INFRACŢIUNEA DE INTERCEPTARE ILEGALĂ A UNEI TRANSMISII DE DATE INFORMATICE

SORIN CIUTUREANU
Consilier juridic, Constanţa

1. Consideraţii introductive

Revoluţia tehnologiei informaţiei a dus la schimbări fundamentale în societate şi este foarte probabil ca aceste schimbări profunde să se producă în continuare.

Unul din efectele progresului tehnologic este impactul asupra evoluţiei telecomunicaţiilor. Comunicarea clasică, prin intermediul telefoniei, a fost depăşită de noile metode de transmitere la distanţă nu numai a vocii, ci şi a datelor, muzicii, fotografiilor ori filmelor. Aceste schimburi de informaţii nu mai apar numai între oameni, dar şi între oameni şi sisteme informatice ori numai între acestea din urmă.

Folosirea poştei electronice sau accesul la pagini web prin intermediul Internetului constituie exemple ale acestei evoluţii, modificând profund societatea noastră. Uşurinţa accesului la informaţii în sistemele informatice, combinată cu posibilităţile practic nelimitate de schimb sau diseminare a acestora, indiferent de graniţele geografice sau naţionale, a dus la o creştere explozivă a cantităţii de informaţie disponibilă şi a cunoştinţelor care pot fi extrase din aceasta. Această evoluţie a dat naştere la schimbări economice şi sociale fără precedent, dar, în acelaşi timp, foloseşte şi scopurilor mai puţin legitime: apariţia unor noi infracţiuni, ori săvârşirea infracţiunilor tradiţionale prin intermediul noii tehnologii.

Conceptele juridice existente sunt puse la încercare de apariţia noii tehnologii. Adesea, locul săvârşirii infracţiunii diferă de locul unde se găseşte infractorul. Printr-o simplă apăsare a unui buton, acesta poate declanşa catastrofe la mii de kilometri depărtare. Dreptul trebuie să facă faţă noilor provocări ridicate de dezvoltările tehnologice. Iată de ce în ultimii ani legiuitorul român a fost preocupat de elaborarea unui cadru normativ care să reglementeze accesul şi desfăşurarea activităţii prin intermediul sistemelor informatice în diferite sectoare.

În prezent, legislaţia penală română traversează o perioadă de tranziţie. Se preconizează o reformă penală de amploare, ce presupune modificări ale structurii Codului penal român. În ceea ce priveşte criminalitatea informatică, în noul Cod penal, preconizat a intra în vigoare în septembrie 2006, a fost introdus un titlu distinct, Titlul X, denumit „Delicte contra datelor şi sistemelor informatice", în care sunt preluate, cu unele modificări, infracţiunile din Legea nr.161/2003. Întrucât noile prevederi sunt mai cuprinzătoare şi respectă dispoziţiile Convenţiei Europene asupra Criminalităţii Informatice din 2001, ratificată de ţara noastră, am considerat oportun să fac referiri în completare.

În cuprinsul legii nr.161/2003 privind unele măsuri pentru asigurarea transparenţei şi exercitarea demnităţilor publice, a funcţiilor publice şi mediul de afaceri, prevenirea şi sancţionarea corupţiei[1], găsim definite trei categorii de infracţiuni, astfel:

a) *infracţiuni contra confidenţialităţii şi integrităţii datelor şi sistemelor informatice*:
- infracţiunea de acces ilegal la un sistem informatic;
- infracţiunea de interceptare ilegală a unei transmisii de date informatice;
- infracţiunea de alterare a integrităţii datelor informatice;
- infracţiunea de perturbare a funcţionării sistemelor informatice;
- infracţiunea de a realiza operaţiuni ilegale cu dispozitive sau programe informatice.

b) *infracţiuni informatice*:
- infracţiunea de fals informatic;
- infracţiunea de fraudă informatică.

c) *pornografia infantilă prin intermediul sistemelor informatice*.

2. Analiza infracţiunii prevăzută în art.43 alin. 1) din Legea nr.161/2003

Potrivit art.43 alin.1) din Legea nr.161/2003 constituie infracţiune „*interceptarea, fără drept, a unei transmisii de date informatice care nu este publică şi care este destinată unui sistem informatic, provine dintr-un asemenea sistem sau se efectuează în cadrul unui sistem informatic*".

[1] Publicată în M.Of. nr.279 din 21 martie 2003.

Constituie o modalitate asimilată infracţiunii, potrivit alin.2), „*interceptarea, fără drept, a unei emisii electromagnetice provenită dintr-un sistem informatic ce conţine date informatice care nu sunt publice*”.

Obiectul juridic special al infracţiunii este reprezentat de relaţiile sociale referitoare la telecomunicaţii şi comunicaţiile informatice, în general, respectiv la comunicaţiile de date (informatice) care nu sunt publice, în special.

Obiectul material este reprezentat de fluxul de pachete informatice (succesiunea de biţi „0” şi „1”, adică succesiunea de impulsuri electrice rezultată din variaţia controlată a tensiunii), care sunt transportate de la un echipament de calcul către altul sau în interiorul aceluiaşi sistem informatic, şi spre care se îndreaptă interesul făptuitorului.

În mod particular, obiectul material poate fi chiar suportul tehnic prin care se realizează comunicaţiile de date între echipamente, pornind de la *port*-urile de ieşire ale staţiilor de lucru (conectorii plăcilor de reţea sau telefonici ai modem-urilor) şi continuând cu cablurile de transport (de reţea sau telefonice), casetele de conexiuni (în care se găsesc comutatoarele de reţea – *switch*-urile), distribuitorii de reţea, *router*-ele etc.).

