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

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

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

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

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

# GHID
# INTRODUCTIV PENTRU APLICAREA DISPOZIŢIILOR LEGALE REFERITOARE LA CRIMINALITATEA INFORMATICĂ

INTERNEWS
*RITI dot-Gov*

**MCTI**

Bucureşti,
Mai 2004

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

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

# Capitolul VI - Bune practici internaționale cu privire la investigațiile informatice

## Generalităţi

Investigarea criminalistică a sistemelor informatice prezintă o serie de particularităţi care o diferenţiază în mod fundamental de alte tipuri de investigaţii. În acest capitol vom prezenta pe scurt elementele esenţiale ale acestui tip de investigaţie.

Investigarea criminalistică a sistemelor informatice poate fi definită ca:

> *Utilizarea de metode ştiinţifice şi certe de asigurare, strângere, validare, identificare, analiză, interpretare, documentare şi prezentare a probelor de natură digitală obţinute din surse de natură informatică în scopul facilitării descoperirii adevărului în cadrul procesului penal.*

Un posibil model de bune practici în domeniul investigaţiilor criminalistice de natură informatică cuprinde următorii paşi:

1. **Identificarea incidentului** - recunoaşterea unui incident şi determinarea tipului acestuia. Nu reprezintă efectiv o etapă a investigaţiei criminalistice dar are un impact semnificativ asupra următoarelor etape.

2. **Pregătirea investigaţiei** - pregătirea instrumentelor, verificarea procedurilor, obţinerea documentelor ce permit percheziţia, etc.

3. **Formularea strategiei de abordare** - formularea unei strategii în funcţie de tehnologia implicată şi de posibilele consecinţe asupra persoanelor şi instituţiilor implicate. Scopul formulării acestei strategii este să maximizeze potenţialul obţinerii de probe relevante minimizând în acelaşi timp impactul negativ asupra victimei.

4. **Asigurarea probelor** - izolarea, asigurarea şi păstrarea probelor de natură fizică şi digitală. Aceasta include îndepărtarea celor care ar putea denatura probele în orice fel.

5. **Strângerea probelor** - înregistrarea ambianţei fizice şi copierea probelor digitale folosind practici şi proceduri comune şi acceptate.

6. **Examinarea probelor** - examinarea în profunzime a probelor, în căutarea elementelor care sunt în legătură cu fapta penală investigată. Acest lucru presupune localizarea şi identificarea probelor precum şi documentarea fiecărui pas, în scopul facilitării analizei.

7. **Analiza probelor** - determinarea semnificaţiei probelor şi relevarea concluziilor cu privire la fapta investigată.

8. **Prezentarea probelor** - sintetizarea concluziilor şi prezentarea lor într-un mod inteligibil pentru nespecialişti. Această sinteză trebuie susţinută de o documentaţie tehnică detaliată.

9. **Restituirea probelor** - dacă este cazul, returnarea către proprietarii de drept a obiectelor reţinute în timpul investigaţiei. Dacă este cazul, determinarea, în funcţie de prevederile legilor procedurale penale, confiscării obiectelor.

Investigarea criminalistică a sistemelor informatice trebuie să prezinte o serie de caracteristici specifice, necesare asigurării unui grad înalt de corectitudine a concluziilor rezultate. Aceste caracteristici sunt:

1. autenticitate (dovada sursei de proveniență a probelor);
2. credibilitate (lipsa oricăror dubii asupra credibilităţii şi solidităţii probelor);
3. completitudine (prelevarea tuturor probelor existente şi integritatea acestora);
4. lipsa interferenţelor şi contaminării probelor ca rezultat al investigaţiei sau al manipulării probelor după ridicarea acestora.

