Asociaţia Grupul pentru Reformă şi Alternativă Universitară (GRAUR)
Cluj-Napoca
Indexul Operelor Plagiate în România
www.plagiate.ro

Decizie de indexare a faptei de plagiat la poziţia 00319 / 3.10.2016 şi pentru admitere la publicare în volum tipărit

care se bazează pe:

A. **Nota de constatare şi confirmare a indiciilor de plagiat** prin fişa suspiciunii inclusă în decizie.

Fişa suspiciunii de plagiat / Sheet of plagiarism's suspicion		
Opera suspicionată (OS)		Opera autentică (OA)
Suspicious work		Authentic work
OS	KÖVESI, Laura Codruţa. Combaterea crimei organizate prin dispoziţii de drept penal. Teză de doctorat. Timişoara: Universitatea de vest. 2011. **Notă**: Conducător ştiinţific: Prof.dr.PAŞCA Viorel. Comisia de doctorat: Nu se cunoaşte. **Notă**: Plagiat semnalat în „* * *. Dr Codruţa Kovesi, precursoarea lui Mang. 25.05.2012. Disponibil la: www.militiaspirituala.ro/investigatii/documente-inedite/detalii.html. Ultima accesare: 3 mai 2016.	
OA	DOBRINOIU, Maxim. *Infracţiuni în domeniul informatic.* Bucureşti. 2006. Disponibil la: e-crime.ro/ecrime/site/files/93361241097364Infractiuniindomeniulinformatic.pdf. Ultima accesare: 30 iunie 2016.	
Incidenţa minimă a suspiciunii / Minimum incidence of suspicion		
p.385:19 – p.386:05		p.161:04 – p.161:21
p.414:06 - p.414:09		p.221:05 – p.221:08
Fişa întocmită pentru includerea suspiciunii în Indexul Operelor Plagiate în România de la Sheet drawn up for including the suspicion in the Index of Plagiarized Works in Romania at www.plagiate.ro		

Notă: Prin „p.72:00" se înţelege paragraful care se termină la finele pag.72. Notaţia „p.00:00" semnifică până la ultima pagină a capitolului curent, în întregime de la punctul iniţial al preluării.

Note: By „p.72:00" one understands the text ending with the end of the page 72. By „p.00:00" one understands the taking over from the initial point till the last page of the current chapter, entirely.

B. **Fişa de argumentare a calificării** de plagiat alăturată, fişă care la rândul său este parte a deciziei.

Echipa Indexului Operelor Plagiate în România

Asociaţia Grupul pentru Reformă şi Alternativă Universitară (GRAUR)
Cluj-Napoca
Indexul Operelor Plagiate în România
www.plagiate.ro

