

Criminalitatea informatică poate cauza multe probleme în societatea modernă. Prin urmare, România a adoptat legislația privind criminalitatea informatică care corespunde pe deplin convențiilor și standardelor internaționale. Totuși, această legislație poate fi complexă din punctul de vedere al aplicării sale pentru autoritățile care o implementează, în special pentru aceia care sunt mai puțin familiarizați cu computerele și serviciile electronice ca parte a vieții de fiecare zi.

Portalul eFrauda a fost realizat de către Ministerul Comunicațiilor și Tehnologiei Informației și este gestionat împreună cu Serviciul de Combatere a Criminalității Informatică din cadrul Ministerului Administrației și Internelor și secția specializată din Parchetul de pe lângă Înalta Curte de Casație și Justiție. Portalul dă oricui posibilitatea de a sesiza autoritățile cu privire la o posibilă fraudă sau alte activități ilegale pe Internet.
www.efrauda.ro

Acest Ghid introductiv pentru aplicarea dispozițiilor legale referitoare la criminalitatea informatică a fost elaborat de către proiectul RITI dot-Gov, în cooperare cu Ministerul Comunicațiilor și Tehnologiei Informației. Ghidul asigură asistență pentru autoritățile care aplică legea și pentru toți cei care sunt implicați în prevenirea criminalității informatică.

Proiectul RITI dot-Gov face parte din Inițiativa pentru Tehnologia Informației în România, RITI, a cărei implementare a fost începută în 2002 de către Misiunea din România a Agenției Statelor Unite pentru Dezvoltare Internațională (USAID), în cooperare cu Ministerul Comunicațiilor și Tehnologiei Informației. Proiectul RITI dot-Gov este implementat în România de Internews Network Inc, o organizație non-profit cu sediul în Statele Unite.

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

GHID INTRODUCTIV PENTRU APLICAREA DISPOZIȚIILOR LEGALE REFERITOARE LA CRIMINALITATEA INFORMATICĂ



INTERNEWS
RITI dot-Gov



MCTI

București,
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.

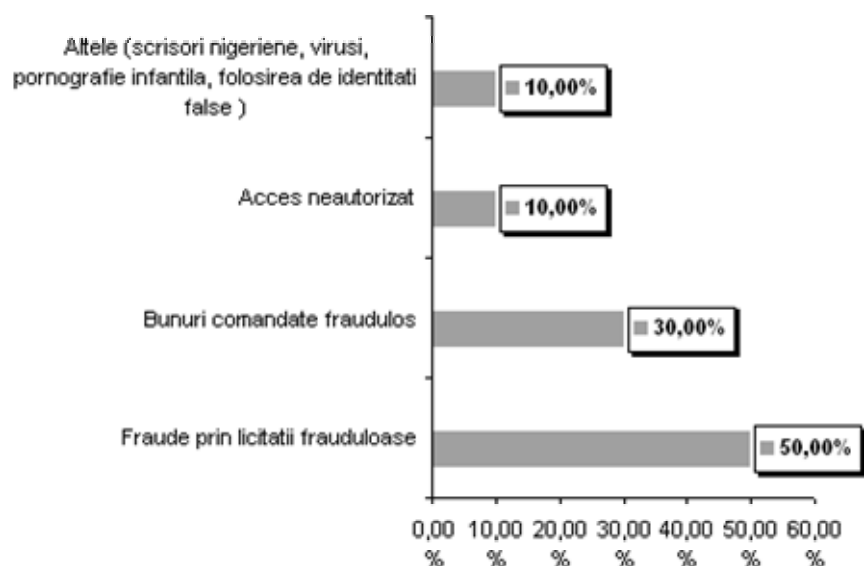
© Internews Network, Inc., 2004. Acest ghid poate fi utilizat și copiat în scop ne-comercial atâta vreme cât "Internews Network, RITI dot-GOV" este creditat ca sursă și "USAID" menționat ca finanțator.

Capitolul V - Reglementarea criminalității informatice

Conceptul de “criminalitate informatică”

Criminalitatea informatică reprezintă un fenomen al zilelor noastre, reflectat în mod frecvent în mass-media. Un studiu indică chiar că teama de atacuri informatice depășește în intensitate pe cea față de furturi sau fraude obișnuite. Cercetările criminologice asupra infracțiunilor realizate prin sistemele informatice se află încă în stadiul tatonărilor. Chiar și cele realizate până în acest moment tind să schimbe modul clasic în care sunt privite infracțiunile în sistemele actuale de justiție penală.

Doar o mică parte din faptele penale legate de utilizarea sistemelor informatice ajung la cunoștința organelor de cercetare penală, astfel încât este foarte greu de realizat o privire de ansamblu asupra amplitudinii și evoluției fenomenului. Dacă este posibil să se realizeze o descriere adecvată a tipurilor de fapte penale întâlnite, este foarte dificilă prezentarea unei sinteze fundamentate asupra întinderii pierderilor cauzate de acestea, precum și a numărului real de infracțiuni comise. umărul cazurilor de infracțiuni informatice este în continuă creștere. Astfel, în Germania au fost înregistrate în 1996 32.128 de astfel de cazuri, în Olanda, în perioada 1981-1992 au fost întâlnite 1400 de cazuri, iar în Japonia, între 1971 și 1995, 6671 de cazuri. S-a estimat că doar 5% din faptele comise ajung la cunoștința organelor de urmărire penală. Pentru a contracara această lipsă de informație, s-a recurs la procedeul sondajelor. Ultimul sondaj efectuat de Computer Crime Institute și Federal Bureau of Investigation (FBI) în 2003 indică pierderi de 201.797.340 de dolari în cazul a 538 de întreprinderi și instituții din SUA chestionate. În cursul anului 2003, serviciile specializate din România au cercetat doar 200 de infracțiuni de natură informatică din care 50% au fost licitații electronice frauduloase, 30% bunuri comandate on-line fraudulos, 10% au privit accesul neautorizat la sisteme informatice și 10% referindu-se la scrisori nigeriene, transmiterea de viruși, pornografie infantilă, folosirea de identități false.



Cifra neagră este motivată de mai multe cauze, dintre care amintim:

- tehnologia sofisticată utilizată de făptuitori;

- lipsa instruirii specifice a ofițerilor din cadrul organelor de urmărire penală;
- lipsa unui plan de reacție în caz de atacuri, din partea victimelor acestor fapte penale, fapt ce poate duce la neidentificarea pierderilor provocate;
- reținerile în a raporta organelor de cercetare penală săvârșirea infracțiunilor.