De asemenea, investigaţia criminalistică mai presupune:

1. existenţa unor proceduri pre-definite pentru situaţiile întâlnite în practică;
2. anticiparea posibilelor critici ale metodelor folosite, pe temeiul autenticităţii, credibilităţii, completitudinii şi afectării probelor oferite;
3. posibilitatea repetării testelor realizate, cu obţinerea unor rezultate identice;
4. anticiparea problemelor legate de admisibilitatea probelor;
5. acceptarea faptului că metodele de cercetare utilizate la un moment dat pot face subiectul unor modificării în viitor.

În legătură cu acest ultim aspect, se reliefează o particularitate a investigaţiei criminalistice a sistemelor informatice, şi anume modificarea tehnicilor criminalistice într-un timp foarte scurt, modificare dată de avansul tehnologic extrem de rapid ce se manifestă la nivel global în domeniul informaticii.

# Probele digitale

Probele digitale sunt acele informaţii cu valoare doveditoare pentru organele de urmărire penală şi pentru instanţele judecătoreşti, care sunt stocate, prelucrate sau transmise prin intermediul unui sistem informatic. Ele sunt definite ca:

> *orice informaţie cu valoare probantă care este fie stocată, prelucrată sau transmisă într-un format digital.*

Probele digitale cuprind probele informatice, probele audio digitale, video digitale, cele produse sau transmise prin telefoane mobile, faxuri digitale, etc.

Una dintre particularităţile acestui tip de probe este că ele aparent nu sunt evidente, fiind conţinute în echipamentele informatice ce le stochează. Este nevoie de echipamente de investigaţie şi de software-uri specifice pentru a face ca aceste probe să fie disponibile, tangibile şi utilizabile.

Un alt aspect este legat de faptul că astfel de probe sunt foarte „fragile", în sensul că pot fi modificate sau pot dispărea foarte uşor, prin metode care de multe ori sunt la îndemâna făptuitorilor. Din această cauză investigatorii trebuie să ia măsuri speciale de protecţie pentru a strânge, păstra şi examina aceste probe. Păstrarea acestor tipuri de probe a devenit o preocupare crescândă a investigatorilor din întreaga lume.

Necesitatea uniformizării practicii în domeniu a dus la elaborarea de standarde cu privire la probele digitale. În Anexele V şi VI sunt prezentate, ca exemplu, Standardele cu privire la probele digitale elaborate de International Organization on Computer Evidence (IOCE) şi de Scientific Working Group on Digital Evidence (SWGDE).

# Bune practici în investigarea sistemelor informatice

*Acesta secţiune cuprinde o prezentare sintetică a bunelor practici internaţionale în materia investigării infracţiunilor informatice. Datorită avansului permanent al tehnicii de calcul, modul efectiv de realizare a investigaţiilor informatice nu poate fi consemnat în acte normative. Din aceasta cauză, organizaţiile răspunzătoare de aplicarea legii dezvoltă în mod continuu practici si proceduri de natură să ghideze modul în care se realizează investigaţiile, la un anumit nivel al tehnicii. Aspectele prezentate în acest capitol sunt preluate din practica INTERPOL, a SUA şi a Marii Britanii şi se concentrează mai degrabă pe principiile investigaţiilor şi mai puţin pe tehnologii sau instrumente folosite la momentul publicării acestui Ghid introductiv.*

## *Prelevarea probelor*

O dată ajunşi la locul în care se află sistemele informatice ce fac obiectul percheziţiei, investigatorii se vor asigura de accesul la acestea. Recomandarea Consiliului Europei (95) 13 menţionează ca necesară includerea în legislaţiile naţionale penale a obligaţiei de a permite accesul la sistemele informatice, atât din partea celor care răspund de, cât şi a oricăror persoane ce au cunoştinţă de modul de funcţionare a acestora. Pe lângă accesul fizic, aceste persoane au datoria de a furniza şi informaţii referitoare la securitatea sistemului, informaţii care să permită investigatorilor accesul la datele stocate în sistemele informatice respective.

