Combaterea crimei organizate prin dispoziţii de...

By: Laura Codruta Kovesi

As of: Oct 1, 2016 4:31:56 PM
23,158 words - 384 matches - 45 sources

Similarity Index
59%

Mode: Similarity Report ▼

paper text:

CAPITOLUL VI CRIMINALITATEA INFORMATICĂ Secţiunea I Criminalitatea informatică în reglementările internaţionale Apariţia şi dezvoltarea fără precedent a tehnologiei informatice a deschis şi posibilitatea apariţiei unei game variate de acţiuni ilicite, unele cu caracter extrem de sofisticat. Astăzi, calculatorul a pătruns în toate domeniile de activitate, iar criminalitatea informatică a luat o amploare deosebită atât în plan intern, cât şi în plan internaţional, datorită rolului jucat de calculatoare, care

nu sunt utilizate doar pentru creşterea performanţelor economice sau sociale **ale unei ţări,** ci **acestea au devenit parte integrantă a vieţii personale a individului.** 1

Expansiunea transnaţională extraordinar de rapidă a reţelelor de calculator **şi extinderea accesului la aceste reţele prin intermediul telefoniei mobile** a **dus la creşterea vulnerabilităţii acestor sisteme şi la crearea de oportunităţi pentru producerea de** 1

infracţiuni343. Cu mulţi ani în urmă au existat comentarii care avertizau că, într-o bună zi, computerul va fi implicat în toate formele de delicvență.344 Dacă luăm în considerare datele statistice din ultimii ani se poate susţine că fenomenul criminalităţii informatice este în continuă creştere. În legătură cu definiţia criminalităţii informatice au existat şi există mai multe opinii atât în plan intern, cât şi internaţional. Astfel,

în studiile elaborate pe plan internaţional, Raportul Comitetului **European pentru** Probleme **Criminale** 4

a adoptat următoarea definiţie:

„Abuzul informatic este orice comportament ilegal sau contrar eticii sau neautorizat care priveşte un tratament automat de date şi/sau transmitere de date” 1

345. O altă definiţie privind criminalitatea prin calculator a fost dată încă din anul 1985, aceasta fiind „toate faptele în care prelucrarea automată a datelor este un mijloc de acţiune şi care motivează bănuirea unei fapte penale”346. Această definiţie include atât delictele criminalităţii prin calculator în sens restrâns, cât și toate delictele în care prelucrarea automată a datelor serveşte la comiterea de fapte penale. 343

Dobrinoiu, Maxim, Infracţiuni în domeniul informatic, Editura **C.H. Beck, Bucureşti 2006,** 7

p. 60 344 Voicu, Costică, Boroi, Al.,

Dreptul penal al afacerilor, , Editura **C.H. Beck, Bucureşti 2006, p.** 6

356 345 Dobrinoiu, M.,

op., cit., p. 62. **346** Dobrinoiu, **M., op., cit., p.** 44

62. 358 Alţi autori definesc criminalitatea informatică:

„Orice acţiune ilegală în care un calculator constituie instrumentul sau obiectul delictului, altfel spus orice infracţiune al cărei mijloc sau scop este influenţarea funcţiei unui calculator” 347. 13

Abuzul informatic este **definit, la rândul său, prin „orice incident legat de tehnica informatică în care o persoană a suferit sau ar fi putut să sufere un prejudiciu şi din care autorul a obţinut sau ar fi putut obţine intenţionat un profit”** 348, **sau prin „totalitatea faptelor comise în zona noilor tehnologii, într-o anumită perioadă de timp şi pe un anumit teritoriu bine determinat”**

349. În faţa acestei creşteri a criminalităţii informatice, legislaţia comunităţii internaţionale este într-o continuă schimbare şi adaptare la noile realităţi.

Din ce în ce mai multe state au procedat la armonizarea propriilor legislaţii în vederea combaterii 1

acestui fenomen.

Problemele ridicate în cadrul reuniunilor internaţionale privind combaterea criminalităţii organizate sunt următoarele: ‣ lipsa unui consens global privind definiţia „criminalităţii informatice”; ‣ lipsa unui consens global privind motivaţia realizării acestor fapte; ‣ lipsa expertizelor din partea persoanelor autorizate aparţinând unor instituţii cu atribuţii de control în domeniu; ‣ inexistenţa unor norme legale adecvate privind accesul şi investigaţia sistemelor informatice, inclusiv lipsa normelor prin care pot fi confiscate bazele de date computerizate; ‣ lipsa armonizării legislative privind investigaţiile în domeniu; ‣ caracterul transnaţional al acestui tip de infracţiune; ‣ existenţa unui număr redus de tratate internaţionale privind extrădarea şi asistenţa mutuală în domeniu. Organizaţia pentru Cooperare Economică şi Dezvoltare (OECD) a fost una dintre primele organizaţii internaţionale care a realizat un studiu privind armonizarea legislaţiei în domeniu. În anul 1983, OECD a publicat un raport 1

347 Dobrinoiu, M., op., cit., p. 62. 348 Vasiu, I., Criminalitatea informatică, Editura Nemira, Bucureşti, 1998, p. 27 349

Amza, T., Amya, C.P., Criminalitatea informatică, Editura Lumina Lex, Bucureşti, 2003, 7

p. 13. 359

prin care a propus diferite recomandări legislative statelor membre ale Uniunii Europene precum şi o listă minimă de activităţi care trebuiau pedepsite: fraudarea şi falsificarea pe calculator, alterarea programelor de calcul şi a datelor, copyright-ul, interceptarea comunicaţiilor sau a altor funcţii a unui calculator, accesul şi utilizarea neautorizată a unui calculator. În completarea raportului OECD, Consiliul Europei a iniţiat propriul studiu de caz pentru dezvoltarea cadrului legal privind combaterea criminalităţii informatice. Comisia de experţi 1

a Consiliului Europei a adoptat Recomandarea R (89)9 care reprezintă un ghid de acţiune pentru statele membre ale Uniunii Europene. Organizaţia Naţiunilor Unite s-a implicat, la rândul ei, în studiul şi combaterea fenomenului analizat. Au fost publicate numeroase documente, dintre care amintim: raportul „Propuneri privind concertarea acţiunilor internaţionale privind combaterea oricărei forme de activitate criminală” (1985); „Rezoluţia introdusă de reprezentantul Canadei privind combaterea criminalităţii pe calculator” (1990); „Declaraţia Naţiunilor Unite privind principiile de bază ale justiţiei aplicabile victimelor abuzului de putere şi crimei” (1990); raportul „Provocarea fără frontiere: Cybercrime - eforturi internaţionale pentru combaterea crimei organizate, transnaţionale” (2000). 9

În ceea ce priveşte criminalitatea informatică, statele membre ale Uniunii Europene, au identificat

patru activităţi distincte: • activităţile **care aduc atingere vieţii private: colectarea, stocarea, modificarea şi dezvăluirea datelor cu caracter personal;** • activităţile **de difuzare a materialelor cu conţinut obscen şi/sau xenofob: materiale cu caracter pornografic,** 1

materiale cu caracter rasist şi care incită la violenţă; • criminalitatea economică, accesul neautorizat şi sabotajul; activităţi prin care se urmăreşte distribuirea de viruşi, spionajul şi frauda realizată prin calculator, distrugerea de date şi programe sau alte infracţiuni; programarea unui calculator de a „distruge" alt calculator 13

• încălcarea dreptului de proprietate intelectuală. În ceea ce priveşte documentele juridice, Consiliul Europei a iniţiat numeroase demersuri pentru reglementarea activităţii informatice, dintre care enumerăm următoarele: ►

Recomandarea R(85)10 - cuprinde **normele de aplicare a Convenţiei Europene de Asistenţă Mutuală în Materie Infracţională, cu referire la comisiile rogatorii privind interceptarea telecomunicaţiilor; ► Recomandarea R(88)2 privind pirateria în contextul existenţei drepturilor de autor şi a drepturilor conexe; ► Recomandarea R(87)15 privind reglementarea utilizării datelor personale în munca de poliţie; ► Recomandarea R(95)4 privind protecţia datelor personale în domeniul serviciilor de telecomunicaţii; ► Recomandarea R(95)13 privind aspecte de procedură penală în legătură cu Tehnologia Informaţiei; ► Rezoluţia 1 adoptată de miniştrii europeni ai justiţiei (1997) care recomandă Comitetului de Miniştri sprijinirea Comitetului European pentru Probleme Infracţionale în combaterea criminalităţii informatice printr-o armonizare a prevederilor legale naţionale în materie;** 1

► „Recomandarea nr.

R(89)9" - este **cea mai importantă** decizie **a Consiliului Europei** 2

şi priveşte

unele norme care trebuie aplicate de statele membre pentru combaterea criminalităţii informatice. 1
Aceasta Recomandare are meritul de a fi realizat o primă definire a faptelor ilegale în legătură cu sistemele informatice, în paralel cu o împărţire a acestora în două secţiuni intitulate sugestiv: lista minimală şi lista facultativă. ► „Lista minimală” cuprinde: frauda informatică; falsul informatic; prejudiciile 361 aduse datelor sau programelor pentru calculator; sabotajul informatic; accesul neautorizat; interceptarea neautorizată; reproducerea neautorizată de programe protejate pentru calculator; reproducerea neautorizată a unei topografii protejate. „Lista facultativă” conţine: alterarea datelor şi programelor pentru calculator; spionajul informatic; utilizarea neautorizată a unui calculator; utilizarea neautorizată a unui program protejat pentru calculator. Recomandarea R(89)9 sugera entităţilor statale să manifeste adaptabilitate, iar listele anterior menţionate să fie completate cu alte fapte susceptibile de incriminare, cum ar fi: crearea şi difuzarea de viruşi informatici, traficul cu parole obţinute ilegal etc. destinate să faciliteze penetrarea unui sistem informatic, tulburând buna funcţionare a acestuia ori a programelor informatice stocate ş.a.m.d.

350; ► „Recomandarea nr.

R(95)13” privind probleme legate de procedura judiciară a cazurilor legate de tehnologia 1
informatică şi de crearea de autorităţi cu atribuţii în acest domeniu. Principalele norme statuate de această Recomandare au constituit baza modificării Codurilor de procedură penală ale statelor europene şi

se referă la următoarele domenii: a) „în

privinţa căutării şi copierii datelor” • trebuie făcută distincţia dintre activităţile de căutare şi 2
copiere a datelor dintr-un calculator şi cea de interceptare a transmisiunii datelor; • Codul de procedură penală trebuie să permită autorităţilor competente să controleze sistemele de calculatoare în condiţii similare celor care au permis scanarea şi furtul datelor. Sancţiunile împotriva acestor fapte trebuie extinse asupra ambelor tipuri de activităţi ilegale; • pe parcursul realizării oricărui tip de investigaţii, autorităţilor specializate trebuie să li se permită, atunci când este necesar, extinderea cercetărilor si asupra altor sisteme de calculatoare legate în reţea cu cel aflat sub investigaţie şi care se află în zona de jurisdicţie.

