ANALIZA INFRACȚIUNILOR INFORMATICE INCRIMINATE ÎN LEGISLAȚIA ÎN VIGOARE ŞI DIN PERSPECTIVA NOULUI COD PENAL

Florescu Valentin valentin@ici.ro

Florescu Gabriela gflores@ici.ro

Institutul Național de Cercetare Dezvoltare în Informatică - ICI București

Rezumat: Acest articol se adresează cititorului fără cunoştinţe speciale în domeniul juridic. Se analizează pe scurt infracțiunile cibernetice renunțându-se la exprimări specifice ştiinţei dreptului, pentru a face informațiile cât mai clare, venindu-se în întâmpinarea principiului general de drept "Nemo censetur ignorare legem" (Nimeni nu poate invoca necunoaşterea legii).

Pentru a preveni şi combate criminalitatea informatică, cu asigurarea respectării drepturilor omului şi protecției datelor personale, statele membre ale Consiliului Europei, împreună cu Statele Unite, Canada, Japonia şi Africa de Sud cu statut de observatori, au conceput şi apoi au semnat (mai puțin SUA) în data de 23-XI-2001, "Convenția asupra criminalității cibernetice" iar în data de 28 ianuarie 2003, a fost remis spre ratificare statelor membre ale Consiliului Europei, „Protocolul Adițional pentru Convenția asupra criminalității cibernetice", privind incriminarea actelor de natură rasială şi xenofobă comise prin intermediul sistemelor informatice care a fost semnat de țara noastră la 9 octombrie 2003.

Prin aceste acte a fost stabilită baza juridică penală necesară anchetării, sancționării şi cooperării internaționale în problematica infracțiunilor informatice.

Legiuitorul Român a reglementat în spiritul „Convenției asupra criminalității cibernetice" a Consiliului Europei această materie, în Titlul III al Cărții I intitulat „Prevenirea şi combaterea criminalității informatice", articolele 34 - 67 din cadrul legii penale speciale 161/2003 – „Privind unele măsuri pentru asigurarea transparenței şi exercitarea demnităților publice a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției".

În noul Cod Penal al României, infracțiunile informatice sunt reglementate ținând cont de directivele Convenției Consiliului Europei din data de 23-XI-2001 asupra criminalității cibernetice, ceea ce face ca prevederile din Legea 161/2003, să fie transferate noului Cod, ca atare sau cu modificări alături de noi reglementări.

Cuvinte cheie: infracțiuni informatice, cod penal, legislație.

Abstract: This article addresses the reader without law background. It briefly reviews cybercrime giving up the specific expression of law science to make clear information as may come to meet the general principle of law "Nemo censetur ignorare legem" (No one can claim not knowing the law).

To prevent and combat cybercrime, ensuring human rights and data protection, Member States of the Europe Council, together with the United States, Canada, Japan and South Africa as observers, were designed and then signed on 23-XI-2001 (less USA), "Convention on cyber crime" and on January 28, 2003, was submitted for ratification by Member States of the Europe Council, "Additional Protocol to the Convention on cyber crime", regarding the incrimination of acts of racial and xenophobic nature committed through computer systems, which was signed by our country on 9 October 2003.

By these acts, it was established the legal basis necessary in criminal investigations, sanctions and international cooperation in cybercrime issues.

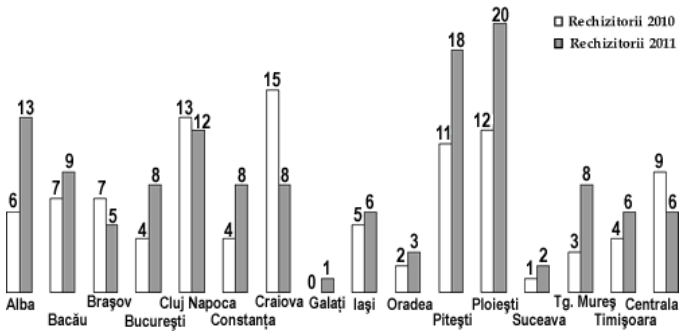
Romanian legislator has regulated in the spirit of "Convention on cyber crime" of Council of Europe that matter, in Title III of Book I, entitled "Preventing and combating cybercrime", Articles 34-67 of the special criminal law 161/2003 - "On some measures to ensure transparency and public exercise of senior civil service and in business environment, corruption preventing and punishing."

In the new Criminal Code of Romania, cybercrimes are covered by the directives given by Council of Europe Convention of 23-XI-2001 on cybercrime, which makes the provisions of Law 161/2003, be transferred to the new Code, as such or with changes and new regulations.

Key words: Cybercrime, Criminal Code, Legislation.

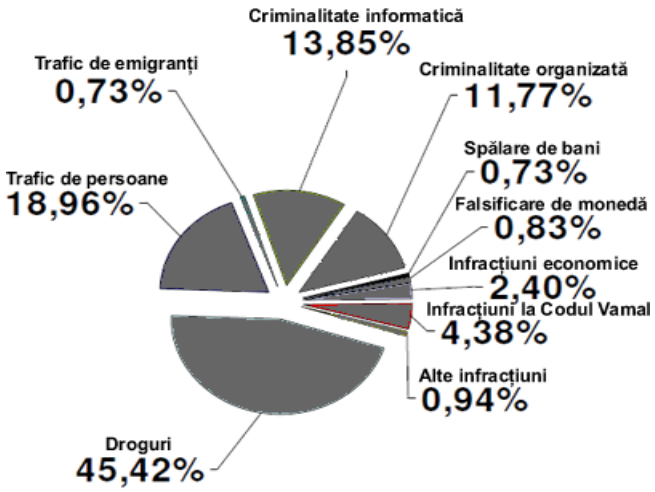
1. Statistici elaborate de Direcția de Investigare a Infracțiunilor de Crimă Organizată şi Terorism (DIICOT), Serviciul de Prevenire şi Combatere a Criminalității Informatice

Conform raportului de activitate pe anul 2011 realizat de DIICOT [5], se poate prezenta o imagine clară a fenomenului de criminalitate informatică.



Criminalitatea informatică comparativă pe anii 2010/2011

Harta judeţelor cu criminalitate informatică ridicată şi ţările preferate pentru desfăşurarea activităţilor infracţionale



Ponderea infracţiunilor pe anul 2011

Infracţiunea predilectă a infractorilor informatici din ţara noastră se referă la licitaţia frauduloasă pe Internet. Acest tip de infracţiune are o asemenea amploare la nivel internaţional, încât organizaţia americană *Internet Crime Compliant Center* (IC3), (înfiinţată de *FBI* şi partener al *National White Collar Crime Center* (NW3C)), care primeşte plângerile în chestiunea infracţiunilor informatice, o pune pe o poziţie distinctă în nomenclatorul său de infracţiuni informatice, sub numele de „licitaţia fraudată – România" [8], [9] .

Compania *ThreatExpert* care monitorizează atacurile informatice la nivel global, raportează că ţările din care provin cu preponderenţă infracţiunile informatice sunt: China 31%, Federaţia Rusă

22%, Brazilia 8%, Marea Britanie 6%, Statele Unite ale Americii 6%, Spania 4%, Germania 4%, Alţii 19% (Include: Canada, India, Iran, Algeria, Egipt, Siria, Irak, Arabia Saudită, Coreea de Sud, şi Turcia) [10].

Se prognozează creşterea ameninţării din partea infractorilor cibernetici din America Centrală şi de Sud, unde 7 din primele 10 ţări mai dezvoltate sunt înregistrate cu atacuri şi distribuiţii de aplicaţii pentru calculator destinate producerii de infracţiuni.