În cazul alin.2), obiectul material este constituit din energia (emisia) electromagnetică, ce radiază sau se găseşte î
N formă reziduală ori necontrolată (necontrolabilă) în imediata vecinătate a echipamentelor electronice care alcătuiesc sistemul informatic vizat. Astfel, emisia electromagnetică din jurul unui echipament (imprimantă, monitor, cablu etc.) nu va putea fi considerată drept obiect material dacă, în momentul acţiunii de interceptare (captare), acesta nu era conectat la un sistem informatic în condiţiile alin.2).

Subiect activ al infracţiunii analizate poate fi orice persoană responsabilă penal. În general, acesta este comun tuturor infracţiunilor informatice. În cazul de faţă, făptuitorul trebuie neapărat să folosească (în mod direct) anumite echipamente electronice special destinate interceptărilor în mediul IT, fără ca deţinerea unor cunoştinţe specifice în domeniu să aibă vreo relevanţă.

În particular, se pune problema cine ar fi aceste persoane interesate de urmărirea sau captarea transmisiilor electronice? Unii pot fi persoane pe care „victima” le cunoaşte, dar care au interesul de a o urmări. De exemplu, un şef (prin intermediul administratorului de reţea) ar putea fi interesat să afle dacă un subordonat transmite documente clasificate prin sistemul email al companiei. Un angajator ar dori să se asigure că angajatul nu este implicat *online* în acţiuni care ar putea să lanseze un proces de hărţuire sexuală ori fraudă informatică sau că nu îşi pierde timpul navigând pe Internet etc.

De asemenea, guvernul este foarte interesat să urmărească traseele *online* ale infractorilor sau suspecţilor în numele conceptului de combatere a criminalităţii organizate, antidrog sau siguranţă naţională. Sistemul *Carnivore* poate fi un foarte bun exemplu în acest sens.

Nu în ultimul rând, *crackerii* (hackerii maliţioşi) doresc să fure identitatea victimelor, să le vandalizeze datele ori să le stânjenească trimiţând în numele lor mesaje nepotrivite diferitelor persoane.

Participaţia este posibilă în toate formele sale: coautorat, instigare sau complicitate.

Subiect pasiv va fi persoana fizică sau juridică deţinătoare de drept a sistemului informatic ori a componentelor de legătură (transmisiuni) între două sau mai multe sisteme informatice. În mod adiacent, subiect pasiv va fi deţinătorul de drept al datelor informatice interceptate sau persoana vizată în mod direct de prelucrarea automată a acestor date[2].

Latura obiectivă. Elementul material. Prin „interceptare” (în sens tehnic) se înţelege acţiunea de a capta, cu ajutorul unui dispozitiv electronic special fabricat în acest scop sau a unui computer, impulsurile electrice, variaţiile de tensiune sau emisiile electromagnetice care tranzitează în interiorul unui sistem informatic sau se manifestă ca efect al funcţionării acestuia ori se află pe traseul de legătură dintre două sau mai multe sisteme informatice care comunică.

Interceptarea pachetelor reprezintă una dintre infracţiunile cele mai dificil de realizat şi este, de asemenea, o ameninţare serioasă la adresa comunicaţiilor prin Internet. Fiecare pachet trimis prin Internet poate tranzita un număr mare de calculatoare şi reţele înainte de a ajunge la destinaţie. Prin intermediul unui interceptor de pachete, hackerii pot intercepta pachetele de date (inclusiv cele cu mesaje de *login*, transmisii ale identificatorilor numerici ai cărţilor de credit, pachete email etc.) care

[2] A se vedea prevederile Legii nr.506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice, publicată în M.Of. nr.1101 din 25 noiembrie 2004.

călătoresc între diferite locaţii din internet. După ce interceptează un pachet, hackerul îl poate deschide şi poate fura numele *host*-ului, al utilizatorului, precum şi parola asociată pachetului. Hackerii folosesc unul dintre cele mai comune tipuri de interceptări de pachete înaintea unor atacuri IP. Experţii în materie de securitate denumesc deseori interceptarea pachetelor ca „spionaj în reţea" (*network snooping*) sau „supraveghere ascunsă" (*promiscous monitoring*).

Pentru a preveni atacurile prin interceptare asupra reţelelor distribuite, administratorii de sistem folosesc în general scheme de identificare, cum ar fi un sistem cu parolă unică (*one-time password systems*) sau un sistem de autentificare prin tichete (cum este *Kerberos*). Administratorii pot folosi o varietate de sisteme cu parolă unică. De exemplu, unele sisteme de acest gen furnizează unui utilizator următoarea parolă de intrare de fiecare dată când utilizatorul iese din sistem. Deşi atât sistemele cu parolă unică, cât şi sistemele *Kerberos* pot îngreuna sensibil interceptarea unei reţele nesecuritate pentru orice hacker, ambele metode sunt expuse la atacuri active dacă nu criptează şi nu semnează fluxul de date.

În general, un dispozitiv sau calculator intrus se poate plasa în orice punct al unui sistem informatic sau al unei reţele de calculatoare, având ca obiectiv interceptarea traficului de mesaje. Atacurile care pot fi executate sunt de două feluri[3]:

- atacuri pasive, în cadrul cărora intrusul „observă" informaţia care trece prin canal, fără să interfereze cu fluxul sau conţinutul mesajelor;

- atacuri active, în care intrusul se angajează fie în furtul mesajelor, fie în modificarea, reluarea sau inserarea de mesaje false etc.