350 I. Vasiu, op. cit., p. 49.

b) „în privinţa tehnicii de supraveghere”: • din punct de vedere al convergenţei dintre tehnologia informatică şi telecomunicaţii, legislaţia trebuie să permită introducerea tehnicii de interpretare **şi supraveghere a sistemului de telecomunicaţii în scopul combaterii criminalităţii informatice; • legislaţia trebuie să permită autorităţilor abilitate să utilizeze întreaga tehnică disponibilă pentru a putea să monitorizeze traficul dintr-o reţea în cazul unei investigaţii; • datele obţinute prin monitorizarea traficului precum şi rezultatele obţinute prin prelucrarea acestora trebuie protejate conform legislaţiei în vigoare; • Codurile de procedură trebuie revizuite pentru a se facilita procedurile oficiale de interceptare, supraveghere şi monitorizare, în scopul evitării aducerii unor atingeri confidenţialităţii, integrităţii şi validităţii sistemului de telecomunicaţii sau al reţelelor de calculatoare. c) „în privinţa obligativităţii** 2

cooperării cu autorităţile abilitate”: • multe dintre reglementările legale ale statelor lumii permit autorităţilor abilitate să le solicite persoanelor care se bucură de un anumit tip de imunitate sau sunt protejate de lege, punerea la dispoziţie a materialului probator. În paralel, prevederile legale trebuie să oblige persoanele implicate să prezinte orice tip de material necesar investigaţiilor unui sistem de calculatoare; • pentru persoanele care se bucură de un anumit tip de imunitate sau sunt protejate de lege, autorităţile abilitate trebuie să aibă puterea şi competenţa de a solicita orice material, aflat sub controlul acestora, necesar investigaţiilor. Codul de procedură penală trebuie să prevadă acelaşi lucru şi pentru alte persoane care au cunoştinţe privind funcţionarea unei reţele de calculatoare şi care aplică măsurile de securitate asupra acestora; • operatorilor reţelelor publice sau private de calculatoare care deservesc sistemele de telecomunicaţii trebuie să li se impună obligaţii specifice care să le permită interceptarea comunicaţiilor la solicitarea organismelor abilitate; • aceleaşi obligaţii specifice trebuie impuse şi administratorilor de reţele ale serviciilor de telecomunicaţii pentru identificarea unui utilizator, la solicitarea autorităţilor în drept. d) „referitor la **evidenta electronică” - activităţile de stocare, protejare şi expediere ale evidenţelor electronice trebuie să se reflecte prin autenticitatea şi integritatea irefutabilă a materialelor, atât pentru necesităţile private, cât şi pentru cele oficiale. Procedurile şi metodele tehnice ale manipulării evidenţelor electronice trebuie dezvoltate, asigurându-se compatibilitatea lor între statele membre. Prevederile Codului de procedură penală aplicabile documentelor obişnuite pe suport de hârtie trebuie aplicate şi documentelor stocate electronic.** 1

e) „în privinţa utilizării

criptării” - trebuie luate măsuri prin care să se prevadă limitarea efectelor negative ale criptografiei în cazul aplicării acesteia în investigaţii oficiale, fără a afecta legitimitatea utilizării acestei metode 1

mai mult decât este necesar. f) „referitor la cercetare, statistică, instruire”: • riscul impunerii noilor aplicaţii tehnologice în raport cu comiterea infracţiunilor informatice trebuie studiat continuu. Pentru a se permite autorităţilor cu atribuţii în combaterea acestui fenomen să ţină pasul cu nivelul tehnic al cauzelor pe care le investighează, trebuie să se realizeze o bază de date care să cuprindă şi să analizeze cazurile cunoscute de criminalitate informatică - modul de operare, aspecte tehnice şi încadrări juridice; • trebuie creat un corp de specialişti pregătiţi şi instruiţi continuu în domeniul expertizelor impuse de fenomenul realizat. g) cooperarea internaţională”: • trebuie impuse competenţe care să permită instituţiilor abilitate să desfăşoare investigaţii şi în afara zonei de jurisdicţie, dacă este necesară o intervenţie rapidă. Pentru a se evita posibilele încălcări ale suveranităţii unui stat sau ale legilor internaţionale, cadrul legal existent in momentul de faţă trebuie modificat şi completat corespunzător pentru eliminarea ambiguităţilor. Trebuie să se negocieze rapid la nivel internaţional pentru obţinerea unui acord care să precizeze cum, când şi ce este permis în efectuarea unei investigaţii; • trebuie realizată îmbunătăţirea acordului mutual de asistenţă care este în vigoare, pentru clarificarea tuturor problemelor care pot apărea în cadrul unei investigaţii privind autorizarea verificării unei anumite reţele informatice, confiscarea unor anumite tipuri de date necesare anchetei, interceptarea telecomunicaţiilor specifice sau monitorizarea traficului. La sfârşitul anului 1997, cu prilejul Summitului G8 de la Denver, miniştrii de interne şi de justiţie ai statelor membre prezenţi la reuniune au luat act de intensificarea fără precedent a acţiunilor criminale în domeniul informaticii, adoptând un document final. Reprezentanţii G8 au discutat despre pericolul acestui tip de infracţionalitate pe care 1 -au clasificat în două mari domenii: ► criminalitatea informatică - are ca ţinte de distrugere reţelele de calculatoare şi sistemul de telecomunicaţii, fapt care produce pagube importante atât autorităţilor oficiale cât şi persoanelor private; ► organizaţiile teroriste sau de crimă organizată - care utilizează facilităţile noilor tehnologii pentru săvârşirea de infracţiuni deosebit de grave. Comunicarea prezentată la sfârşitul Summitului G8 din anul 1997 cuprinde 10 principii şi direcţii de acţionare pentru combaterea criminalităţii informatice, idei care vor fi

adoptate începând din anul 1998. Aceste principii sunt: ‣

nu trebuie să existe nici un loc sigur pentru cei care comit abuzuri prin intermediul tehnologiei 1 informaţiei; ‣ investigaţiile şi pedepsele aplicate acestor infracţiuni trebuie coordonate cu sprijinul tuturor statelor, chiar dacă nu se produce nici un fel de pagubă; ‣ legea trebuie să combată explicit fiecare infracţiune de acest tip; 365 ‣ legea trebuie să protejeze confidenţialitatea, integritatea şi utilitatea bazelor de date informatice, precum şi să sancţioneze pătrunderea neautorizată în sistemele informatice; ‣ legea trebuie să permită apărarea şi conservarea bazelor de date cu caracter rapid, cele mai expuse din punct de vedere al atacurilor exterioare; ‣ regimul de asistenţă mutuală al statelor trebuie să permită informarea periodică şi în caz de necesitate, în situaţiile unor infracţiuni trans- continentale; ‣ accesul

la baza de date electronice deschise trebuie să se poată realiza liber, fără acordul statului pe teritoriul căruia se află acestea; ‣ regimul juridic privind trimiterea şi autentificarea datelor electronice utilizate în cazul investigaţiilor informatice trebuie dezvoltat; ‣ extinderea unui sistem de telecomunicaţii practic şi sigur trebuie cumulată cu implementarea unor mijloace de detecţie şi prevenire a abuzurilor; ‣ activitatea în acest domeniu trebuie coordonată de instituţii şi foruri internaţionale specializate în domeniul informatic. Planul de acţiune cuprinde următoarele direcţii; • utilizarea reţelei proprii de calculatoare şi a cunoştinţelor acumulate în domeniu pentru a asigura o comunicare exactă şi eficientă privind cazurile de criminalitate care apar în reţelele mondiale; • realizarea paşilor necesari creării unui sistem legislativ modern eficace pentru combaterea fenomenului care să fie pus la dispoziţia statei membre; • revizuirea legislaţiei naţionale a ţărilor membre şi armonizarea acesteia cu legislaţia penală necesară combaterii criminalităţii informatice; • negocierea unor acorduri de asistentă şi cooperare; • dezvoltarea soluţiilor tehnologice care să permită căutarea transfrontalieră şi realizarea unor investigaţii de la distanţă; • dezvoltarea procedurilor prin care se pot obţine date de interes de la 366 responsabilii sistemelor de telecomunicaţii; • concertarea eforturilor ca ramurile industriale pentru obţinerea celor mai noi tehnologii utilizate în combaterea criminalităţii informatice; • asigurarea de asistenţă în cazul unor solicitări urgente prin întregul sistem tehnologic propriu; • încurajarea organizaţiilor internaţionale din sistemul informatic şi cele din telecomunicaţii pentru creşterea standardelor şi măsurilor de protecţie oferite sectorului privat; • realizarea unor standarde unice privind transmiterea datelor electronice utilizate în cazul investigaţiilor oficiale sau private.

Secţiunea a 2-a Aspecte de drept comparat privind criminalitatea informatică 30

Africa de Sud În Africa de Sud, stat semnatar al Convenţiei Europene asupra criminalităţii informatice, este în vigoare Legea Comunicaţiilor Electronice şi Tranzacţiilor din 2 august 2002351. În cuprinsul acestei legi, în Capitolul XIII, intitulat „Criminalitatea informatică” (art. 85-89), sunt incriminate infracţiunile de accesare neautorizată şi intercepţia datelor într-un sistem informatic, precum și distrugerea și restricţionarea accesului la asemenea date. De asemenea, se pedepsește 1

persoana care, în mod ilegal, produce, comercializează, distribuie, procură pentru folosinţă programe informatice ori 1

componente dar si persoanele care utilizează in mod ilegal unul dintre dispozitivele ori programele informatice. Legea din republica Africa de Sud sancţionează și falsul și frauda informatică, precum si tentativa, complicitatea sau instigarea la faptele penale descrise mai sus. 351 http://cybberlawsa.co.za Australia Legea criminalităţii informatice, din anul 2001, incriminează următoarele fapte352: ‣ modificarea neautorizată a datelor informatice; ‣ accesul neautorizat

la respectivele date sau la oricare alte date stocate în sistemul informatic;	1

‣ cel care atentează la siguranţa, securitatea şi operarea oricăror asemenea date; ‣ perturbarea neautorizată a unei comunicaţii electronice; ‣ accesul neautorizat sau modificarea unor date restricţionate; ‣

punerea în pericol, fără drept, a datelor stocate pe un suport de memorie;	1

‣

deţinerea sau controlul de date informatice cu scopul comiterii unei infracţiunii **informatice;**	1

‣

producerea, distribuirea sau obţinerea de date cu scopul de a comite infracţiuni informatice.	1

Austria Legea privind protecţia datelor private, din anul 2002, în

Secţiunea 10, prevede că în situaţiile în care delictele produse prin intermediul calculatorul **nu au relevanţă juridică pentru instanţă sau nu sunt pedepsite prin alte** cauze **penale administrative, acestea se sancţionează** doar **cu amendă. Belgia Prin Legea criminalităţii informatice, din 28 noiembrie** 2000, **a fost modificat Codul penal belgian**	9

şi incriminează în plus (art. 210 bis, 550 bis 550ter)353: ‣

persoana care comite un fals prin introducerea, modificarea sau ştergerea de date informatice stocate ori transmise printr **-un sistem informatic**	1

352 http://cybbercrimelaw.net/countries/australia.html 353 http://cybbercrimelaw.net/countries/belgium.html 368

ori prin restricţionarea prin orice mijloace tehnice a accesului la aceste date dintr **-un sistem informatic;** 1

‣

persoana care utilizează date informatice astfel obţinute, ştiind că sunt false; 1