În aceasta din urmă situație, chiar dacă infracțiunea a fost sesizată, victimele nu înștiințează organele de urmărire penală în vederea descoperirii și sancționării făptuitorului. Motivațiile acestui comportament sunt multiple. Dintre acestea, amintim preocupările față de imaginea publică, ce ar putea fi afectată de publicitatea în jurul infracțiunii; dorința de a nu suporta costurile unei eventuale investigații, având în vedere complexitatea unei asemenea cercetări; nu în ultimul rând, lipsa posibilității de a recupera pierderile suferite, chiar în cazul identificării făptuitorului.

În același timp, investigațiile în domeniul infracționalității informatice sunt, prin natura lor, complexe și implică utilizarea de echipamente sofisticate, cu costuri ridicate. De asemenea, pregătirea personalului de specialitate este un proces de durată și implică costuri mari. Asemenea investigații sunt consumatoare de timp. Un investigator în domeniul criminalității informatice poate lucra la maximum 3-4 cazuri pe lună, în timp ce un investigator tradițional poate soluționa între 40 și 50 de cazuri în aceeași perioadă de timp.

Pentru scopul lucrării de față vom adopta definiția de lucru dată faptelor penale de natură informatică de către grupul de experți ai OECD în 1983:

orice comportament ilegal, neetic sau neautorizat ce privește un tratament automat al datelor și/sau o transmitere de date

Această definiție, deși formulată în urmă cu două decenii, își dovedește utilitatea în primul rând prin faptul că permite integrarea dezvoltărilor ulterioare ale tehnicii în domeniul informatic.

Tot în scopul lucrării de față, vom opera cu două definiții formulate de UNAFEI.

Astfel, prin infracțiune informatică în sens larg se înțelege:

orice infracțiune în care un calculator sau o rețea de calculatoare este obiectul unei infracțiuni, sau în care un calculator sau o rețea de calculatoare este instrumentul sau mediul de îndeplinire a unei infracțiuni.

Prin infracțiune informatică în sens restrâns se înțelege:

orice infracțiune în care făptuitorul interferează, fără autorizare, cu procesele de prelucrare automată a datelor.

Conținutul noțiunii de faptă penală de natură informatică este deosebit de variat, fiind abordat din diferite perspective în cadrul lucrărilor de specialitate. Astfel, în raportul Comitetului European pentru probleme criminale, infracțiunile informatice sunt sistematizate în următoarele categorii:

- infracțiunea de fraudă informatică;
- infracțiunea de fals în informatică;
- infracțiunea de prejudiciere a datelor sau programelor informatice;

- infrațiunea de sabotaj informatic;
- infrațiunea de acces neautorizat la un calculator;
- infrațiunea de interceptare neautorizată;
- infrațiunea de reproducere neautorizată a unui program informatic protejat de lege;
- infrațiunea de reproducere neautorizată a unei topografii;
- infrațiunea de alterare fără drept a datelor sau programelor informatice;
- infrațiunea de spionaj informatic;
- infrațiunea de utilizare neautorizată a unui calculator;
- infrațiunea de utilizare neautorizată a unui program informatic protejat de lege.

Manualul Națiunilor Unite pentru prevenirea și controlul infracționalității informatice sintetizează următoarele categorii de infracțiuni:

- fraude prin manipularea calculatoarelor electronice;
- fraude prin falsificarea de documente;
- alterarea sau modificarea datelor sau a programelor pentru calculator;
- accesul neautorizat la sisteme și servicii informatice;
- reproducerea neautorizată a programelor pentru calculator protejate de lege.

În studiul “Aspectele legale ale infracționalității informatice în cadrul societății informaționale” (studiul COMCRIM), realizat pentru Comisia Europeană de către prof. dr. Ulrich Sieber, de la Universitatea din Wurzburg, Germania, sunt prezentate următoarele categorii și sub-categorii de infracțiuni informatice:

- atingeri aduse dreptului la viața privată;
- infracțiuni cu caracter economic:
- penetrarea sistemelor informatice în scopul depășirii dificultăților tehnice de securitate (“hacking”);
- spionajul informatic;
- pirateria programelor pentru calculator;
- sabotajul informatic;
- fraudă informatică;
- distribuirea de informații cu caracter ilegal sau prejudiciabil (propagandă rasistă, difuzare de materiale pornografice, etc.);
- alte infracțiuni:
- infracțiuni contra vieții;
- infracțiuni legate de crima organizată;
- război electronic.

Infracțiunile informatice pot fi clasificate urmând diverse criterii. Vom utiliza pentru clasificarea infracțiunilor informatice criteriul rolului avut de sistemele informatice în comiterea infracțiunii. Din această perspectivă, infracțiunile informatice se clasifică în:

- *infrațiuni săvârșite cu ajutorul sistemelor informatice*, în care sistemele informatice constituie un instrument de facilitare a comiterii unor infracțiuni. Este vorba de infracțiuni “tradiționale” perfecționate prin utilizarea sistemelor informatice; și
- *infrațiuni săvârșite prin intermediul sistemelor informatice*, în care sistemele informatice, incluzând și datele stocate în acestea, constituie ținta infracțiunii. Aceste infracțiuni pot fi săvârșite doar prin intermediul sistemelor informatice. Ele au făcut obiect de reglementare în ultimii ani.

Amintim aici și un alt rol pe care sistemele informatice îl pot juca în ancheta criminalistică: rolul de mediu de stocare și regăsire a indiciilor sau probelor ce privesc modul de săvârșire a unei infracțiuni.

Conștientizarea existenței pericolului social al faptelor penale de natură informatică a atras după sine încriminarea acestora în numeroase state ale lumii. A luat astfel ființă conceptul de “drept penal cu specific informatic”, ca o reflectare a numeroaselor elemente de noutate introduse în materia dreptului penal de noile forme de criminalitate bazate pe tehnologia modernă. Legiferarea în domeniul criminalității informatice a urmat, începând din anii '70, mai multe “valuri”. Primul “val” a fost determinat de necesitatea protejării dreptului la viața privată. Legi privind protecția persoanei fizice față de prelucrarea datelor cu caracter personal au fost adoptate în Suedia (1973), SUA (1974), Germania (1977), Austria, Danemarca, Franța și Norvegia (1978), sau mai recent în Belgia, Spania, Elveția (1992), Italia și Grecia (1997). Al doilea “val” este legat de represiunea infracțiunilor cu caracter economic, producând modificări legislative în SUA și Italia (1978), Australia (1979), Marea Britanie (1981), sau Elveția (1994) și Spania (1995). A treia serie de reglementări este legată de intervenția legislativă în vederea protecției proprietății intelectuale în domeniul tehnologiei informatice, în țări ca SUA (1980), Ungaria (1983), Germania, Franța, Japonia, Marea Britanie (1985), sau Austria (1993), România (1996), Luxemburg (1997). Al patrulea “val” de reforme privește reglementarea distribuirii de informații ilegale sau prejudiciabile, și a fost puternic impulsivat la sfârșitul anilor '80 de amploarea luată de rețeaua Internet. Al cincilea “val” este legat de modificările intervenite în materia dreptului procesual, cu privire la aspectele de procedură penală ridicate de incidența tehnologiei informației, în timp ce al șaselea “val” privește impunerea unor obligații și limite în materia securității informatice.