Fişa de argumentare a calificării

Nr. crt.	Descrierea situaţiei care este încadrată drept plagiat	Se confirmă
1.	Preluarea identică a unor pasaje (piese de creaţie de tip text) dintr-o operă autentică publicată, fără precizarea întinderii şi menţionarea provenienţei şi însuşirea acestora într-o lucrare ulterioară celei autentice.	✓
2.	Preluarea a unor pasaje (piese de creaţie de tip text) dintr-o operă autentică publicată, care sunt rezumate ale unor opere anterioare operei autentice, fără precizarea întinderii şi menţionarea provenienţei şi însuşirea acestora într-o lucrare ulterioară celei autentice.	
3.	Preluarea identică a unor figuri (piese de creaţie de tip grafic) dintr-o operă autentică publicată, fără menţionarea provenienţei şi însuşirea acestora într-o lucrare ulterioară celei autentice.	
4.	Preluarea identică a unor tabele (piese de creaţie de tip structură de informaţie) dintr-o operă autentică publicată, fără menţionarea provenienţei şi însuşirea acestora într-o lucrare ulterioară celei autentice.	
5.	Republicarea unei opere anterioare publicate, prin includerea unui nou autor sau de noi autori fără contribuţie explicită în lista de autori	
6.	Republicarea unei opere anterioare publicate, prin excluderea unui autor sau a unor autori din lista iniţială de autori.	
7.	Preluarea identică de pasaje (piese de creaţie) dintr-o operă autentică publicată, fără precizarea întinderii şi menţionarea provenienţei, fără nici o intervenţie personală care să justifice exemplificarea sau critica prin aportul creator al autorului care preia şi însuşirea acestora într-o lucrare ulterioară celei autentice.	✓
8.	Preluarea identică de figuri sau reprezentări grafice (piese de creaţie de tip grafic) dintr-o operă autentică publicată, fără menţionarea provenienţei, fără nici o intervenţie care să justifice exemplificarea sau critica prin aportul creator al autorului care preia şi însuşirea acestora într-o lucrare ulterioară celei autentice.	
9.	Preluarea identică de tabele (piese de creaţie de tip structură de informaţie) dintr-o operă autentică publicată, fără menţionarea provenienţei, fără nici o intervenţie care să justifice exemplificarea sau critica prin aportul creator al autorului care preia şi însuşirea acestora într-o lucrare ulterioară celei autentice.	
10.	Preluarea identică a unor fragmente de demonstraţie sau de deducere a unor relaţii matematice care nu se justifică în regăsirea unei relaţii matematice finale necesare aplicării efective dintr-o operă autentică publicată, fără menţionarea provenienţei, fără nici o intervenţie care să justifice exemplificarea sau critica prin aportul creator al autorului care preia şi însuşirea acestora într-o lucrare ulterioară celei autentice.	
11.	Preluarea identică a textului (piese de creaţie de tip text) unei lucrări publicate anterior sau simultan, cu acelaşi titlu sau cu titlu similar, de un acelaşi autor / un acelaşi grup de autori în publicaţii sau edituri diferite.	
12.	Preluarea identică de pasaje (piese de creaţie de tip text) ale unui cuvânt înainte sau ale unei prefeţe care se referă la două opere, diferite, publicate în două momente diferite de timp.	

Notă:

a) Prin „provenienţă" se înţelege informaţia din care se pot identifica cel puţin numele autorului / autorilor, titlul operei, anul apariţiei.

b) Plagiatul este definit prin textul legii[1].

> *„ …plagiatul – expunerea într-o operă scrisă sau o comunicare orală, inclusiv în format electronic, a unor texte, idei, demonstraţii, date, ipoteze, teorii, rezultate ori metode ştiinţifice extrase din opere scrise, inclusiv în format electronic, ale altor autori, fără a menţiona acest lucru şi fără a face trimitere la operele originale…".*

Tehnic, plagiatul are la bază conceptul de **piesă de creaţie** care[2]:

> *„…este un element de comunicare prezentat în formă scrisă, ca text, imagine sau combinat, care posedă un subiect, o organizare sau o construcţie logică şi de argumentare care presupune nişte premise, un raţionament şi o concluzie. Piesa de creaţie presupune în mod necesar o formă de exprimare specifică unei persoane. Piesa de creaţie se poate asocia cu întreaga operă autentică sau cu o parte a acesteia…"*

cu care se poate face identificarea operei plagiate sau suspicionate de plagiat[3]:

> *„…O operă de creaţie se găseşte în poziţia de operă plagiată sau operă suspicionată de plagiat în raport cu o altă operă considerată autentică dacă:*
> *i) Cele două opere tratează acelaşi subiect sau subiecte înrudite.*
> *ii) Opera autentică a fost făcută publică anterior operei suspicionate.*
> *iii) Cele două opere conţin piese de creaţie identificabile comune care posedă, fiecare în parte, un subiect şi o formă de prezentare bine definită.*
> *iv) Pentru piesele de creaţie comune, adică prezente în opera autentică şi în opera suspicionată, nu există o menţionare explicită a provenienţei. Menţionarea provenienţei se face printr-o citare care permite identificarea piesei de creaţie preluate din opera autentică.*
> *v) Simpla menţionare a titlului unei opere autentice într-un capitol de bibliografie sau similar acestuia fără delimitarea întinderii preluării nu este de natură să evite punerea în discuţie a suspiciunii de plagiat.*
> *vi) Piesele de creaţie preluate din opera autentică se utilizează la construcţii realizate prin juxtapunere fără ca acestea să fie tratate de autorul operei suspicionate prin poziţia sa explicită.*
> *vii) In opera suspicionată se identifică un fir sau mai multe fire logice de argumentare şi tratare care leagă aceleaşi premise cu aceleaşi concluzii ca în opera autentică…"*

