stabilite în aplicarea art. 3-5, art. 7, 8 și a art. 9 paragraful 1 subparagrafele a) și c).

3. Fiecare parte își va putea rezerva dreptul de a nu aplica, în totalitate sau parțial, paragraful 2 al prezentului articol.

ARTICOLUL 12 - Răspunderea persoanelor juridice

1. Fiecare parte va adopta măsurile legislative și alte măsuri care se dovedesc necesare pentru ca persoanele juridice să poată fi trase la răspundere pentru infracțiunile stabilite în aplicarea prezentei convenții, atunci când acestea sunt comise pe cont propriu de către orice persoană fizică care acționează fie individual, fie în calitate de membru al unui organ al persoanei juridice, care exercită o funcție 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 excepția 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 absența supravegherii sau a controlului din partea persoanei fizice menționate la paragraful 1 a permis comiterea infracțiunilor stabilite în aplicarea prezentei convenții pentru numita persoană juridică de către o persoană fizică care acționează sub autoritatea acesteia.

3. În funcție de principiile juridice ale părții, 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 infracțiunea.

ARTICOLUL 13 - Sancțiuni și măsuri

1. Fiecare parte va adopta măsurile legislative și alte măsuri care se dovedesc necesare pentru ca infracțiunilor stabilite în aplicarea art. 2-11 să li se poată aplica sancțiuni efective, proporționale și 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 sancțiunilor sau măsurilor penale ori nepenale efective, proporționale și convingătoare, care cuprind sancțiuni pecuniare.

SECȚIUNEA a 2-a - Drept procedural

TITLUL 1 - Dispoziții comune

ARTICOLUL 14 - Aria de aplicare a măsurilor procedurale

1. Fiecare parte va adopta măsurile legislative și alte măsuri care se dovedesc necesare pentru a stabili prerogativele și procedurile prevăzute în prezenta secțiune, în scopul desfășurării anchetelor sau procedurilor penale specifice.

2. Cu excepția dispoziției contrare care figurează la art. 21, fiecare parte va aplica prerogativele și procedurile menționate la paragraful 1 al prezentului articol:

- a) infracțiunilor stabilite în conformitate cu art. 2-11;
- b) tuturor celorlalte infracțiuni comise prin intermediul unui sistem informatic; și
- c) strângerii dovezilor electronice referitoare la orice infracțiune.

3. a) Fiecare parte își va putea rezerva dreptul de a nu aplica măsurile menționate la art. 20 decât infracțiunilor sau categoriilor de infracțiuni specificate în rezervă, astfel încât sfera acestor infracțiuni sau categorii de infracțiuni să nu fie mai redusă decât cea a infracțiunilor cărora aceasta le aplică măsurile menționate 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 menționate la art. 20.

b) În cazul în care o parte, din cauza restricțiilor impuse de legislația sa în vigoare la momentul adoptării prezentei convenții, nu va fi în măsură să aplice măsurile vizate la art. 20 și 21 comunicațiilor transmise într-un sistem informatic al unui furnizor de servicii:

- (i) care este folosit în beneficiul unui grup închis de utilizatori; și
- (ii) care nu utilizează rețelele publice de telecomunicații și care nu este conectat la un alt sistem informatic, public sau privat,

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

ARTICOLUL 15 - Condiții și măsuri de protecție

1. Fiecare parte va veghea ca stabilirea, realizarea și aplicarea prerogativelor și a procedurilor prevăzute în prezenta secțiune să fie supuse condițiilor și măsurilor de protecție prevăzute în dreptul său intern, care trebuie să asigure o protecție adecvată a drepturilor și a libertăților omului, în special a drepturilor stabilite în conformitate cu obligațiile pe care aceasta le-a subscris în aplicarea Convenției Consiliului Europei pentru apărarea drepturilor omului și a libertăților fundamentale (1950), a Pactului internațional privind drepturile civile și politice al Națiunilor Unite (1966), precum și a altor instrumente internaționale aplicabile privind drepturile omului, și care trebuie să integreze principiul proporționalității.

2. Ținând cont de natura procedurii sau a prerogativelor acordate, aceste condiții și măsuri de protecție vor include, între altele, atunci când situația o impune, o supervizare judiciară sau alte forme de supervizare independentă a motivelor care justifică aplicarea, precum și limitarea ariei de aplicare și 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 justiției, fiecare parte va examina efectul prerogativelor și al procedurilor în această secțiune privind drepturile, responsabilitățile și interesele legitime ale terților.

TITLUL 2 - Conservarea rapidă a datelor informatice stocate

ARTICOLUL 16 - Conservarea rapidă a datelor informatice stocate

1. Fiecare parte va adopta măsurile legislative și alte măsuri care se dovedesc necesare pentru a permite autorităților sale competente să ordone sau să impună într-un alt mod conservarea rapidă a datelor informatice menționate, 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 menționate care se găsesc în posesia sau sub controlul său, această parte va adopta măsurile legislative, precum și măsurile care se dovedesc necesare pentru a obliga această persoană să păstreze și să protejeze integritatea datelor pentru atât timp cât este necesar, cel mult 90 de zile, în scopul de a permite autorităților competente să obțină dezvăluirea acestora. O parte poate prevedea ca ordinul să fie ulterior reînnoit.

3. Fiecare parte va adopta măsurile legislative și alte măsuri care se dovedesc necesare pentru a obliga persoana care veghează asupra datelor sau o altă persoană însărcinată să le păstreze să păstreze confidențialitatea cu privire la aplicarea numitelor proceduri pe durata prevăzută în dreptul său intern.

4. Prerogativelor și procedurilor menționate în prezentul articol li se aplică prevederile art. 14 și 15.

ARTICOLUL 17 - Conservarea și dezvăluirea parțială 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 și măsurile care se dovedesc necesare:

- a) pentru a veghea ca păstrarea rapidă a datelor referitoare la trafic să fie posibilă, indiferent dacă în transmiterea comunicației au fost implicați unul sau mai mulți furnizori de servicii; și
 - b) pentru a asigura dezvoltarea rapidă către autoritatea competentă a părții sau către o persoană desemnată de această autoritate a unei cantități de date referitoare la trafic, suficientă pentru a permite părții identificarea furnizorilor de servicii și a canalului prin intermediul căruia comunicația a fost transmisă.
2. Prerogativelor și procedurilor menționate în prezentul articol li se aplică prevederile art. 14 și 15.