În acest sens, la nivel internațional, Consiliul Europei a inițiat o serie de reglementări cu privire la criminalitatea informatică. Astfel, dacă în 1995 a fost adoptată Recomandarea nr. R (95) 13 cu privire la problemele de procedură penală legate de tehnologiile informaționale, în 23 noiembrie 2001 a fost semnată la Budapesta Convenția privind criminalitatea informatică. Convenția își propune să prevină 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 încriminării unor asemenea conduite și prin încurajarea adoptării unor măsuri de natură a permite combaterea eficace a acestor tipuri de 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. Convenția a fost ratificată de România prin Legea 64/2004 (pentru ratificarea Convenției Consiliului Europei privind criminalitatea informatică, adoptată la Budapesta la 23 noiembrie 2001). După ratificarea, în martie 2004, de către al cincilea stat, Convenția va intra în vigoare la data de 4 iulie 2004. Textul original al convenției poate fi găsit în limba engleză la adresa <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm> și în limba franceză la adresa <http://conventions.coe.int/Treaty/FR/Treaties/Html/185.htm>. Traducerea română poate fi găsită în Anexa II.

Infracțiuni săvârșite cu ajutorul sistemelor informatice

O serie de infracțiuni prevăzute de legea penală prezintă particularități ce permit perfecționarea modalităților de îndeplinire a acestora prin recurgerea la ajutorul dat de sistemele informatice. Ele sunt acele infracțiuni în care “*modus operandi*” nu este îndreptat împotriva funcționării corespunzătoare a unui sistem informatic, sau asupra informațiilor cuprinse în el, ci *rezultatul procesării datelor este utilizat pentru îndeplinirea unor infracțiuni clasice*. Făptuitorii fac astfel apel la mijloace ne-tradiționale pentru îndeplinirea unor infracțiuni cu caracter “tradițional”.

Cu titlu de exemplu, menționăm:

- Infracțiunea de *aducere, fără drept, a operei* (creației intelectuale protejate prin legea dreptului de autor) *la cunoștință publică*, reglementată de art. 140, lit. a din legea nr. 8/1996 privind dreptul de autor și drepturile conexe;
- Infracțiunea de *reproducere, fără drept, a unei opere*, reglementată de art. 142, lit. a din legea nr. 8/1996 privind dreptul de autor și drepturile conexe;
- Infracțiunea de *spălare a banilor*, reglementată de art. 23 din legea nr. 21/1999, pentru prevenirea și sancționarea spălării banilor;
- Infracțiunea de *trădare prin transmitere de secrete*, reglementată de art. 157 din Codul Penal;
- Infracțiunea de *divulgare a secretului care periclitizează siguranța statului*, reglementată de art. 169 din Codul Penal și art. 12 alin. 2 din legea 51/1991 privind siguranța națională;
- Infracțiunea de *divulgare a secretului profesional*, reglementată de art. 196 din Codul Penal;
- Infracțiunea de *gestiune frauduloasă*, reglementată de art. 214 din Codul Penal;
- Infracțiunea de *falsificare de monede sau de alte valori*, reglementată de art. 282 din Codul Penal;

B.O.N., în vârstă de 23 de ani, referent la Ministerul Finanțelor, V.M., 49 de ani, mama acestuia, M.D., 53 de ani, amantul acesteia, au falsificat 1.723 de bancnote de 50.000 de lei, și trei de 100.000 de lei, cu ajutorul unui calculator Tatung, un scanner Genius și o imprimantă.

În perioada iulie – decembrie 1998, Z.D., din Galați, electrician la Asociația Fluvială a Dunării de Jos, a falsificat 60 de bancnote de 50.000 de lei cu ajutorul unui calculator al unității la care lucra.

C.M., din București, absolvent al liceului de informatică, C.S., din Otopeni, sergent angajat, S.D., sergent angajat, M. A., zis “Chioru”, A.A., I.D.R., T.F.I., din Oradea, folosind calculatorul personal al lui C.M. au falsificat aproape 1 miliard de lei. La percheziție polițiștii au descoperit 54 de milioane de lei în bancnote de 50.000 de lei, având seria 0005B477753.

O.I.D., din Cluj, redactor șef al revistei “E.H.”, și redactor la editura “E.H.” a falsificat bancnote de 100.000 de lei folosind calculatorul, cu scanner și imprimantă, din dotarea redacției.

D.G., 47 de ani, din Caransebeș, de meserie tâmplar, I.B., 47 de ani, din Caransebeș, S.P., 32 de ani, din Ocna Șugatag, jud. Maramureș, F.C., 22 de ani, din Timișoara, A.D.C., 28 de ani, din Râmnicu Vâlcea, au falsificat 110 bancnote de 50.000 de lei, având seriile 006B3291121, 005A0971406 și 001D4428770.

- *Infrațiunea de falsificare a instrumentelor oficiale*, reglementată de art. 286 din Codul Penal.

C.V., 27 de ani, din Galați, administrator al SC “Genda Prod” SRL, a luat în luna noiembrie 1998, de la SC “SDB Internațional” SRL din București, bonuri de compensare pentru energie electrică în valoare de 4 miliarde lei, pentru care a emis un ordin de plată falsificat prin scanarea ștampilei filialei Galați a Bancorex.

La percheziția efectuată la domiciliul lui M.I. din Săcele, jud. Brașov, pe hard discul calculatorului au fost descoperite modele de ștampile ale IPJ Suceava, utilizate pentru falsificarea autorizației de circulație provizorie a autoturismului personal.

- *Infrațiunea de fals material în înscrisuri oficiale*, reglementată de art. 288 din Codul Penal.

Un grup de 13 persoane conduse de C.O., din Coteana, jud. Olt și G.L., din București au falsificat, cu ajutorul unui calculator electronic și al unei imprimante color, vize și permise de muncă pentru Spania, acte de înmatriculare, cărți de identitate ale vehiculelor, autorizații de circulație provizorie, etc. Prejudiciul estimat s-a cifrat la 200.000.000 de lei, din care au fost recuperați 41.000.000.

- *Infrațiunea de divulgare a secretului economic*, reglementată de art. 298 din Codul Penal.
- *Infrațiunea de deturnare de fonduri*, reglementată de art. 3021 din Codul Penal.
- *Infrațiunea de propagandă naționalist-șovină*, reglementată de art. 317 din Codul Penal.