[1] Legea nr. 206/2004 privind buna conduită în cercetarea ştiinţifică, dezvoltarea tehnologică şi inovare, publicată în Monitorul Oficial al României, Partea I, nr. 505 din 4 iunie 2004
[2] ISOC, D. *Ghid de acţiune împotriva plagiatului: bună-conduită, prevenire, combatere*. Cluj-Napoca: Ecou Transilvan, 2012.
[3] ISOC, D. *Prevenitor de plagiat*. Cluj-Napoca: Ecou Transilvan, 2014.

Dr. Maxim Dobrinoiu

INFRACȚIUNI ÎN DOMENIUL INFORMATIC

BUCUREŞTI

2006

CUPRINS

CAPITOLUL I – SISTEME INFORMATICE 6

SECȚIUNEA 1 – ASPECTE INTRODUCTIVE 6

1.1 Teoria Generală a Sistemelor **6**
1.1.1 Sistem şi structură **6**
1.1.2 Sistemul. Noțiune şi model **8**

1.2 Știința Ciberneticii **10**
1.2.1 Conceptul de cibernetică **10**
1.2.2 Semnificația ciberneticii **14**

SECȚIUNEA 2 – ARHITECTURA SISTEMELOR DE CALCUL 18

2.1 Chestiuni generale despre calculator **18**
2.2 Arhitectura unui calculator personal **19**
2.3 Mediile de stocare **24**
2.4 Dispozitive periferice **33**

SECȚIUNEA 3 – REȚELE DE CALCULATOARE 41

3.1 Teleprelucrarea datelor **41**
3.2 Tipuri de rețele **42**
3.3 Transmisia informației în cadrul rețelelor **47**
3.4 Protocoale de comunicații **49**
3.4.1 Modelul de referință ISO/OSI **50**
3.4.2 Modelul TCP/IP **52**
3.5 Elemente de interconectare a rețelelor **53**
3.5.1 Repetorul **54**
3.5.2 Puntea **54**
3.5.3 Routerul **55**
3.5.4 Porțile **56**

SECȚIUNEA 4 – INTERNETUL 57

4.1 Introducere **57**
4.2 Structura pachetului TCP/IP **59**
4.3 Moduri de conectare la Internet **66**
4.4 Aplicații de rețea în Internet **68**
4.5 World Wide Web **73**