Explicaţii terminologice

Legea penală specială 161/2003 [4] stabileşte din punct de vedere juridic, în art. 35, sensul noţiunilor de „sistem informatic", „prelucrare automată a datelor", „program informatic", „date informatice", „furnizor de servicii", „date referitoare la traficul informaţional", „date referitoare la utilizatori", „măsuri de securitate" [1].

Termenii şi expresiile de mai sus, au următorul înţeles:

- sistem informatic = orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relaţie funcţională, dintre care unul sau mai multe asigură prelucrarea automată a datelor, cu ajutorul unui program informatic;
- prelucrare automată a datelor = procesul prin care datele dintr-un sistem informatic sunt prelucrate prin intermediul unui program informatic;
- program informatic = un ansamblu de instrucţiuni care pot fi executate de un sistem informatic în vederea obţinerii unui rezultat determinat;
- date informatice = orice reprezentare a unor fapte, informaţii sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic. În această categorie se include şi orice program informatic care poate determina realizarea unei funcţii de către un sistem informatic;
- furnizor de servicii:

  a) orice persoană fizică sau juridică ce oferă utilizatorilor posibilitatea de a comunica prin intermediul sistemelor informatice,

  b) orice altă persoană fizică sau juridică ce prelucrează sau stochează date informatice pentru persoanele prevăzute la pct. 1 şi pentru utilizatorii serviciilor oferite de acestea;
- date referitoare la traficul informaţional = orice date informatice referitoare la o comunicare realizată printr-un sistem informatic şi produse de acesta, care reprezintă o parte din lanţul de comunicare, indicând originea, destinaţia, ruta, ora, data, mărimea, volumul şi durata comunicării, precum şi tipul serviciului utilizat pentru comunicare;
- date referitoare la utilizatori = orice informaţie care poate duce la identificarea unui utilizator, incluzând tipul de comunicaţie şi serviciul folosit, adresa poştală, adresa geografică, numere de telefon sau alte numere de acces şi modalitatea de plată a serviciului respectiv, precum şi orice alte date care pot conduce la identificarea utilizatorului;
- măsuri de securitate = folosirea unor proceduri, dispozitive sau programe informatice specializate, cu ajutorul cărora accesul la un sistem informatic este restricţionat sau interzis pentru anumite categorii de utilizatori;

Prin materiale pornografice cu minori = se înţelege 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, deşi nu prezintă o persoană reală, simulează, în mod credibil, un minor având un comportament sexual explicit.

- acţionare fără drept = persoana care se află într-una din următoarele situaţii:

[1] Expunerea de motive la proiectul legii privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei, pag. 4.

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

b) depăşeşte limitele autorizării,

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 desfăşura cercetări ştiinţifice sau de a efectua orice altă operaţiune într-un sistem informatic.

În legea penală specială nr.161/2003 [3] sunt prevăzute **categoriile de infracţiuni cibernetice:**

1. 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.

2. Infracţiuni informatice:

- infracţiunea de fals informatic;
- infracţiunea de fraudă informatică.

3. Pornografia infantilă prin intermediul sistemelor informatice.

2. Analiza infracţiunilor cibernetice

În general sau generic, prin incriminarea infracţiunilor informatice, legiuitorul apără relaţiile sociale care se referă la ocrotirea datelor care se găsesc în interiorul sistemelor informatice şi a sistemelor informatice în sine.

2.1 Infracţiuni contra confidenţialităţii şi integrităţii datelor şi sistemelor informatice

2.1.1 Infracţiunea de acces ilegal la un sistem informatic

Este incriminată în art. 42 al legii şi distinge trei etape în ceea ce priveşte gravitatea acestei fapte, respectiv: accesul fără drept, care este infracţiunea de bază, la care se adaugă prima condiţie agravantă, aceea a accesului în scopul obţinerii de date informatice şi a doua condiţie agravantă, anume accesul prin încălcarea măsurilor de securitate.

Ce apără legiuitorul sau care este obiectul juridic special al acestei incriminări?

În special, în situaţia acestui tip de infracţiune, sunt apărate juridic relaţiile sociale dezvoltate în baza integrităţii datelor şi a securităţii sistemului informatic dar în secundar şi relaţiile sociale dintre persoanele titulare de drepturi (adică deţin un drept) asupra sistemului sau a informaţiilor stocate în acel sistem accesat fără drept, ţinând cont de faptul că proprietarul sistemului nu este obligatoriu şi proprietarul informaţiilor stocate în sistemul său.

De exemplu: accesul neautorizat la un sistem informatic din domeniul transportului aerian de pasageri (aeroport) loveşte atât în siguranţa pasagerilor, cât şi în instituţia sau persoana titulară a sistemului penetrat ori a informaţiilor accesate, care, aparţin mai multor companii aeriene de transport.

De asemenea, din punct de vedere fizic, material sunt apărate echipamentele electronice şi electromecanice care compun sistemele informatice: calculatoare, reţele de calculatoare cu echipamentele specifice care le compun, echipamente periferice, cabluri electrice sau cabluri optice, canalele radio, blocuri de memorie, servere etc. dar şi programele şi aplicaţiile care rulează în sistemul informatic, baze de date şi datele informatice conţinute de sistem, care reprezintă ţinta infractorului.

Cine poate fi infractorul, sau subiectul activ al infracțiunii?

Textul incriminării nu prevede o anumită calitate persoanei. Rezultă că orice persoană ce întruneşte condițiile generale pentru a răspunde penal, poate avea rolul de subiect activ, inclusiv persoana juridică cu limitările şi în condițiile prevăzute în art. 19^1 Cod penal [2].

Participanți la săvârşirea acestei ilegalități, care răspund în fața legii alături de autorul infracțiunii sunt: coautorii, instigatorii sau complicii.

În unele studii, se propagă ideea că subiectul activ ar trebui să posede cunoştințe în domeniul tehnologiei informației, ceea ce nu este neapărat adevărat datorită faptului că, programele specializate, care joacă rolul de unelte în săvârşirea infracțiunii, împreună cu descrierea modului de utilizare, se găsesc în mod liber pe site-urile unor persoane sau grupuri de persoane cunoscătoare ale tehnologiilor informatice şi care le publică pentru a-şi a câştiga notorietate.

Prin urmare nu are nici o relevanță faptul că subiectul activ este expert în sisteme de calcul şi rețelele de calculatoare, familiarizat cu tehnici de înlăturare a măsurilor de securitate (cu toate că aceştia sunt cei mai mulți) sau nu are cunoştințe în domeniu.

Cine este victima infractorului sau subiectul pasiv?

Poate fi persoana fizică sau juridică deținătoare de drept a sistemului informatic.

Concomitent, în secundar, poate fi şi altă persoană decât deținătoarea sistemului informatic, în cazul în care datele informatice vizate de accesul ilegal se referă la o persoană fizică sau juridică, alta decât deținătoarea sistemului informatic, de exemplu, făptuitorul accesează ilegal, fără drept, serverul de date privind personalul angajat al unei instituții, de unde extrage date confidențiale personale ale angajaților. Pentru această dispoziție legală, nu prezintă interes modul sau scopul în care făptuitorul utilizează aceste informații, aceasta făcând subiectul unui alt tip de infracțiune.

Din punct de vedere obiectiv, din ce constă fapta incriminată sau elementul material al infracțiunii?