‣ tentativa la aceste infracţiuni se pedepseşte; ‣

persoana care obţine, pentru sine sau pentru altul, un avantaj patrimonial ilicit prin introducerea, modificarea sau ştergerea de date informatice stocate sau transmise prin intermediul unui sistem informatic ori prin restricţionarea prin orice mijloace tehnice a accesului la aceste date dintr **-un sistem informatic;** 1

‣ se sancţionează şi

persoana care accesează un sistem informatic, ştiind că nu **este autorizată; ‣ de** 1

asemenea, este culpabilă de săvârşire a unei infracţiuni informatice

persoana care, în scop fraudulos sau pentru a cauza un prejudiciu îşi depăşeşte drepturile la un sistem informatic; 1

‣ persoana care dispune comiterea uneia dintre infracţiunile informatice sau care incită la comiterea unor asemenea fapte;

persoana care, cunoscând ca datele informatice au fost obţinute ca rezultat al 1

unor infracţiuni informatice, le deţine ori le divulgă altei persoanei; pedepsele

vor fi dublate dacă o infracţiune de acest fel va fi comisă într-un interval de 5 ani de **la** pronunțarea **unei condamnări definitive;** 1

‣ constituie infracţiune şi fapta persoanei

care, cu intenţia de a cauza un prejudiciu, direct sau indirect, introduce, modifica, şterge sau restricţionează prin orice modalitate accesul la dalele **unui sistem informatic;** 1

‣ persoana care, prin comiterea de infracţiuni informatice

cauzează o pagubă datelor conţinute într-un sistem informatic sau în alt sistem informatic la distanţa, 1

se pedepseşte; ‣ se pedepseşte şi

persoana care, cu intenţie ilicită sau cu scopul de a cauza un prejudiciu, pune la dispoziţie, difuzează sau comercializează date informatice stocate sau transmise printr-un sistem informatic, ştiind că respectivele date ar putea fi utilizate pentru producerea unei pagube sau pentru împiedicarea funcţionării corespunzătoare a unui sistem informatic. 1

Canada Codul penal, în Secţiunea 342.1, sancţionează faptul că354: „O persoană în

mod fraudulos sau neautorizat: a) utilizează, direct sau indirect, un serviciu informatic; b) interceptează, direct sau indirect, cu ajutorul unui dispozitiv electromagnetic, acustic, mecanic sau de orice alt tip orice funcţiune a unui calculator; c) utilizează sau produce utilizarea unui sistem informatic pentru realizarea unei acţiuni prevăzute la lit. a) sau b) sau altei infracţiuni informatice; d) posedă, utilizează, navighează sau permite altei persoane să aibă acces la parola unui calculator pentru a 1

săvârşi o infracţiune informatică”.

Franţa Codul penal francez prevede în Capitolul III, denumit **„Acţiuni îndreptate contra sistemelor automatizate”, următoarele** infracţiuni:355 ‣ **accesul fraudulos într-un sistem întreg sau parţial de prelucrare automată de date** 1

(art. 423-1); ‣

împiedicarea sau deformarea funcţionării unui sistem de prelucrare automată 1

(323-2); ‣

introducerea frauduloasă a datelor într-un sistem de prelucrare automată sau oprimarea **sau modificarea frauduloasă a datelor pe care le** 1

conține (art.

323-3); ‣ importarea, deţinerea, oferirea, cedarea, punerea la dispoziţie fără vreun anumit motiv, a unui echipament, instrument, program informatic sau 1

354 www.lexinformatica.org/cybbercrime 355 O.G. nr. 916/2000 şi Legea nr. 575/2004.

vreunei date concepute sau special adoptate **pentru comiterea** unor **sau mai multor infracţiuni** informatice (art. **323-** 1

31); ‣

participarea la o grupare formată sau la o înţelegere stabilită în vederea pregătirii caracterizată de unul sau mai multe fapte materiale, a uneia sau mai multor infracţiuni, se pedepseşte (art. **323-** 1

4); ‣ persoanele fizice vinovate de infracţiuni informatice pot primi una sau mai multe din pedepsele complementare prevăzute de lege (art. 323-5); ‣

persoanele juridice pot fi declarate penal responsabile pentru comiterea **de** 1

infracţiuni juridice şi pot fi sancţionate cu amendă şi pedepse complementare; ‣ tentativa la aceste infracţiuni se pedepseşte ca şi infracţiunea consumată. Trebuie să mai precizăm că

legislaţia franceză incriminează numai faptele care aduc atingere integrităţii şi securităţii sistemelor informatice. Nu incriminează în schimb falsul şi frauda informatică, considerând că sunt acoperite de prevederile dreptului comun. 1

Germania Codul penal federal conţine anumite prevederi legale, disparate în articole separate şi nu într-un titlu distinct,

care tratează modalităţi electronice de comitere a unor infracţiuni considerate drept 1
tradiţionale356. Astfel, **art. 202** incriminează **„spionajul datelor”**

ca fiind fapta persoanei

care, fără autorizaţie, obţine, pentru sine sau pentru altul, date care nu îi sunt **adresate ori erau** 1
în mod special protejate împotriva accesului neautorizat.

Art. 263 din Codul penal german sancţionează „frauda informatică” ca fiind fapta persoanei

care, cu intenţia de a obţine ilegal, pentru sine sau pentru altul, un avantaj, provoacă un prejudiciu patrimonial unei alte persoane prin influenţarea rezultatului unei procesări automate de date informatice prin 1

configurarea incorectă a unui program informatic, folosirea unor date incorecte sau incomplete, folosirea neautorizată a unor date sau orice altă influenţă 1

356 http://icpo-vad.tripod.com/crimen.html neautorizată asupra ordinii evenimentelor. Codul penal german incriminează şi „alterarea integrităţii datelor” (art.303); „sabotarea unui sistem informatic” (art. 303 b); „ingerinţa într-un sistem de

telecomunicaţii” (art. 317). Grecia Codul penal al Greciei prevede357 în art. 370 §. 2 că: ‣ se pedepseşte

accesul ilegal la date stocate electronic sau transmise prin reţea **de telecomunicaţii;** 1

‣

dacă activităţile ilegale prejudiciază relaţiile internaţionale sau securitatea statului grec, 1

fapta este sancţionată mai aspru (circumstanţă agravantă).

Grecia nu incriminează decât accesul ilegal, celelalte incriminări fiind acoperite de prevederile dreptului comun. 1

Danemarca Codul penal danez, în art. 263358, prevede: ‣

acţiunea prin care o persoană obţine acces la datele sau programele unei alte persoane şi le utilizează în folos personal se pedepseşte; 1

‣

acţiunea prin care se obţine accesul la date considerate secrete constituie circumstanţă agravantă. 1

Danemarca incriminează numai accesul ilegal, celelalte fapte putând fi acoperite în legislaţia daneză de prevederile de drept comun. Elveţia Codul penal 1

elveţian359 incriminează următoarele fapte: ‣ „sustragerea de date informatice” - constă în fapta aceluia

care, cu intenţia de a obţine pentru sine sau pentru altul **un folos material injust sustrage pentru sine sau pentru altul, date înregistrate sau transmise electronic sau printr-** 1

357 http://cybbercrimelaw.net/countries/grece 358 http://cybbercrimelaw.net/countries/denmark 359 http://cybbercrime.admin.ch

o modalitate similară, care nu îi erau destinate şi care erau în mod expres protejate împotriva accesului ilegal 1

(art. 143); ‣ **„accesul ilegal la un sistem informatic”** 1

- constituie fapta aceluia

care, fără a avea intenţia de a obţine un avantaj material injust, cu ajutorul unui mijloc de transmisie a datelor, accesează ilegal un sistem informatic aparţinând altei **persoane, protejat în mod** fraudulos **contra pătrunderii neautorizate** 1

(art. 143 bis); ‣ „alterarea datelor informatice” - constituie fapta aceluia

care, fără drept, modifică, şterge sau deteriorează date informatice stocate sau transmise cu ajutorul unui sistem informatic 1

(art. 144 bis); ‣ „utilizarea frauduloasă a unui calculator” - constituie fapta aceluia

care, cu intenţia de a obţine pentru sine sau **pentru altul un avantaj material ilegal, foloseşte de o manieră incorectă (nelegală) sau incompletă date informatice, influenţând un proces electronic de prelucrare automată sau de transmitere de date, obţinând prin aceasta date neconforme cu adevărul sau un transfer de patrimoniu, dacă prin aceasta s-a produs un prejudiciu unei persoane** 1

(art. 147).

Legislaţia elveţiană prevede atât infracţiuni de drept comun săvârşite prin intermediul sistemelor informatice, cât şi infracţiuni îndreptate împotriva confidenţialităţii, integrităţii şi securităţii datelor şi sistemelor informatice. 1

Estonia Codul penal estonian, modificat, a intrat în vigoare la I **septembrie 2002. Estonia a ratificat Convenţia Europeană asupra Criminalităţii Informatice la 12 mai 2003. Prevederile Codului penal referitoare la** infracțiunile **informatice sunt următoarele:** 360 ‣ **art. 206 - sabotajul informatic;** 1

‣ art. 207 - perturbarea conexiunilor unei reţele informatice ‣ art. 208 - răspândirea de viruşi informatici; ‣ art. 213 - frauda informatică; ‣

art. 217 - folosirea neautorizată a unui sistem informatic; 1

‣ art. 284 - furnizarea de coduri de protecţie. 360 www.techlawed.org/page.php?0=24&c=estonia 373 Finlanda Codul penal finlandez incriminează361 în

Capitolul 38 infracţiuni privitoare la regimul datelor şi comunicaţiilor: ‣ „Interceptarea corespondenţei” - **Secţiunea** 1

a 3-a; ‣ „Interceptarea corespondenţei în circumstanţe agravante” - Secţiunea a 4-a; ‣ „Imixtiunea” - Secţiunea a 5-a; ‣ „Accesarea ilegală a unui computer” - Secţiunea a 8-a; ‣

„Infracţiuni privind dispozitive ilegale folosite pentru a accesa servicii restricţionate” 1

- Secţiunea a 8-a; ‣ „Infracţiuni privind regimul computerelor” - Secţiunea a 9-a.

China În Republica Populară Chineză, aspectele legate de criminalitatea informatică sunt acoperite din punct de vedere juridic printr-o serie de legi şi ordine care reglementează activităţile în Internet362. **Cele mai importante două organizaţii responsabile pentru securitatea internă şi externă sunt: Biroul Securităţii Publice - intern şi Ministerul pentru Securitatea Statului - extern. Pe linia combaterii infracţionalităţii cibernetice, responsabilităţile Biroului pentru** 1

Securitate Publică sunt în mod formal prevăzute în Legea de reglementare a reţelelor informatice, a securităţii, protecţiei şi managementului în Internei, aprobată de Consiliul de Stat pe II decembrie 1997 Responsabilitatea pentru asigurarea securităţii în Internet revine fiecărui IS8 (furnizor de servicii Internet), întrucât în caz de încălcare a legislaţiei în domeniu acesta va fi posibil de anularea licenţei de funcţionare, de amendă şi chiar de dosar penal. Alături de 1

aceste

reglementări, Codul penal al R.P. Chineze (cu modificările aprobate la 14 martie 1997) conţine următoarele prevederi: 1

361

www.wipo.org/clea/docs_news/en/fi/ fioo4en .html 1

362 http://cybbercrimelaw.net/regions/china.html 374 ‣ „pătrunderea neautorizată

într-un sistem informatic ce conţine date privitoare la afaceri de stat, construcţia de echipamente militare sau alte aspecte ce ţin de domeniul ştiinţei sau tehnologiei” 1

- art. 285; ‣

„oricine încalcă legislaţia şi şterge, alterează, introduce date informatice sau abuzează de un sistem informatic, dacă prin aceasta s- a cauzat perturbări ale funcţionării sistemului sau alte consecinţe grave” 1

- art. 286; ‣

„oricine foloseşte un sistem informatic în scopul comiterii unei fraude financiare, furt, unui act de corupţie, unei obţineri ilegale de fonduri, furtului de date confidenţiale sau altor infracţiuni” 1

- art. 287.