Infrațiuni săvârșite prin intermediul sistemelor informatice

Legea nr. 21/1999, pentru prevenirea și sancționarea spălării banilor a introdus pentru prima oară în legislația română noțiunea de “infrațiuni săvârșite prin intermediul calculatoarelor”. Potrivit textului art. 23, lit. a, *constituie infrațiunea de spălare a banilor*

[...] schimbarea sau transferul de valori, cunoscând ca acestea provin din săvârșirea unor infracțiuni: [...] infracțiunile săvârșite prin intermediul calculatoarelor, [...] în scopul ascunderii sau disimulării originii ilicite acestora, precum și în scop de tănuire sau de favorizare a persoanelor implicate în astfel de activități sau presupuse că s-ar sustrage consecințelor juridice ale faptelor lor.

În momentul de față, legea penală română reglementează un număr de 10 infracțiuni ce corespund definiției de mai sus. Ele sunt prevăzute în Titlul III (Prevenirea și combaterea criminalității informatice) din Legea privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției precum și în Legea dreptului de autor și a drepturilor conexe.

Legea criminalității informatice reglementează trei categorii de infracțiuni:

1. Infracțiuni contra confidențialității și integrității datelor și sistemelor informatice:
 - Infracțiunea de *acces ilegal la un sistem informatic*;
 - Infracțiunea de *interceptare ilegală a unei transmisii de date informatice*;
 - Infracțiunea de *alterare a integrității datelor informatice*;
 - Infracțiunea de *perturbare a funcționării sistemelor informatice*;
 - Infracțiunea de *a realiza operațiuni ilegale cu dispozitive sau programe informatice*.
2. Infracțiuni informatice
 - Infracțiunea de *fals informatic*;
 - Infracțiunea de *fraudă informatică*.
3. Pornografie infantilă prin sisteme informatice
 - Infracțiunea de *pornografie infantilă prin intermediul sistemelor informatice*.

Legea dreptului de autor reglementează următoarele infracțiuni:

- Infracțiunea de *permitere a accesului public la bazele de date pe calculator, care conțin sau constituie opere protejate*;
- Infracțiunea de *punere la dispoziția publicului de unor mijloace tehnice de neutralizare a protecției programelor pentru calculator*.

Accesul ilegal la un sistem informatic

Infracțiunea de acces fără drept la un sistem informatic este prevăzută în art. 42 din Legea criminalității informatice. Textul de lege prevede:

(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.

Reglementarea legală urmărește să protejeze sistemele informatice și datele stocate pe acestea de accesul neautorizat la acestea. *Sistemul informatic* este definit de lege ca fiind 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. Un *program informatic* este de asemenea definit de lege ca fiind un ansamblu de instrucțiuni care pot fi executate de un sistem informatic în vederea obținerii unui rezultat determinat. Prin *măsuri de securitate*, legea 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.

S.A, student în vârstă de 24 de ani, zis Tony-Celularu' a pătruns ilegal pe pagina de Internet oficială a Eclipsei 1999, și a modificat conținutul acesteia, înlocuind pagina principală cu un mesaj de avertizare asupra problemelor de securitate de pe situl respectiv.

În luna aprilie 1999, persoane neidentificate au pătruns pe situl de Internet al cotidianului Pro Sport, înlocuind pagina principală cu mesajul "Dragă, da' v-ați protejat, nu glumă!", semnat "Superdepartamentul IT".

Luni, 30 martie 1998, serverul Universității Ștefan cel Mare din Suceava a fost penetrat de un operator din SUA, conectat la Internet prin intermediul serverului cu adresa *pearljam.cts.com*. Pătrunderea nu s-a soldat cu pierderi de date, ele fiind recuperate după o muncă intensă de 48 de ore.

Obiectul juridic special îl constituie relațiile sociale care vizează securitatea sistemului informatic, inviolabilitatea acestuia și care sunt de natură a garanta confidențialitatea și integritatea atât a datelor cât și a sistemelor informatice.

Obiectul material este constituit de componentele sistemului informatic asupra căruia s-a îndreptat activitatea infracțională (cum ar fi discurile de stocare a datelor) sau prin intermediul cărora s-a realizat accesul fără drept (de exemplu, componentele rețelelor informatice.)

Subiectul activ poate fi orice persoană iar subiectul pasiv este proprietarul sistemului informatic sau a datelor de pe acesta.

Latura obiectivă. Elementul material al infracțiunii se realizează printr-o activitatea de acces fără drept la un sistem informatic. Accesul *fără drept* la un sistem informatic înseamnă, în sensul legii, că persoana respectivă se află în una din următoarele situații:

a) nu este autorizată, în temeiul legii sau al unui contract;

Persoanele care operează în bazele de date cu personalul unei instituții o fac în baza autorizării primite de la conducerea instituției, deoarece ele respectă legislația muncii și pe cea privitoare la datele personale.

b) depășește limitele autorizării;

Depășirea limitelor autorizării poate însemna accesul la resurse din Intranetul companiei/instituției aflate la nivele de acces superioare cele permise utilizatorului.

c) 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.

Accesul poate fi realizat mai multe tipuri de acțiuni (prezentate mai sus în capitolul IV), cum ar fi:

- *Autentificare (authenticate)* – prezentarea identității cuiva unui program și, dacă este nevoie, verificarea acestei identități, cu scopul de a primi acces pe sistemul țintă;
- *Evitarea (bypass)* – evitarea unui proces sau program folosind o metoda alternativă de a accesa ținta;
- *Citire (read)* – obținerea conținutului unui mediu de date;
- *Copiere (copy)* – reproducerea ținte fără a o modifica;
- *Furt (steal)* – preluarea posesiei unei ținte, fără a păstra o copie în locația originală.

Unele dintre aceste modalități de acces (cum ar fi evitarea sau autentificarea) se realizează prin încălcarea măsurilor de securitate, îndeplinind ipoteza formei agravante a infracțiunii, prevăzută în alin. 2 al art. 42.

Latura subiectivă este determinată de intenție, directă sau indirectă.

Consumarea se realizează în momentul obținerii propriu-zise a accesului la sistemul informatic atacat, indiferent de consecințele accesului asupra sistemului informatic și a datelor conținute de acesta. Momentul accesului poate fi determinat prin mijloace tehnice specifice (fișiere jurnal, etc.).

Tentativa se pedepsește, potrivit prevederilor art. 47.

Sanctiunea. Infracțiunea de acces ilegal la un sistem informatic este sancționată cu închisoare de la 3 luni la 6 ani sau cu amendă. Varianta agravantă este sancționată cu închisoare de la 3 la 12 ani.

Interceptarea ilegală a unei transmisii de date informatice

Infracțiunea de interceptare, fără drept, a unei transmisii de date informatice care nu este publică este prevăzută în art. 43 al Legii criminalității informatice. Textul de lege prevede:

(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.