TITLUL 3 - Ordinul de punere la dispoziție a datelor

ARTICOLUL 18 - Ordinul de punere la dispoziție a datelor

1. Fiecare parte va adopta măsurile legislative și alte măsuri care se dovedesc necesare pentru a conferi autorităților sale competente dreptul de a ordona:
 - a) unei persoane prezente pe teritoriul său să comunice datele informatice menționate, aflate în posesia sau sub controlul său, care sunt stocate într-un sistem informatic ori pe un suport de stocare informatic; și
 - b) unui furnizor de servicii care oferă prestații pe teritoriul părții să comunice datele din posesia sau de sub controlul său referitoare la abonați și la astfel de servicii.
2. Prerogativelor și procedurilor menționate în prezentul articol li se aplică prevederile art. 14 și 15.
3. În sensul prezentului articol, expresia date referitoare la abonați va desemna orice informație, sub formă de date informatice sau sub orice altă formă, deținută de un furnizor de servicii, referitoare la abonații acestor servicii, altele decât datele referitoare la trafic sau conținut, și care permit stabilirea:
 - a) tipului de serviciu de comunicații utilizat, dispozițiilor tehnice luate în această privință și perioadei serviciului;
 - b) identității, adresei poștale sau geografice, numărului de telefon al abonatului și oricărui alt număr de contact, precum și a datelor referitoare la facturare și plată, disponibile în baza unui contract sau a unui aranjament de servicii;
 - c) oricărei alte informații referitoare la locul în care se găsesc echipamentele de comunicație, disponibile în baza unui contract sau a unui aranjament de servicii.

TITLUL 4 - Percheziția și sechestrarea datelor informatice stocate

ARTICOLUL 19 - Percheziția și sechestrarea datelor informatice stocate

1. Fiecare parte va adopta măsurile legislative și alte măsuri care se dovedesc necesare pentru a conferi autorităților sale competente dreptul de a percheziționa sau de a accesa într-un mod similar:

- a) un sistem informatic sau o parte a acestuia, precum și datele informatice care sunt stocate în acesta; și
- b) un suport de stocare informatic care permite stocarea datelor informatice pe teritoriul său.

2. În cazul în care autoritățile părții vor percheziționa sau vor accesa într-un mod similar un sistem informatic specific ori o parte din acesta, în conformitate cu paragraful 1 subparagraful a), și 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 și că aceste date sunt în mod legal accesibile de la sistemul inițial ori sunt disponibile pentru acest sistem inițial, fiecare parte va adopta măsurile legislative și alte măsuri care se dovedesc necesare pentru ca numitele autorități să fie în măsură de a extinde rapid percheziția sau accesarea într-un mod similar a celui alt sistem.

3. Fiecare parte va adopta măsurile legislative și alte măsuri care se dovedesc necesare pentru a conferi autorităților sale competente dreptul de a sechestra sau de a obține 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 obținerea într-un mod similar a unui sistem informatic ori a unei părți din acesta sau a unui suport de stocare informatic;
- b) realizarea și conservarea unei copii a acestor date informatice;
- c) menținerea integrității datelor informatice relevante stocate;
- d) suprimarea accesării sau îndepărtarea acestor date informatice din sistemul informatic accesat.

4. Fiecare parte va adopta măsurile legislative și alte măsuri care se dovedesc necesare pentru a conferi autorităților sale competente dreptul de a ordona oricărei persoane care cunoaște funcționarea sistemului informatic sau măsurile aplicate pentru protecția datelor informatice să pună la dispoziție toate informațiile considerate necesare pentru a permite aplicarea măsurilor vizate la paragrafele 1 și 2.

5. Prerogativelor și procedurilor menționate în prezentul articol li se aplică prevederile art. 14 și 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 și alte măsuri care se dovedesc necesare pentru a conferi autorităților sale competente următoarele drepturi:

a) de a culege sau de a înregistra prin aplicarea mijloacelor tehnice care există pe teritoriul său; și

b) de a obliga un furnizor de servicii, în limita capacităților sale tehnice existente, la:

(i) strângerea sau înregistrarea prin aplicarea mijloacelor tehnice care există pe teritoriul său;

sau la

(ii) acordarea concursului și asistenței sale autorităților competente, pentru culegerea sau înregistrarea,

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

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

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

4. Prerogativelor și procedurilor menționate în prezentul articol li se aplică prevederile art. 14 și 15.

ARTICOLUL 21 - Interceptarea datelor referitoare la conținut

1. Fiecare parte va adopta măsurile legislative și alte măsuri care se dovedesc necesare pentru a conferi autorităților sale competente, cu privire la o serie de infracțiuni grave care să fie definite în legislația internă, următoarele drepturi:

a) de a culege sau de a înregistra prin aplicarea mijloacelor tehnice care există pe teritoriul său; și

b) de a obliga un furnizor de servicii, în limita capacităților sale tehnice, la:

(i) strângerea sau înregistrarea prin aplicarea mijloacelor tehnice care există pe teritoriul său;

sau la

(ii) acordarea sprijinului și asistenței sale autorităților competente, pentru colectarea sau înregistrarea,

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

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

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

4. Prerogativelor și procedurilor menționate în prezentul articol li se aplică prevederile art. 14 și 15.

SECȚIUNEA a 3-a - Competența

ARTICOLUL 22 - Competența

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

a) pe teritoriul său; sau

b) la bordul unui vas sub pavilionul acestei părți; sau

c) la bordul unei aeronave înmatriculate în conformitate cu legislația acestei părți; sau

d) de către unul dintre cetățenii săi, dacă infracțiunea poate atrage răspunderea penală în locul în care aceasta a fost comisă sau dacă infracțiunea nu este de competența teritorială a nici unui stat.

2. Fiecare parte își va putea rezerva dreptul de a nu aplica sau de a aplica doar în cazuri ori în condiții specifice regulile de competență 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 competența sa cu privire la orice infracțiune menționată la art. 24 paragraful 1, în cazul în care autorul prezumat al infracțiunii este prezent pe teritoriul său și nu

poate fi extrădat spre o altă parte decât în baza naționalității sale, în urma unei cereri de extrădare.

4. Prezenta convenție nu va exclude nici o competență penală exercitată de o parte în conformitate cu dreptul său intern.

5. În cazul în care mai multe părți își revendică jurisdicția cu privire la o infracțiune stabilită în conformitate cu prezenta convenție, părțile 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 internațională

SECȚIUNEA 1 - Principii generale

TITLUL 1 - Principii generale referitoare la cooperarea internațională

ARTICOLUL 23 - Principii generale referitoare la cooperarea internațională

Părțile vor coopera între ele, în conformitate cu dispozițiile prezentului capitol și în aplicarea instrumentelor internaționale relevante cu privire la cooperarea internațională în materie penală, a acordurilor încheiate pe baza legislațiilor uniforme sau reciproce și a dreptului lor intern, în cea mai largă măsură posibilă, în scopul investigărilor sau al aplicării procedurilor privind infracțiunile în legătură cu sisteme și date informatice sau pentru a culege dovezile unei infracțiuni în format electronic.