Constă în accesul fără drept, într-un sistem informatic (a cărui complexitate nu prezintă interes) sau rețea informatică.

Accesul la un sistem informatic desemnează intrarea la nivelul informațiilor conținute de acel sistem informatic indiferent de modul în care se face aceasta: fizic, exploatând resursele proprii de comunicare ale sistemului sau de la distanță, prin rețeaua Intranet a unei instituții, rețeaua globală Internet sau în orice alt mod şi prin orice tip de legătură: cablu electric, cablu telefonic, cablu optic, radio, radiosatelit, etc.

Accesul fără drept la un sistem informatic înseamnă interacțiunea făptuitorului cu sistemul de calcul vizat prin intermediul echipamentelor periferice de control: tastatura, mouse-ul sau touchscreen-ul. Esențial pentru existența elementului material al acestei norme de incriminare este ca accesul la sistemul informatic să se realizeze de către persoana care se află într-una din următoarele situații: nu este autorizată în temeiul legii sau al unui contract, depăşeşte limitele autorizării, 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 desfăşura cercetări ştiințifice sau de a efectua orice altă operațiune într-un sistem informatic, adică fără drept, în înțelesul dat de lege.

Nu este necesar ca accesul fără drept să se exercite numai prin acționarea fizică, nemijlocită, a sistemului de către făptuitor. Acesta poate fi manipulat şi de la distanță prin intermediul rețelei de calculatoare dacă sistemul țintă este conectat la ea.

Condiția agravantă a accesării fără drept în scopul de a obține date informatice se materializează dacă acestea pot fi vizualizate de către făptuitor pe un monitor sau copia pe diferite suporturi, cum ar fi listarea lor pe hârtie prin intermediul unei imprimante, copierea pe un suport extern de stocare magnetic, optic sau de orice altă natură.

În condiția agravantă de acces prin încălcarea măsurilor de securitate, făptuitorul va acționa asupra sistemului informatic prin forțarea măsurilor de securitate, care pot fi de natură fizică, prin izolarea sistemelor informatice într-un loc securizat prin dispozitive mecanice cu cheie sau cifru,

camere de luat vederi cu înregistratoare, senzori de mişcare etc. sau logică, prin parole, criptarea datelor conținute, etc.

Forțarea unei protecții fizice dublează infracțiunea de acces fără drept a sistemului informatic, cu aceea de furt calificat conform art. 209 lit. i Cod penal [2].

Forțarea unei protecții logice variază de la încercarea de aflare a combinației corecte prin introducerea repetată, de la tastatură, a unor secvențe alfanumerice, până la rularea unor programe specializate care identifică secvența de acces, ori comandă sistemului anumite instrucțiuni ce permit eludarea dispozitivului logic de blocare.

De reținut că măsurile de securitate reprezintă parte integrantă a sistemului informatic, în consecință consumarea infracțiunii se realizează atunci când intrusul acționează asupra măsurilor de securitate, indiferent dacă a reuşit sau nu neutralizarea ori înlăturarea acestora, nu numai când făptuitorul accesează resursele sistemului informatic în mod direct sau de la distanță.

Tentativa se pedepseşte în conformitate cu prevederile art. 47 al legii [4].

Cum se sancționează?

Pedeapsa principală prevăzută pentru infracțiunea de bază (accesul fără drept) este închisoarea de la 6 luni la 3 ani sau amendă. Pentru existența primei condiții agravante, aceea a accesului în scopul obținerii de date informatice, pedeapsa este închisoare de la 6 luni la 5 ani, iar în cazul celei de a doua condiții agravante, anume accesul prin încălcarea măsurilor de securitate pedeapsa este închisoare de la 3 la 12 ani.

2.1.2 Infracțiunea de interceptare ilegală a unei transmisii de date informatice

Este incriminată în art. 43 al legii şi distinge două forme:

1) Interceptare, 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;

2) Interceptarea fără drept, a unei emisii electromagnetice provenite dintr-un sistem informatic ce conține date informatice care nu sunt publice.

Ce apără legiuitorul sau care este obiectul juridic special al acestei incriminări?

Obiectul juridic special este reprezentat de relațiile sociale care se nasc şi se dezvoltă cu privire la confidențialitatea datelor informatice. Aceste relații sociale sunt puse în pericol prin interceptarea fără drept a unei transmisii de date informatice, care nu este publică sau a unei emisii electromagnetice provenite dintr-un sistem informatic ce conține date informatice care nu sunt publice.

De asemenea, din punct de vedere fizic, material este apărat fluxul de date informatice emise sau recepționate de un sistem informatic sau vehiculate în interiorul acestuia şi care reprezintă ținta de interes pentru făptuitor.

În cazul formei a doua, obiectul material este energia electromagnetică purtătoare de informații care este radiată de sistemul informatic. Această emisie poate fi o legătură radio sau emisia electromagnetică care scapă din ecranajul sistemului şi/sau a perifericelor conectate la acesta cum ar fi imprimanta, ecranul monitor, cablurile de interconectare.

Cine poate fi infractorul, sau subiectul activ al infracțiunii?

Comun tuturor infracțiunilor informatice, subiect activ poate fi orice persoană ce întruneşte condițiile generale ale răspunderii penale.

Făptuitorul, ale cărui cunoştințe în domeniu nu au relevanță, trebuie să folosească nemijlocit dispozitive electronice special destinate interceptărilor din mediul informatic pentru a-şi duce la îndeplinire intenția.

De cele mai multe ori, totuşi, autorul este o persoană cu cunoştințe în domeniul calculatoarelor sau al electronicii. Subiectul activ poate fi de asemenea o persoană juridică în condițiile şi cu

limitările prevăzute în art. 19^1 Cod penal [2].

Participanţi la săvârşirea acestei ilegalităţi, care răspund în faţa legii alături de autorul infracţiunii sunt: coautorii, instigatorii, complicii.

Cine este victima infractorului sau subiectul pasiv?

Este persoana fizică sau juridică deţinătoare de drept a sistemului informatic ori a componentelor de transmisie dintre două sau mai multe sisteme informatice.

În secundar, subiect pasiv va fi şi deţinătorul de drept al datelor informatice interceptate sau persoana vizată în mod direct de prelucrarea informatizată a acestor date.

Din punct de vedere obiectiv, din ce constă fapta incriminată sau elementul material al infracţiunii?

Constă în interceptarea fără drept, a unei transmisii de date informatice care nu este publică. Pentru existenţa elementului material al infracţiunii analizate este necesar ca acţiunea ilicită să se comită fără drept, în înţelesul arătat în lege iar pentru ambele ipoteze de incriminare este necesar ca datele informatice să nu fie publice.

Fapta, în ambele ipoteze de incriminare, se săvârşeşte printr-o acţiune de interceptare, ceea ce înseamnă că din punct de vedere tehnic, făptuitorul captează prin intermediul unui dispozitiv special construit în acest scop sau a unui calculator, semnalele electrice sau electromagnetice care sunt vehiculate în interiorul sistemului informatic ţintă a infracţiunii sau se manifestă ca efect al funcţionării acestuia ori se află pe traseul de legătură dintre două sau mai multe sisteme informatice în timp ce acestea comunică.

Interceptarea prin mijloace tehnice cuprinde monitorizarea fluxului comunicaţiilor şi obţinerea conţinutului datelor informatice vizate. Prima ipoteză prevede că acest lucru se poate realiza direct prin interacţiunea făptuitorului cu componentele externe ale sistemului informatic.