Reglementarea legală protejează transmisiile de date informatice din cadrul sau între sisteme informatice, indiferent de modul cum se realizează acestea. *Datele informatice* sunt definite ca fiind orice reprezentare a unor fapte, informații sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic, în aceeași categorie fiind inclus și orice program informatic care poate determina realizarea unei funcții de către un sistem informatic.

Obiectul juridic special îl constituie relațiile sociale ce protejează confidențialitatea comunicațiilor. Secretul corespondenței este un drept constituțional, art. 28 din Constituția României republicată prevăzând că:

*Secretul scrisorilor, al telegramelor, al altor trimiteri poștale, al convorbirilor telefonice și **al celorlalte mijloace legale de comunicare** este inviolabil.*

Reglementarea constituie până la un punct o paralelă a infracțiunii clasice de violare a secretului corespondenței, prevăzut la art. 195 din Codul Penal. Comunicațiile în formă electronică pot însă să se refere la mai mult decât simpla corespondență, protejată în virtutea dreptului la viață privată. Din ce în ce mai multe activități sunt informatizate, atât în cadrul mediului de afaceri (vezi descrierea *Intranet*-ului, în Capitolul II al acestui Ghid) cât și în sectorul public. Titlul II, „Transparența în administrarea informațiilor și serviciilor publice prin mijloace electronice” a Legii 161/2003 creează Sistemul Electronic Național (SEN) și urmărește „promovarea utilizării Internetului și a tehnologiilor de vârf în cadrul instituțiilor publice”. Strategia Guvernului privind informatizarea administrației publice prevede de asemenea că „trebuie încurajate crearea arhivelor, garantarea calității datelor conținute și permiterea accesului larg și complet la acestea prin intermediul portalurilor de informații, care ușurează accesul prin Internet și explorarea bazei de date a administrației publice.” Toate aceste comunicații conțin date ce trebuie protejate de interceptarea lor ilegală.

Obiectul material este constituit de suportul fizic prin intermediul căruia se realizează accesul, indiferent că transferul de informații se realizează prin intermediul unor rețele prin cabluri sau de tip WLAN (una dintre situațiile reglementate de alin. 2 al art. 43). O altă situație de interceptare, prevăzută de ipoteza alin. 2 al art. 43 este cunoscută sub numele de interceptarea cablurilor și a semnalelor emise (*Wiretapping, Eavesdropping on Emanations*).

Subiectul activ poate fi orice persoană iar subiectul pasiv este proprietarul datelor interceptate fără drept.

Latura obiectivă. Elementul material este caracterizat prin acțiunea de interceptare, prin orice mijloc și folosind orice tip de unelte, a unei comunicații de natură informatică.

Latura subiectivă este caracterizată de intenție.

Consumarea se realizează în momentul realizării interceptării datelor. Infracțiunea este continuă, epuizarea ei intervenind în momentul în care interceptarea încetează, din orice motiv.

Tentativa se pedepsește, potrivit prevederilor art. 47.

Sancțiunea. Infracțiunea de interceptare ilegală a unei transmisii de date informatice se sancționează cu închisoare de la 2 la 7 ani.

Alterarea integrității datelor informatice

Infrațiunea este reglementată de art. 44 din Legea criminalității informatice, textul de lege precizând:

(1) Fapta de a modifica, șterge sau deteriora date informatice ori de a restricționa accesul la aceste date, fără drept, constituie infrațiune 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.

Reglementarea legală urmărește să protejeze datele informatice stocate în cadrul sistemelor informatice, urmărind să împiedice modificarea, ștergerea sau deteriorarea datelor informatice, restricționarea accesului la ele, transferul neautorizat de date dintr-un sistem informatic sau dintr-un mijloc de stocare a datelor informatice.

Obiectul juridic special îl constituie pe de o parte relațiile sociale ce protejează încrederea în corectitudinea datelor stocate în sistemele informatice și pe de altă parte relațiile sociale ce protejează confidențialitatea datelor stocate în sistemele informatice sau pe alte mijloace de stocare.

Obiectul material este constituit de suportul material (hard disk sau alt sistem de stocare a datelor) pe care se află datele modificate, șterse, deteriorate, transferate sau la care a fost restricționat accesul.

Subiectul activ poate fi orice persoană, iar subiectul pasiv este proprietarul datelor modificate, șterse, deteriorate, transferate sau la care a fost restricționat accesul.

Latura obiectivă. Elementul material constă în acțiunile de:

- modificare; sau
- ștergere; sau
- deteriorare; sau
- transferare; sau
- restricționare a accesului la datele respective.

Ele corespund setului de rezultate neautorizate, descrise în capitolul IV - Vulnerabilități - ale acestui Ghid.

Latura subiectivă este caracterizată de intenție.

Consumarea se realizează în momentul în care se produce una din acțiunile caracteristice elementului material. Infracțiunea este continuă, epuizarea ei intervenind în momentul în care încetează aceste acțiuni.

Tentativa se pedepsește, potrivit prevederilor art. 47.

Sanctiunea. Infracțiunea de alterare a datelor informatice se pedepsește cu închisoare de la 2 la 7 ani pentru situațiile prevăzute la alin. 1 și cu închisoare de la 3 la 12 ani pentru cea prevăzută în alin. 2.

Perturbarea funcționării sistemelor informatice

Infracțiunea, prevăzută de art. 45 al Legii criminalității informatice, este reglementată de următorul text de lege:

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.

Ieșeanul care a produs și eliberat pe Internet un virus informatic a fost trimis în judecată, sub acuzația de perturbare gravă a unui sistem informatic și deținere fără drept a unui program informatic conceput în scopul săvârșirii de infracțiuni. D.C., în vârstă de 26 de ani, absolvent al Universității Tehnice “Gh. Asachi” din Iași, a fost reținut în septembrie 2003 deoarece a virusat calculatoarele respectivei instituții, dar și computere din Belgia și Olanda, cu ajutorul unei variante modificate a virusului MsBlast.

Reglementarea legală urmărește să protejeze datele informatice stocate în cadrul sistemelor informatice. Observăm că spre deosebire de infracțiunea reglementată în articolul 44, accentul este pus aici pe efectul pe care îl au pentru sistemele informatice afectate acțiunile asupra datelor informatice (introducere, transmitere, modificare, ștergere, deteriorare, restricționarea accesului).

Obiectul juridic special îl constituie relațiile sociale ce protejează integritatea datelor informatice conținute pe suporturile specifice sistemelor informatice. Așa cum arătam mai sus, acțiunile asupra datelor conținute de sistemele informatice este reglementată de art. 44, iar efectele pe care aceste acțiuni le au asupra sistemelor informatice care le conțin și-a găsit reglementarea în prevederile art. 45.