TITLUL 2 - Principii referitoare la extrădare

ARTICOLUL 24 - Extrădarea

1. a) Prezentul articol se va aplica extrădării între părți pentru infracțiunile stabilite în conformitate cu art. 2-11, cu condiția ca acestea să poată fi sancționate, potrivit legislațiilor ambelor părți implicate, printr-o pedeapsă privativă de libertate, al cărei maxim special este de cel puțin 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 părți, inclusiv Convenția europeană de extrădare (STE nr. 24), sau a unui acord care are la bază legislații uniforme sau reciproce, se va aplica pedeapsa minimă prevăzută prin acest tratat ori aranjament.

2. Infracțiunile descrise la paragraful 1 vor fi considerate incluse în categoria infracțiunilor care pot atrage extrădarea în orice tratat de extrădare care există

între părți. Părțile se vor angaja să includă astfel de infracțiuni ca infracțiuni care pot atrage extrădarea în orice tratat de extrădare care va fi încheiat între părți.

3. Dacă o parte care condiționează extrădarea de existența unui tratat primește o cerere de extrădare de la altă parte cu care nu a încheiat un tratat de extrădare, aceasta va putea considera prezenta convenție drept bază juridică pentru extrădarea cu privire la orice infracțiune menționată la paragraful 1 al prezentului articol.

4. Părțile care nu condiționează extrădarea de existența unui tratat vor recunoaște infracțiunile menționate la paragraful 1 al prezentului articol ca infracțiuni care pot atrage extrădarea între acestea.

5. Extrădarea va fi supusă condițiilor prevăzute de dreptul intern al părții solicitate sau de tratatele de extrădare în vigoare, inclusiv în ceea ce privește motivele pentru care partea solicitată poate refuza extrădarea.

6. Dacă extrădarea pentru o infracțiune menționată la paragraful 1 al prezentului articol va fi refuzată doar pe motivul cetățeniei persoanei sau pentru că partea solicitată consideră că este competentă cu privire la această infracțiune, partea solicitată va supune cauza, la cererea părții solicitante, autorităților sale competente, în scopul urmăririi, și va raporta în timp util, la încheierea cauzei, părții solicitante. Autoritățile în cauză vor decide și vor desfășura ancheta și procedura în același mod ca pentru orice altă infracțiune de natură comparabilă, în conformitate cu legislația acestei părți.

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 și adresa fiecărei autorități responsabile de trimiterea ori de primirea unei cereri de extrădare sau de arestare provizorie, în absența unui tratat.

b) Secretarul general al Consiliului Europei va realiza și va actualiza un registru al autorităților astfel desemnate de către părți. 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 asistența mutuală

ARTICOLUL 25 - Principii generale referitoare la asistența mutuală

1. Părțile își vor acorda asistență mutuală într-o măsură cât mai largă posibil, în scopul investigărilor sau al aplicării procedurilor privind infracțiunile în legătură cu sisteme și date informatice sau pentru a culege dovezile unei infracțiuni în format electronic.

2. De asemenea, fiecare parte va adopta măsurile legislative, precum și măsurile care se dovedesc necesare pentru a-și îndeplini obligațiile stabilite în cuprinsul art. 27-35.

3. În caz de urgență fiecare parte va putea formula o cerere de asistență mutuală sau comunicările care se raportează acesteia prin mijloace rapide de comunicare, precum faxul sau poșta electronică, cu condiția ca aceste mijloace să ofere condiții suficiente de securitate și 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 și va răspunde prin oricare dintre mijloacele sale rapide de comunicare.

4. Cu excepția unei dispoziții contrare expres prevăzute în prezentul capitol, asistența mutuală va fi supusă condițiilor fixate de dreptul intern al părții solicitate sau de tratatele de asistență mutuală aplicabile, inclusiv în ceea ce privește motivele pe baza cărora partea solicitată poate refuza cooperarea. Partea solicitată nu își va exercita dreptul de a refuza asistența mutuală privind infracțiunile vizate la art. 2-11 doar din motivul că cererea vizează o infracțiune pe care aceasta o consideră de natură fiscală.

5. În cazul în care, în conformitate cu dispozițiile prezentului capitol, părții solicitate îi este permis să condiționeze asistența mutuală de existența dublei incriminări, această condiție va fi considerată îndeplinită dacă fapta care constituie infracțiunea pentru care asistența mutuală este solicitată este calificată drept infracțiune de dreptul său intern, indiferent dacă dreptul intern include sau nu infracțiunea în cadrul aceleiași categorii de infracțiuni ori dacă o definește sau nu prin aceeași terminologie ca dreptul părții solicitante.

ARTICOLUL 26 - Informarea spontană

1. O parte va putea, în limitele dreptului său intern și în absența unei cereri prealabile, să comunice unei alte părți informații obținute 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 infracțiuni stabilite în conformitate cu prezenta convenție sau în cazul în care aceste informații ar putea conduce la o cerere de cooperare formulată de această parte în virtutea prezentului capitol.

2. Înainte de a comunica astfel de informații, partea care le furnizează va putea solicita ca acestea să rămână confidențiale sau să nu fie utilizate decât în anumite condiții. Dacă partea destinatară nu va putea îndeplini această cerință, va informa cealaltă parte, care va stabili în acest caz dacă informațiile în cauză ar trebui totuși furnizate. Dacă partea destinatară va accepta informațiile cu condițiile prescrise, partea destinatară va fi legată de acestea din urmă.

TITLUL 4 - Procedurile referitoare la cererile de asistență mutuală în absența acordurilor internaționale aplicabile

ARTICOLUL 27 - Procedurile referitoare la cererile de asistență mutuală în absența acordurilor internaționale aplicabile

1. În absența unui tratat de asistență mutuală ori a unui acord care are la bază legislații uniforme sau reciproce în vigoare între partea solicitantă și partea solicitată, se vor aplica dispozițiile paragrafelor 2-9 din prezentul articol. Acestea nu se vor aplica atunci când există un tratat, un acord sau o legislație de acest tip, în afară de cazul în care părțile 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 autorități centrale însărcinate să trimită cererile de asistență mutuală sau să răspundă, să le execute ori să le transmită autorităților competente pentru executarea lor.
- b) Autoritățile 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 și adresele autorităților desemnate în aplicarea prezentului paragraf.
- d) Secretarul general al Consiliului Europei va stabili și va actualiza un registru al autorităților centrale desemnate de către părți. Fiecare parte va veghea în permanență asupra exactitudinii datelor care figurează în registru.

3. Cererile de asistență mutuală adresate în baza prezentului articol vor fi executate în conformitate cu procedura menționată de partea solicitantă, cu excepția cazului în care aceasta este incompatibilă cu legislația părții solicitate.