A. *Cel mai simplu atac Hacker*[4]

Fiecare calculator dintr-o reţea are o adresă IP unică. În cazul unei conexiuni, calculatorul ataşează fiecărui pachet trimis adresa IP de destinaţie şi un număr unic, denumit „număr de secvenţă". În cadrul unei conexiuni TCP/IP, calculatorul receptor, la rândul său, acceptă numai pachete cu adrese IP şi numere de secvenţă corecte. De asemenea, multe dispozitive de securitate, inclusiv *router*-ele, permit transmisiunea în cadrul unei reţele numai spre şi dinspre calculatoarele cu anumite adrese IP. Atacul TCP/IP cu predicţia numărului de secvenţă foloseşte modalitatea de adresare a calculatoarelor în reţea şi schimburile de pachete pentru a obţine acces într-o reţea.

În esenţă, hackerul efectuează atacul TCP/IP cu predicţia numărului de secvenţă în două etape. În prima etapă, hackerul încearcă să determine adresa IP a serverului, fie prin interceptarea pachetelor din Internet, încercând în ordine unele numere de host, fie prin conectarea la un site printr-un *browser Web* şi urmărirea adresei de IP a site-ului în bara de stare. Deoarece hackerul ştie că alte calculatoare din reţea au adrese IP identice cu adresa serverului pe unele porţiuni, acesta va simula un număr de adresă IP pentru a evita *router*-ul şi a accesa sistemul ca un utilizator intern. De exemplu, dacă un sistem are adresa IP 1902.0.0.15, hackerul (care ştie că o reţea de clasă C poate conţine maximul 256 de calculatoare) va încerca să ghicească toate numerele de adresă reprezentate de ultimul octet din serie. După ce începe să încerce adresele de reţea, hackerul trece la monitorizarea numerelor de secvenţă ale pachetelor transferate de la un calculator la altul în reţea. După supravegherea transmisiunilor, hackerul va încerca să anticipeze următorul număr de secvenţă pe care îl va genera serverul, iar apoi „simulează" acel număr, plasându-se efectiv între utilizator şi server.

Deoarece dispune, de asemenea, de adresa IP a serverului, hackerul va genera pachete cu numere de secvenţă şi adresele IP corecte care îi permit interceptarea transmisiunilor cu utilizatorul. După ce hackerul a dobândit acces intern la sistem prin predicţia numărului de secvenţă, acesta poate accesa orice informaţie transmisă serverului de către sistemul de comunicaţie, inclusiv fişierele-parolă, nume de *login*, date confidenţiale sau orice alte informaţii transmise prin reţea. De obicei, un hacker va folosi predicţia numărului de secvenţă pentru a pregăti un atac mai puternic asupra serverului sau pentru a-şi asigura o bază de unde să-şi lanseze atacurile asupra unui server apropiat din reţea.

B. *Atacurile active prin desincronizare*

O conexiune TCP impune un schimb sincronizat de pachete. De fapt, dacă din anumite motive numerele de secvenţă ale pachetelor nu sunt cele aşteptate de către calculatorul receptor, acesta va

[3] V.V. Patriciu, *Criptografia şi securitatea reţelelor de calculatoare*, Editura Tehnică, Bucureşti, 1994, p.22.
[4] L. Klander, *Anti-Hacker*, Editura All Educaţional, Bucureşti, 1998, p.248.

refuza (sau ignora) pachetul şi va aştepta pachetul cu numărul corect. Hackerul poate exploata cererea de număr de secvenţă a protocolului TCP pentru interceptarea conexiunilor.

Pentru a ataca un sistem folosind atacurile prin desincronizare, hackerul induce sau forţează ambele extremităţi ale unei conexiuni TCP într-o stare desincronizată, astfel încât aceste sisteme să nu mai poată efectua schimburi de date. Apoi, hackerul foloseşte un *host* terţ (adică un alt calculator conectat la mediu fizic care transportă pachetele TCP) pentru a intercepta pachetele reale şi pentru a crea pachete de înlocuire acceptabile pentru ambele calculatoare din conexiunea originală. Pachetele generate de *host*-ul terţ mimează pachetele reale pe care sistemele aflate în conexiune le-ar fi schimbat în mod normal.

C. *Deturnarea prin postsincronizare*

Să presupunem, pentru moment, că hackerul jpoate asculta orice pachet schimbat între două sisteme care formează o conexiune TCP. În continuare, să presupunem că după interceptarea fiecărui pachet, hackerul poate falsifica orice tip de pachet IP doreşte şi să înlocuiască originalul. Pachetul falsificat al hackerului îi permite să se dea drept client sau drept server (iar mai multe pachete falsificate permit hackerului să folosească ambele identităţi). Dacă hackerul este capabil să pună în aplicare toate aceste consideraţii, atunci acesta poate determina toate transmisiunile client-server să devină transmisiuni client-hacker, respectiv server-hacker.

D. *Furtuna TCP ACK*

Atacul de deturnare detaliat anterior are un singur dezavantaj de bază, în sensul că generează pachete TCP ACK (de confirmare) în număr extrem de mare. Specialiştii reţelelor numesc aceste mari cantităţi de pachete ACK furtună TCP ACK. Când un *host* (client sau server) primeşte un pachet inacceptabil va confirma pachetul prin trimiterea numărului de secvenţă aşteptat înapoi către generatorul pachetului. Acesta este un pachet de conformare sau pachet TCP ACK.