Spre exemplu, comunicaţia între două computere într-o reţea locală Intranet sau LAN a unei entităţi, poate fi interceptată de un răufăcător, după ce acesta se conectează fizic la traseul de cablu al reţelei vizate, prin violarea firelor de comunicaţie şi legarea acestora cu cablul conectat la propriul computer, unde va recepţiona în paralel fluxul de date informatice.

În general, un dispozitiv sau calculator intrus, se poate plasa în orice punct al unei reţele de calculatoare, având ca obiectiv interceptarea traficului cu mesaje. Acţiunile care pot fi executate sunt de două feluri:

- atacuri pasive, în cadrul cărora intrusul vede informaţia care trece prin canalul de date, 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.

Ipoteza a doua reglementează cazul interceptării indirecte sau de la distanţă, când interceptarea reprezintă captarea radiaţiilor ori câmpurilor electromagnetice prezente pe o anumită distanţă în jurul oricărui dispozitiv tranzitat de impulsuri electrice sau electromagnetice, distanţă care, deşi standardizată internaţional, în fapt poate varia de la sistem, la sistem, în funcţie de integritatea elementelor de ecranare. Radiaţiile electromagnetice din jurul monitorului sistemului de calcul ţintă, de exemplu, pot fi captate cu ajutorul unui dispozitiv special fabricat pentru radiaţii care conţin date ce se tranzitează între calculator şi monitor, care sunt amplificate, filtrate şi în cele din urmă transformate în semnale electrice şi convertite în caractere inteligibile.

Interceptarea fără drept a transmisiilor de date este una dintre infracţiunile cel mai dificil de realizat şi este totodată una dintre cele mai serioase ameninţări la adresa comunicaţiilor prin Internet.

Dacă persoana care procedează la interceptare are dreptul de a dispune de datele comunicate, dacă ea acţionează la comanda sau cu autorizaţia participanţilor sau a destinatarului transmisiei, dacă datele sunt destinate uzului propriu sau marelui public sau dacă, pe fondul unei dispoziţii

legale specifice, supravegherea este autorizată, în interesul securității naționale sau pentru a permite serviciilor speciale ale statului să aducă la lumină infracțiuni grave ori este autorizată în condițiile prevăzute de Codul de procedură penală în cursul unui proces penal, interceptarea va fi legitimă.

Tentativa se pedepseşte conform art. 47 din lege.

Cum se sancționează?

Pentru ambele forme ale infracțiunii, pedeapsa principală este închisoarea de la 2 ani la 7 ani.

2.1.3 Infracțiunea de alterare a integrității datelor informatice

Este incriminată în art. 44 al legii şi distinge trei etape în ceea ce priveşte gravitatea acestei fapte: 1) modificarea, ştergerea sau deteriorarea datelor informatice ori restricționarea accesului la aceste date, fără drept; 2) transferul neautorizat de date dintr-un sistem informatic; 3) transferul neautorizat de date dintr-un mijloc de stocare a datelor informatice.

Ce apără legiuitorul sau care este obiectul juridic special al acestei incriminări?

Pe de o parte relațiile sociale ce protejează încrederea în corectitudinea datelor stocate în sistemele informatice şi pe de altă parte relațiile sociale ce protejează confidențialitatea datelor stocate în sistemele informatice sau pe alte mijloace de stocare.

De asemenea, din punct de vedere fizic, material este apărat suportul material de orice fel folosit pentru stocarea datelor, pe care se află datele modificate, şterse, deteriorate, transferate sau la care a fost restricționat accesul, precum şi entitățile materiale numite date informatice, reprezentate fizic prin variații ale stării materiei pe care sunt memorate.

Cine poate fi infractorul, sau subiectul activ al infracțiunii?

Poate fi orice persoană fizică ce întruneşte condițiile generale ale răspunderii penale precum şi o persoană juridică. Făptuitorul nu trebuie să fie neapărat o persoană cu cunoştințe în domeniul calculatoarelor sau al electronicii. Oricum, aspectul acesta este nerelevant. În principiu, autorul este, însă, o persoană cu cunoştințe în domeniul calculatoarelor sau al electronicii.

Participanți la săvârşirea acestei ilegalități, care răspund în fața legii alături de autorul infracțiunii sunt: coautorii, instigatorii, complicii.

Cine este victima infractorului sau subiectul pasiv?

Victima este proprietarul datelor modificate, şterse, deteriorate, transferate sau la care a fost restricționat accesul.

Acesta poate fi o persoană fizică sau juridică care deține de drept sistemul informatic ori mijloacele de stocare a datelor sau datele şi informațiile care constituie obiectul material al infracțiunii.

Din punct de vedere obiectiv, din ce constă fapta incriminată sau elementul material al infracțiunii?

Constă în acțiunile de modificare, ştergere, deteriorare, transferare fără autorizare, restricționare a accesului la datele informatice.

Actele prin care se realizează acestea, implică efecte negative asupra stării datelor, mai ales în ceea ce priveşte capacitatea lor de a funcționa în maniera prevăzută de persoana care dispune de ele. Sunt, deci, excluse modificările, ştergerile etc. care nu au asemenea consecințe, adică, spre exemplu, care merg până la a perfecționa programul sau datele din punct de vedere al finalității lor subiective [2].

Modificarea constă în acțiunea făptuitorului de a introduce date noi sau de a şterge porțiuni ale datelor informatice, având ca rezultat noi date informatice, diferite de cele inițiale şi neconforme cu valoarea de adevăr pe care ar trebui să o reprezinte.

[2] I. Vasiu, L. Vasiu, Informatica juridică şi drept informatic, Ed. Albastră, 2002, pag.160

Ştergerea constă în acţiunea de modificare a modului de reprezentare a datelor informatice din mediile de stocare, ceea ce conduce implicit la dispariţia respectivelor date. Ştergerea de date poate echivala şi cu distrugerea fizică a suportului de stocare a acestor date.

Modul de ştergere frauduloasă a datelor poate fi rezultatul unor acţiuni fizice, concrete, asupra mediilor de stocare prin acte de terorism clasice, acte de sabotaj sau informatice prin introducerea de programe pentru calculator care execută această acţiune, numite şi bombe logice. Cele mai periculoase sunt programele-virus care se reproduc şi se pun în lucru în alte programe şi fişiere de date, ca programe de distrugere.

Deteriorarea înseamnă alterarea conţinutului binar al datelor informatice, prin inserţii controlate sau aleatoare de secvenţe informatice unitare, astfel încât noua secvenţă rezultată să nu mai poată avea un corespondent inteligibil.

Restricţionarea accesului la datele informatice este rezultatul uneia sau mai multor acţiuni exercitate de către făptuitor asupra sistemelor de calcul sau mediilor de stocare, astfel încât utilizatorul de drept să nu le mai poată regăsi în forma lor iniţială sau prin procedurile standard de operare a sistemelor de calcul. Datele nu mai sunt accesibile persoanelor autorizate şi în consecinţă, acestea nu se pot servi de ele.

Restricţionarea fizică este înfăptuită prin acţionarea directă în scopul blocării accesului la resursele unui sistem informatic prin dezafectarea componentelor periferice gen tastatură sau mouse.

Restricţionarea logică este înfăptuită prin modificarea datelor destinate organizării interne de către sistemul informatic a mediilor de stocare a datelor informatice, astfel încât acestea nu mai pot fi regăsite de utilizatorul de drept. Datele care au suferit acest gen de restricţionare sunt recuperabile în tot sau în parte de către echipe de specialişti dar cu sacrificii materiale şi de timp.