Obiectul material este dat de sistemul informatic a cărui activitate este grav perturbată de făptuitor. Țintele atacului, așa cum au fost ele definite în capitolul IV al acestui Ghid sunt:

- *Componentă (component)* – una din părțile care formează un calculator sau o rețea;

- *Calculator (computer)* – un dispozitiv care constă în una sau mai multe componente asociate, incluzând unități de procesare și periferice și care este controlat de programe stocate intern;
- *Rețea (network)* – un grup interconectat de calculatoare, echipamente de comutare și ramuri de interconectare;
- *Internet (internetwork)* – o rețea de rețele.

Perturbarea gravă poate avea ca obiect fie întregul sistem informatic fie părți ale acestuia sau servicii sau programe deservite sau rulate de acesta.

Subiect activ poate fi orice persoană, subiectul pasiv fiind proprietarul sistemului atacat.

Latura obiectivă. Elementul material îl constituie consecințele pe care acțiunile de:

- introducere de date; sau
- transmitere de date; sau
- modificare de date; sau
- ștergere de date; sau
- deteriorare a datelor informatice; sau
- restricționarea accesului la date informatice în sau asupra sistemului informatic care le conține.

Latura subiectivă este determinată de intenție.

Consumarea se realizează în momentul producerii de perturbări asupra sistemului informatic, indiferent de momentul în care a avut loc acțiunea asupra datelor, acțiune ce face obiectul infracțiunii de la art. 44.

Tentativa se pedepsește, potrivit prevederilor art. 47.

Sanctiunea. Infracțiunea de perturbare a funcționării sistemelor informatice se sancționează cu închisoare de la 3 la 15 ani.

Operațiuni ilegale cu dispozitive sau programe informatice

Infracțiunea este prevăzută în art. 46 din Legea criminalității informatice. Textul de lege prevede:

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

- a) fapta de a produce, vinde, importa, distribui sau 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, importa, distribui sau 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.

Înscrierea acestei infracțiuni în lege urmărește să limiteze accesul la instrumente (dispozitive, programe informatice, parole, coduri de acces etc.) care permit săvârșirea infracțiunilor reglementate de legea criminalității informatice.

Obiectul juridic special îl constituie relațiile sociale ce protejează buna funcționare a sistemelor informatice de către cei îndreptățiți să le utilizeze în scopul pentru care acestea au fost create.

Obiectul material este dat de dispozitivele sau programele informatice ce facilitează înlăptuirea infracțiunilor de la art. 42-45 (infracțiunea de acces ilegal la un sistem informatic; infracțiunea de interceptare ilegală a unei transmisii de date informatice; infracțiunea de alterare a integrității datelor informatice și infracțiunea de perturbare a funcționării sistemelor informatice).

Obiectul material se concretizează în:

- dispozitive
- programe informatice
- parolă
- cod de acces
- de natură a permite accesul total sau parțial la un sistem informatic.

Conform prezentării din capitolul IV al acestui Ghid, uneltele pot consta în:

- Script sau program;
- Agent independent:
 - Virus; sau
 - Troian;
- Program integrat
- Unelte distribuite; sau
- Interceptor de date.

Subiectul activ îl constituie acele persoane care:

- produce; sau
- vinde; sau
- importă; sau
- distribuie; sau
- pune la dispoziție; sau
- deține

mijloacele de înfăptuire a infracțiunilor contra confidențialității și integrității datelor și sistemelor informatice.

Latura obiectivă. Elementul material este concretizat de acțiunile de producere, vîndere, importare, distribuire sau punere la dispoziție sau, în ipoteza alin. 2 al art. 46, deținerea de unelte de natură a permite săvârșirea infracțiunilor amintite.

Latura subiectivă este caracterizată de intenție. Nu este necesar a se proba intenția de a utiliza efectiv uneltele pentru săvârșirea de infracțiuni.

Consumarea se realizează în momentul producerii, vînderii, importării, distribuției, punerii la dispoziție sau deținerii mijloacele de înfăptuire a infracțiunilor contra confidențialității și integrității datelor și sistemelor informatice. Deținerea caracterizează o infracțiune continuă.

Tentativa se pedepsește, potrivit prevederilor art. 47.

Sanctiunea. Infracțiunea de săvârșire de operațiuni ilegale cu dispozitive sau programe informatice se sancționează cu închisoare de la 1 la 3 ani.

Falsul informatic

Infracțiunea este prevăzută în art. 48 din Legea criminalității informatice. Textul de lege prevede:

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.

Reglementarea urmărește protejarea securității juridice prin încriminarea tuturor acelor acțiuni care pot, prin modificarea unor date aflate pe suport informatic, să atragă după sine consecințe juridice nedorite de sau pentru persoanele care au conceput, realizat, implementat sau asupra cărora își manifestă efectele informația modificată.

Obiectul juridic special îl constituie relațiile sociale circumscrise protejării securității circuitului juridic.

Obiectul material îl constituie suportul pe care se află stocate datele informatice alterate în scopul producerii de consecințe juridice.

Subiectul activ poate fi orice persoană, subiect pasiv fiind fie proprietarul datelor informatice alterate în scopul producerii de consecințe juridice fie cei afectați de modificările respective.

Latura obiectivă. Elementul material este dat de acțiunea de a:

- introduce; sau
- modifica; sau
- șterge; sau
- restricționa accesul

la date informatice, în scopul producerii de efecte juridice.

Latura subiectivă este caracterizată de intenție directă.

Consumarea se realizează în momentul inițierii procesului de alterare a datelor.

Tentativa se pedepsește, potrivit prevederilor art. 50.

Sanctiunea. Infracțiunea de fals informatic se pedepsește cu închisoare de la 2 la 7 ani.

Frauda informatică

Infracțiunea este prevăzută în art. 49 din Legea criminalității informatice. Textul de lege prevede:

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.

Obiectul juridic special îl constituie relațiile sociale ce protejează patrimoniul unei persoane.

Obiectul material este dat de sistemele informatice care conțin datele informatice alterate sau care sunt împiedicate să funcționeze ca urmare a activității făptuitorului.

Subiect activ poate fi orice persoană, iar subiect pasiv poate fi orice persoană fizică sau juridică, afectată patrimonial prin acțiuni asupra sistemelor informatice pe care le deține sau pe care le utilizează.

Latura obiectivă. Elementul material îl constituie acțiunea de a:

- introduce date informatice; sau
- modifica date informatice; sau
- șterge date informatice; sau
- restricționează accesul la date informatice; sau
- împiedică funcționarea unui sistem informatic.

Latura subiectivă este caracterizată de intenție.

Consumarea se realizează în momentul acțiunii ce are ca rezultat cauzarea prejudiciului patrimonial.

Tentativa se pedepsește, potrivit prevederilor art. 50.

Sanctiunea. Infracțiunea de fraudă informatică se sancționează cu închisoare de la 3 la 12 ani.

