

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.



GHID INTRODUCȚIV

PENTRU APLICAREA DISPOZIȚIILOR LEGALE REFERITOARE LA CRIMINALITATEA INFORMATICĂ



București, mai 2004



Introducere

Apariția, acum mai bine de 50 de ani, a primelor calculatoare electronice a declanșat o adevărată revoluție în societatea umană. Consecința primordială a avansului tehnologic apărut a reprezentat-o tranziția de la societatea industrială la societatea informațională. Umanitatea a evoluat în ultimii 50 de ani mai mult decât în orice altă perioadă. Unealtă tehnologică în continuă perfecționare, a cărei pătrundere în toate aspectele vieții economice, sociale și culturale a punctat această evoluție, calculatorul electronic a devenit în ultimii ani o componentă normală a vieții noastre.

Dezvoltarea tehnologică și utilizarea pe scară largă a sistemelor informatice a adus după sine și o serie de riscuri. Dependența din ce în ce mai accentuată a agenților economici, a instituțiilor publice și chiar a utilizatorilor individuali de sistemele informatice ce le gestionează în mare măsură resursele, face ca aceștia să fie tot mai vulnerabili la impactul pe care îl poate avea criminalitatea informatică.

Calculatoarele electronice nu au constituit o atracție numai pentru cei interesați de dezvoltare, ci și pentru cei care au văzut în exploatarea tehnologiei moderne un mod de a dobândi foloase necuvenite. Analog modulului în care noile tehnologii informaționale sunt mai întâi aplicate vechilor sarcini industriale pentru perfecționarea lor pentru ca apoi să dea naștere unor activități, procese și produse noi, calculatoarele electronice au fost utilizate inițial pentru a perfecționa modul de comitere a unor infracțiuni tradiționale, pentru ca în cele din urmă să apară noi forme de încălcări ilicite, specifice domeniului informatic. Calculatorul electronic este un factor criminogen de prim ordin, ce pune la dispoziția conduitei criminale atât un nou obiect (informația, conținută și procesată de sistemele informatice) cât și un nou instrument. El oferă un repertoriu deosebit de întins de tehnici și strategii de îndeplinire a infracțiunilor, dar în același timp îmbogățește sfera criminalității cu noi infracțiuni. Criminalitatea informatică prezintă numeroase elemente de diferențiere față de fenomenul criminal tradițional, ridicând o serie de probleme în fața autorităților responsabile pentru eradicarea acesteia.

În acest context, considerăm că prezentul „Ghid pentru aplicarea dispozițiilor legale referitoare la criminalitatea informatică” va fi foarte folositor tuturor celor interesați de combaterea acestor fenomene periculoase pentru societatea noastră. Sperăm ca acest Ghid, dincolo de menirea sa de material informativ, să constituie un material de referință util în activitatea zilnică a destinatarilor lui. De asemenea, el poate fi punctul de plecare pentru programe de perfecționare profesională a persoanelor implicate în acțiuni de combatere a criminalității informatice.

Ghidul este structurat pe două secțiuni. Secțiunea I, „Ghid de referință cu privire la sisteme informatice și traficul informațional” cuprinde, în cadrul a patru capitole, o prezentare într-un limbaj accesibil a sistemelor informatice, rețelelor de calculatoare, componentelor acestora și a principalelor programe utilizate și care au incidență asupra descoperirii, investigării și urmăririi penale a infracțiunilor informatice. Primul capitol prezintă calculatoare personale și componentele lor. Sunt prezentate: suporturile de stocare a datelor (hard-disk, CD-ROM, memorii amovibile, etc.), perifericele, precum și aspectele legate de PDA-uri și telefoane mobile. Cel de-al doilea capitol analizează rețelele de calculatoare și componentele lor (servere, hub-uri, routere, etc.). Un loc important îl constituie analiza rețelelor de tip Intranet VPN și a Internetului. Capitolul

3 ia în discuție serviciile (www, email, ftp, IRC, *instant messaging*) și software-ul incident (softuri de rețea, programe de criptare, etc.). Ultimul capitol al primei secțiuni, capitolul 4, prezintă vulnerabilități ale sistemelor informatice.

Secțiunea a II-a, „Dispoziții legale referitoare la criminalitatea informatică”, conține trei capitole ce privesc reglementarea criminalității informatice, prezentarea unor noțiuni cu privire la investigațiile informatice și problematica probelor digitale. Capitolul al cincilea prezintă noțiunea de infracțiune informatică. În deschiderea capitolului sunt descrise tipurile de atacuri informatice. Apoi sunt prezentate și analizate infracțiunile cuprinse în reglementarea română curentă (Titlul III din Legea nr. 161/2003, privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției). Capitolul șase prezintă bune practici internaționale legate de probele digitale și aspecte legate de investigația la fața locului, proceduri de ridicare a probelor, proceduri de investigație criminalistică în laborator. Ghidul este însoțit de o serie de anexe:

- (i) Legea nr. 161/2003, Titlul III, Prevenirea și combaterea criminalității informatice
- (ii) Convenția Consiliului Europei privind criminalitatea informatică
- (iii) Recomandarea Consiliului Europei nr. R (95) 13 cu privire la problemele de procedură penală legate de tehnologiile informaționale
- (iv) Reguli de bază pentru obținerea de probe digitale de către ofițerii de poliție (Australia)
- (v) Standarde în domeniul probelor digitale (SWGDE)
- (vi) Principii în domeniul probelor digitale (IOCE)
- (vii) Proceduri model de examinare criminalistică a sistemelor informatice (IACIS)
- (viii) Codul etic al IACIS