Transferul neautorizat este copierea pe un alt suport de stocare, fără drept, a datelor ce prezintă interes, din mediul de stocare în care au fost depuse în mod autorizat sau mutarea datelor în altă parte a aceluiaşi mijloc de stocare sau în alt mijloc de stocare.

Diferenţa între forma 2) şi forma 3) a infracţiunii este dată de mediul autorizat din care provin datele informatice, respectiv dintr-un sistem informatic ori dintr-un mediu de stocare extern.

Cerinţa esenţială pentru existenţa elementului material al infracţiunii analizate este necesitatea ca acţiunea ilicită să se comită fără drept.

Instrumentele cele mai periculoase care alterează datele informatice şi care sunt utilizate cel mai frecvent de către infractorii informatici sunt programele informatice de tip Virus, Vierme sau Cal Troian.

American Criminal Law Review (Revista Americană de drept penal) [11], defineşte aceste ameninţări astfel:

- Viruşi - programe informatice care modifică alte programe informatice, astfel încât acestea să efectueze funcţiile destinate de către creatorul virusului.
- Worms - programe informatice cu funcţionalitate de viruşi biologici, având proprietatea de a se răspândi în sistemele informatice prin intermediul internetului şi în special cu ajutorul serviciului de poştă electronică.
- Cal Troian - aşa cum indică denumirea lor, aceşti intruşi pretind a fi programe oneste. Utilizatorii sunt convinşi să le instaleze în sistemele lor informatice. Calul Troian activează apoi un program informatic distructiv încorporat.
- Bombele Logice - sunt programe informatice distructive, activate de un eveniment sau o anumită dată sau oră. Acelaşi concept este utilizat în mod legal de către companiile care distribuie mostre limitate în timp a programelor lor informatice. Astfel de programe informatice se dezactivează după trecerea a 30 sau 60 de zile.
- Sniffers - aceste programe sunt folosite în mod legitim pentru monitorizarea şi analizarea

rețelelor informatice. Acestea pot fi însă utilizate într-un mod infracțional pentru furtul parolelor, datelor cardurilor de credit, identității sau pentru spionajul activității dintr-o rețea informatică.

- Atacuri distribuite asupra unui serviciu informatic - astfel de atacuri sunt îndreptate spre site-urile Web, pentru a face ca mai multe sisteme informatice să trimită în mod ilegal cât mai multe cereri serviciului de conectare la un site-țintă dintr-un sistem informatic, cauzând astfel blocarea sistemului [3].

Tentativa se pedepseşte conform art. 47 din lege.

Cum se sancționează?

Pedeapsa prevăzută în forma de bază 1) este închisoare de la 2 la 7 ani. Pedeapsa prevăzută pentru formele agravante 2) şi 3) este închisoarea de la 3 la 12 ani.

2.1.4 Infracțiunea de perturbare a funcționării sistemelor informatice

Art. 45 incriminează fapta de a perturba grav, fără drept, funcționarea unui sistem informatic, prin introducerea, transmiterea, modificarea, ştergerea sau deteriorarea datelor informatice sau prin restricționarea accesului la aceste date.

Ce apără legiuitorul sau care este obiectul juridic special al acestei incriminări?

Este constituit de relațiile sociale ce protejează integritatea datelor informatice conținute pe suporturile specifice sistemelor informatice.

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 sunt reglementate în prevederile acestui articol.

De asemenea, din punct de vedere fizic, material este apărat sistemul informatic a cărui activitate este grav perturbată de făptuitor.

Țintele atacului sunt:

- una din părțile care formează un sistem informatic sau o rețea de sisteme informatice;
- sistem informatic care constă în una sau mai multe componente asociate, incluzând unități de procesare şi periferice şi care este controlat de programe stocate intern;
- rețea de sisteme informatice care reprezintă un grup interconectat de sisteme informatice, echipamente de comutare şi ramuri de interconectare;
- internetul ca rețea de rețele.

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

Cine poate fi infractorul, sau subiectul activ al infracțiunii?

Subiectul activ nemijlocit poate fi orice persoană ce întruneşte condițiile răspunderii penale.

În principiu, autorul este o persoană cu cunoştințe în domeniul calculatoarelor sau al electronicii. Subiectul activ poate fi şi o persoană juridică.

Participanți la săvârşirea acestei ilegalități, care răspund în fața legii alături de autorul infracțiunii sunt: coautorii, instigatorii, complicii.

Cine este victima infractorului sau subiectul pasiv?

Subiectul pasiv este persoana fizică sau juridică deținătoare de drept a sistemului informatic a cărui funcționare este perturbată.

[3] http://definitions.uslegal.com/c/computer-crime/

Din punct de vedere obiectiv, din ce constă fapta incriminată sau elementul material al infracțiunii?

Elementul material constă într-o acțiune de perturbare gravă a funcționării unui sistem informatic adică alterarea totală sau parțială a parametrilor funcționali ai acestuia, de natură să provoace un dezechilibru temporar sau permanent, prin una din următoarele modalități alternative: introducerea, transmiterea, modificarea, ştergerea sau deteriorarea datelor informatice, sau prin restricționarea accesului la date informatice.

Introducerea de date informatice constă în inserarea de astfel de date într-un sistem informatic. Aceasta se poate realiza, spre exemplu, în cazul operatorului unui sistem informatic de control al activității unei hidrocentrale care introduce de la tastatură, în mod voit sau ca urmare a neatenției, o serie de parametrii ce sunt în mod greşit interpretați de programul sau aplicația de baza, rezultatul fiind funcționarea haotică a sistemului ori blocarea anumitor segmente de execuție.

Transmiterea de date informatice se realizează de la distanță, folosind facilitățile oferite de conectarea sistemului vizat la o rețea informatică. Este cazul unei persoane care, indiferent de motiv, trimite prin intermediul internetului un număr mare de mesaje către sistemul informatic al unei instituții, supraaglomerând intrările de date şi blocând accesul acestuia. De asemenea poate fi vorba şi despre plasarea, în sistemul informatic vizat, de viruşi, viermi sau troieni.

Articolul 45 incriminează acțiunile care sunt de natură să aducă grave atingeri funcționării unui sistem informatic, cu un impact de o importanță capitală pentru colectivitate.

Cerința esențială este necesitatea ca acțiunea ilicită să se comită fără drept.

Va acționa îndreptățit, persoana fizică sau juridică, care, în baza unui contract încheiat în acest sens cu proprietarul sau deținătorul de drept al sistemului informatic, execută o operațiune de perturbare în vederea determinării vulnerabilităților sistemului informatic, provocând o perturbare gravă a funcționării.

Perturbarea funcționării sistemelor informatice intră sub incidența legii penale numai dacă este fără drept şi gravă, adică în raport de consecințele şi celelalte împrejurări în care a fost comisă fapta. Aceste condiții esențiale din conținutul incriminării trebuie îndeplinite cumulativ pentru a se realiza elementul material al perturbării funcționării sistemelor informatice.

Tentativa se pedepseşte conform art. 47 din lege.

Cum se sancționează?

Infracțiunea analizată prezintă şase forme de săvârşire, respectiv introducerea, transmiterea, modificarea, ştergerea, deteriorarea, restricționarea accesului la date informatice.

Pedeapsa prevăzută este închisoarea de la 3 la 15 ani.