În cazul unui atac TCP activ, primul pachet TCP ACK include propriul număr de secvenţă al serverului. Calculatorul-client nu va accepta acest pachet de conformare, deoarece clientul nu a trimis la început pachetul cu cererea modificată. Ca atare, clientul îşi generează propriul pachet de confirmare, care, la rândul său, determină serverul să genereze un alt pachet de confirmare etc., creând ceea ce se numeşte, cel puţin în teorie, un ciclu infinit pentru fiecare pachet de date trimis.

Deoarece pachetele de confirmare nu transportă date, emiţătorul pachetului ACK nu retransmite pachetul dacă receptorul îl pierde. Cu alte cuvinte, dacă un sistem pierde un pachet în ciclul de furtună ACK, ciclul se încheie. Din fericire, TCP foloseşte IP pe un nivel de reţea nesigur. Cu o rată de pierdere a pachetelor nenulă, nivelul de reţea încheie rapid ciclul. De asemenea, cu cât mai multe pachet sunt pierdute în reţea, cu atât mai scurtă este durata furtunii ACK. În plus, ciclurile ACK sunt cu autoreglare, astfel,, cu cât hackerul creează mai multe cicluri, cu atât mai mult creşte traficul primit de client şi de server, ceea ce determină o creştere a congestiei, deci a pierderilor de pachete şi, implicit, a ciclurilor încheiate.

Interceptarea informatică se poate realiza, în mod direct, prin interacţiunea făptuitorului cu componentele externe ale sistemului informatic (cabluri, comutatoare, *routere*, computere etc.). Spre exemplu, comunicaţia între două computere într-o reţea locală LAN (*Local Area Network*) a unei instituţii poate fi interceptată de un intrus după ce acesta se conectează fizic la traseul de cablu al reţelei vizate, prin secţionarea firelor şi legarea acestora (în paralel) cu cablul conectat la propriul computer unde va recepţiona fluxul de date informatice.

Indirect sau de la distanţă, interceptarea poate să ia forma utilizării unor aplicaţii specializate (aşa-numitele *sniffere* – „a mirosi”) care sunt capabile să monitorizeze traficul pachetelor într-o reţea şi să salveze datele de interes în cadrul unor fişiere de tip *log*. În general, *sniffer*-ele sunt utilizate de administratorii de reţea sau de *Internet Service Provideri* (ISP) pentru realizarea analizei de trafic în cadrul unei reţele în scop tehnic, de mentenanţă. Totodată, acestea sunt folosite de către administratorii reţelelor unor instituţii pentru monitorizarea comunicaţiilor (interne sau externe) ale angajaţilor, adesea pentru a preîntâmpina scurgerile de informaţii, desfăşurarea de activităţi ilegale în cadrul sistemului (de ex., descărcarea de programe supuse protecţiei copyright-ului, expunerea de materiale cu conţinut pornografic infantil etc.) ori chiar pentru ca managementul să aibă o reprezentare cât mai exactă a timpului petrecut de subordonaţi în reţea ori în Internet.

E. *Sistemul Carnivore*[5]

Specialiştii sunt la curent cu existenţa aplicaţiei *Carnivore*, un program controversat dezvoltat de către Biroul Federal de Investigaţii al SUA (FBI), menit să faciliteze agenţiei accesul la activităţile informatice desfăşurate de potenţialii infractori.

Deşi proiectul *Carnivore* a fost abandonat de FBI în favoarea unor sisteme informatice integrate comerciale din ianuarie 2005, programul ce promitea odată reînnoirea influenţei specifice a Biroului în lumea comunicaţiilor şi tehnologiei informaţiilor continuă să stârnească curiozitatea şi să alarmeze societatea civilă, date fiind structura şi modalităţile sale de operare.

În ceea ce priveşte evoluţia proiectului, *Carnivore* a reprezentat cea de-a treia generaţie de programe şi aplicaţii de supraveghere electronică folosite de FBI.

Informaţii despre prima versiune nu au fost niciodată date publicităţii, mulţi specialişti susţin că aceasta stă la baza unui program comercial actual denumit *Etherpeek*.

În 1997, FBI a dezvoltat şi pus în serviciu o a doua generaţie de programe de interceptare şi monitorizare IT sub titulatura *Omnivore*. Potrivit unor date furnizate chiar de FBI, *Omnivore* a fost creat în special pentru supravegherea traficului de mesaje de poştă electronică ce ajungeau (rutate) printr-un anumit ISP (*Internet Service Provider*) şi captarea acestora în funcţie de emitent (sursă). *Omnivore* a fost abandonat la sfârşitul lui 1999 în favoarea unui alt sistem, mult mai complex, intitulat *Dragon Ware Suite*, care permitea FBI să reconstruiască (recompună, reconfigureze) mesaje de e-mail, fişiere descărcate din Internet şi chiar pagini Web.

Suita de programe *Dragon Ware* era alcătuită din trei părţi:

- *Carnivore* – un program ce rula pe o platformă *Windows NT* sau 2000 în scopul captării de informaţii;

- *Packeteer* – aplicaţie de reasamblare a pachetelor de reţea captate sau a elementelor unor pagini de Web;

- *Coolminer* – aplicaţie de analiză a informaţiilor extrase (conform nor algoritmi sau criterii de căutare) din conţinutul mesajelor sau pachetelor de date captate (monitorizate).

Pe baza acestor succinte informaţii furnizate de FBI s-a putut, iniţial, contura concluzia că programul *Carnivore* nu era altceva decât un *Packet Sniffer* (Interceptor de pachete de reţea) mai evoluat.