Pornografia infantilă prin intermediul sistemelor informatice

Infracțiunea este prevăzută în art. 51 din Legea criminalității informatice. Textul de lege prevede:

(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.

Această infracțiune se află la limita între infracțiunile săvârșite cu ajutorul sistemelor informatice și cele prin sistemele informatice. Infracțiunea de pornografie infantilă este reglementată de legislația penală română în vigoare. Introducerea prevederilor de față în legea criminalității informatice dă naștere unei noi infracțiuni, diferită de cea reglementată anterior. Acest lucru se înscrie pe linia protecției copiilor prin diferite instrumente legislative la nivelul Uniunii Europene.

Pornografia infantilă este reglementată de alte două legi, și anume:

- a) Legea 678/2001 privind prevenirea și combaterea traficului de persoane, care, la art. 18, prevede:

(1) Fapta de a expune, a vinde sau a răspândi, a închiria, a distribui, a confecționa ori de a deține în vederea răspândirii de obiecte, filme, fotografii, diapozitive, embleme sau alte suporturi vizuale, care reprezintă poziții ori acte sexuale cu caracter pornografic, ce prezintă sau implică minori care nu au împlinit vârsta de 18 ani, sau importarea ori predarea de astfel de obiecte unui agent de transport

sau de distribuire în vederea comercializării ori distribuirii lor constituie infracțiunea de pornografie infantilă și se pedepsește cu închisoare de la 2 la 7 ani.

(2) Faptele prevăzute la alin. (1), săvârșite de o persoană care face parte dintr-un grup organizat, se pedepesc cu închisoare de la 3 la 10 ani.

b) Legea 196/2003 privind prevenirea și combaterea pornografiei, care, la art. 12, prevede:

(1) Distribuirea materialelor cu caracter obscen, care prezintă imagini cu minori având un comportament explicit sexual, se pedepsește cu închisoare de la 1 la 5 ani.

(2) Cu aceeași pedeapsă se pedepsește și deținerea de materiale prevăzute la alin. (1), în vederea răspândirii lor.

Obiectul juridic special îl constituie relațiile sociale ce urmăresc protejarea minorilor.

Obiectul material reprezintă suporturile de stocare a datelor din sistemele informatice ce conțin materialele pornografice cu minori. Prin *materiale pornografice cu minori* legea 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.

Subiect activ poate fi orice persoană.

Latura obiectivă. Elementul material este constituit din două modalități alternative de executare și anume:

- producerea în vederea răspândirii; sau
- oferirea; sau
- punerea la dispoziție; sau
- răspândirea; sau
- transmiterea; sau
- procurarea pentru sine sau pentru altul

de materiale pornografice cu minori prin sisteme informatice; și:

- deținerea, fără drept, de materiale pornografice cu minori într-un sistem informatic sau un mijloc de stocare a datelor informatice.

Observăm că legea nu determină ce înseamnă deținere legitimă de materiale pornografice cu minori, nici categoriile de persoane îndreptățite la deținerea lor legitimă.

Latura subiectivă este caracterizată de intenție.

Consumarea se realizează în momentul declanșării acțiunii de producere, oferire, punere la dispoziție, răspândire, transmitere, procurare sau deținere.

Tentativa se pedepsește, potrivit prevederilor alin. 2 al art. 51.

Sanctiunea. Infracțiunea de pornografie infantilă prin intermediul sistemelor informatice se pedepsește cu închisoare de la 3 la 12 ani și interzicerea unor drepturi.

Permiterea accesului public la bazele de date pe calculator ce conțin sau constituie opere protejate

Infracțiunea de permitere, fără drept, a accesului public la bazele de date pe calculator care conțin sau constituie opere protejate este prevăzută în art. 140, lit. c din legea nr. 8/1996, privind dreptul de autor și drepturile conexe. Textul de lege prevede:

Constituie infracțiune și se pedepsește cu închisoare de la o lună la 2 ani sau amendă de la 200.000 lei la 3 milioane lei, dacă nu constituie o infracțiune mai gravă, fapta persoanei care, fără a avea autorizarea sau, după caz, consimțământul titularului drepturilor recunoscute prin prezenta lege:

...

c) *permite accesul public la bazele de date pe calculator, care conțin sau constituie opere protejate*

Reglementarea legală urmărește să protejeze drepturile autorului unor baze de date pe calculator, baze de date ce constituie în sine opere protejate, sau conțin astfel de opere protejate. Prin *autor*, legea înțelege persoana fizică sau persoanele fizice care au creat opera. Prin *operă protejată*, legea înțelege opera originală de creație intelectuală în domeniul literar, artistic sau științific, oricare ar fi modalitatea de creație, modul sau forma concretă de exprimare și independent de valoarea și destinația acesteia. Legea nu definește noțiunea de bază de date. Prin *bază de date* se înțelege o colecție de date organizată conform unei structuri conceptuale care descrie caracteristicile acestor date și relațiile dintre entitățile lor corespondente, destinată unuia sau mai multor domenii de aplicație.

Obiectul juridic special al infracțiunii îl constituie relațiile sociale ce asigură respectarea dreptului patrimonial distinct și exclusiv al autorului de a autoriza accesul public la bazele de date pe calculator, în cazul în care aceste baze de date conțin sau constituie opere protejate.

Obiectul material îl formează opera sau operele protejate, fie că este vorba de baza de date în întregul său, fie de componente ale acesteia.

Subiectul. Infracțiunea poate fi săvârșită de orice persoană. Subiectul pasiv al infracțiunii este autorul operei protejate.

Latura obiectivă a infracțiunii constă în fapta persoanei care permite, fără autorizarea sau consimțământul titularului dreptului de autor, accesul public la bazele de date pe calculator, în cazul în care aceste baze de date conțin sau constituie opere protejate, dacă

fapta nu constituie o infracțiune mai gravă. Din definiția legală a infracțiunii, rezultă următoarele condiții care se cer a fi întrunite cumulativ:

- a. săvârșirea unei fapte de permitere a accesului public la bazele de date pe calculator;
- b. bazele de date pe calculator să conțină sau să constituie opere protejate;
- c. fapta să fie săvârșită fără autorizarea sau consimțământul titularului dreptului de autor;
- d. fapta să nu constituie o infracțiune mai gravă.

Urmarea imediată constă în accesul public la bazele de date protejate în tot sau în parte de dreptul de autor, fapt ce conduce la apariția unui prejudiciu material cauzat titularului dreptului de autor prin utilizarea neautorizată și fără plata remunerației cuvenite.

Latura subiectivă. Infracțiunea este săvârșită cu vinovăție sub forma intenției directe, întrucât făptuitorul are conștiința rezultatului faptei de a permite accesul public la bazele de date, și urmărește acest rezultat prin fapta sa, săvârșită fără autorizație sau consimțământ.