Înainte de a trece la examinarea sistemelor informatice, nu trebuie neglijate procedurile criminalistice tradiţionale de analiză a spaţiului percheziţionat, cum ar fi prelevarea probelor fizice (amprente, alte urme materiale). De asemenea poate avea relevanţă imaginea aflată pe ecranul monitorului în momentul pătrunderii organelor de cercetare penală. Aceasta poate fi păstrată prin fotografiere, filmare, etc.

O primă decizie ce trebuie luată priveşte analiza sistemului informatic la faţa locului, sau ridicarea acestuia şi analiza în laborator.

În luarea acestei decizii, trebuie avute în vedere următoarele aspecte:

- calitatea superioară a analizei efectuate în condiţii de laborator;
- măsura în care ridicarea sistemului informatic afectează activitatea suspectului.

În acest sens, trebuie reţinute recomandările Camerei Internaţionale de Comerţ ce menţionează regula evitării ridicării sistemelor informatice ale întreprinderilor, dacă aceasta ar duce la afectarea desfăşurării activităţilor lor normale.

Următoarele criterii sunt utile în aprecierea oportunităţii ridicării sistemelor informatice:

*a.* *criteriul volumului probelor.*

Particularitatea sistemelor informatice de a permite stocarea unui volum foarte mare de informaţie într-un spaţiu de dimensiuni fizice reduse face ca investigaţia să necesite un volum mare de timp pentru obţinerea probelor relevante. Astfel de cercetări pe o perioadă de timp mare pot fi conduse mult mai eficient în laborator.

*b.* *criteriul dificultăţilor de natură tehnică.*

1. problema evitării distrugerii datelor în decursul investigaţiei. Analiza sistemelor informatice de către investigatori ce nu au cunoştinţe suficiente asupra echipamentului sau programelor utilizate poate duce la distrugerea din greşeală a datelor.
2. problema reconstituirii sistemului în laborator. Datorită varietăţii foarte mari a componentelor tehnice ale calculatoarelor, pentru ca sistemul să poată funcţiona corect în laborator, este necesară ridicarea tuturor echipamentelor prezente la locul percheziţiei. În cazul ridicării parţiale a componentelor sistemului, este posibilă prezenţa unor incompatibilităţi fie între echipamentele sistemului informatic ridicat şi cele din laborator (de exemplu incompatibilitatea calculatorului cu echipamentele periferice - imprimante, etc.), fie între programele de pe sistemul ridicat şi echipamentele din laborator.

O dată decisă ridicarea sistemului informatic aflat la locul percheziţiei, trebuie luate unele măsuri care să permită reconstituirea exactă a acestuia în laborator. În primul rând, trebuie consemnat modul de aranjare în spaţiu a echipamentelor sistemului informatic ridicat. Aceasta se poate face fie prin fotografierea sistemului din toate unghiurile, fie prin filmare video. In procesul de fotografiere

sau filmare, este necesar să se insiste asupra cablajelor ce conectează diferitele componente ale echipamentului. Consemnarea, în variantă foto sau video, are relevanţă şi pentru a arăta starea în care se găsea echipamentul în momentul ridicării, prevenind astfel plângerile legate de o eventuală deteriorare a acestuia în decursul anchetei.

În procesul de ridicare a componentelor sistemului trebuie să fie avută în vedere necesitatea păstrării integrităţii şi identităţii datelor. Orice avariere a suportului pe care se află datele duce în mod inevitabil la distrugerea acestora. Organele de cercetare penală trebuie instruite în mod special pentru a proteja probele de natură electronică.

Procedura ridicării sistemelor informatice este următoarea:

*etapa 1: închiderea sistemului.* Dacă sistemul a fost găsit închis în momentul pătrunderii investigatorilor, nu trebuie sub nici un motiv pornit. Se va proceda în continuare trecând la celelalte etape. Dacă sistemul a fost găsit deschis, el trebuie închis pentru a se putea proceda la ridicarea lui. Pentru închiderea sistemului se pot folosi următoarele procedee:

- deconectarea de la alimentarea cu energie electrică;
- închiderea conform procedurii normale.