Legislaţia chineză acoperă prevederile Convenţiei în ceea ce priveşte recomandările acesteia în domeniul infracţiunilor îndreptate împotriva confidenţialităţii, integrităţii şi securităţii datelor şi sistemelor informatice. De asemenea, sunt incriminate infracţiuni de drept comun săvârşite prin intermediul sistemelor informatice, cum ar fi: folosul, **înşelăciunea, furtul, faptele de corupţie, şantajul.** 1

Marea Britanie Legea pentru prevenirea abuzului asupra computerelor, în vigoare din anul 1990, **a fost creată pentru a preveni accesarea neautorizată a sistemelor informatice şi, totodată, pentru a împiedica elementele infracţionale din societatea britanică să folosească tehnica de calcul ca instrument în comiterea de fapte penale sau să dispună într-o manieră ilegală de date** informatice363. **Legea introduce trei noi infracţiuni, astfel: accesul neautorizat la resursele unui sistem informatic; accesul neautorizat cu scopul de a facilita comiterea de alte infracţiuni** şi **modificarea neautorizată a resurselor unui sistem informatic. Accesul ilegal la resursele unui sistem informatic reprezintă cea mai des întâlnită infracţiune informatică. Ea cuprinde, de exemplu, obţinerea sau aflarea parolei de acces a unei persoane, apoi folosirea acesteia pentru a intra într-un** 1

363

http://www.unix.geek.org.uk/~arny/cmuse.html. 1

375 sistem informatic şi obţinerea de date informatice364.

Accesul neautorizat cu scopul de a facilita comiterea de alte infracţiuni se constituie pe scheletul infracţiunii anterioare. 1

Modificarea neautorizată a resurselor unui sistem informatic poate însemna ştergerea de fişiere, schimbarea setărilor hardware sau software iniţiale sau introducerea unui **cod maliţios cu intenţia de a** perturba funcţionarea **respectivului sistem informatic.** 1

Secţiunea a 3-a Incriminarea infracţiunilor de fraudă informatică VI.3.1. Aspecte generale de reglementare Dată fiind amploarea criminalităţii informatice din ultimii ani şi avându- se în vedere şi Recomandările Consiliului Europei,

legiuitorul român s **-a preocupat de elaborarea unui cadru normativ care să reglementeze accesul şi desfăşurarea activităţii prin intermediul sistemelor informatice în diferite sectoare. În prezent, în România, există în vigoare mai multe prevederi legale, cuprinse în legi speciale, care reglementează diferite fapte în legătură cu sistemele informatice ori societatea informaţională în ansamblul ei.** Considerăm **ca relevante** în acest domeniu **următoarele prevederi legale; ‣ „Legea** 1

nr. 365/2002 privind reglementarea comerţului electronic” 365 ‣ **„Hotărârea de Guvern nr. 1308/2002 privind** adoptarea **normelor metodologice pentru aplicarea Legii** 2

nr.

365/2002”. 366 ‣ **„Ordonanţa de Guvern nr. 130/2000 privind regimul juridic al contractelor la** distanţă367, modificată prin **Legea nr.** 2

51/2003”368; 364 Maxim Dobrinoiu, op., cit., p. 116. 365

Publicată în Monitorul Oficial, partea I, nr. 483 din 5 iulie 2002 20

366

Publicată în Monitorul Oficial, partea I, nr. 877 **din** 5 **decembrie** 2002. 367 **Publicată în Monitorul Oficial, partea I, nr.** 431 **din** 12

2 septembrie 2000. 368

Publicată în Monitorul Oficial, partea I, **nr.** 57 **din 31** ianuarie **2003.** 376 ‣ **„Legea nr.** 81/1996 **privind** 15

drepturile de autor şi drepturile conexe369 **împreună cu Legea** 1

nr. 285/2004370 şi

Ordonanţa de Urgenţă a Guvernului **nr 123/** 2005371 **pentru modificarea şi completarea Legii nr. 8/1996";** 35

‣ „Legea

nr. 455/2001 privind semnătura electronică" 45

372; ‣

„Legea nr. 677/2001 privind protecţia persoanelor cu privire la prelucrarea datelor **cu caracter personal şi libera** circulaţie **a acestor date."** 373 ‣ **„Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în** domeniul **comunicaţiilor electronice"** 23

374; ‣ „Legea nr.

102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere şi Protecţie a Datelor cu Caracter Personal375; ‣ **„Legea** 1

nr. 64

/2004 pentru ratificarea Convenţiei Consiliului Europei asupra criminalităţii 15

informatice376; ‣

„Legea nr. 196/2003 privind prevenirea şi combaterea pornografiei377, **modificată** de **Legea nr. 496/2004"** 13

378; ‣ „Legea nr. 451/2004 privind marca temporală379; ‣ „Legea nr. 589/2004 privind reglementarea activităţii electronice notariale380“ ‣

„Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenţei şi exercitarea demnităţilor publice, a funcţiilor publice şi mediului de afaceri, prevenirea şi sancţionarea corupţiei381. Această lege 2

este cea mai importantă reglementare în materia criminalităţii informatice. 369

Publicată în Monitorul Oficial, partea I, nr. 60 din 26 martie 1996 370 Publicată în Monitorul Oficial, partea I, nr. 587 din 12

30 iunie 2004. 371

Publicată în Monitorul Oficial, partea I, nr. 843din 19 septembrie 2005 37

372

Publicată în Monitorul Oficial, partea I, nr. 429 din 31 iulie 2001 373 Publicată în Monitorul Oficial, partea I, nr. 790 din 12 decembrie 2001 374 Publicată în Monitorul Oficial, partea I, nr. 1101 din 6

25

noiembrie 2004 375 Publicată în Monitorul Oficial, partea I, nr. 12

391din 9 mai 2005 376

Publicată în Monitorul Oficial, partea I, nr. 343 din 20 aprilie 2004 377 Publicată în Monitorul Oficial, partea I, nr. 342 din 12

20 mai 2003 378

Publicată în Monitorul Oficial, partea I, nr. 1070 **din** 18 **noiembrie** 2004 379 **Publicată în Monitorul Oficial, partea I, nr.** 1021 **din** 12

5 noiembrie 2004. 380

Publicată în Monitorul Oficial, partea I, nr. 1227 **din 20** decembrie 2004 381 **Publicată în Monitorul Oficial, partea I, nr.** 279 **din** 21 **aprilie** 12

2009 377 ‣

Aceasta introduce un număr de 7 infracţiuni, ce corespund clasificărilor şi definiţiilor prezentate odată cu analiza prevederilor Convenţiei asupra criminalităţii informatice. 1

Infracţiunile sunt clasificate şi structurate în 3 secţiuni: • Secţiunea I,

„Infracţiuni contra confidenţialităţii şi integrităţii datelor şi sistemelor informatice”, care cuprinde: **accesul ilegal la un sistem informatic, interceptarea ilegală a unei transmisii de date informatice, alterarea integrităţii datelor informatice, perturbarea funcţionării sistemelor informatice, operaţiuni ilegale cu dispozitive sau programe informatice;** 1

•

Secţiunea a II-a, „Infracţiuni informatice”: falsul informatic **şi** frauda informatică; • **Secţiunea a III-a, „Pornografia infantilă prin sisteme informatice”;** 12

‣ Noul Cod penal (adoptat prin Legea nr. 286/2009)382 - care reglementează în Capitolul VI, din Titlul VII,

„Infracţiuni contra siguranţei şi integrităţii sistemelor şi datelor informatice” (art. 360- 19

365). Noul Cod penal reglementează, în plus faţă de infracţiunile prevăzute în Secţiunea I a Legii nr. 161/2003, următoarele: transferul neautorizat de date informatice (art.364) şi

operaţiuni ilegale cu dispozitive sau programe informatice (art. 365),	39

în Titlul VII,

Capitolul VI, intitulat **„Infracţiuni contra siguranţei şi integrităţii sistemelor şi datelor informatice”;**	19

falsul informatic este reglementat în art. 325 la Capitolul „Fals în înscrisuri”; frauda informatică este reglementată în art. 249 la Capitolul

„Fraude comise prin sisteme informatice şi mijloace de plată electronice”; pornografia infantilă în **art.** 374, la **Capitolul** „Infracţiuni contra ordinii **şi**	19

liniştii publice”. Deoarece noul Cod penal va

intra în vigoare la data care va fi stabilită în legea pentru punerea în aplicare a acestuia	19

(art. 446), vom analiza frauda informatică prin prisma infracţiunilor reglementate de Legea nr. 161/2003. Textul reglementat atât de Legea nr. 161/2003, cât şi de noul Cod penal în ce priveşte frauda informatică este o adaptare rapidă si eficientă la mediul 382

Publicată în Monitorul Oficial, partea I, nr.510 din 24 iulie 2009	6

378

românesc a prevederilor Convenţiei Consiliului Europei asupra criminalităţii informatice si reprezintă un instrument eficient în lupta împotriva acestui flagel.	1

VI.3.2. Explicaţii terminologice

Pentru început este necesară o definire a instrumentelor sau conceptelor cu care legiuitorul a înţeles să opereze în acest 1

domeniu383. Această definire a unor concepte juridice în materie de fraudă informatică este făcută de către legiuitor în art. 35, astfel:

a) prin „sistem informatic” se înţelege 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; b) prin „prelucrare automată a datelor” se înţelege procesul prin care datele dintr-un sistem informatic sunt prelucrate prin intermediul unui program informatic; c) prin „program informatic” se înţelege un ansamblu de instrucţiuni care pot fi executate de un sistem informatic în vederea obţinerii unui rezultat determinat; d) prin „date informatice” se înţelege orice reprezentare a unor fapte, informaţii sau concepte într-o formă care ponte **fi prelucrată printr-un sistem informatic;** 2

e) prin „furnizor de servicii” se înţelege: • orice persoană fizică sau juridică ce oferă utilizatorilor posibilitatea de a comunica prin intermediul sistemelor informatice; • orice alta persoană fizică sau juridică ce prelucrează sau stochează date informatice pentru persoanele prevăzute la pct. I **şi pentru utilizatorii serviciilor oferite de acestea;** 1

383 Pentru amănunte, vezi

Hotca, Mihai Adrian, Dobrinoiu, Maxim, Infracţiuni prevăzute în legi speciale, 2

vol.I,

Comentarii şi explicații, **Editura C.H. Beck, Bucureşti,** 2008, **p.** 12

572.;

Voicu, C., Boroi, Al., **Dreptul penal al afacerilor,** Ediția 3, **Editura C.H. Beck. București, 2006,** 27

p.357;