2.1.5 Infracțiunea de a realiza operațiuni ilegale cu dispozitive sau programe informatice

Art. 46 incriminează: 1) fapta de a produce, vinde, de a importa, distribui sau de a pune la dispoziție, sub orice altă formă, fără drept, a unui dispozitiv sau program informatic conceput sau adaptat în scopul săvârşirii uneia dintre infracțiunile analizate mai sus (art. 42-45); 2) fapta de a produce, vinde, de a importa, distribui sau de a pune la dispoziție, sub orice altă formă, fără drept, a unei parole, cod de acces sau alte asemenea date informatice care permit accesul total sau parțial la un sistem informatic, deținerea, fără drept, a unui dispozitiv, program informatic, parolă, cod de acces sau dată informatică în scopul săvârşirii uneia dintre infracțiunile analizate mai sus (art. 42-45).

Ce apără legiuitorul sau care este obiectul juridic special al acestei incriminări?

Sunt apărate relațiile sociale referitoare la încrederea în datele informatice şi sistemele informatice aşa cum sunt definite în lege, precum şi în desfăşurarea legală a operațiunilor de vânzare, cumpărare, distribuție, legate de acestea.

Totodată, din punct de vedere fizic, material, sunt apărate dispozitivele electronice ori programele informatice special create sau adaptate pentru a fi folosite ca mijloace pentru comiterea altor infracțiuni informatice, precum şi datele informatice care țin de protecția sistemului.

Cine poate fi infractorul, sau subiectul activ al infracțiunii?

Subiectul activ nemijlocit este orice persoană ce întruneşte condițiile generale pentru răspunderea penală, de asemenea, acele persoane care produc, vând, importă, distribuie, pun la dispoziție sau dețin mijloacele de înfăptuire a infracțiunilor contra confidențialității şi integrității datelor şi sistemelor informatice.

Subiectul activ poate fi şi o persoană juridică în condițiile prevăzute în art. 19^1 Cod penal [2].

Participanți la săvârşirea acestei ilegalități, care răspund în fața legii alături de autorul infracțiunii sunt: coautorii, instigatorii, complicii.

Cine este victima infractorului sau subiectul pasiv?

Victimă a infracțiunii este persoana fizică sau juridică deținătoare a sistemului informatic, susceptibil de a i se aduce atingere prin săvârşirea faptelor incriminate precum şi proprietarul ori deținătorul dreptului de autor pentru dispozitivele electronice sau programele informatice modificate sau adaptate în scop infracțional. De asemenea va avea rol de subiect pasiv şi persoana fizică sau juridică deținătoare de drept sau proprietară a datelor informatice care țin de securitatea şi protecția sistemului, care au fost în mod fraudulos utilizate pentru a permite accesul într-un sistem informatic.

Din punct de vedere obiectiv, din ce constă fapta incriminată sau elementul material al infracțiunii?

Este concretizată de acțiunile de producere, vindere, importare, distribuire, punere la dispoziție, deținere de unelte de natură a permite săvârşirea infracțiunilor mai sus menționate.

Producerea unui dispozitiv informatic constă în executarea activităților tehnice necesare conectării unor componente electronice astfel îmbinate şi interconectate încât produsul obținut să poată interacționa cu un sistem informatic sau să devină o parte integrantă a acestuia.

Crearea unui program informatic presupune elaborarea unui proiect logic a programului în funcție de scopul urmărit şi scrierea în conformitate cu acel proiect a unui set de instrucțiuni inteligibile unui sistem informatic.

Este incriminată şi fapta aceluia care, deşi nu are nici o contribuție la crearea dispozitivului sau programului informatic, îl importă, îl distribuie ori îl pune la dispoziția persoanei care acționează în mod nemijlocit asupra sistemului informatic.

De asemenea sunt sancționate producerea, vânzarea, importul, distribuirea ori punerea la dispoziția persoanelor neautorizate a datelor informatice de protecție care permit accesul, la un sistem informatic.

Cerința esențială pentru existența faptei infracționale este aceea ca acțiunea ilicită să se comită fără drept.

Tentativa se pedepseşte conform art. 47 din lege.

Cum se sancționează?

Infracțiunea analizată prezintă şase forme, respectiv producerea, vânzarea, importul, distribuirea, punerea la dispoziție sau deținerea, fără drept, a unui dispozitiv, program informatic, parolă, cod de acces sau alte date informatice şi se pedepseşte cu închisoare de la unu la 6 ani.

2.2 Infracțiuni informatice

2.2.1 Infracțiunea de fals informatic

Sancționată de art. 48 al legii, incriminează fapta de a introduce, modifica sau şterge, 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.

Ce apără legiuitorul sau care este obiectul juridic special al acestei incriminări?

Sunt apărate relațiile sociale referitoare la încrederea publică în siguranța sistemelor informatice, la valabilitatea şi autenticitatea datelor informatice, a procesului informatic de prelucrare, stocare şi tranzacționare automată a datelor de interes public sau privat.

Odată cu devenirea indispensabilă a datelor informatice a devenit necesară protejarea juridică a securității lor prin incriminarea tuturor acelor acțiuni, care pot prin modificarea unor date aflate pe suport informatic, să atragă după sine consecințe juridice nedorite de persoanele care au conceput, realizat, implementat sau asupra cărora îşi manifestă efectele informația modificată.

Totodată, din punct de vedere fizic, material este apărat suportul pe care se află stocate datele informatice alterate în scopul producerii de consecințe juridice.

Acționând asupra acestor date este echivalent cu a acționa asupra mediilor de stocare.

Cine poate fi infractorul, sau subiectul activ al infracțiunii?

Infractorul, poate fi orice persoană ce întruneşte condițiile generale pentru răspunderea penală.

Manipulările frauduloase de acest gen sunt, în general, realizate de către inițiați în ştiința calculatoarelor ori de persoane care, prin natura serviciului, au acces la date şi sisteme informatice, de asemenea, poate fi şi o persoană juridică în condițiile prevăzute în art. 19^1 Cod penal [2].

Participanți la săvârşirea acestei ilegalități, care răspund în fața legii alături de autorul infracțiunii sunt: coautorii, instigatorii, complicii.

Cine este victima infractorului sau subiectul pasiv?

Subiectul pasiv este persoana fizică sau juridică proprietar al datelor informatice alterate în scopul producerii de consecințe juridice, prejudiciată în propriile interese în urma contrafacerii datelor informatice.

Poate exista şi o victimă secundară în persoana proprietarului, deținătorului de drept sau utilizatorii autorizați ai sistemului informatic afectați de modificările respective.

Din punct de vedere obiectiv, din ce constă fapta incriminată sau elementul material al infracțiunii?

Fapta constă în acțiunea de introducere, modificare sau ştergere de date informatice sau de restricționarea accesului la aceste date în scopul producerii de efecte juridice.

Acele modalități prin care se asigură existența faptei infracționale, implică efecte negative asupra stării datelor în ce priveşte capacitatea lor de a funcționa şi atesta fapte ori situații de maniera prevăzută de persoana care dispune de ele, ajungându-se la o situație care corespunde fabricării unor documente false sau falsificării unor documente autentice[4].

Falsificarea datelor informatice s-ar putea realiza sub următoarele forme:

- inserarea, modificarea sau ştergerea de date în câmpurile unei baze de date existente la nivelul unui centru de evidență informatizată a persoanei, unei bănci sau societăți de asigurări etc. – prin acțiunea directă a făptuitorului asupra tastaturii ori prin copierea datelor de pe un suport de stocare extern;
- alterarea documentelor stocate în format electronic, prin modificarea sau ştergerea directă a cuvintelor, etc.

Tentativa se pedepseşte în conformitate cu art. 50 din lege.