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

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

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

6. Înainte de a refuza sau de a suspenda cooperarea, partea solicitată va examina, ulterior consultării părții solicitante, dacă poate da curs parțial cererii ori cu rezerva condițiilor pe care le consideră necesare.

7. Partea solicitată va informa rapid partea solicitantă asupra răspunsului pe care intenționează să îl dea cererii de asistență 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 asistență mutuală sau care ar fi susceptibil de a o întârzia în mod semnificativ.

8. Partea solicitantă va putea cere ca partea solicitată să păstreze confidențialitatea faptului că a fost formulată o cerere în baza prezentului capitol, precum și a obiectului acesteia, cu excepția măsurilor necesare executării cererii în cauză. Dacă partea solicitată nu va putea da curs acestei cereri de confidențialitate, aceasta va trebui să informeze rapid partea solicitantă, care va trebui în acest caz să determine dacă cererea trebuie totuși executată.

9.

- a) În caz de urgență, cererile de asistență mutuală sau comunicările care se raportează acestora vor putea fi transmise direct de către autoritățile judiciare ale părții solicitante autorităților similare ale părții solicitate. Într-un asemenea caz, o copie va fi adresată simultan autorităților centrale ale părții solicitate prin intermediul autorității centrale a părții solicitante.
- b) Orice cerere sau comunicare formulată în baza prezentului paragraf va putea fi avansată prin intermediul Organizației Internaționale de Poliție Criminală (Interpol).
- c) În cazul în care o cerere a fost formulată în aplicarea subparagrafului a) al prezentului paragraf și în cazul în care autoritatea nu va fi competentă pentru a o analiza, aceasta o va transmite autorității naționale competente și 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 autoritățile competente ale părții solicitante la autoritățile competente ale părții 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 eficiență, cererile formulate în baza acestui paragraf vor trebui adresate autorităților sale centrale.

ARTICOLUL 28 - Confidențialitatea și restricția de utilizare

1. În absența unui tratat de asistență mutuală sau a unui aranjament care să aibă la bază legislații uniforme ori reciproce în vigoare între partea solicitantă și partea solicitată, se vor aplica dispozițiile prezentului articol. Acestea nu se vor aplica în cazul în care există un tratat, un aranjament sau o legislație de acest tip, cu excepția cazului în care părțile implicate decid să aplice în locul acestora totul sau o parte din acest articol.

2. Partea solicitată va putea condiționa comunicarea de informații sau de materiale, reprezentând răspunsul la cerere, de:

- a) păstrarea confidențialității acestora, în cazul în care cererea de asistență mutuală nu ar putea fi respectată în absența acestei condiții; sau
- b) neutilizarea acestora pentru alte anchete sau proceduri decât cele indicate în cerere.

3. Dacă partea solicitantă nu va putea îndeplini una dintre condițiile enunțate la paragraful 2, aceasta va informa rapid partea solicitată, care va determina în acest caz dacă informația trebuie totuși furnizată. Dacă partea solicitantă va accepta această condiție, aceasta va fi legată de condiția menționată.

4. Orice parte care va furniza informații sau materiale ce se supun uneia dintre condițiile enunțate la paragraful 2 va putea solicita celeilalte părți să-i ofere explicații în legătură cu această condiție privind utilizarea acestor informații sau a acestui material.

SECȚIUNEA a 2-a - Dispoziții speciale

TITLUL 1 - Asistența mutuală în materie de măsuri provizorii

ARTICOLUL 29 - Conservarea rapidă a datelor informatice stocate

1. O parte va putea solicita unei alte părți să ordone sau să impună printr-un alt mijloc conservarea rapidă a datelor stocate prin intermediul unui sistem informatic care se găsește pe teritoriul acestei alte părți și la adresa cărora partea solicitantă are intenția de a formula o cerere de asistență mutuală în vederea percheziției ori accesării printr-un mijloc similar, sechestrului sau obținerii 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) infracțiunea care va face obiectul anchetei sau procedurilor penale, precum și o scurtă expunere a faptelor care au legătură cu aceasta;

- c) datele informatice stocate care vor trebui conservate și natura legăturii lor cu infracțiunea;
- d) toate informațiile disponibile care vor permite identificarea posesorului datelor informatice stocate sau locația sistemului informatic;
- e) necesitatea măsurii conservării; și
- f) faptul că partea are intenția de a formula o cerere de asistență mutuală în vederea percheziției ori accesării printr-un mijloc similar, sechestrului sau obținerii printr-un mijloc similar, ori divulgării datelor informatice în cauză.

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

4. O parte care va solicita dubla incriminare ca o condiție pentru a răspunde unei cereri de asistență mutuală în vederea percheziției ori accesării printr-un mijloc similar, sechestrului sau obținerii printr-un mijloc similar ori divulgării datelor stocate, va putea, pentru alte infracțiuni decât cele stabilite în conformitate cu art. 2-11 să-și 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, condiția 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 infracțiune pe care partea solicitată o consideră ca fiind de natură politică ori legată de o infracțiune politică; sau
- b) partea solicitată consideră că faptul de a da curs cererii ar risca de a aduce atingere suveranității sale, securității, ordinii publice sau altor interese esențiale.

6. În cazul în care partea solicitată va considera că simpla conservare nu va fi suficientă pentru garantarea disponibilității viitoare a datelor, va compromite confidențialitatea anchetei părții 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 totuși executată.

7. Orice conservare efectuată ca răspuns la o cerere menționată la paragraful 1 va fi valabilă pentru o perioadă de cel puțin 60 de zile, în scopul de a permite părții solicitante de a formula o cerere în vederea percheziției ori accesării printr-un mijloc similar, sechestrului sau obținerii printr-un mijloc similar ori divulgării datelor. După primirea unei astfel de cereri, datele vor trebui în continuare conservate în așteptarea 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 părții solicitante o cantitate suficientă de date referitoare la trafic, pentru identificarea acestui furnizor de servicii și 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 infracțiune pe care partea solicitată o consideră de natură politică ori legată de o infracțiune de natură politică; sau
- b) partea solicitată consideră că faptul de a da curs cererii ar risca să aducă atingere suveranității sale, securității, ordinii publice sau altor interese esențiale.

TITLUL 2 - Asistența mutuală privind prerogativele de investigare

ARTICOLUL 31 - Asistența mutuală privind accesarea datelor stocate

1. O parte va putea solicita unei alte părți să percheziționeze sau să acceseze într-un mod similar, să sechestreze sau să obțină într-un mod similar, să dezvăluie date stocate prin intermediul unui sistem informatic care se găsește pe teritoriul acestei alte părți, inclusiv date conservate în conformitate cu art. 29.