Consumarea acestei infracțiuni are loc în momentul în care făptuitorul permite accesul, chiar și a unei persoane, la bazele de date protejate. Permitearea accesului în mod repetat, pentru mai multe persoane, constituie infracțiune continuată, a cărei epuizare are loc în momentul în care ultima persoană a avut acces la bazele de date respective.

Tentativa nu este prevăzută.

Sanctiunea. Infracțiunea se pedepsește cu închisoare de la o lună la 2 ani, sau cu amendă de la 200.000 la 3.000.000 lei.

Punerea la dispoziția publicului a mijloacelor tehnice de neutralizare a protecției programelor pentru calculator

Infracțiunea de punere la dispoziția publicului în orice mod și cu orice titlu a unor mijloace tehnice de ștergere neautorizată sau de neutralizare a dispozitivelor tehnice de protecție a programelor pentru calculator este reglementată de art. 143, lit. a din legea nr. 8/1996 privind dreptul de autor și drepturile conexe. Textul legal prevede:

Constituie infracțiune și se pedepsește cu închisoare de la 3 luni la 2 ani sau cu amendă de la 500.000 lei la 5 milioane lei, dacă nu constituie o infracțiune mai gravă, fapta persoanei care:

- a) pune la dispoziția publicului prin vânzare sau prin orice alt mod de transmitere cu titlu oneros ori cu titlu gratuit mijloace tehnice destinate ștergerii neautorizate sau neutralizării dispozitivelor tehnice care protejează programul pentru calculator.

...

Înscrierea acestei infracțiuni în lege urmărește să apere dreptul titularului dreptului de autor asupra unui program pentru calculator de a proteja programul împotriva oricărui acces neautorizat la funcțiile acestuia, ori la datele obținute sau oferite de calculator în urma utilizării lor. Acest drept nu este *expressis verbis* formulat în lege, el fiind dedus din interpretarea corelată a dispozițiilor privitoare la drepturile autorului programului pentru calculator și a celor referitoare la prevenirea prejudiciilor produse titularului dreptului de autor sau exploatării normale a programului pentru calculator.

Prin *program pentru calculator* se înțelege o secvență de declarații și/sau instrucțiuni într-un limbaj de programare necesare soluționării unei anume funcțiuni sau a unei probleme. Observăm o inconsistență terminologică a legiuitorului care denumește în Legea criminalității informatice aceeași noțiune prin sintagma *program informatic*. *Mijloacele tehnice de protecție a programelor pentru calculator* sunt acele modalități soft (componente ale programelor pentru calculator), caracteristice securității programelor pentru calculator, ce sunt introduse de autor în vederea prevenirii faptelor de copiere și distribuire neautorizată a programelor.

Obiectul juridic special îl constituie relațiile sociale ce se formează și se dezvoltă în domeniul protecției programelor pentru calculator.

Obiectul material este format de mijloacele tehnice destinate ștergerii neautorizate sau neutralizării mijloacelor de protecție a programelor pentru calculator.

Subiectul. Infracțiunea poate fi săvârșită de orice persoană fizică, ce poate răspunde penal. Subiectul pasiv al infracțiunii este titularul drepturilor patrimoniale de autor asupra programului pentru calculator. În materia programelor pentru calculator, prin derogare de la dispozițiile comune, titularul drepturilor patrimoniale de autor este, în lipsa unor convenții contrare, angajatorul, în cazul în care programele pentru calculator sunt create de unul sau mai mulți angajați, în exercitarea funcțiilor de serviciu sau după instrucțiunile angajatorului.

Latura obiectivă constă în fapta persoanei care pune la dispoziția publicului, în orice mod, mijloace tehnice destinate ștergerii neautorizate sau neutralizării dispozitivelor tehnice de protecție a programelor pentru calculator, dacă fapta nu constituie o infracțiune mai gravă. Punerea la dispoziția publicului poate fi realizată prin vânzare sau prin alte moduri de transmitere cu titlu oneros sau cu titlu gratuit. Din definiția legii, reies următoarele condiții ce trebuie întrunite cumulativ:

- a. săvârșirea unei fapte de punere la dispoziția publicului a unor mijloace tehnice destinate ștergerii protecției programelor pentru calculator;
- b. mijloacele tehnice să realizeze ștergerea sau neutralizarea elementelor de protecție a programului pentru calculator;
- c. fapta să fie săvârșită prin vânzare sau prin orice alt mijloc de transmitere cu titlu oneros sau gratuit;
- d. fapta să nu constituie o infracțiune mai gravă.

Urmarea imediată constă în starea de pericol pentru integritatea programului pentru calculator, fapt ce permite utilizarea acestuia fără permisiunea titularului dreptului de autor.

Latura subiectivă. Infracțiunea este săvârșită cu vinovăție sub forma intenției directe.

Consumarea infracțiunii are loc în momentul în care mijloacele tehnice respective sunt puse în orice mod (inclusiv prin distribuire prin mijloace de natură electronică) la dispoziția publicului. Infracțiunea este continuă, epuizarea ei intervenind în momentul în care punerea la dispoziția publicului încetează, din orice motiv.

Tentativa nu este incriminată.

Sancțiunea acestei infracțiuni este închisoarea de la 2 luni la 3 ani, sau amendă de la 500.000 la 5.000.000 lei.

Viitorul

Din analiza datelor referitoare la criminalitatea informatică, putem evidenția următoarele tendințe de evoluție în viitor:

- *Infracțiunile informatice devin din ce în ce mai frecvente.* Societatea informațională depinde din ce în ce mai mult de calculatoare. Componente importante ale vieții sociale sunt coordonate de sisteme informatice. Ca o consecință, atacurile prin intermediul și asupra acestora se vor înmulți.
- *Infracțiunile informatice pot fi comise în zilele noastre de, virtual, orice persoană, și pot atinge, virtual, toate persoanele.* Dacă sistemele informatice constituiau, la apariția lor, un atribut al mediilor științifice, militare și guvernamentale, în ziua de astăzi, datorită creșterii performanțelor corelată cu reducerea prețurilor, ele au devenit disponibile pentru oricine.
- *Infracțiunile informatice au un caracter din ce în ce mai mobil, și din ce în ce mai internațional.* Procesarea electronică a datelor este din ce în ce mai mult convergentă cu domeniul telecomunicațiilor. Infracțiunile informatice sunt în măsură sporită comise prin intermediul rețelelor de telecomunicații.
- *Infracțiunile informatice și rețeaua Internet constituie în mod special o atracție pentru grupările crimei organizate.* Anonimitatea oferită de rețelele mondiale de calculatoare, precum și metodele de criptare a transmițerii mesajelor prin intermediul acestora, corelate cu imposibilitatea forțelor de menținere a ordinii publice de a controla fluxul de informații prezintă avantaje deosebite pentru grupările crimei organizate, inclusiv cele cu caracter transnațional.