Prima alternativă este de preferat în cazul în care investigatorul nu are cunoştinţe de informatică. Unele calculatoare dispun de surse de alimentare neinteruptibile (UPS). În acest caz, pe lângă deconectarea de la sistemul de alimentare cu energie electrică, trebuie oprit şi acest sistem. Deconectarea nu va produce, în cele mai multe cazuri, pierderea de date, dar poate evita ştergerea unor informaţii relevante, cum ar fi fişierele temporare, care se pot şterge în cadrul procesului normal de închidere a calculatorului.

Cea de-a doua alternativă este de preferat atunci când calculatorul este conectat în reţea, sau atunci când investigatorul este asistat de o persoană ce are cunoştinţe asupra modului de funcţionare a sistemului respectiv, precum şi asupra procedurilor ce sunt folosite pentru închiderea lui.

*etapa a 2-a: etichetarea componentelor*. În cazul în care se impune dezasamblarea fiecare componentă a sistemului trebuie etichetată înainte de modificarea configuraţiei în vederea ridicării probelor. În cazul cablurilor, se etichetează atât cablul, cât şi suporturile de unde a fost debranşat. În cazul existenţei unor suporturi care nu au conectate cabluri, este recomandabil ca să fie

etichetate "neocupat". Se poate realiza şi o schiţă a componentelor, cu precizarea simbolurilor folosite pentru etichetare.

*etapa a 3-a: protejarea la modificare*. Toate suporturile magnetice de stocare a datelor trebuie protejate împotriva modificării conţinutului lor. Unele tipuri de hard-discuri au contacte speciale care realizează protejarea la scriere. În cazul dischetelor, protejarea se va face prin mutarea martorului de permitere a modificărilor în poziţia "închis".

*etapa a 4-a: ridicarea propriu-zisă*. Ridicarea probelor trebuie făcută cu multă grijă, evitându-se orice avariere a componentelor. Este recomandabilă împachetarea componentelor în ambalajul original, dacă acesta poate fi găsit, sau în ambalaj special ce asigură protecţia electrostatică a acestora. De asemenea, toate suporturile magnetice de stocare a datelor, vor fi ambalate şi sigilate în aşa fel încât accesul la ele nu este permis, până la desfacerea in laborator.

## *Suspectul*

În timpul investigaţiei, dacă suspectul este prezent, organul de urmărire penală trebuie să împiedice orice apropiere a acestuia de sistemul informatic. Mai ales dacă suspectul are pregătire superioară în domeniul informatic, acesta poate altera voit datele aflate pe calculatorul său, fără ca investigatorii să poată sesiza acest lucru. Calculatorul suspectului poate conţine unele comenzi ce pot produce pierderea datelor, comenzi ce pot fi mascate sub numele unor comenzi uzuale ale sistemului de operare folosit.

Dacă suspectul insistă să ajute investigatorii în procesul de închidere a calculatorului sau a procesului de ridicare a componentelor sistemului, aceştia pot cere suspectului să le descrie operaţiunile pe care acesta doreşte să le execute, şi chiar să le scrie pe hârtie. Investigatorii nu vor urma indicaţiile suspectului, ci le vor remite experţilor ce efectuează analiza probelor. Aceştia vor putea fi avertizaţi în acest mod de eventualele capcane introduse de suspect.

## *Rolul altor persoane*

De la persoanele prezente la percheziţie, sau de la alte persoane care au cunoştinţă de modul de operare a sistemului informatic respectiv pot fi obţinute informaţii importante. Fiecare martor trebuie intervievat asupra modului în care sunt folosite sistemele informatice ridicate. Sunt relevante modalităţile de introducere, sortare şi stocare a datelor pe computer, precum şi practicile referitoare la diverse aspecte legate de utilizarea lui curentă.