2. Partea solicitată va răspunde cererii cu aplicarea instrumentelor internaționale, a aranjamentelor și a legislațiilor menționate la art. 23 și conformându-se dispozițiilor 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 și legislațiile vizate la paragraful 2 prevăd o cooperare rapidă.

ARTICOLUL 32 - Accesarea transfrontalieră a datelor stocate, cu consimțământ sau în cazul în care acestea sunt accesibile publicului

O parte va putea, fără autorizația unei alte părți:

- 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 obține consimțământul persoanei legal autorizate să-i dezvăluie aceste date prin intermediul acestui sistem informatic.

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

1. Părțile își vor acorda asistență mutuală pentru strângerea în timp real a datelor referitoare la trafic, asociate comunicărilor menționate pe teritoriul acestora, transmise prin intermediul unui sistem informatic. Cu rezerva dispozițiilor paragrafului 2, asistența mutuală este guvernată de condițiile și procedurile prevăzute în dreptul intern.

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

ARTICOLUL 34 - Asistența mutuală în domeniul interceptării datelor referitoare la conținut

Părțile își vor acorda asistență mutuală, în măsura permisă de tratatele și legislația internă aplicabile, pentru strângerea sau înregistrarea în timp real a datelor referitoare la conținutul comunicațiilor specifice, transmise prin intermediul unui sistem informatic.

TITLUL 3 - Rețeaua 24/7

ARTICOLUL 35 - Rețeaua 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 asistențe imediate pentru investigațiile referitoare la infracțiunile privind sisteme sau date informatice, sau pentru a strânge dovezile unei infracțiuni în format electronic. Această asistență va cuprinde facilitarea sau, dacă dreptul și practica internă o permit, aplicarea directă a următoarelor măsuri:

- a) asistența tehnică;
- b) conservarea datelor, în conformitate cu art. 29 și 30;
- c) strângerea dovezilor, furnizarea de informații cu caracter juridic și localizarea suspectilor.

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

b) Dacă punctul de contact desemnat de către o parte nu va depinde de autoritatea sau de autoritățile acestei părți responsabile de asistența mutuală

internațională sau de extrădare, punctul de contact va veghea să poată acționa în coordonare cu această sau aceste autorități, potrivit unei proceduri accelerate.

3. Fiecare parte va întreprinde măsurile necesare pentru a dispune de un personal specializat și echipat corespunzător pentru facilitarea funcționării rețelei.

CAPITOLUL IV - Clauze finale

ARTICOLUL 36 - Semnarea și intrarea în vigoare

1. Prezenta convenție va fi deschisă spre semnare statelor membre ale Consiliului Europei și statelor membre care au participat la elaborarea sa.

2. Prezenta convenție 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 convenție 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 puțin 3 state membre ale Consiliului Europei, își vor fi exprimat consimțământul de a fi legate prin convenție, în conformitate cu dispozițiile paragrafelor 1 și 2.

4. Pentru oricare stat semnatar care își va exprima ulterior consimțământul de a fi legat prin prezenta convenție, aceasta va intra în vigoare în prima zi a lunii care urmează expirării unei perioade de 3 luni după data exprimării consimțământului său de a fi legat prin prezenta convenție, în conformitate cu dispozițiile paragrafelor 1 și 2.

ARTICOLUL 37 - Aderarea la convenție

1. După intrarea în vigoare a prezentei convenții, Comitetul de Miniștri al Consiliului Europei, după consultarea statelor contractante la convenție și după obținerea asentimentului unanim, vor putea invita orice stat nemembru al Consiliului Europei, care nu a participat la elaborarea sa, să adere la prezenta convenție. Decizia va fi luată cu majoritatea prevăzută la art. 20 d) din Statutul Consiliului Europei și cu unanimitatea reprezentanților statelor contractante care au dreptul să facă parte din Comitetul de Miniștri.

2. Pentru orice stat care a aderat la prezenta convenție, în conformitate cu paragraful 1 sus-menționat, convenția 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 convenție.
2. În orice moment următor, prin declarație adresată secretarului general al Consiliului Europei, oricare stat va putea lărgi aplicarea prezentei la convenții la oricare alt teritoriu desemnat în declarație. Convenția 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 declarației de către secretarul general.
3. Orice declarație formulată cu aplicarea celor două paragrafe precedente va putea fi retrasă, cu privire la orice teritoriu desemnat în această declarație, 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 menționate de către Secretarul general.

ARTICOLUL 39 - Efectele convenției

1. Scopul prezentei convenții este de a completa tratatele sau acordurile multilaterale ori bilaterale aplicabile, existente între părți, inclusiv dispozițiile:
 - Convenției europene de extrădare, deschisă spre semnare la 13 decembrie 1957 la Paris (STE nr. 24);
 - Convenției europene de asistență judiciară în materie penală, deschisă spre semnare la 20 aprilie 1959 la Strasbourg (STE nr. 30);
 - Protocolului adițional la Convenția europeană de asistență judiciară în materie penală, deschis spre semnare la 17 martie 1978 la Strasbourg (STE nr. 99).
2. Dacă două sau mai multe părți au încheiat deja un acord ori un tratat referitor la domeniile cuprinse în prezenta convenție sau dacă și-au stabilit în alt mod relațiile privind aceste subiecte ori dacă o vor face în viitor, acestea vor avea, de asemenea, dreptul de a aplica acordul sau tratatul menționat ori de a-și stabili relațiile în consecință, în locul prezentei convenții. Totuși, în cazul în care părțile își vor stabili relațiile privind domeniile care fac obiectul prezentei convenții într-un mod diferit decât cel prevăzut, acestea o vor face într-un mod care să nu fie incompatibil cu obiectivele și principiile convenției.
3. Nici o prevedere a prezentei convenții nu va afecta alte drepturi, restricții, obligații și responsabilități ale unei părți.

ARTICOLUL 40 - Declarații

Prin declarație 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 folosește 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 și art. 27 paragraful 9 subparagraful e).

ARTICOLUL 41 - Clauza federală

1. Un stat federal își va putea rezerva dreptul de a onora obligațiile cuprinse în cap. II în măsura în care acestea vor fi compatibile cu principiile fundamentale care guvernează relațiile dintre guvernul său central și statele constitutive sau alte entități teritoriale analoage, cu condiția 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 substanțial obligațiile sale în baza cap. II. În orice caz, acesta va folosi mijloace largite și efective care vor permite aplicarea măsurilor prevăzute în capitolul menționat.
3. În ceea ce privește dispozițiile acestei convenții, a căror aplicare ține de competența legislativă a fiecărui stat constitutiv sau a altor entități teritoriale analoage care, în baza sistemului constituțional al federației, nu sunt obligate să ia măsuri legislative, guvernul federal va aduce la cunoștință autorităților competente ale statelor constitutive dispozițiile menționate, 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 folosește 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 și la art. 41 paragraful 1. Nici o altă rezervă nu va putea fi formulată.