Tehnic, *Packet Sniffing*-ul este o operaţiune larg răspândită printre administratorii de reţele, care o folosesc în scopul de a monitoriza activitatea echipamentelor, a traficului derulat sau pentru a executa programe speciale de diagnostic sau a trata diferite probleme. Un *sniffer* este un program care poate „observa" şi analiza absolut toate pachetele de date care tranzitează reţeaua la care este conectat. În mod normal, un computer este „interesat" doar de pachetele de date care îl privesc sau care îi sunt adresate şi ignoră restul traficului din reţea. Când o aplicaţie (sau un dispozitiv) *Packet Sniffer* rulează pe un computer, interfaţa acestuia cu reţeaua este automat setată pe modul „amestecat" (*promiscous*), ceea ce înseamnă că va capta şi analiza fiecare dată sau informaţie tranzitată. Adesea, cantitatea de informaţii (pachete de date) tranzitată printr-un calculator conectat la o reţea depinde de localizarea echipamentului în cadrul reţelei respective. Astfel, un „client" izolat va putea „vedea" doar un mic segment din datele traficate în cadrul reţelei, în timp ce un server de domeniu principal va putea capta totul.

Un *Packet Sniffer* poate fi setat să opereze în două moduri:

- nefiltrant – captează absolut toate pachetele de date;

- filtrant – captează doar acele pachete care conţin date de interes.

Astfel, pachetele interceptate care au în conţinut datele căutate de *sniffer*, vor fi copiate şi livrate imediat înapoi în trafic. În funcţie de configurare, *sniffer*-ul va copia datele în memorie sau direct pe *Hard Disk*-ul computerului pe care rulează.

Când un utilizator se conectează la Internet, în mod obligatoriu el se alătură unei reţele coordonate de un ISP. Această reţea va fi conectată la alte reţele deservite de alţi ISP-işti. Un eventual *sniffer* care ar rula pe serverele ISP-ului de bază va putea monitoriza activitatea utilizatorului astfel: ce pagini au fost vizitate şi ce conţinut a fost vizualizat pe respectivele pagini, căror adrese le-a fost expediat un mesaj de e-mail, conţinutul mesajelor transmise de către utilizator, conţinutul descărcat din Internet, dacă se folosesc în Internet aplicaţii audio-video sau de telefonie şi cine vizitează pagina de Web a utilizatorului.

[5] L. Bird, *Internet-Ghid complet de utilizare*, Editura Corint, Bucureşti, 2004, p.331.

În ceea ce priveşte modul de operare al aplicaţiei *Carnivore*, în general, FBI-ul obţine prim mijloace şi metode specifice date şi informaţii privind eventuala activitate infracţională a unei persoane. Pe baza acestora, agenţia obţine adesea mandat pentru începerea supravegherii operative a persoanei în cauză, în principal a comunicaţiilor. O componentă importantă a comunicaţiilor unei persoane o reprezintă astăzi Internetul. Cele mai obişnuite mandate emise prevăd posibilitatea ca FBI să procedeze la interceptarea şi copierea conţinutului mesajelor de poştă electronică.

Folosit în materia interceptărilor telefonice, termenul de „ascultarea conţinutului" (*content-wiretap*) se referă la faptul că tot conţinutul pachetelor va fi captat şi folosit. O altă modalitate este „interceptează şi urmăreşte" (*trap-and-trace*), astfel că FBI va putea să capteze doar informaţiile privind destinaţia unui anumit mesaj de e-mail sau adresa paginii de *Web* pe care suspectul a vizitat-o, fără a putea lua la cunoştinţă cu privire la conţinutul comunicărilor. Varianta inversă se numeşte *pen register* şi determină adresele de la care au fost trimise mesaje de e-mail către adresa suspectului sau cine anume (IP-urile) a vizitat un anumit site Web.

După obţinerea informaţiilor din interceptări, conform mandatului emis de instanţă, FBI contactează ISP-ul în reţeaua căruia activează suspectul şi solicită copii *back-up* ale operaţiunilor derulate de acesta *online*. În mod normal, un ISP nu păstrează informaţii despre activităţile *online* ale clienţilor ca parte a rutinei sale de *back-up*. Pentru a elimina acest „neajuns", FBI procedează la „plantarea" unui computer pe care rulează aplicaţia *Carnivore*. În esenţă, echipamentul este compus din: sistem Pentium III cu sistem de operare *Windows NT/2000*, cu 128 Mb de RAM; software de comunicaţii; aplicaţie scrisă în C++ care lucrează în conjuncţie cu programul de comunicaţii pentru interceptarea şi filtrarea pachetelor de date; un sistem de protecţie cu parolă a sistemului; un „dispozitiv de izolare în reţea", care va face aplicaţia *Carnivore* invizibilă în reţea (pentru a preîntâmpina orice atac asupra sistemului din afară); medii externe de stocare.

FBI va configura aplicaţia *Carnivore* prin furnizarea adresei IP a suspectului, astfel încât programul va intercepta numai traficul înspre sau dinspre această adresă şi va ignora celelalte pachete de date.

Copierea pachetelor de interes de la/către computerul suspectului se va face fără afectarea fluxului de pachete în reţea. Odată pachetele copiate, acestea ajung la un program de filtrare care va reţine doar pachetele corespunzătoare mesajelor e-mail. Filtrul este în măsură să determine conţinutul pachetelor pe baza protocolului SMTP.

Acest tip de supraveghere electronică nu poate dura mai mult de o lună fără un ordin expres al instanţei. De îndată ce au fost strânse datele necesare, sistemul este debranşat de la reţeaua ISP. Ulterior, datele astfel captate şi stocate sunt procesate corespunzător cu ajutorul programelor *Packeter* şi *Coolminer*. Dacă rezultatul furnizează destule dovezi, FBI le va putea folosi în cazul penal instrumentat împotriva suspectului în cauză.