CAPITOLUL II – REGLEMENTĂRI JURIDICE INTERNAȚIONALE ...81

SECȚIUNEA 1 – CRIMINALITATEA INFORMATICĂ ÎN REGLEMENTĂRI INTERNAȚIONALE 81

1.1 Introducere. Istoric **81**

1.2 Fenomenul criminalității informatice **83**

1.3 Recomandări. Rezoluții. Convenții **86**

SECȚIUNEA 2 – ASPECTE DE DREPT COMPARAT PRIVIND CRIMINALITATEA INFORMATICĂ 98

CAPITOLUL III – REGLEMENTĂRI JURIDICE INTERNE 155

SECȚIUNEA 1 – CADRUL LEGAL 155

SECȚIUNEA 2 – ANALIZA INFRACȚIUNILOR PREVĂZUTE ÎN LEGEA 161/2003 159

2.1 Explicații terminologice **159**

2.2 Accesul ilegal la un sistem informatic **162**

2.3 Interceptarea ilegală a unei transmisii de date informatice **174**

2.4 Alterarea integrității datelor informatice **189**

2.5 Perturbarea funcționării sistemelor informatice **205**

2.6 Operațiuni ilegale cu dispozitive şi programe informatice **209**

2.7 Falsul informatic **213**

2.8 Frauda informatică **225**

2.9 Pornografia infantilă prin intermediul sistemelor informatice **233**

SECȚIUNEA 3 – ASPECTE PRIVIND UNITATEA ŞI CONCURSUL DE INFRACȚIUNI 238

3.1 Aspecte privind unitatea şi concursul de infracțiuni **238**

3.1.1 Unitatea şi concursul de infracțiuni în cazul infracțiunilor îndreptate împotriva confidențialității şi integrității datelor informatice **238**

3.1.2 Unitatea şi concursul de infracțiuni în cazul infracțiunilor informatice **242**

3.2 Diferențierea între infracțiunile îndreptate împotriva datelor şi sistemelor informatice şi alte infracțiuni **244**

3.2.1 Infracțiunea de acces ilegal la un sistem informatic şi infracțiunea de accesare neautorizată a unui sistem electronic, prevăzută de art. 279 alin 2 din Legea 297/2004 privind piața de capital **245**

3.2.2 Infracțiunea de interceptare ilegală a unei transmisii de date informatice şi infracțiunea de violare a secretului corespondenței, prevăzută de art. 195 C.pen. **246**

3.2.3 Infracțiunea de alterare a integrității datelor informatice şi infracțiunile de distrugere şi furt, prevăzute de art. 217, respectiv 208 C.pen. **246**

3.2.4 Infracțiunea de fals informatic şi infracțiunile de fals prevăzute în Titlul VII din C.pen. **247**

3.2.5 Infracțiunea de fraudă informatică şi infracțiunea de înşelăciune, prevăzută de art. 215 C.pen **248**
3.2.6 Infracțiuni săvârşite prin intermediul sistemelor informatice în domeniul drepturilor de autor şi drepturilor conexe prevăzute în Legea 8/1996 ..... **250**
3.2.7 Infracțiunile prevăzute în art. 24-28 din Legea 365/2002 privind comerțul electronic şi infracțiunile contra datelor şi sistemelor informatice **251**

CAPITOLUL IV – ASPECTE DE PROCEDURĂ 253

SECȚIUNEA 1 – ASPECTE DE DREPT PROCESUAL PRIVIND CRIMINALITATEA INFORMATICĂ LA NIVEL INTERNAȚIONAL 253

1.1 Introducere **253**
1.2 Competența organelor de cercetare penală de a descoperi şi strânge probe dintr-un mediu informatizat **254**
1.3 Identificarea şi ridicarea de date informatice înregistrate sau stocate în sisteme sau pe suporți informatici **255**
1.4 Obligația cooperării active **257**
1.5 Punerea sub supraveghere a sistemelor informatice şi de telecomunicații **259**
1.6 Legalitatea strângerii, înregistrării şi interconexiunii de date cu caracter personal în cadrul procedurii penale **260**
1.7 Admisibilitatea probelor produse în cadrul sistemelor informatice în procedura penală..... .....**262**

SECȚIUNEA 2 – ASPECTE DE PROCEDURĂ ÎN DREPTUL INTERN 266

2.1 Introducere **266**
2.2 Sfera de aplicare.....**267**
2.3 Conservarea datelor informatice.....**268**
2.4 Ridicarea probelor care conțin date informatice **269**
2.5 Percheziția **270**
2.6 Interceptarea şi înregistrarea comunicațiilor desfăşurate prin intermediul sistemelor informatice **272**