ARTICOLUL 43 - Statutul și 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 menționate. Dacă notificarea va indica faptul că retragerea unei rezerve trebuie să intre în vigoare la o dată precisă și 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 menționate 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 părților care au formulat una sau mai multe rezerve dintre cele menționate la art. 42 informații cu privire la aspectele retragerii lor.

ARTICOLUL 44 - Amendamente

1. La prezenta convenție 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 convenții, precum și oricărui stat care a aderat sau care a fost invitat să adere, în conformitate cu dispozițiile 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 Miniștri cu privire la amendamentul menționat.

3. Comitetul de Miniștri va examina amendamentul propus și avizul prezentat de către CDPC și, după consultarea statelor nemembre care sunt părți la prezenta convenție, va putea adopta amendamentul.

4. Textul oricărui amendament adoptat de către Comitetul de Miniștri în conformitate cu paragraful 3 al prezentului articol va fi comunicat părților 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 părțile 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 și aplicarea prezentei convenții.

2. În cazul dezacordului între părți cu privire la interpretarea și aplicarea prezentei convenții, părțile se vor strădui să ajungă la o rezolvare a acestuia prin negociere sau prin orice alt mijloc pașnic pe care îl vor alege, inclusiv prin prezentarea dezacordului CDPC, unui tribunal arbitrar care va lua decizii ce vor lega părțile sau Curții Internaționale de Justiție, potrivit unui acord între părțile implicate.

ARTICOLUL 46 - Reuniunea părților

1. Părțile se vor reuni periodic, dacă va fi nevoie, în vederea facilitării:

- a) utilizării și aplicării efective a prezentei convenții, inclusiv identificării oricărei probleme în domeniu, precum și efectelor oricărei declarații sau rezerve făcute în conformitate cu prezenta convenție;
 - b) schimbului de informații cu privire la noutățile juridice, politice sau tehnice importante în domeniul criminalității informatice și strângerii dovezilor în formă electronică;
 - c) examinării eventualității de a completa sau de a amenda convenția.
2. CDPC va fi ținut periodic la curent cu privire la rezultatul reuniunilor internaționale menționate la paragraful 1.
3. CDPC va facilita, dacă va fi nevoie, întâlnirile menționate la paragraful 1 și va adopta măsurile necesare pentru a ajuta părțile în efortul lor care vizează completarea sau amendarea convenției. La expirarea unui termen de 3 ani începând de la data intrării în vigoare a prezentei convenții, cel mai târziu, CDPC va proceda, în cooperare cu părțile, la reexaminarea tuturor dispozițiilor convenției și va propune, dacă este cazul, amendamentele potrivite.
4. Cu excepția cazului în care Consiliul European le va suporta, cheltuielile ocazionate de aplicarea dispozițiilor paragrafului 1 vor fi suportate de către părți în maniera pe care acestea o vor alege.
5. Părțile vor fi asistate în exercitarea funcțiilor care decurg din prezentul articol de către Secretariatul Consiliului European.

ARTICOLUL 47 - Denunțarea

1. Orice parte va putea, în orice moment, să denunțe prezenta convenție printr-o notificare adresată secretarului general al Consiliului European.
2. Denunțarea 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 European va notifica statelor membre ale Consiliului European, statelor nemembre care au participat la elaborarea prezentei convenții, precum și 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 convenții, în conformitate cu art. 36 și 37;
- d) orice declarație 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 convenție.

În acest sens, subsemnații, autorizați pe deplin în acest scop, au semnat prezenta convenție.

Adoptată la Budapesta la 23 noiembrie 2001, în limbile franceză și 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 convenției, precum și oricărui stat invitat să adere o copie certificată conformă cu originalul.

Anexa III

Rec(1995)013

CONSILIUL EUROPEI

COMITETUL DE MINIȘTRI

Recomandarea nr. R (95) 13

a Comitetului de Miniștri către statele membre cu privire la problemele de procedură penală legate de tehnologiile informaționale

(adoptată de Comitetul de Miniștri la 11 septembrie 1995, în cadrul celei de-a 543-a reuniuni a Delegaților Miniștrilor)

Comitetul de Miniștri, 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 informaționale și aplicarea lor în toate sectoarele societății contemporane;

Realizând că dezvoltarea sistemelor electronice de informare va accelera transformarea societății tradiționale într-o societate a informației și va crea un nou spațiu pentru orice tip de comunicare și de relații;

Conștient de impactul tehnologiilor informaționale asupra modului în care este organizată societatea și asupra felului în care indivizii comunică și interacționează;

Conștient de faptul că o parte tot mai mare a relațiilor economice și sociale va avea loc prin intermediul sau cu ajutorul sistemelor informaționale electronice;

Preocupat de riscul ca sistemele electronice informaționale și informația electronică să poată fi de asemenea utilizate pentru comiterea de infracțiuni criminale;

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

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

Amintind faptul că, în fața dezvoltării tehnologiilor informaționale, lipsa unor puteri speciale corespunzătoare poate aduce atingere bunei executări, de către autoritățile însărcinate cu ancheta, a funcțiilor proprii;

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

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

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

Amintind Recomandarea nr. R (81) 20 cu privire la armonizarea legislațiilor în materie de exigență a dovezilor scrise și în materie de admisibilitate a reproducerilor de documente și a înregistrărilor informatice, Recomandarea nr. R (85) 10 cu privire la comisiile rogatorii pentru supravegherea telecomunicațiilor, Recomandarea nr. (87) 15 cu privire la reglementarea utilizării datelor cu caracter personal în domeniul poliției și 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 își revizuiesc legislația și practicile lor interne; și
- ii. de a aduce aceste dispoziții la cunoștința autorităților însărcinate cu ancheta și a altor servicii profesionale, în special a celor din sectorul tehnologiilor informaționale, 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 informaționale

I. Percheziție și sechestrul

1. Distincția făcută prin lege între percheziția sistemelor informaționale precum și sechestrarea datelor pe care le conțin, pe de o parte, și interceptarea datelor în timpul transmisiunii, pe de altă parte, ar trebui să fie clar stabilită și aplicată.

2. Legile de procedură penală ar trebui să permită autorităților însărcinate cu ancheta să facă percheziții în sistemele informaționale și să sechestreze datele găsite, în condiții similare celor utilizate în cadrul drepturilor tradiționale de percheziție și sechestrul. Persoana care are responsabilitatea sistemului ar trebui să fie informată despre faptul că sistemul a făcut obiectul unei percheziții și despre natura datelor sechestrate. Recursurile juridice prevăzute de legislație în general împotriva percheziției și a sechestrului ar trebui să fie aplicabile în egală măsură în cazul percheziției unui sistem informațional și în cel al sechestrării datelor pe care acesta le conține.