Dobrinoiu, Maxim, Infracțiuni **in domeniul informatic,** Editura **C.H. Beck, București, 2006,** 7

p.141. 379

f) prin „date referitoare la traficul internaţional” **se înţelege 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, mărimea, volumul şi durata comunicării, precum si tipul serviciului utilizat pentru comunicare; g) prin „date referitoare la utilizatori” se înţelege 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 alte date care pot conduce la identificarea utilizatorului; h) prin „măsuri de securitate” se înţelege 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; i) 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** cu **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.** De asemenea, **în sensul** 2

Legii

nr. 161/2003, „acţionează fără drept” persoana care se află în una din **următoarele situaţii: ▸ nu este autorizată, în temeiul legii sau** a **unui contract; ▸ depăşeşte limitele autorizării; ▸ nu are permisiunea, din partea persoanei fizice sau juridice competente** potrivii **legii, să o acorde, de a folosi, administra sau controla un sistem informatic ori de a desfăşura cercetări** științifice **sau de a efectua orice altă operaţiune într-un sistem informatic.** 2

VI.3.3. Analiza conţinutului constitutiv al infracţiunilor prevăzute de Legea nr. 161/2003 VI.3.3

.1. Infracţiunea de acces ilegal la un sistem informatic – art. 42 17

Sediul materiei îl constituie

art. 42 din Legea nr. 161/2003: „(1) Accesul fără drept, la un sistem informatic constituie infracţiune şi se pedepseşte cu închisoare de la 3 luni la 3 ani sau cu amendă. (2) Fapta prevăzută în **alin.(** I), **săvârşită în scopul obţinerii de date informatice, se pedepseşte cu închisoare de la 6 luni la 5 ani. (3) Dacă fapta prevăzută** în **alin.(** I) **sau (2) este săvârşită prin încălcarea măsurilor de securitate, pedeapsa este închisoarea de la 3 la 12 ani".** 7

Cum rezultă din analiza textului legal de mai sus, alin.(I) al art. 42 consideră ca infracţiune

„accesul, fără drept, la un sistem informatic", iar **în** 1

alineatele următoare sunt prevăzute două agravante: atunci când

fapta este săvârşită în scopul obţinerii de date informatice 26

şi atunci când

este săvârşită prin încălcarea măsurilor de securitate. A. **Obiectul juridic** 11

Obiectul juridic special îl constituie relaţiile sociale care apără **securitatea sistemului informatic, inviolabilitatea acestuia şi care sunt de** naturii **a garanta confidenţialitatea şi integritatea atât a datelor, cât şi a sistemelor informatice.** 4

Aşadar, această infracţiune lezează mai multe relaţii sociale, precum patrimoniul organizaţiei, instituţiei, persoanei fizice, persoanei juridice, relaţiile privind protecţia acestui patrimoniu şi cele privind încrederea publică în măsurile de siguranţă ale integrităţii datelor şi programelor informatice.

Reglementarea legală urmăreşte să protejeze sistemele informatice şi datele stocate pe acestea, de accesul neautorizat. 4

Putem afirma că în raport cu dispoziţia legală aceste infracţiuni lezează mai multe relaţii sociale şi ca atare

au două sau mai multe obiecte juridice, dintre care unul principal şi altul secundar. În cazul de faţă, de exemplu, accesul neautorizat la un sistem informatic în **domeniul apărării loveşte atât în siguranţa naţională şi capacitatea de apărare a statului, cât şi în instituţia sau persoana titulară a sistemului penetrat** sau **a informaţiilor** accesate384. ► Obiectul **material constă în** 1

anumite entităţi cum ar fi

sistemele sau reţelele informatice (hardware-cabluri, servere, **plăci,** programe **etc.)** 7

asupra cărora se îndreaptă fapta de a accesa, fără drept, la un sistem informatic. B. Subiecţii infracţiunii ► Subiectul activ

poate fi orice persoană fizică sau juridică **care îndeplineşte condiţiile** legale **pentru a răspunde din punct de vedere penal,** 12

legea neprevăzând o calitate specială pentru aceasta. Astfel, persoana fizică răspunde penal dacă a

împlinit vârsta de 14 ani şi a săvârşit fapta **cu vinovăţie** 4

şi are discernământ, iar persoana juridică dacă a comis fapta în

realizarea obiectului de activitate sau în interesul ori în numele persoanei juridice 19

(art. 19 C.pen. în vigoare, introdus prin Legea nr. 278/2006 şi art. 135

din noul Cod penal, adoptat prin **Legea nr. 286/2009).** 41

De precizat, în legătură cu aceste infracţiuni de fraudă informatică, că

practica judiciară a stabilit **că, în marea majoritate a cazurilor, asemenea persoane posedă** aptitudini şi **cunoştinţe în domeniul** 1

utilizării unui sistem informatic sau chiar angajat într-o firmă cu profil informatic ori un funcţionar public.

Dintre aceştia, un procent important **îl reprezintă** adevăraţii experţi **în sisteme de calcul şi** reţele **de calculatoare, familiarizaţi cu „spargerea" măsurilor de securitate** a **calculatoarelor sau reţelelor de calculatoare.** 1

Din evaluarea grupurilor criminale dezmembrate de către procurorii DIICOT, în anul 2008385,

care au acţionat în domeniul criminalităţii informatice se desprind următoarele **caracteristici:** 5

- supra **-specializarea**

membrilor grupărilor, formarea de celule independente specializate în desfăşurarea **unei activităţi infracţionale specifice;** 5

-

recrutarea tinerilor cu abilităţi în a utiliza computerele şi noile 5

384 Hotca, M.A., op.cit, p.576 385 Din raportul de activitate pe anul 2008 a

Direcţiei de Investigare a Infracţiunilor de Crima Organizata si Terorism din cadrul Parchetului de pe lângă înalta Curte de Casaţie si Justiţie. 29

382

tehnologii prin subordonarea sau cointeresarea acestora de către lideri ai unor grupări infracţionale tradiţionale; ‣ trecerea de la fraudele informatice clasice (licitaţii) la fraude informatice complexe, în care predominant este factorul tehnic, respectiv folosirea de programe informatice şi scheme de fraudare (activităţi de phising, infectarea cu diverse forme de malware în scopul obţinerii de date); ‣ caracterul transnaţional, fie că este dat de locul în care sunt săvârşite faptele, fie că este vorba de localizarea victimelor; permanenta preocupare în 5

identificarea unor noi moduri de operare; ‣

investiţia financiară efectivă în crearea/cumpărarea de scheme infracţionale producătoare de venituri substanţiale dintr-o singură operaţiune; 5

‣

recrutarea prin mijloace din ce în ce mai sofisticate a „săgeţilor”, precum şi specializarea acestora după necesităţi (deschiderea de conturi bancare, transportul unor sume de bani etc.); 6

‣

orientarea grupărilor infracţionale şi către fraudarea mijloacelor de plată electronică româneşti. 5

Participaţia penală la aceste infracţiuni

este posibilă sub toate formele: coautorat, instigare, complicitate. ► Subiectul pasiv poate fi persoana fizică sau juridică al cărei sistem informatic a fost accesat fără drept. De 2

regulă

este persoana fizică sau juridică proprietara sau deţinătoarea **de drept a sistemului informatic accesat ilegal sau a datelor informatice vizate.** Acest subiect pasiv **poate** fi şi unul **colectiv, alcătuit dintr-o mulţime de persoane fizice sau juridice, atunci când accesul în sistemul informatic generează în mod automat accesul ilegal în alte sisteme similare interconectate cu primul.** 1

C. Latura obiectivă C1. Elementul material se realizează printr

-o acţiune şi anume „accesul interzis", adică **fără drept,** într **-un sistem informatic.** 11
Aşadar, **pentru** realizarea acestei infracţiuni, **trebuie**

ca subiectul activ să nu fie autorizat.

Accesul fără drept la un sistem informatic presupune, 1

potrivit

art. 35 alin.(2) din Legea nr. 161/2003, că **persoana** respectivă **se află în una** din **următoarele situaţii: ▸ nu este autorizată, în temeiul legii sau** a **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** activităţi **ştiinţifice sau de a** desfăşura **orice altă operaţiune într-un sistem informatic.** 2

Accesul, în înţelesul dat de lege, desemnează intrarea în tot sau numai într-o parte a sistemului informatic. Metoda de comunicare - la distanţă, inclusiv prin satelit sau nu, ori de aproape - nu prezintă importanţă, în forma sa cea mai simplă, accesul fără drept la un sistem informatic presupune o acţiune **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 aplicaţii în beneficiul intrusului. Va exista acces ilegal în formă simplă şi în cazul în care intrusul, manipulând propriile echipamente periferice, de la** 1

distanţă, găseşte şi utilizează o cale externă de intrare într-un alt sistem de calcul. Este cazul tipic al accesării unei alte stații de aflate într-o rețea. Pentru obţinerea accesului, făptuitorul va încerca o gamă variată de procedee tehnice, cum ar fi: atacul prin parolă, atacul

care exploatează slăbiciunile tehnologice, atacul care exploatează bibliotecile partajate, atacul IP ori atacul de deturnare prin TCP etc.386. 5

Un tip interesant de acces ilegal, utilizat din ce în ce mai des azi, îl reprezintă atacurile prin inginerie sociala. Acestea au devenit mai frecvente și mai periculoase pe măsură ce tot mai mulţi utilizatori se conectează la Internet și la reţele interne. Un exemplu frecvent de inginerie sociala este ca un „hacker” să 1

386 A se vedea Kandler, L., Anti-Hacker, Editura Educațional, București, 1998, pp.22-25, 250, 430. 431, 508, 509 5

384 trimită mesaje e-mail

către utilizatori (sau pur si simplu să folosească telefonul) pentru a-i anunţa pe aceştia că el este administratorul sistemului. Deseori, mesajele solicită utilizatorilor să-şi trimită parola prin e-mail către administrator, fiindcă sistemul este într-o pană sau că va fi dezafectat temporar. Un atac prin inginerie socială se bazează cel mai mult pe ignoranţa utilizatorilor în materie de calculatoare şi reţele. Cea mai bună reţetă împotriva acestor atacuri o reprezintă educaţia utilizatorilor. Practica a demonstrat că, în marea majoritate a cazurilor, făptuitorul acţionează pentru obţinerea de date informatice, care pot să însemne: captarea vizuală a acestor date pe monitor; intrarea în posesia unei 1

imprimante alfa numerice;

rularea unor programe sau aplicaţii care gestionează date informatice. De pildă, practica judiciară a 1

considerat că

fapta de a monta, la un bancomat, un dispozitiv de citire a benzii magnetice a cardurilor 6
întruneşte elementele constitutive ale infracţiunii de acces, fără drept, la un sistem informatic prin încălcarea măsurilor de securitate, prevăzută de **art. 42 alin.(** l) **şi (3) din Legea nr. 161/2003, întrucât** bancomatul **constituie sistem informatic în sensul art. 35 alin.(** l) **lit. a) din această lege, prin montarea dispozitivului de citire a benzii magnetice se încalcă măsurile de securitate ale bancomatului, care au scop asigurarea secretului numărului de cont şi al** operațiunii **efectuate, precum și prevenirea folosirii frauduloase a cardurilor.** 387 Prin obținerea **de**

date informatice se înțelege **inclusiv copierea acestora, pe suporţi de stocare (Floppy Disk, CD,** 1
Memory Stick, Card etc,).