SECȚIUNEA 3 – COOPERAREA INTERNAȚIONALĂ 274

CAPITOLUL V – ASPECTE CRIMINOLOGICE PRIVIND INFRACȚIONALITATEA INFORMATICĂ 276

SECȚIUNEA 1 – VULNERABILITATEA SISTEMELOR INFORMATICE 276

1.1 Factori care generează pericole **276**
1.2 Forme de manifestare a pericolelor în sistemele informaționale **280**

SECȚIUNEA 2 – INFRACTORII DIGITALI 284

SECȚIUNEA 3 – ACTIVISM, HACKTIVISM ŞI TERORISM INFORMATIC..... 297

3.1 Informație şi război informațional **297**

3.2 Concepte **298**

3.3 Activismul **301**
3.3.1 Colectarea de informații **302**
3.3.2 Publicarea **304**
3.3.3 Dialogul **309**
3.3.4 Coordonarea acțiunilor **310**
3.3.5 Acțiuni de lobby pe lângă factorii de decizie **312**

3.4 Hacktivismul **314**
3.4.1 Protestul virtual şi blocada **315**
3.4.2 Bombele Email **316**
3.4.3 Penetrarea paginilor de Web şi accesul neautorizat în sistemele de calcul **318**
3.4.4 Atacuri virale **321**

3.5 Terorismul informatic **323**
3.5.1 Cyberterorismul – un termen atipic **324**
3.5.2 Potențialul terorismului informatic **325**
3.5.3 Organizații cu potențial terorist în domeniul IT **328**
3.5.4 Cauzele recurgerii la cyberterorism **330**
3.5.5 Caracteristici ale cyberterorismului **331**
3.5.6 Domenii de risc **333**
3.5.7 Necesitatea elaborării unui cadrul legislativ **335**
3.5.8 Măsuri de prevenire a terorismului informatic **336**

3.6 Concluzii **338**

CONCLUZII ŞI PROPUNERI DE LEGE FERENDA 342

BIBLIOGRAFIE 350

spune că au două (sau mai multe) obiecte juridice, dintre care unul principal şi altul secundar (sau adiacent). În cazul de față, de exemplu, accesul neautorizat la un sistem informatic din domeniul apărării loveşte atât în siguranța națională şi capacitatea de apărare a statului, cât şi în instituția sau persoana titulară a sistemului penetrat ori a informațiilor accesate.

c) Obiect material

Constă în entitățile materiale care compun sistemele informatice (calculatoare, rețele de calculatoare, elemente Hardware – echipamente periferice, cabluri, plăci, servere etc. şi Software – programe, aplicații, baze de date etc.) şi din datele informatice spre care se îndreaptă atenția făptuitorului.

B. Subiecții infracțiunii

a) Subiectul activ

Poate fi orice persoană[91] responsabilă penal, textul neprevăzând o calitate specială pentru aceasta.

Practica judiciară a demonstrat însă că, în marea majoritate a cazurilor, asemenea persoane posedă cunoştințe în domeniul tehnologiei informației. Dintre aceştia, un procent însemnat îl reprezintă experții în sisteme de calcul şi rețelele de calculatoare, familiarizați cu „spargerea" măsurilor de securitate ale calculatoarelor sau rețelelor de calculatoare.

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

b) Subiectul pasiv

Este persoana fizică sau juridică proprietară sau deținătoare de drept a sistemului informatic accesat ilegal sau a datelor informatice vizate. Prin extensie, poate exista subiect pasiv colectiv, alcătuit dintr-o mulțime de persoane fizice sau juridice, atunci când accesul în sistemul informatic generează în mod automat accesul ilegal în alte sisteme similare interconectate cu primul.

Poate exista subiect pasiv secundar în cazul în care datele informatice vizate de accesul ilegal se referă la o persoană fizică sau juridică, alta decât proprietarul sau deținătorul de drept al respectivului sistem informatic. Spre exemplu, făptuitorul accesează ilegal sistemul integrat de evidență informatizată a persoanei şi intră în posesia datelor personale referitoare la un anumit individ (evident, cu scopul de a le folosi ulterior).

3. Conținutul constitutiv

A. Latura obiectivă

[91] Potrivit dispozițiilor noului Cod Penal, subiect activ al infracțiunii poate fi şi o persoană juridică (art.448). Aceasta va răspunde penal dacă fapta a fost săvârşită în numele sau în interesul persoanei juridice, de către organe sau reprezentanți ai acesteia.

a) Elementul material

Se realizează prin accesul fără drept într-un sistem informatic (stație de lucru, server ori rețea informatică).