3. În timpul executării percheziției, autoritățile însărcinate cu ancheta ar trebui să aibă dreptul, sub rezerva garanțiilor corespunzătoare, de a extinde percheziția asupra altor sisteme informaționale din jurisdicția lor care sunt conectate prin intermediul unei rețele și de a sechestra datele conținute în ele, cu condiția ca o acțiune imediată să fie necesară.

4. În cazul în care există o echivalență funcțională între datele care constituie obiectul prelucrării automatizate și un document tradițional, dispozițiile dreptului de procedură penală referitoare la documente ar trebui să se aplice, de asemenea, la date.

II. Supraveghere tehnică

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

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

7. Atunci când sunt colectate în cursul unei anchete penale și în special când sunt obținute prin mijloace de interceptare a telecomunicațiilor, datele protejate prin lege și prelucrate de un sistem informațional ar trebui să fie protejate în mod corespunzător.

8. Legile de procedură penală ar trebui să fie revizuite pentru a permite interceptarea telecomunicațiilor și colectarea datelor de trafic în cadrul anchetelor privind infracțiuni grave împotriva confidențialității, integrității și disponibilității sistemelor de telecomunicații sau informatice.

III. Obligații de cooperare cu autoritățile însărcinate cu ancheta

9. Sub rezerva privilegiilor sau protecției prevăzute de lege, majoritatea legislațiilor permit autorităților însărcinate cu ancheta să dispună unor persoane predarea obiectelor care se află sub controlul lor și care sunt necesare în calitate de probe. În același mod, dreptul de procedură penală ar trebui să stipuleze dreptul autorităților însărcinate cu ancheta de a dispune unor persoane să prezinte orice date specifice aflate sub controlul lor, într-un sistem informațional, în forma cerută de către aceste autorități.

10. Sub rezerva privilegiilor sau protecției prevăzute de lege, autoritățile însărcinate cu ancheta ar trebui să aibă dreptul de a dispune persoanelor care dețin, sub controlul lor, date specifice, de a furniza toate informațiile necesare pentru a permite accesul la sistemul informațional și la datele pe care acesta le conține. Legile de procedură penală ar trebui să asigure dreptul autorităților însărcinate cu ancheta de a da o dispoziție similară altor persoane care cunosc funcționarea sistemului informațional sau orice altă măsură utilizată pentru a proteja datele pe care acesta le conține.

11. Ar trebui să fie stabilite obligații specifice pentru operatorii de rețele publice și private ca, atunci când oferă servicii de telecomunicații publicului, să aplice orice măsură tehnică necesară de natură să permită interceptarea telecomunicațiilor de către autoritățile însărcinate cu ancheta.

12. Ar trebui să fie stabilite obligații specifice pentru furnizorii de servicii care oferă servicii de telecomunicații publicului prin intermediul rețelilor de telecomunicații publice sau private, pentru a elibera informația necesară, atunci

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

IV. Proba electronică

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

V. Folosirea cifrărilor

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

VI. Cercetare, statistici și instruire

15. Riscul pe care îl implică dezvoltarea și utilizarea tehnologiilor informaționale în privința săvârșirii infracțiunilor penale ar trebui să facă obiectul unei evaluări permanente. Pentru a permite autorităților competente să se familiarizeze cu noile fenomene în materie de crimă informațională și pentru a putea dezvolta contramăsuri adecvate, ar trebui să fie favorizate colectarea și analiza datelor referitoare la infracțiuni, inclusiv *modus operandi* și aspectele tehnice.

16. Ar trebui să fie examinată crearea de unități specializate pentru reprimarea infracțiunilor a căror urmărire cere o experiență specială în domeniul tehnologiilor informaționale. Ar trebui să fie promovate programe de instruire care să permită personalului justiției penale aprofundarea cunoștințelor în domeniu.

VII. Cooperare internațională

17. Ar trebui să fie de asemenea aplicabil dreptul de a extinde percheziția la alte sisteme informaționale atunci când sistemul se află sub o jurisdicție străină, cu condiția ca o acțiune imediată să fie necesară. În scopul de a evita eventuale

violări ale suveranității Statelor sau ale dreptului internațional, ar trebui creată o bază legală explicită pentru astfel de percheziții sau sechestre extinse. În consecință, există o necesitate urgentă de negociere a unor instrumente internaționale pentru a stabili cum, când și în ce măsură astfel de percheziții sau sechestre pot fi permise.

18. Ar trebui să fie disponibile proceduri accelerate și corespunzătoare precum și un sistem de legături care să permită autorităților însărcinate cu ancheta să ceară autorităților străine să colecteze cu promptitudine dovezi. În acest scop, autoritățile solicitate ar trebui să fie autorizate să percheziționeze un sistem informațional și să sechestreze date în scopul transferării lor ulterioare. Autoritățile solicitate ar trebui de asemenea să fie autorizate să comunice datele de trafic care se referă la o telecomunicație specifică, să intercepteze o astfel de telecomunicație sau să-i identifice sursa. În acest scop instrumentele de asistență judiciară existente ar trebui să fie completate.

Anexa IV

Reguli de bază pentru obținerea de probe digitale de către ofițerii de poliție

(Sursa: Australasian Centre for Policing Research)

- **SIGURANȚA OFIȚERULUI ESTE PE PRIMUL PLAN!**
- Caută orice cablu vizibil sau rupt. Dacă ai îndoieli referitoare la siguranța în manipulare, întreabă un expert.
- Asigură-te că ai dreptul să percheziționezi și să ridici probe.
- **NU** folosi tastatura sau *mouse*-ul.
- **NU** încerca să examinezi conținutul calculatorului, ai putea altera probele.
- Înregistrează toate acțiunile 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 siguranță.
- **NU** ignora celelalte tipuri de probe, cum ar fi amprente 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 acurateții și a încrederii în acestea, organizațiile vor stabili și respecta un sistem eficient de control al calității. Procedurile Operaționale Standard (POS) vor constitui baza sistemului de control al calității ce trebuie să fie sprijinite de înregistrări corespunzătoare și să facă apel la proceduri, echipamente și materiale acceptate pe scară largă.

Standarde și criterii 1.1.

Toate organizațiile care realizează investigații asupra probelor digitale vor respecta un document de tip POS. Toate aspectele legate de politicile și procedurile referitoare la probele digitale vor fi evidențiate în mod clar în POS, document emis de conducerea organizației.

Standarde și criterii 1.2.

Conducerea organizației va reevalua POS anual în scopul asigurării eficienței acestora.

Standarde și criterii 1.3.