Astfel, mai mulţi inculpați au fost trimiși în judecată pentru că, în nume personal ori folosindu-se de identitatea unor complici, au transmis prin e-mail, în mod repetat, în scopul obţinerii unor sume de bani, dale de identificare ale unor instrumente de plată electronică în posesia cărora au ajuns în mod ilicit.388 Din activitatea infracţionala desfășurată de inculpaţi, a fost obţinută suma de cca. 60.700 USD. Urmare a sesizării Biroului FBI din Las Vegas, SUA, 387 Î.C.C.J., Secț. pe., dec, nr. 5288

/2006, disponibilă pe site-ul www. scj **.ro** 34

388

disponibilă pe site-ul www. scj **.ro** 385 organele **de** 34

urmărire penala române s-au sesizat din oficiu cu privire la săvârşirea unor infracţiuni informatice de către mai multe persoane. În cadrul investigaţiilor sub acoperire au fost identificaţi autorii faptelor, care au intrat în contact, pe site-ul Dolnet, în camera de chat (chat room) cu o persoană identificată iniţial doar de un nickname şi care s-a arătat dispus să tranzacţioneze (vândă) date (numere, serii) ale unor cărţi de credit. Mai apoi, investigatorii au intrat în contact şi cu alte persoane, ce păreau a forma, împreună cu primul contact, un grup cunoscut sub numele de „Defender's Team”. În cadrul operaţiunii sub acoperire desfășurate de către investigatorii FBI şi verificările referitoare la datele furnizate, aceştia au fost de acord să cumpere informaţiile oferite. Se reţine că între investigatori şi grupul infracţional organizat s-a purtat o

corespondenţă e-mail, context în care au fost achiziţionate un număr de 42 de date de identificare ale unor instrumente de plată electronică (cărţi de credit), în acest sens, s-au purtat mai multe corespondenţe între grupul de infractori şi investigatori, prin care au fost obţinute date de identificare a peste 1.000 de cărţi de credit. Din actele de urmărire penala a rezultat că datele privind instrumentele de plată, precum şi dalele de identificare ale posesorilor (adrese, număr de asigurări sociale ori soldul contului) nu ar fi trebuit să se afle în posesia vreunei alte persoane decât cele autorizate să le deţină şi cu atât mai mult, nu ar fi trebuit să fie transmise prin Internet. Astfel, într-o cauză

instanţa a reţinut că, în luna mai 2005, inculpaţii 6

s

-au înţeles să folosească dispozitivele de citire a benzii magnetice a cardurilor şi o minicameră, pe care le-au procurat anterior, în vederea obţinerii datelor necesare pentru donarea **mai multor** 6

date. Apoi

inculpaţii s-au deplasat în mai multe **localităţi, au montat dispozitivele de citire a benzii magnetice a cardurilor şi minicamera pe mai multe** 6

bancomate, pe care le-au descărcat şi le-au stocat într-un computer la domiciliul altui inculpat. **După ce toate datele obţinute au fost stocate** pe **computer, inculpaţii au achiziţionat carduri neinscripţionate şi au lipit pe fiecare dintre** acestea **câte o etichetă** clonată **pe care au scris codul sau codurile PIN** 386 **citite anterior cu minicameră, la computerul inculpatului I.F. fiind ataşat şi un dispozitiv de inscripţionare electronică, cu ajutorul căruia inculpatul G.M. a realizat inscripţionarea benzii magnetice a fiecărui blank, cu contul** anterior **copiat, corespunzător codului PIN înscris pe etichetă.** 6

Ulterior, în mai multe zile,

inculpaţii au retras numerar cu ajutorul cardurilor clonate de la bancomatele mai multor bănci. 6

389 C2. Urmarea imediată constă în punerea în pericol a confidenţialităţii şi a integrităţii

datelor pe care le conţine un sistem informatic. 2

În practică, urmarea formei simple de acces fără drept este trecerea într-o stare de nesiguranţă a sistemului informatic şi/sau resurselor sale (hardware, software etc.). Dacă scopul accesului neautorizat 1

[art. 42 alin.(2)] a

fost obţinerea de date informatice, starea de nesiguranţă a sistemului de calcul este dublată de starea de nesiguranţă a datelor informatice stocate în acesta sau prelucrate de către acesta. Încălcarea măsurilor de securitate 1

[art. 42 alin.(3)]

va determina însă o transformare efectivă adusă obiectului material al infracţiunii, măsura de securitate fiind, în acest caz, parte integrantă a sistemului informatic. C3. Legătura **de** 1

cauzalitate rezultă din simpla comitere a elementului material al infracţiunii. În cazul de

acces fără drept trebuie demonstrată forţarea măsurilor de securitate (parole, coduri de acces etc.). 9
D. **Latura subiectivă** Sub aspect subiectiv, **infracţiunea de** accesare neautorizată **se** poate **comite cu intenţie directă sau indirectă, în cazul obţinerii de date informatice** [art. 42 **alin.(2)], intenţia acestuia este calificată prin** scop390. E. **Forme. Modalităţi. Sancţiuni.** Aspecte procesuale E1. **Forme**

389 Î.C.C.J., Secția penală, dec, nr. 432/2008, disponibila pe site-ul www.scj.ro 390 Dobrinoiu, M., op.cit., p.159 387

Actele pregătitoare, deşi posibile, nu sunt incriminate şi, ca atare, nu se pedepsesc. **Anumite acte pregătitoare sunt incriminate ca infracţiuni de sine stătătoare, cum ar fi cazul art. 46, „Operaţiuni ilegale cu dispozitive sau programe informatice”** 391. **Tentativa se pedepseşte, conform** 3

art. 47 din lege. Consumarea infracţiunii în modalitatea prevăzută la alin.(l) se realizează în momentul în care făptuitorul accesează în mod direct sau de la distanţă resursele sistemului informatic. În modalitatea prevăzută la alin.(2), consumarea infracţiunii are loc atunci când intrusul acţionează asupra măsurilor de securitate, indiferent dacă a reuşit sau nu neutralizarea ori înlăturarea acestora. E2. Modalităţi Infracţiunea analizată prezintă o singură modalitate normativă,

accesul fără drept la un sistem informatic. Acestei modalităţi normative pot să-i corespundă însă variate modalităţi de fapt. Infracţiunea prezintă şi două modalităţi agravate. Astfel, fapta este mai gravă [alin.(2)] dacă este săvârşită în scopul obţinerii de date informatice ori prin încălcarea sau înlăturarea măsurilor de securitate [alin.(3)]. E3. Sancţiuni Pedeapsa principală 1

pentru forma simplă de la alin.(l)

este închisoarea de la 3 luni la 3 ani sau amenda. Pentru agravanta de la alin.(2), pedeapsa este închisoarea de la 6 luni la 5 ani, iar fapta prevăzută în alin.(3) se pedepseşte cu închisoare de la 3 la 12 ani392. E4. Aspecte procesuale Acţiunea penală se pune în mişcare din oficiu. 3

VI

.3.3. 2. Interceptarea ilegală a unei transmisii de date informatice 17

– art. 43 Sediul materiei îl constituie

art. 43 din Legea nr. 161/2003. „(l) Interceptarea, fără drept, a unei transmisii de date informatice care 2

391 Hotca,M.A., op. Cit., p. 581 392 Noul Cod penal sancţionează infracţiunea de la alin.(1) și (2) la fel ca cea din art. 42 alin.(1) și (2), adică cu

închisoare de la 3 luni la 3 ani sau cu amenda, respectiv, închisoarea de la 6 luni la 5 ani. 26

Pentru forma agravată de la alin.(3), noul Cod penal prevede o sancţiune mai puţin severa ca în legea specialii, și anume, închisoare de la 2 la 7 ani. 388

nu este publică şi care este destinată unui sistem informatic, provine dintr-un asemenea sistem sau se efectuează în cadrul unui sistem informatic, constituie infracţiune şi se pedepseşte cu închisoare de la 2 la 7 ani. (2) Cu aceeaşi pedeapsă se sancţionează şi interceptarea, fără drept, a unei emisii electromagnetice provenite dintr-un sistem informatic ce conţine date informatice care nu sunt publice”. Prin **reglementarea** 4

acestei infracţiuni s-a urmărit protejarea transmisiilor de

date informatice din cadrul sau între sisteme informatice, indiferent de modul cum se realizează acestea. 4

Incriminarea acestei fapte a fost necesară, deoarece

în ultimul timp a cunoscut o amploare deosebită fenomenul interceptării cumpărăturilor „on-line” făcute de diverşi cetăţeni români sau străini care au ales ca modalitate de plată cardul de credit, interceptări care au avut ca scop furtul datelor aflate pe respectivele cârduri, pentru ca acestea să fie folosite ulterior de către alte persoane decât adevăraţii titulari. În prezent, traficanţii de informaţii desfăşoară activităţi în special **în sfera financiară şi cea de** business, **de cele mai multe ori încercând să vândă informaţiile interceptate unor companii** 11

rivale393.

A. Obiectul juridic ► Obiectul juridic **special 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.** 1

Ca atare, prin intermediul acestei infracţiuni se apără dreptul la o viaţă privată neperturbată (protejat şi prin art. 18 al Convenţiei Europene de salvgardare a

drepturilor omului şi libertăţii fundamentale) şi dreptul la exclusivitate a comunicaţiilor datelor. 4

Secretul corespondenţei este un drept constituţional, garantat de art. 28 2

393 Voicu,C., Boroi, Al., op. cit., p.361. din Constituţia României, republicată394, care prevede

că: „Secretul scrisorilor, al telegramelor, al altor trimiteri poştale, al convorbirilor telefonice şi al celorlalte mijloace legale este inviolabil”. 2

Comunicaţiile în formă electronică se referă la mai mult decât o simplă corespondenţă, protejată în virtutea dreptului la viaţă privată. Din ce în ce mai multe activităţi sunt informatizate, atât în cadrul mediului de afaceri, cât şi în sectorul public. 4

Toate aceste comunicaţii conţin date ce trebuie protejate de interceptarea lor ilegală. ► Obiectul material 4

al infracţiunii îl constituie suporturile materiale

prin care se realizează comunicaţiile de date între echipamente (cablurile de conexiuni, casetele de 1

conexiuni,

distribuitorii de reţea). În cazul alin .(2), obiectul material este constituit din energia (emisia) electromagnetică, ce radiază sau se găseşte în formă reziduală ori necontrolată în imediata vecinătate a echipamentelor electronice care alcătuiesc sistemul informatic vizat. Astfel, emisia electromagnetică din jurul unui echipament (imprimantă, monitor, cablu ele.) nu va putea fi 3

considerată drept obiect material dacă, în momentul acţiunii de interceptare (captare), acesta nu era conectat la un sistem informatic în condiţiile alin.(2) 395 B. Subiecţii infracţiunii ► Subiectul activ poate fi orice persoană fizică sau juridică, responsabilă

din punct de vedere penal.