La vremea dezvoltării aplicaţiei, FBI folosea *Carnivore* numai în cazuri bine determinate, cu relevanţă în lupta împotriva terorismului, pornografiei infantile şi exploatării copiilor, spionajului, războiului informaţional şi fraudelor cibernetice.

Bineînţeles, au fost (şi încă sunt) şi aspecte care au ridicat anumite semne de întrebare asupra legalităţii folosirii sistemului *Carnivore* din punctul de vedere al:

- intimităţii – oamenii au perceput utilizarea aplicaţiei drept o „violare gravă a vieţii private a unei persoane". În fapt, legalitatea interceptării este pe deplin asigurată de mandatul sau ordinul instanţei de judecată, singura în măsură să analizeze gravitatea faptelor imputabile unei persoane;

- reglementării – a existat o temere generală cu privire la posibilitatea ca sistemul să permită Guvernului un control strict asupra resurselor Internet. Însă, pentru ca acest lucru să fie posibil, ar fi fost necesară o infrastructură gigantică, cu puncte de lucru la fiecare ISP din lume, ceea ce este aproape imposibil;

- libertatea de exprimare – oamenii trăiesc cu impresia că acest gen de instrumente de interceptare sunt programate să filtreze conţinuturile tuturor mesajelor de poştă electronică ce ar conţine cuvinte comune, nu doar a acelora care ar putea reprezenta dovezi privind implicarea în activităţi infracţionale, ceea ce ar însemna o îngrădire a libertăţii de opinie sau de exprimare;

- *Echelon* – mulţi specialişti au făcut adesea referire la utilitarul *Carnivore* ca făcând parte din sistemul integrat *Echelon*, dezvoltat de Agenţia pentru Securitate Naţională a SUA (NSA) – specializată în spionaj electronic şi protecţie a telecomunicaţiilor guvernamentale americane.

F. *Banala tastatură – aliata spionilor*[6]

Pentru a descoperi ce se află într-un sistem informatic, persoanele interesate au la dispoziţie o nouă metodă diabolic de simplă, căreia nu-i rezistă nici un *Firewall*, antivirus sau alt program de securitate informatică. În esenţă, se pot decoda sunetele produse de butoanele tastaturii.

Cercetătorii de la Berkley, Universitatea California, au descoperit că o simplă înregistrare a sunetelor produse de tastatură poate fi folosită pentru descifrarea textului scris de utilizator, indiferent dacă este o parolă, o scrisoare de dragoste sau un secret de stat.

Experţii în computere ai renumitei instituţii academice au înregistrat timp de 10 minute sunetele produse de o tastatură. Fişierul audio rezultat a fost introdus într-un computer şi „decriptat" cu ajutorul unui software special. Au fost recuperate cu exactitate 96% din caracterele scrise de utilizator. Asta înseamnă că textul a putut fi dedus fără nici o problemă, chiar dacă mai lipsea câte o literă la câteva cuvinte.

Cercetări asemănătoare au fost făcute de doi experţi ai IBM: Rakesh Agrawal şi Dimitri Asonov. Aceştia au reuşit să descifreze 80% din text. În cazul IBM, studiul a fost făcut în cazul unei singure persoane, care a utilizat aceeaşi tastatură, cu ajutorul unui algoritm bazat pe un text cunoscut şi a unei mostre de sunet corespunzătoare.

Spre deosebire de studiile IBM, programul de decriptare folosit de cercetătorii de la Berckley descifrează scrisul, indiferent de stilul de tastare folosit de diverşi utilizatori şi filtrează fără probleme zgomotele de fond din încăpere[7].

Aceasta înseamnă că utilizatorul nu prea are la dispoziţie metode de protecţie, în caz că cineva se hotărăşte să-i „asculte" sunetele tastaturii de la distanţă. Microfoanele direcţionale capabile să înregistreze o şoaptă de la sute de metri distanţă există pe piaţă de zeci de ani. De asemenea, aparate cu laser care înregistrează sunetele dintr-o încăpere analizând vibraţia ferestrelor. Ultimul refugiu al secretelor rămâne camera izolată fonic, fără ferestre.

O altă metodă de interceptare indirectă sau de la distanţă o constituie folosirea programelor tip *keylogger, adware, spyware*. Programele de tip *adware şi spyware* se încarcă automat în PC-ul personal în momentul vizitării unei anumite pagini Web. Scopul lor este de a înregistra „traseul *online*" şi transmite înapoi celor care le-au trimis (de obicei este vorba despre companii care fac comerţ prin Internet, firme de marketing şi publicitate) date şi informaţii despre preferinţele utilizatorului în materie de pagini Web, conţinut tematică etc.[8] Un program *keylogger* este o aplicaţie specializată care înregistrează fiecare tastă pe care o apasă un utilizator şi trimite informaţiile către persoana care a instalat programul. Acest software poate extrage informaţii extrem de folositoare pentru un hacker, cum ar fi numărul cărţii de credit, rapoarte ale companiei, informaţii secrete dintr-o instituţie sau date cu caracter financiar. Tot în aceeaşi gamă există şi programele de monitorizare a email-urilor (*Websense, MIMEsweeper, FastTrack* etc.).