Accesul, în înțelesul dat de lege, desemnează intrarea în tot sau numai într-o parte a sistemului informatic. Metoda de comunicare – la distanță, inclusiv grație legăturii prin satelit sau nu, ori de aproape – nu prezintă importanță.

În forma sa cea mai simplă, **accesul fără drept la un sistem informatic** presupune *o interacțiune a făptuitorului cu tehnica de calcul vizată* prin intermediul echipamentelor sau diverselor componente ale sistemului vizat (sursă de alimentare, butoane de pornire, tastatură, mouse, joystick). Manipularea acestor dispozitive se transformă în solicitări către Unitatea Centrală de Prelucrare (UCP) a sistemului, care va procesa date ori va rula programe de aplicații în beneficiul intrusului.

Va exista acces ilegal în formă simplă şi în cazul în care intrusul, manipulând propriile echipamente periferice, de la distanță, găseşte şi utilizează o cale externă de intrare într-un alt sistem de calcul. Este cazul tipic al accesării unei alte stații de lucru aflate într-o rețea.

Pentru obținerea accesului, făptuitorul va încerca o gamă variată de procedee tehnice, cum ar fi: atacul prin parolă, atacul de acces liber, atacul care exploatează slăbiciunile tehnologice, atacul care exploatează bibliotecile partajate, atacul IP ori atacul prin deturnarea TCP etc..[92]

Atacuri prin parolă. Spargerea parolelor în rețea

Pentru înțelegerea modului de operare al hackerilor în cazul atacurilor asupra parolelor în rețele, am ales ca exemplu sistemele de operare Windows NT şi UNIX.

Pentru a prelua parolele dintr-o rețea Windows NT, un hacker trebuie să aibă acces la cel puțin un nume de utilizator şi la implementarea NT a algoritmului MD4. După ce copiază baza de date (unicul loc în care poate găsi numele de utilizator şi funcția hash MD4), hackerul va efectua un *atac prin forță brută* sau un *atac prin dicționar* împotriva fişierului cu parole.

Deoarece numai administratorii de sistem pot accesa directorul *sam* (unde Windows NT îşi localizează baza de date cu parole), unica modalitate pentru hacker de a găsi baza de date este fie de la consolă, fie dintr-o copie backup a bazei de date (situată, de exemplul, pe un disc de reparații). Cu alte cuvinte, pentru a ajunge la baza de date, hackerul trebuie să aibă acces fizic la consolă sau la o copie a bazei de date. Dacă serverul şi copiile backup de server sunt securizate fizic, riscul de atac prin intermediul bazei de date cu parole se reduce semnificativ.

Atacul parolelor prin forță brută la Windows NT

[92] L. Klander, *Anti-Hacker*, Ed. All Educational, Bucureşti, 1998, p. 22, 23, 24, 25, 250, 430, 431, 508, 509

simulată. Dacă hackerul creează o bară de meniuri simulată, acesta poate afişa caseta de dialog cu informaţiile despre document folosind informaţii manipulate.

Pe scurt, hackerul poate anula toate posibilele indicii pe care victima le poate accesa pentru a determina o falsă conexiune Web prin limbaje de Scripting. Unica apărare a victimei atacate este de a dezactiva limbajele de scripting din browser.

Se afirmă că unica modalitate de prevenire a unui atac prin simularea Web-ului este localizarea şi pedepsirea hackerului. Datorită naturii atacului, serverul hackerului trebuie să-şi precizeze locaţia pentru a putea realiza atacul. Dacă victima detectează atacul, locaţia serverului va fi aproape sigur dezvăluită. Din păcate, hackerii care realizează atacuri prin simularea Web-ului vor acţiona în majoritatea cazurilor de pe computere furate. Sistemele furate reprezintă baza ideală pentru atacurile prin simularea Web-ului, din acelaşi motiv pentru care spărgătorii de bănci folosesc maşini furate pentru a dispărea[138].

b) Urmarea imediată constă în obţinerea de date necorespunzătoare adevărului şi, prin aceasta, crearea unei stări de pericol pentru încrederea care se acordă datelor informatice şi, în general, prelucrării automate a acestora.

c) Legătura de cauzalitate între activitatea făptuitorului şi urmarea produsă trebuie dovedită.