În cazul infracţiunii de faţă, făptuitorul trebuie 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. Participaţia este posibilă în 10

toate formele sale: coautorat, instigare, complicitate. ► Subiectul pasiv poate fi persoana fizică sau juridică, deţinătoare de drept a sistemului informatic ori a componentelor de legătură (transmisiuni) 1

394 Constituția României a fost modificată şi completată prin Legea

nr. 429 din 18 septembrie 2003, publicată în Monitorul Oficial, Partea I, nr. 669 din 22 septembrie 2003. 15

395 Hotca, M. A., Dobrinoiu, M., op. cit., p. 583. 390

între două sau mai multe sisteme informatice. În mod adiacent, subiect pasiv poate fi deţinătorul de drept al datelor informatice interceptate sau persoana vizată în mod direct de prelucrarea automată a acestor date396. C. Latura obiectivă C1. Elementul material este realizat prin acţiunea de interceptare, 10

prin orice mijloace, a unor transmisii de date sau de emisii electromagnetice. 2

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. 1

În

cazul comiterii infracţiunii prin interceptarea unei transmisii de date informatice care nu este publică, trebuie îndeplinite următoarele condiţii alternative cu privire la transmisia de date: ‣ aceasta trebuie să fie destinată unui sistem informatic, să provină dintr-un asemenea sistem sau să se efectueze în cadrul unui sistem informatic; 2

‣

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; 1

•

daca 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). 1

396

A se vedea, Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal, 10

publicată în Monitorul Oficial, Partea I, nr, 1101 din 25 noiembrie 2004. 15

391

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. 1

Interceptarea

prin mijloace tehnice cuprinde ascultarea conţinutului comunicaţiilor, obţinerea conţinutului datelor, fie direct, accesând sistemul informatic şi folosindu-l, fie indirect, recurgând la procedee electronice de ascultare clandestine. 4

Prin intermediul unui interceptor de pachete, hackerii pot intercepta pachetele de date, 1

care 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” sau „supraveghere ascunsă”. 10

Atacurile care pot fi executate sunt de două feluri397; ‣ „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 înserarea de mesaje false 15

etc. În alin.(2) al art. 43 este prevăzută o modalitate asimilată de săvârşire a infracţiunii, respectiv interceptarea, fără drept, a unei emisii electromagnetice provenite dintr-un sistem 1

informatic ce conţine date 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).

C2.

Urmarea imediată constă în starea de pericol, de ameninţare **pentru valoarea socială pe care legea o apără, şi** 7

anume interesele

persoanelor care afectează **în mod legal transmisii de date informatice.** 2

Textul de lege nu cere în mod expres producerea unui anume prejudiciu. Este suficientă interceptarea 397 Patriciu,

V.V., Criptografia şi securitatea reţelelor de calculatoare, Editura Tehnică, Bucureşti, 1994, p.22. 10

392 transmisiilor, fără a se impune ca datele astfel obţinute să fie divulgate către alte persoane. C3. Legătura de cauzalitate rezultă din simpla interceptare neautorizată a unei transmisii de date. D. Latura subiectivă Din punct de vedere subiectiv, infracţiunea neautorizată a unei transmisii de date

se comite doar **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** şi **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** rezultatului398. E. **Forme. Modalităţi. Sancţiuni. Aspecte procesuale** E1. Forme **Actele pregătitoare, deşi posibile, nu** 10

se pedepsesc.

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 conform **art. 47 din lege. Consumarea infracţiunii** are loc **în** 1

momentul interceptării fără drept a unei transmisii de date informatice sau a emisiei electromagnetice a uneia dintre componentele sistemului informatic. E2. Modalităţi Infracţiunea analizată prezintă două modalităţi normative: interceptarea unei transmisii de date şi, respectiv, captarea emisiei electromagnetice. Acestor modalităţi normative pot să le corespundă variate modalităţi de fapt.

398 Hotca, M. A., Dobrinoiu, M., op. cit., p. 587 E3.

Sancţiuni Pentru ambele forme ale infracţiunii, pedeapsa principală este închisoarea de la 2 la 7 ani. E4. Aspecte procesuale Acţiunea penală se pune în mişcare din oficiu. 1

VI.3.3

.3, Infracţiunea de alterare a integrităţii datelor informatice - art.44 17

Sediul materiei îl constituie

art. 44 din Legea nr. 161/2003. „(1) Fapta de a modifica, şterge sau deteriora date informatice ori de a restricţiona accesul la aceste date, fără drept, constituie infracţiune şi se pedepseşte cu închisoare de la 2 la 7 ani. (2) Transferul neautorizat de date dintr-un sistem informatic se pedepseşte cu închisoare de la 3 la 12 ani. (3) Cu pedeapsa prevăzută la alin.(2) se sancţionează şi 2

transferul neautorizat de date dintr-un mijloc de stocare a datelor informatice". Această infracţiune are în vedere, în general, comportamentul oricărei persoane care, cu bună ştiinţă şi fără autorizare, alterează, avariază sau distruge un computer, un sistem informatic, o reţea de computere, datele stocate pe acestea sau orice parte a acestora. Incriminarea urmăreşte să protejeze datele informatice stocate în cadrul sistemelor informatice, urmărind să împiedice modificarea, ştergerea sau deteriorarea datelor informatice, restricţionarea accesului la ele. transferul neautorizat de date dintr-un sistem informatic sau dintr-un mijloc de stocare a datelor informatice. 2

A. Obiectul juridic ► Obiectul juridic special este unul complex, constituit,

pe de o parte, din **relaţiile sociale ce protejează încrederea în corectitudinea datelor stocate în sistemele informatice şi, pe de altă parte, relaţiile sociale ce protejează confidenţialitatea datelor stocate în sistemele informatice sau pe alte mijloace de stocare.** 17

Interesul juridic protejat va fi acela al proprietarului sau deţinătorului de drept al datelor informatice pentru ca acesta să fie în măsură să dispună efectiv de respectivele informaţii. ► Obiectul **material** 1

al infracţiunii îl constituie suportul material

pe care se află datele modificate, şterse, deteriorate, transferate sau la care a fost restricţionat accesul. 17

Prin extensie, obiect material ar putea fi considerat şi mediul de stocare pe care se găsesc datele informatice, respectiv Hard Disk, **discuri magnetice, optice, chipuri de memorie, memorii flash etc. ► Subiecţii infracţiunii ► Subiectul activ poate fi orice persoană fizică** sau juridică, **responsabilă** 3

din punct de vedere penal. În general, cum rezultă din practică,

autorul este o persoană cu cunoştinţe în domeniul calculatoarelor sau al electronicii, deşi există si unele cazuri (mai rar) în care acest aspect nu mai **are nici o relevanţă. Participaţia este posibilă în toate formele sale: coautorat. instigare, complicitate. ► Subiectul pasiv al infracţiunii este persoana fizică sau juridică** deţinătoarea **de drept a datelor şi informaţiilor care constituie obiectul material al infracţiunii.** 1

Acesta este proprietarul ori deţinătorul

datelor modificate, şterse, deteriorate, transferate sau la care a fost restricţionat accesul. C. **Latura obiectivă** C1. **Elementul material** al infracţiunii **în** 4

varianta tip se realizează prin acțiunea de a modifica, şterge, deteriora datele informatice ori pentru transferarea acestora sau restricţionarea accesului la acestea. Infracţiunea analizată are conţinut alternativ, putându-se săvârşi prin oricare dintre acţiunile menţionate. Spre exemplu, într-o cauză, inculpaţii

au fost trimişi în judecata pentru comiterea **infracţiunilor** prevăzute **de**	13

art. 25 C.pen. raportat la

art. 44 alin. (1) şi 395 **art.** 44 alin.(2) **din Legea nr. 161**	1

din 2003, respectiv pentru

săvârşirea infracţiunilor prevăzute art. 41 **alin. (1),** (2) **şi (3) din Legea nr. 161** din 2003 **şi art.**	32

44 alin. (l) si alin.(2) din Legea nr. 161 din 2003. S-a reţinut, în esenţă, că inculpatul C.C. 1-a instigat pe inculpatul B.M.S., la data de 2 septembrie 2007, să acceseze fără drept sistemul informatic (laptop) al numitei G.E., soţia primului inculpat, prin utilizarea frauduloasă a sistemului de parolare, obţinând date informatice, respectiv conţinutul mesajelor aflate pe adresa acesteia de pe serverul yahoo, computerul fiind destinat exclusiv utilizării profesionale ca avocat. Datele au fost transferate pe un memory stick în care au fost stocate, iar apoi au fost transferat pe adresa de e-mail a surorii inculpatului C.C. S-a mai reţinut că, după utilizare, inculpatul B.M.S. ar fi pus o nouă parolă de acces la căsuţa de corespondenţă electronică399. Modificarea constă în acţiunea făptuitorului de alterare a formei iniţiale a datelor informatice, prin introducerea de

noi secvenţe sau de a şterge anumite porţiuni ale datelor informatice, având drept consecinţa **noi date informatice, diferite de cele iniţiale.**	1

Prin ştergere se înţelege acţiunea de înlăturare **în tot sau în parte a datelor informatice din**	1

sistemul informatic sau alte dispozitive pe care sunt stocate.	11

Ştergerea de date echivalează oarecum cu distrugerea de obiecte 1

materiale400. S- a reţinut aceasta infracţiune într-o cauza când persoana deţinătoare a lăsat calculatorul conectat la reţeaua Internet

pentru a finaliza un download de mari dimensiuni, iar un hacker i-a accesat PC-ul prin conexiunea DSL şi a instalat un program care i-a permis să controleze calculatorul, să fure fişiere importante şi să şteargă informaţiile de pe hard 11

disk-uri401. În săvârşirea infracţiunii în această varianta

poate fi vorba şi de distrugerea suportului de date, de supraimprimarea pe benzi, platane magnetice, discuri optice 1

etc. Trebuie să mai reţinem,

însă, faptul că ştergerea datelor informatice nu înseamnă întotdeauna şi eliminarea lor 1

399 Kövesi, L. C. și colab., op. cit., p. 137. 400 Vaiu,

I., Vasiu, L., Informatica juridica și drept informatic, Editura Albastră, 2002, p .160 1

401 disponibilă pe site-ul www.scj.ro 396 definitivă. Deteriorarea presupune alterarea

conţinutului respectivelor date informatice ce are drept consecinţă imposibilitatea folosirii acestor date în scopul în care au fost 2

create. De exemplu, se accesează ilegal un sistem informatic şi se modifică conţinutul unui mesaj ce urmează a fi trimis prin e- mail. În acest caz se va reţine

un concurs de infracţiuni între accesul ilegal la un sistem informatic şi 1

alterarea integrităţii datelor informatice.