În alin.2) este prevăzută o modalitate asimilată de săvârşire a infracţiunii, respectiv interceptarea, fără drept, a unei emisii electromagnetice provenite dintr-un sistem informatic ce conţine date informatice care nu sunt publice. Aceasta presupune captarea emisiilor parazite ori a câmpurilor electromagnetice prezente (pe o anumită distanţă determinată ştiinţific) în jurul oricărui dispozitiv tranzitat de impulsuri electrice sau electromagnetice. Astăzi este de notorietate modalitatea modernă prin casre persoane interesate captează, cu ajutorul unor dispozitive speciale, radiaţiile electromagnetice existente în imediata vecinătate a monitorului computerului ţintă, pe care le „traduc" transformându-le în impulsuri electrice şi, mai apoi, în caractere alfanumerice. Tehnologia de protecţie a sistemelor de calcul împotriva captării emisiilor se numeşte TEMPEST – *Transient ElectroMagnetic Pulse Emanation STandardizing*.

G. *Securitatea radiaţiilor*[9]

Toate echipamentele are funcţionează pe bază de energie electrică produc energie electrică, emisă prin semnale electromagnetice necontrolabile, transmisibile prin aer, ca undele radio, sau de-a lungul firelor sau materialelor conductibile, ca orice curent electric. Este în natura lucrurilor un astfel de fenomen şi nimic nu îl poate stopa. Astfel de radiaţii de la calculatoare sau de la cablurile de

[6] http://www.berkeley.edu.
[7] http://www.securizare.ro/informatii/banala-tastatura-aliata-spionilor.html.
[8] L. Bird, op.cit., p.329.
[9] D. Oprea, op.cit., p.207.

comunicaţii pot fi purtătoare de informaţii, ce pot fi extrase de către persoane interesate din afară, după o analiză mai specială.

Protecţia echipamentelor de prelucrare automată a datelor utilizate pentru informaţiile speciale împotriva riscului generat de propriile lor radiaţii este una dintre cele mai dificile probleme puse în faţa agenţiilor specializate. Ele nu sunt de competenţa utilizatorilor finali şi nici a personalului cu atribuţii în cadrul sistemelor, dar este foarte important ca aceştia să cunoască şi să conştientizeze efectele unor astfel de procese.

Zgomotele care însoţesc funcţionarea sistemelor informatice se numesc „radiaţii acustice". În paralele cu acestea, echipamentele electronice şi cele electromagnetice mai furnizează în mediul înconjurător şi „radiaţii electrice sau electromagnetice".

În general, complexitatea radiaţiilor emise de echipamente depinde de felul lor şi de mediul în care se utilizează:

a) echipamentele periferice, în special imprimantele şi aparatura video, emit semnale puternice, fără zgomote, ce pot fi uşor „percepute" de la distanţă;

b) semnalele produse de unitatea centrală de prelucrare sunt mult mai complexe şi mai greu de descifrat. De asemenea, zonele aglomerate cu multe echipamente video şi imprimante, cum sunt oficiile de calcul, produc semnale sesizabile mai greu, dar nu imposibil de descifrat, prin „citirea" numai a unora dintre ele, cele care prezintă interes pentru atacatori;

c) modul în care un echipament anume produce radiaţii depinde, în mare parte, de măsurile de protecţie încorporate în fazele de proiectare, fabricaţie, instalare şi utilizare ale respectivului echipament;

d) de regulă, radiaţiile de la un echipament de birou pot fi detectate de la o distanţă de până la 100 de metri, deşi există şi numeroase excepţii.

Pentru preîntâmpinarea sau diminuarea pericolelor radiaţiilor s-au realizat echipamente speciale, despre care literatura de specialitate are următoarele păreri:

- există o mare preocupare pe linia promovării şi comercializării aparaturii de distrugere a radiaţiilor necontrolate tip TEMPEST. În Marea Britanie a fost mediatizată descoperirea unui cercetător care a demonstrat că oricine dispune de un aparat TV cu anumite modificări, ar putea citi ecranul unui computer de la o distanţă de 15 km;

- semnalele interceptate sunt numai cele care se transmit la un moment dat. Pentru detectarea datelor cu regim special, cum ar fi cazul parolelor, trebuie să fie urmărite toate radiaţiile, ceea ce presupune un mare consum de timp şi de resurse;

- pentru a se obţine un semnal corect şi util, este nevoie ca atacatorii să se situeze la o distanţă optimă, care să le permită efectuarea cu succes a interceptării. Ori, în cazul unui microbuz străin staţionat în apropierea unui centru de calcul, practic în zona de securitate, oricine poate să-i sesizeze prezenţa şi să-i anunţe pe cei în drept. Echipamentele cu gabarit mai redus sunt mai puţin performante, iar cele portabile au o utilitate foarte mică;

- fenomenul captării radiaţiilor necontrolate nu este foarte lesne de realizat. Acest lucru presupune înalte cunoştinţe tehnice, echipamente scumpe, timp şi şansă, dar şi expunerea persoanei care interceptează la un mare risc (în cazul interceptării ilegale).