În cazurile în care se anchetează incidente legate de pătrunderea neautorizată în sisteme informatice ale unor întreprinderi, de cele mai multe ori specialiştii întreprinderii-victimă sunt cele mai importante ajutoare ale investigatorilor. Astfel investigatorii nu trebuie să folosească tehnici de pătrundere activă în sistem pentru prelevarea probelor, bucurându-se de sprijinul celor care administrează sistemul.

În unele situaţii speciale, calculatoarele altor persoane, situate la aceeaşi locaţie pot deţine probe relevante. De exemplu, se citează cazuri în care documente relevante au fost găsite în calculatorul secretarelor persoanelor investigate.

## *Transportarea probelor în laborator*

Transportarea probelor reţinute trebuie făcută cu multă grijă, având în vedere fragilitatea lor. Este necesar să fie luate precauţiuni legate de protejarea faţă de şocuri fizice, umiditate, căldură şi mai ales de influenţa undelor electromagnetice. În legătură cu acest din urmă aspect trebuie evitată plasarea echipamentelor în apropierea surselor de radiaţii electromagnetice, cum ar fi aparate de fax, copiatoare, staţii radio, telefoane celulare. Este recomandabilă măsurarea cu instrumente speciale a câmpului electromagnetic în spaţiile unde sunt depozitate echipamentele ridicate.

## *Analiza probelor*

O dată aduse în laborator, componentele trebuie asamblate pentru a reconstitui sistemul original. Pentru aceasta se vor folosi fotografiile sau casetele video filmate înainte de ridicarea probelor, respectându-se conexiunile originale, precum şi informaţiile obţinute de la martori în legătură cu practicile de utilizare a sistemului informatic respectiv.

Primul pas în analiza probelor de natură electronică este legat de necesitatea asigurării veridicităţii lor. Pentru a putea dovedi veridicitatea probelor, este necesară ambalarea şi sigilarea acestora în modul amintit mai sus .

Primul pas în asigurarea protecţiei împotriva modificării datelor din sistemele informatice trebuie făcut chiar în timpul percheziţiei, prin luarea măsurilor de protejare fizică la scriere a mediilor de stocare.

Se recomandă ca analiza criminalistică a conţinutului discului să se realizeze pe o copie fidelă a discului original, realizată în laborator cu ajutorul unor programe şi dispozitive speciale. Procedeul nu presupune doar copierea tuturor fişierelor aflate pe disc, ci a întregului conţinut al discului, sector cu sector, inclusiv

fişierele temporare, fişierele de schimb, fişierele şterse, chiar informaţia aflată pe porţiunile avariate ale discului, etc. O asemenea copiere de această natură se realizează cu ajutorul unor programe speciale. Se recomandă realizarea a două copii, pe una dintre ele realizându-se analiza propriu-zisă, cealaltă fiind o copie de rezervă.

Copierea trebuie realizată după un procedeu demn de încredere. Pentru a putea avea această caracteristică, copierea trebuie:

- să asigure posibilitatea verificării de către terţi; instanţa de judecată sau partea adversă trebuie să poată să verifice acurateţea copiei realizate.
- să aibă ca rezultat copii sigure, ce nu pot fi falsificate.

Este recomandată consemnarea detaliată a întregului proces de copiere, indicând echipamentele, programele şi mediile de stocare utilizate.

Păstrarea în siguranţă a probelor se realizează în primul rând prin copierea conţinutului sistemelor informatice originale, şi desfăşurarea investigaţiei criminalistice asupra unei copii de lucru, având aceleaşi caracteristici cu originalul.