Infracțiunea analizată prezintă patru forme de manifestare, respectiv introducerea, modificarea, ştergerea de date informatice, precum şi restricționarea accesului la aceste date.

[4] I.Vasiu, L.Vasiu, op.cit., pag.169.

Cum se sancţionează?

Pedeapsa prevăzută pentru această infracţiune este închisoarea de la 2 la 7 ani.

2.2.2 Infracţiunea de fraudă informatică

Incriminată în art. 49, este reprezentată de fapta care cauzează un prejudiciu patrimonial unei persoane prin introducerea, modificarea sau ştergerea de date informatice, prin restricţionarea accesului la aceste date sau prin împiedicarea în orice mod a funcţionării unui sistem informatic, în scopul de a obţine un beneficiu material pentru sine sau pentru altul.

Ce apără legiuitorul sau care este obiectul juridic special al acestei incriminări?

Obiectul juridic special este constituit de relaţiile sociale care protejează patrimoniul unei persoane, atunci când persoana deţine în spaţiul informatic o cantitate de date informatice stocate într-un sistem informatic sau vehiculate într-o reţea informatică.

În dreptul penal, noţiunea de patrimoniu în legătură cu infracţiunile care se pot comite împotriva acestuia are înţeles mai restrâns şi se referă la bunuri nu ca universalitate, ci în individualitatea lor susceptibilă de a fi apropriate de făptuitor prin mijloace frauduloase ori de a fi distruse, deteriorate, tăinuite, gestionate fraudulos etc.[5]

De asemenea, din punct de vedere fizic şi material sunt apărate sistemele informatice care conţin datele informatice alterate sau care sunt împiedicate să funcţioneze ca urmare a activităţii făptuitorului, precum şi datele informatice stocate în sistemele informatice vizate, cât şi entităţile materiale care compun un sistem informatic, individual sau aflat în comunicare cu alte sisteme prin intermediul unei reţele.

Cine poate fi infractorul, sau subiectul activ al infracţiunii?

Poate fi orice persoană ce întruneşte condiţiile generale pentru răspunderea penală.

Manipulările frauduloase de acest gen sunt realizate de cele mai multe ori de iniţiaţi în domeniul calculatoarelor ori de persoane care, prin natura serviciului, au acces la date şi sisteme informatice[6], de asemenea, poate fi şi o persoană juridică în condiţiile prevăzute în art. 19^1 Cod penal.

Participanţi la săvârşirea acestei ilegalităţi, care răspund în faţa legii alături de autorul infracţiunii sunt: coautorii, instigatorii, complicii.

Cine este victima infractorului sau subiectul pasiv?

Victime pot fi principale şi/sau secundare.

Victima principală este persoana al cărei interes patrimonial a fost prejudiciat prin acţiunea făptuitorului.

Victima secundară este proprietarul, deţinătorul de drept sau utilizatorul legal al unui sistem informatic.

Din punct de vedere obiectiv, din ce constă fapta incriminată sau elementul material al infracţiunii?

În acest caz, fapta incriminată este acţiunea de a introducere, modifica sau şterge date informatice sau de a restricţiona accesul la respectivele date sau de a împiedica în orice mod funcţionarea unui sistem informatic.

Împiedicarea funcţionării sistemului informatic, presupune înfăptuirea oricărui act de natură a duce la imposibilitatea utilizării, parţial sau total, temporar sau permanent, a respectivului sistem.

De exemplu, făptuitorul acţionează la o anumită dată şi la o anumită oră asupra sistemului informatic al Bursei, reuşind să paralizeze tranzacţiile electronice de acţiuni, ceea ce are repercusiuni

[5] I.Pascu, M. Gorunescu, Drept penal partea specială ediţia a II-a, editura Hamangiu, 2009, pag. 228.
[6] I. Vasiu, L. Vasiu, op.cit., pag. 159.

asupra afacerilor şi câştigurilor entităţilor aflate în plin proces de vânzare-cumpărare.

Tentativa se pedepseşte în conformitate cu art. 50 din lege.

Delictul analizat, prezintă cinci forme: introducerea, modificarea, ştergerea datelor informatice, restricționarea accesului la aceste date sau împiedicarea în orice mod a funcționării unui sistem de calcul.

Cum se sancționează?

Pedeapsa prevăzută este închisoarea de la 3 la 12 ani.

2.3. Pornografia infantilă

Pornografia infantilă prin intermediul sistemelor informatice este combătută prin articolul 51 care arată: "Constituie infracțiune 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". Material pornografic de acest gen este şi acela în care, deşi nu prezintă o persoană reală, se simulează, în mod credibil, un minor având un comportament sexual explicit.

Ce apără legiuitorul sau care este obiectul juridic special al acestei incriminări?

Alături de alte norme şi aceasta apără relațiile sociale ce urmăresc protejarea minorilor.

Din punct de vedere fizic, material sunt avute în vedere suporturile de stocare a datelor din sistemele informatice ce conțin materialele pornografice cu minori.

Cine poate fi infractorul, sau subiectul activ al infracțiunii?

Subiectul activ este orice persoană ce întruneşte condițiile generale pentru răspunderea penală.

În cazul producerii în vederea răspândirii sunt considerați subiecți activi ai infracțiunii, toate persoanele care iau parte la diferite stadii ale procesului de producere a materialelor pornografice cu minori, inclusiv cele care au servit drept model.

Participanți la săvârşirea acestei ilegalități, care răspund în fața legii alături de autorul infracțiunii sunt: coautorii, instigatorii, complicii.

Cine este victima infractorului sau subiectul pasiv?

Victima este minorul ale cărui ipostaze pornografice au fost înregistrate, stocate ori transmise prin sisteme informatice.

Din punct de vedere obiectiv, din ce constă fapta incriminată sau elementul material al infracțiunii?

Acesta este constituit din mai multe moduri alternative de executare şi anume: producerea în vederea răspândirii; oferirea; punerea la dispoziție; răspândirea; transmiterea; procurarea pentru sine sau pentru altul de materiale pornografice cu minori prin sisteme informatice; deținerea, fără drept, de materiale pornografice cu minori într-un sistem informatic sau un mijloc de stocare a datelor informatice.

În înțelesul legii, deținerea fără drept a materialelor pornografice cu minori constă în a le avea în proprietate sau în păstrare împotriva dispozițiilor legale.

Tentativa se pedepseşte în conformitate cu alin. 2 al acestui articol.

Cum se sancționează?

Pedeapsa prevăzută este închisoarea de la 3ani la 12 ani precum şi interzicerea unor drepturi.

3. Reglementarea infracțiunilor din spațiul informatic în noul Cod Penal

„Pentru asigurarea unității în reglementarea infracțiunilor este necesară includerea în conținutul proiectului Codului penal a unor infracțiuni prevăzute în prezent în legi penale speciale şi care au o mai mare frecvență în practica judiciară.

Astfel, în proiectul Codului penal trebuie introduse toate acele fapte incriminate în legi speciale, care merită în mod real o sancțiune penală, iar în aceste cazuri textul incriminator trebuie conceput astfel încât să se integreze organic în structura proiectului" [7].

3.1 Infracțiuni contra patrimoniului

Fraudele patrimoniale săvârşite prin sisteme informatice au fost incluse în Titlul II, Capitolul IV.

Aici sunt integrate şi prevederile cuprinse în prezent în Legea penală specială nr. 161/2003 în Secțiunea a II-a intitulată Infracțiuni informatice.

Aceste fapte se pedepsesc cu închisoarea de la 2 la 7 ani.