Există un număr substanţial de măsuri, relativ ieftine, de diminuare a pericolului răspândirii datelor prin intermediul radiaţiilor necontrolate. Dintre ele amintim:

a) zonele sterile – se recomandă crearea unor zone sterile în jurul echipamentelor de prelucrare automată a datelor, în special al monitoarelor şi imprimantelor, prin îndepărtarea tuturor corpurilor metalice din apropierea lor. Nu se recomandă folosirea birourilor metalice, nici măcar cu picioare din metal şi nici coşuri de gunoi metalice;

b) telefoanele – monitoarele sunt veritabile surse de informaţii, iar pentru bunul mers al operării, alături de ele se plasează telefonul, numai că, în timp ce datele se afişează pe ecran, telefonul, chiar dacă este în repaus, poate transmite datele oriunde în afara organizaţiei. De aceea, pe cât posibil, toate componentele telefonului, inclusiv cablurile, să fie ţinute la distanţă de echipamentele ce prelucrează date speciale;

c) curenţii filtranţi – radiaţiile necontrolate pot fi diminuate prin transmiterea în cablu a unor curenţi filtranţi;

d) accesul – un rol important va reveni controlului accesului în organizaţie al persoanelor sau al prezenţei vehiculelor în apropierea centrului de prelucrare a datelor;

e) amplasarea echipamentelor în birouri – este recomandat a se evita plasarea echipamentelor de calcul lângă ferestre, monitoarele se vor poziţiona cu ecranele spre interiorul camerei, deşi radiaţiile necontrolate pot fi oricum interceptabile. De asemenea, se vor plasa toate componentele fizice în centrul sălii sau clădirii, pentru a beneficia de rolul protector al zidurilor şi altor materiale izolatoare;

f) echipamentele moderne – seturile actuale de echipamente electronice de calcul tind să dea mai puţine radiaţii în afară decât vechile modele. Preocupările au fost concentrate spre protejarea operatorilor de a nu mai fi expuşi radiaţiilor, ceea ce a dus implicit la diminuarea radiaţiilor necontrolate;

g) curăţirea ecranelor – scurgerile de date pot avea loc doar atunci când ele sunt afişate pe ecran sau în timpul procesului de imprimare. Personalul va trebui instruit să şteargă ecranul după ce nu mai are nevoie de datele afişate şi, de asemenea, nu se recomandă listarea de probă de prea multe ori a documentelor ce conţin date secrete;

h) derutarea – datele importante pot fi protejate prin crearea unui val de scurgeri de informaţii nesemnificative, ceea ce se concretizează prin aglomerarea, în jurul pieselor de bază ale centrului de prelucrare automată a datelor, a unor echipamente care să prelucreze date lipsite de importanţă, dar care vor fi interceptate de inamicii sistemului.

O cerinţă a existenţei infracţiunii este aceea ca făptuitorul *să fi acţionat fără drept*. Actul va fi legitim dacă persoana care procedează la interceptare:

- are dreptul de a dispune de datele cuprinse în pachetele de transmisie (este cazul proprietarilor sau deţinătorilor sistemelor informatice);

- dacă acţionează în baza unui contract, la comanda sau cu autorizaţia participanţilor la procesul de comunicaţie (este cazul administratorilor de reţea, furnizorilor de servicii Internet – ISP);

- dacă datele sunt destinate uzului propriu sau marelui public;

- dacă, pe fondul unei dispoziţii legale specifice, supravegherea este autorizată în interesul securităţii naţionale sau pentru a permite serviciilor speciale ale statului să aducă la lumină infracţiuni grave (este cazul organelor specializate care deţin aparatură corespunzătoare şi sunt abilitate prin lege).

Orice acţiune care se situează în afara celor de mai sus sau depăşeşte termenii de legitimitate va fi considerată în mod automat ca fiind fără drept.

Urmarea imediată şi legătura de cauzalitate. Din punct de vedere fizic, urmarea constă în interferenţa cu căile prin care se realizează comunicaţiile de date. Spre exemplu, branşarea la cablurile de fibră optică ce leagă un sistem „client" de unul „server" într-o reţea.

Din punct de vedere juridic, sub aspectul consecinţelor pe care acţiunea incriminată le are asupra valorii sociale ce constituie obiectul juridic, urmarea este tocmai starea de pericol, de ameninţare, pentru valoarea socială pe care legea penală o apără.

Între activitatea făptuitorului şi urmarea produsă trebuie să existe o legătură de cauzalitate. Aceasta rezultă *ex re*, adică din materialitatea faptei.

Latura subiectivă. Infracţiunea de interceptare ilegală se comite numai cu intenţie directă. Din analiza elementului material al laturii obiective, rezultă că este imposibil ca făptuitorul, prevăzând rezultatul acţiunii sale, să capteze (şi, eventual, să înregistreze) pachetele de date ale unei comunicaţii într-un sistem informatic sau între două astfel de sisteme, fără să urmărească acest lucru, acceptând numai posibilitatea producerii rezultatului.

Forme. Modalităţi. Sancţiuni şi aspecte procesuale

Actele pregătitoare, deşi posibile, nu sunt incriminate şi, ca atare, nu sunt pedepsite. Anumite acte pregătitoare sunt incriminate ca infracţiuni de sine stătătoare, cum ar fi art.42 – accesul ilegal la un sistem informatic ori art.46 – operaţiuni ilegale cu dispozitive sau programe informatice. Tentativa se pedepseşte (art.47 din lege). Consumarea infracţiunii se realizează în momentul interceptării fără drept a unei transmisii de date informatice sau a emisiei electromagnetice a uneia din componentele sistemului informatic.

Infracţiunea analizată prezintă două modalităţi normative, respectiv interceptarea unei transmisii de date şi captarea emisiei electromagnetice radiante. Acestor modalităţi normative pot să le corespundă variate modalităţi de fapt. Pentru ambele forme ale infracţiunii, pedeapsa principală este închisoarea de la 2 la 7 ani[10].

Acţiunea penală se pune în mişcare din oficiu.

[10] Aceeaşi pedeapsă principală este prevăzută şi la art.441 din noul Cod penal. În plus, persoana juridică se sancţionează cu amendă între 1.000 şi 500.000 RON, la care se pot adăuga una sau mai multe din pedepsele complementare.