Ca o metodă de siguranţă în plus, se poate realiza autentificarea matematică a conţinutului unui mediu de stocare, fie el hard-disc sau dischetă, mediu optic, etc. Acest procedeu constă în realizarea prin procedee matematice a unei imagini a mediului de stocare respectiv, imagine ce poate servi ca referinţă în cazul în care este contestată integritatea acestuia. Autentificarea se realizează cu ajutorul unor programe speciale ce oferă un grad de siguranţă de 1 la câteva milioane.

## *Pregătirea membrilor echipei ce participă la investigaţie*

Natura infracţiunilor cere ca cercetarea penală să se realizeze în cadrul unei echipe de investigatori. Necesitatea investigaţiei în echipă reiese din nevoia garantării unei obiectivităţi sporite şi eficiente, derivată din conjugarea competenţelor şi specializărilor membrilor echipei. Atât datorită caracteristicilor speciale ale echipamentelor ce fac obiectul investigaţiei, cât şi a metodelor întrebuinţate în investigarea criminalistică a sistemelor informatice, membrii echipei de investigatori trebuie să posede cunoştinţe şi aptitudini adecvate specificului investigaţiei.

Se apreciază că un bun investigator trebuie să posede:

1. cunoştinţe suficiente asupra tehnicilor informatice, care să îi permită să înţeleagă filozofia funcţionării unui sistem informatic, să analizeze documentaţia tehnică şi să apeleze, dacă este nevoie, la tehnici informatice evoluate care să-l ajute în atingerea scopului urmărit;
2. cunoştinţe suficiente asupra tehnicilor utilizate de firme, în special asupra sistemelor contabile, pentru a putea înţelege caracteristicile sistemelor care ar putea face obiectul unor fraude, astfel încât să poată stabili atât modul de operare cât şi să dirijeze investigaţia până acolo unde ar putea găsi probele delictului;
3. cunoştinţe suficiente asupra tehnicilor de securitate internă, astfel încât investigaţia să poată fi efectuată cu rapiditate şi fiabilitate, şi să fie îndreptată în direcţia justă.

Pe lângă nivelul de cunoştinţe al anchetatorilor, au fost reliefate aptitudinile ce trebuie să existe sau să fie dezvoltate în persoana investigatorilor, pentru ca aceştia să poată conduce ancheta. Astfel, putem aminti: personalitate extrovertită (datorită faptului că, în general, specialiştii în domeniile tehnice, şi în special informatice, posedă mai puţine abilităţi de comunicare inter-umană), înclinare spre detaliu (foarte importantă, mai ales având în vedere specificul probelor electronice: abundenţa informaţiilor aflate pe un spaţiu de stocare de dimensiuni fizice reduse; cu toate acestea, este importantă păstrarea unei viziuni de ansamblu asupra anchetei), gândire logică, comunicare bună (importantă mai ales pentru a asigura prezentarea rezultatelor investigaţiei într-un mod relevant, atât în scris, cât şi în faţa instanţei), obiectivitate. Pregătirea investigatorilor în domeniul infracţiunilor informatice este o preocupare permanentă a organelor de cercetare penală din întreaga lume.

## *Instrumente (echipamente şi programe pentru calculator) necesare investigaţiei*

Investigarea criminalistică a sistemelor informatice necesită utilizarea unor instrumente specifice. Ca echipamente, echipa de investigatori trebuie să dispună de medii de stocare a datelor, în cantitate suficientă, şi de calitate superioară, pentru a permite copierea acestora de pe sistemul informatic analizat.

În analiza sistemelor informatice este folosit un număr semnificativ de programe de calculator. Cu titlu de exemplu se pot menţiona programe pentru copierea exactă a conţinutului memoriei fizice, pentru analiza şi compararea fişierelor, pentru catalogarea conţinutului discului, pentru validarea şi autentificarea matematică a datelor, pentru recuperarea fişierelor şterse, programe de

decriptare sau programe antivirus. Este necesar ca programele de calculator folosite de organele de urmărire penală să fie înregistrate din punct de vedere al protecţiei drepturilor de autor aparţinând producătorilor acestor programe.