B. Latura subiectivă

Infracţiunea de fals informatic se săvârşeşte numai cu ***intenţie directă***, calificată prin scop.

În condiţiile inserării, modificării sau ştergerii de date informatice, va exista infracţiune chiar dacă persoana a alterat adevărul din cuprinsul acestor date cu un scop „legitim" (de exemplu, pentru a crea proba unei situaţii juridice reale). De asemenea, nu este necesară utilizarea efectivă a acestor date, ci numai obţinerea lor în vederea realizării scopului propus.

Scopul urmărit îl reprezintă utilizarea datelor necorespunzătoare obţinute în vederea producerii unei consecinţe juridice. Datele sunt susceptibile să producă consecinţe juridice dacă sunt apte să dea naştere, să modifice sau să stingă raporturi juridice, creând drepturi şi obligaţii[139].

---

[138] Bineînţeles că prin acţiunea de săvârşire a infracţiunii de fals informatic se pot întruni şi elementele constitutive ale altor infracţiuni îndreptate împotriva datelor şi sistemelor informatice (spre exemplu, se poate folosi falsul informatic pentru a realiza o interceptare a datelor informatice, ori se poate realiza falsul informatic ca urmare a accesului ilegal la un sistem informatic ori pentru săvârşirea unei fraude informatice, etc…). Am analizat aceste modalităţi în cazul infracţiunii de fals informatic datorită specificului pe care îl prezintă, respectiv obţinerea de date necorespunzătoare adevărului şi aptitudinea de a produce consecinţe juridice.

[139] Vezi în acest sens Vintilă Dongoroz, Siegfried Kahane, Ion Oancea, Iosif Fodor, Nicoleta Iliescu, Constantin Bulai, Rodica Stănoiu, Victor Roşca, Explicaţii teoretice ale codului penal român, vol. IV, Editura Academiei Române, Bucureşti, 1972 , pag.428, V.Dobrinoiu şi colaboratorii, op.cit., pag.618; A. Boroi, G.Nistoreanu, Drept penal, partea specială, Editura AllBeck, Bucureşti, 2004, pag.723; O.Loghin, A.Filipaş, Drept penal român. Partea specială, Casa de Editură şi

4. Forme. Modalităţi. Sancţiuni

A. Forme. Actele pregătitoare, deşi posibile, nu sunt incriminate şi ca atare nu sunt pedepsite.

Tentativa se pedepseşte (conform art. 50 din lege).

Infracţiunea se consideră consumată atunci când făptuitorul a introdus, modificat ori şters în vreun fel acele date informatice dintr-un sistem ori a restricţionat accesul la respectivele date dacă prin aceasta s-au produs alte date sau situaţii juridice necorespunzătoare valorii de adevăr iniţiale.

B. Modalităţi. Infracţiunea analizată prezintă patru modalităţi normative, respectiv introducerea, modificarea, ştergerea de date informatice, precum şi restricţionarea accesului la aceste date.

Acestor modalităţi normative pot să le corespundă variate modalităţi de fapt.

C. Sancţiuni. Pedeapsa prevăzută este închisoarea de la 2 la 7 ani[140].

5. Aspecte procesuale

Acţiunea penală se pune în mişcare din oficiu.

Presă „Şansa" S.R.L., Bucureşti, 1992, p.269; T. Toader, Drept penal, partea specială, Editura AllBeck, Bucureşti, 2002, pag.386

[140] Aceeaşi pedeapsă este prevăzută şi de art. 445 din noul Cod Penal.