Se observă că dispozițiile privind infracțiunile informatice (art. 48 şi art.49) au fost reunite aproape complet în art. 249 numit fraudă informatică din noua reglementare.

Modificări

Au fost reduse condițiile necesare pentru ca fapta să devină infracțiune. Astfel:

- s-a renunțat la cerința esențială ca activitățile ilicite să fi fost făcute fără drept;
- nu mai este necesar ca în urma acțiunii ilicite să rezulte date necorespunzătoare adevărului în scopul de a fi utilizate în vederea producerii unei consecințe juridice;
- condiția de a cauza un prejudiciu patrimonial unei persoane este înlocuit de condiția mai generală a cauzării unei pagube persoanei.

Sancționarea a fost stabilită la pedeapsa închisorii de la 2 ani la 7 ani, constatându-se o micşorare a pedepsei.

3.2 Infracțiuni contra siguranței şi integrității sistemelor şi datelor informatice

În Titlul VII - Infracțiuni contra siguranței publice al noului Cod penal, articolul 360 - Accesul ilegal la un sistem informatic, se reiau fără modificări reglementările din art. 42. Varianta agravată a articolului 42 din legea 161/2003 se referă la accesul, fără drept, la un sistem informatic cu scopul obținerii de date informatice, pe când noua reglementare se referă la un sistem informatic care este protejat doar față de anumite categorii de utilizatori. Astfel, persoanele care accesează fără drept un sistem informatic, al cărui acces nu le este restricționat sau interzis, săvârşesc infracțiunea în varianta neagravantă, pe când celelalte persoane săvârşesc această infracțiune în varianta agravantă.

Sancțiunea de bază rămâne aceeaşi, mai puțin varianta agravantă, a cărei pedeapsă este diminuată la închisoare de la 2 la 7 ani în loc de închisoare de la 3 la 12 ani.

3.3 Interceptarea ilegală a unei transmisii de date informatice

În Titlul VII - Infracțiuni contra siguranței publice al noului Cod penal, la Capitolul VI, art. 361 preia fără modificări art. 43 al legii 161/2003, însă sancționarea a fost modificată în scădere de la închisoare între 2 ani şi 7 ani la închisoare între 1 şi 5 ani.

3.4 Alterarea integrității datelor informatice

Tot în Titlul VII - al noului Cod penal, la Capitolul VI, art. 362 preia fără modificări art. 44, în afară de sancțiune, care este scăzută de la închisoare de la 2 la 7 ani la închisoare de la unu la 5 ani.

[7] Expunerea de motive la proiectul noului Cod penal din 25 februarie 2009.

3.5 Perturbarea funcționării sistemelor informatice

De asemenea, Titlul VII al noului Cod penal, la Capitolul VI, art. 363, preia reglementarea art. 45 micşorând însă sancțiunea închisorii de la 3 la 15 ani la închisoare de la 2 la 7 ani.

3.6 Transferul neautorizat de date informatice

Art. 364 din Titlul VII al noului Cod penal, la Capitolul VI preia în textul său art. 44 al legii 161/2003.

Modificarea în noul Cod penal apare doar în privința sancțiunii micşorate la închisoare de la 2 la 7 ani în loc de 3 la 15 ani reglementat anterior.

3.7 Operațiuni ilegale cu dispozitive sau programe informatice

În sfârşit, art. 365 al noului Cod penal, reformulează reglementarea corespondentă din art. 46. în sensul că nu se mai face referire la acțiunea expresă de a vinde, ca formă de acțiune în cadrul operațiunilor ilegale cu dispozitive sau programe informatice fiind asimilată în sens mai larg acțiunii de distribuție.

Sancțiunea închisorii de la 1 la 6 ani a reglementarii actuale este micşorată şi diferențiată după cum persoana fără drept, utilizează echipamente şi produse informatice în scop infracțional, la închisoare de la 6 luni la 3 ani sau amenda. In cazul deținerii acestor produse în acelaşi scop, sancțiunea este închisoare de la 3 luni la 2 ani. Inedit este introducerea pedepsei opționale a amenzii.

3.8 Pornografia infantilă

Titlul VIII - Infracțiuni care aduc atingere unor relații privind conviețuirea socială în Capitolul I - Infracțiuni contra ordinii şi liniştii publice, la art. 374 aliniatele 2 şi 3 se reglementează înfăptuirea infracțiunii prin sisteme informatice sau alt mijloc de stocare a datelor informatice.

Ca sancțiuni, pedeapsa cu închisoarea de la 3 la 12 ani şi pedeapsa complementară a interzicerii unor drepturi stabilită în art. 51 al reglementării actuale este în mod bizar diminuată la închisoare de la 2 la 7 ani, iar accesarea fără drept, prin intermediul sistemelor informatice sau altor mijloace de comunicații electronice este închisoare de la 3 luni la 3 ani sau pedeapsa opțională a amenzii.

4. Concluzii

Analiza dispozițiilor cu caracter penal, arată existența unui cadru legal coerent în conformitate cu dispoziții internaționale în această materie, care conferă o protecție eficientă valorilor sociale din acest domeniu, realizându-se scopul prevenției generale a săvârşirii de infracțiuni.

Schimbările aduse în noul Cod penal se caracterizează prin ordonarea şi clarificarea normelor, dar, din păcate şi printr-o diminuare vădită a pedepselor, nemotivată de schimbarea relațiilor şi a valorilor sociale, pe care aceste norme legale ar trebui să le apere, culminând cu îmblânzirea neverosimilă a aceleia privind fapta deosebit de gravă a pornografiei infantile.

Expansiunea tehnologică şi scăderea prețurilor sistemelor informatice, crează în mod indirect posibilitatea diversificării modalităților de înfăptuire a ilicitului, extinderea valorilor şi relațiilor sociale puse în pericol, mărirea prejudiciilor şi creşterea exponențială a numărului de infractori virtuali.

De aceea este necesar ca în viitorul cât mai apropiat, să se poată vorbi despre apariția ştiinței dreptului penal informatic, pentru a înlocui aplicarea dreptului penal societății informatice, aşa cum este cazul acum. Dar pentru aceasta este nevoie de un efort conjugat, interdisciplinar.

BIBLIOGRAFIE

1. Constituția României, modificată şi completată prin Legea de revizuire a Constituției României nr. 429/2003, publicată în Monitorul Oficial, Partea I, nr. 758 din 29 octombrie 2003;
2. Noul Cod penal al României, iulie 2009;
3. Convenția Consiliul Europei din 23/11/2001 privind criminalitatea informatică, publicat în Monitorul Oficial, Partea I nr. 343 din 20/04/2004, Seria Tratatelor Europene nr. 185;
4. Legea nr. 161 din 19 aprilie 2003 privind unele masuri pentru asigurarea transparentei în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției, Titlul III, publicată în Monitorul Oficial nr. 279 din 21 aprilie 2003;
5. Direcția de Investigare a Infracțiunilor de Criminalitate Organizată şi Terorism, Raport de activitate 2011 http://www.diicot.ro/index.php?option=com_content&view=article&id=52&Itemid=69;
6. Decizia Consiliului Uniunii Europene nr.375 privind combaterea pornografiei infantile prin Internet, 9 iunie 2000;
7. Internet Crime Compliant Center (IC3) - http://www.ic3.gov/default.aspx
8. National White Collar Crime Center (NW3C)http://www.nw3c.org/
9. ThreatExpert – http://www.threatexpert.com
10. American Criminal Law Review - http://www.americancriminallawreview.com