Procedurile folosite trebuie să fie acceptate pe scară largă în domeniu sau sprijinite de date obținute și înregistrate corect din punct de vedere științific.

Standarde și criterii 1.4.

Organizația va deține copii scrise ale procedurilor tehnice.

Standarde și criterii 1.5.

Organizația va folosi hardware și programe informatice corespunzătoare și eficiente pentru îndeplinirea procedurilor de investigare și examinare.

Standarde și criterii 1.6.

Toate acțiunile în legătură cu investigația, depozitarea, examinare sau transferul probelor digitale trebuie să fie înregistrate în scris și să fie disponibile pentru evaluare și pentru prezentare în instanță.

Standarde și criterii 1.7.

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

Anexa VI

Principii în domeniul probelor digitale

(Sursa: International Organization on Computer Evidence)

1. În procesul de obținere a probelor digitale, acțiunile 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 activitățile în legătură cu investigația, depozitarea, examinarea sau transferul probelor digitale trebuie să fie în întregime înregistrate în scris, păstrate și să fie disponibile pentru evaluare.
4. O persoană este responsabilă pentru toate activitățile în legătură cu probele digitale atâta timp cât ele se află în posesia acesteia.
5. Orice organizație, 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 condiții sterile din punct de vedere criminalistic. Toate mediile de stocare folosite în timpul procesului de examinare sunt pregătite recent, curățite de date neesențiale, verificate anti-virus și testate înainte de utilizare;
2. Toate programele informatice folosite au licență și pot fi folosite de instituția respectivă;
3. Sistemul informatic original este examinat fizic. Se realizează o descriere a hardware-ului care este înregistrată. Se comentează orice element ieșit din comun întâlnit în timpul examinării fizice a sistemului informatic.
4. Sunt luate toate precauțiunile în timpul copierii sau accesului la mediile de stocare originale în scopul de a preveni transferul de viruși, programe distructive sau orice alte conținuturi inadvertente de pe/pe mediile de stocare originale. Se recunoaște faptul că datorită limitărilor hardware și ale sistemelor de operare acest lucru nu este tot timpul posibil;
5. Sunt verificate conținutul CMOS și ceasul intern, iar corectitudinea datei și orei este înregistrată. Data și ora ceasului intern este în mod frecvent importantă în stabilirea datei și orei creării sau modificării unor fișiere.
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 și o descriere a ceea ce s-a observat va fi înregistrată.
8. Datele de *boot*-are precum și fișierele de comandă operaționale și de configurare a sistemului, definite de utilizator (cum ar fi CONFIG. SYS sau AUTOEXEC.BAT) sunt examinate și o descriere a ceea ce s-a observat va fi înregistrată.
9. Toate fișierele șterse care mai pot fi recuperate vor fi salvate. Atunci când este util sau posibil, primul caracter al fișierelor 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 fișierelor conținute de mediul de stocare examinat, indiferent dacă acestea conțin sau nu potențiale probe.
11. Dacă este cazul, spațiul nealocat este examinat pentru identificarea de date ascunse sau pierdute.
12. Dacă este cazul, spațiul inactiv corespunzător fiecărui fișier este examinat pentru identificarea de date ascunse sau pierdute.
13. Se examinează conținutul fiecărui fișier de date din directoarele rădăcină și fiecare sub-director (dacă este cazul).
14. Fișierele protejate cu parolă sunt deblocate și examinate.
15. Se realizează o imprimare sau o copie a tot ceea ce aparent constituie probe. Fișierul sau locația de unde aceste posibile probe au fost obținute este notat(ă) pe fiecare foaie imprimată. Toate probele sunt marcate, numerotate în ordine și asigurate și transmise în mod corespunzător.
16. Programele executabile de interes specific vor fi examinate. Fișierele de date ale utilizatorului care nu au putut fi accesate prin alte mijloace vor fi examinate folosind aplicația implicită.
17. Comentariile și concluziile vor fi documentate în mod corespunzător.

Examinarea dischetelor

1. Sunt stabilite condiții sterile din punct de vedere criminalistic. Toate mediile de stocare folosite în timpul procesului de examinare sunt pregătite recent, curățite de date neesențiale, verificate anti-virus și testate înainte de utilizare;
2. Toate programele informatice folosite au licență și pot fi folosite de instituția 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 precauțiile în timpul copierii sau accesului la mediile de stocare originale în scopul de a preveni transferul de viruși, programe distructive sau orice alte conținuturi inadvertente de pe/pe discheta originală. Se recunoaște faptul că datorită limitărilor hardware și 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 și o descriere a ceea ce s-a găsit va fi înregistrată. Orice aspect ieșit din comun va fi notat.
8. Datele de *boot*-are precum și fișierele de comandă operaționale și de configurare a sistemului, definite de utilizator (dacă sunt prezente) sunt examinate și o descriere a ceea ce s-a observat va fi înregistrată.
9. Toate fișierele șterse care mai pot fi recuperate vor fi salvate. Atunci când este util sau posibil, primul caracter al fișierelor recuperate va fi modificat din HEX E5 în „-„ sau în alt caracter unic, în scop de identificare.
10. Spațiul nealocat este examinat pentru date ascunse sau pierdute.
11. Spațiul inactiv corespunzător fiecărui fișier este pentru date ascunse sau pierdute.

12. Se examinează conținutul fiecărui fișier de date din directoarele rădăcină și fiecare sub-director (dacă este cazul).
13. Fișierele protejate cu parolă sunt deblocate și examinate.
14. Dacă discheta conține aparent probe ce pot fi folosite, se realizează o listare a tuturor fișierelor conținute pe dischetă, indiferent dacă acestea conțin sau nu potențiale probe. Listarea va indica ce fișiere 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. Fișierul sau locația de unde aceste posibile probe au fost obținute este notat(ă) pe fiecare foaie imprimată. Toate probele sunt marcate, numerotate în ordine și asigurate și transmise în mod corespunzător.
16. Programele executabile de interes specific vor fi examinate. Fișierele de date ale utilizatorului care nu au putut fi accesate prin alte mijloace vor fi examinate folosind aplicația implicită.
17. Comentariile și concluziile vor fi documentate în mod corespunzător.

Anexa VIII

Codul etic al IACIS

(Sursa: International Association of Computer Investigation Specialists)

1. Menține cel mai ridicat nivel de obiectivitate în toate investigațiile criminalistice și prezintă în mod corect faptele;
2. Examinează și analizează în cele mai mici detalii probele;
3. Realizează examinarea respectând principiile consacrate și 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 investigații;
6. Nu îți prezenta în mod fals educația, experiența și calitatea de membru în organizații profesionale;
7. Ajută și consiliază pe oricare investigator membru IACIS, indiferent de instituția pentru care lucrează.