Într-un sens mai grav, distrugerea de date poate fi rezultatul unor atingeri concrete ale unor instalaţii informatice prin acte de terorism, acte specifice de sabotaj, elaborate sau foarte simple, precum şi ştergerea de date cu magneţi sau prin înserarea de programe incidente, bombe biologice etc. Din punct de vedere tehnic, una dintre cele mai simple modalităţi de distrugere a dalelor este plasarea unui magnet în imediata vecinătate sau în contact cu un media de stocare electronic sau magnetic (platanele Hard Disk -ului, folia magnetică a Floppy-disk-ului, chip-ul unei memorii flash etc.) Există restricționare atunci când autorul face să dispară datele fără ca ele să fie în fapt şterse ca rezultat al operării unor instrucțiuni corespunzătoare. 1

Restricționarea accesului cuprinde reţinerea, ascunderea, incriptarea, modificarea autorizărilor pentru utilizatorii legitimi sau permiterea accesului cu mare întârziere la datele informatice402. Aşadar,

restricţionarea accesului la dalele informatice este rezultatul uneia sau mai multor acţiuni exercitate de făptuitor asupra sistemelor de calcul sau mediilor de stocare, astfel încât utilizatorul de drept şti nu le mai poată regăsi în forma lor iniţială ori prin procedurile standard de operare a sistemelor de calcul403. În cazul restricționării fizice, făptuitorul acţionează direct pentru blocarea accesului la resursele unui sistem prin dezafectarea componentelor periferice gen tastatură sau mouse. În cazul restricționării logice, spre exemplu, făptuitorul poate modifica tabele de alocare a fişierelor FAT - File Allocation Table o componentă a sistemului de operare care alocă fiecărui fişier una sau mai multe porţiuni pe 1

402 Vasiu, I., Vasiu, L., Frauda informatică, în revista de Drept penal, nr. 1/2005, p.46 403 Hotca, M.A., Dobrinoiu, M., op. cit., p. 591 397

suportul de stocare prin menţionarea unor adrese corespunzătoare de regăsire. Un exemplu actual de restricţionare îl reprezintă atacurile informatice la adresa paginilor web, care au ca rezultat imposibilitatea de afişare a paginii sau chiar blocarea întregului „site web”, privând atât proprietarii sau deţinătorii de drept, cât mai ales vizitatorii de conţinutul informaţional. Prin transfer neautorizat se 1

înţelege mutarea fără drept a reprezentării binare a informaţiilor din mediul de stocare curent (autorizat) pe un alt suport de stocare extern sau chiar în interiorul aceluiaşi sistem informatic, dar în altă locaţie.

Astfel, s-a reţinut într-o cauză penală că inculpatul D.V. a constituit un grup infracţional organizat în

scopul săvârşirii de infracţiuni în **domeniul informatic şi au efectuat în repetate rânduri** 14 **operaţiuni de acces neautorizat al conturilor de e-mail aparţinând clienţilor şi angajaţilor eBay, în scopul obţinerii de date informatice. Prin încălcarea măsurilor de securitate,** inculpații **au transferat neautorizat o serie de date informatice atât pe laptopul personal, cât și pe** forumul **eBay, au pus la** dispoziție **și au deţinut fără drept programe informatice și aplicaţii destinate săvârșirii infracţiunilor informatice și de asemenea, au introdus date informatice rezultând aspecte neadevărate în mai multe domenii de Internet în vederea producerii de consecinţe juridice. Prejudiciul total reclamat de partea vătămată eBay Inc. este de 7.500.000** USD, **constituit** atât **din costul importantelor daune de natură morală, în urma alterării încrederii în rândul clienţilor acestei companii, cât și de costurile necesare** reconstituirii **programelor de securitate, protecţie servere, noi coduri de parole.**

404 Într-o altă cauză penală s-a reţinut că membrii unui grup infracţional organizat, în scopul obţinerii unor sume de bani de la cetăţeni străini, au organizat licitaţii frauduloase prin intermediul site-ului eBay, oferind la vânzare telefoane mobile sau aparatură electronică pe care în realitate nu le deţineau, inducând în eroare în această modalitate 183 de cetăţeni străini, de la care au primit suma 404 disponibilă pe site-ul www.scj.ro totală de 114.700 USD405 . O altă forma de infracţiune informatică o constituie

migrarea datelor de pe un sistem informatic cu o anumită configuraţie „hardware" sau „software", 1 **pe un alt sistem cu o configuraţie diferită poate determina disfuncţionalităţi, iar informaţia să nu se mai regăsească în formatul cu care utilizatorul era obişnuit. Cele mai**

periculoase instrumente care alterează datele informatice sunt însă programele tip Virus, Vierme 1 **sau Cal Troian, care se reproduc şi se pun în lucru în alte programe ori fişiere de date ca programe de distrugere.**

C2. Urmarea imediată este constituită de

existenţa de date informatice alterate (modificate, şterse, distruse ori de negăsit), care nu mai prezintă caracteristicile iniţiale şi, deci. nici importanţa ori valoarea iniţială. În cazul transferului de date informatice, urmarea o constituie, pe de o parte, ştergerea datelor informatice din locaţia iniţială, astfel că acestea nu mai există pentru utilizatorul de drept şi crearea concomitentă a unei replici a datelor informatice, pe acelaşi suport de stocare sau pe un altul, extern, în posesia făptuitorului. C3. Legătura de cauzalitate dintre activitatea făptuitorului şi urmarea produsă trebuie dovedită. D. Latura subiectivă Infracţiunea de alterare a datelor informatice se realizează cu intenţie directă sau indirectă. În majoritatea cazurilor, autorul caută să aducă daune. Intenţia de a scoate dintr-un asemenea act un profit ilicit nu este necesară şi nici tipică acestei forme de comportament delictual. Este, totuşi, posibil să existe o motivaţie 3

indirectă, cum ar fi

dorinţa de a face rău unui concurent. Daunele informatice sunt adesea motivate de dorinţa de răzbunare a unui angajat al cărui contract de muncă a fost reziliat sau este pe cale de a fi. Motivaţiile politice sau ideologice sunt şi ele caracteristice, de exemplu în actele teroriste. În fine, 1

405 disponibilă pe site-ul www.scj.ro

dorinţa de a atrage atenţia publicului sau a unor organizaţii nu este rară. 406 E. Forme. Modalităţi. Sancţiuni. Aspecte procesuale E1. Forme Actele pregătitoare sunt posibile, dar nu sunt incriminate şi ca atare nu sunt pedepsite. 1

Tentativa se pedepseşte conform art. 47 din lege. Infracţiunea se consideră consumată atunci când făptuitorul a modificat, şters sau deteriorat în vreun fel datele dintr-un sistem informatic, a împiedicat accesul la aceste date de către deţinătorii de drept sau a reuşit transferul datelor selectate pe un alt mediu de stocare. Infracţiunea 1

este continuă, epuizarea ei intervenind în momentul în care încetează aceste acţiuni. 2

E2.

Modalităţi Infracţiunea analizată prezintă patru modalităţi normative în varianta tip și anume: 1
modificarea, ştergerea, deteriorarea ori restricționarea **accesului la date informatice. Infracţiunea prezintă și două modalităţi agravate: transferul de date dintr- un sistem informatic [alin,(2)| și transferul de date dintr-un mediu de stocare [alin.(3)].**

E3. Sancţiuni Pedeapsa pentru varianta tip a infracţiunii este de

la 2 la 7 ani închisoare. **Pedeapsa prevăzută pentru modalităţile agravate este închisoarea de la** 3
3 la 12 ani. E4. **Aspecte procesuale Acţiunea penală se pune în mişcare din oficiu.**

VI.3.3

.4. Infracţiunea de perturbare a funcţionării sistemelor informatice – art. 45 17

Sediul materiei îl constituie art. 45 din Legea nr. 161/2003. 406 Vasiu, I., Vasiu, L., op. cit., p. 161.

„Fapta de a perturba grav, fără drept, funcţionarea unui sistem informatic, prin introducerea, 2
transmiterea, modificarea, ştergerea sau deteriorarea datelor informatice sau prin restricţionarea accesului la date informatice **constituie infracţiune si se pedepseşte cu închisoare de la 3 la 15 ani”.**

Prin incriminarea acestei fapte penale s-a urmărit să se protejeze în primul rând

datele informatice stocate în cadrul sistemelor informatice. Spre deosebire de infracţiunea 4
reglementată în art. **44,** aici s-a **pus** accentul **pe efectul pe care îl au pentru sistemele informatice, acţiunile asupra datelor informatice (introducere, transmitere, modificare, ştergere, deteriorare, restricţionarea accesului).** A. **Obiectul juridic** ► Obiectul juridic **special îl constituie relaţiile sociale** care **protejează**

buna funcţionare a sistemelor informatice. ►

Obiectul material este sistemul informatic al **cărui activitate este grav perturbată de făptuitor** 4

şi care se poate referi la următoarele entităţi materiale: componentă, calculator (computer), reţea, Internet.

B. Subiecţii infracţiunii ► Subiectul activ poate fi orice persoană fizică sau juridică care este **responsabilă** 2

din punct de vedere penal. ►

Subiectul pasiv este persoana fizică sau juridică deţinătoarea **de drept a sistemului informatic a cărui funcţionare este perturbată.** 1

C.

Latura obiectivă C1. **Elementul material se realizează prin orice acţiune** care **perturbă grav funcţionarea unui sistem informatic. Textul legal** incriminează **modalităţile** 1

de acţiune şi

anume: introducerea, transmiterea, modificarea, ştergerea sau deteriorarea, precum şi restricţionarea accesului la date informatice. Introducerea de date informatice 1

presupune implementarea acestora în cadrul unui sistem informatic.

Datele pot fi introduse direct, de la tastatură, ori transfer de pe un mijloc extern de stocare. De la tastatură (sau din mouse), atacatorul poate accesa anumite zone rezervate ale echipamentului **de calcul (cum ar fi: zona de BIOS-Basic Input Output System, care controlează activitatea Unităţii Centrale de Prelucrare) sau ale sistemului de operare. Datele greşite pot afecta progresiv şi funcţionarea altor componente, mai ales în condiţiile unei reţele. Poate fi cazul operatorului unui sistem informatic de control al activităţii unei hidrocentrale, care introduce de la tastatură o serie de parametri ce sunt în mod** 3

greşit interpretaţi de programul sau aplicaţia de bază, rezultatul fiind funcţionarea haotică a sistemului ori blocarea anumitor segmente de execuţie. Transmiterea de date informatice

presupune deturnarea acestora către un alt sistem informatic.

Transmiterea de date informatice se realizează de la distanţă, folosind facilităţile oferite de conectarea sistemului vizat la o reţea informatică (de tip LAN - locală sau WAH - de largă utilizare). Este 1

cazul unei persoane

care, indiferent de motiv, trimite prin intermediul Internetului un număr mare de mesaje către sistemul informatic ale unei instituţii, supraaglomerând portalul de date şi blocând accesul acestuia în exterior. Un astfel de exemplu este „Denial of Service" (refuzarea serviciului) în care o sursă de pe Internet, cum ar fi un server sau un site „web" nu mai funcţionează corespunzător deoarece atacatorii lansează un atac coordonat care supraîncarcă ţinta cu atât de multe solicitări false, încât sistemul nu mai poate să le administreze şi este copleşit. Cel mai comun tip de atac „DOS" are ca efect împiedicarea accesului utilizatorilor de Internet la un anumit „site web", ceea ce poate avea ca rezultat pierderi financiare imense în contextul unei organizaţii ale cărei afaceri depind de Internet. O altă modalitate prin care un atacator poate să preia controlul asupra unui sistem informatic sau să introducă aplicaţii maliţioase este prin intermediul Codului Mobil. 1

Astfel, inculpatul D.C. a fost trimis în judecată pentru că

a produs şi a eliberat pe Internet un virus informatic, reţinându-se în sarcina sa acuzaţia de perturbare gravă a unui sistem informatic şi deţinere fără drept 4

de date 402 informatice. S-a reţinut că a virusat calculatoarele instituţiei unde era angajat,

dar şi computere din Belgia şi Olanda, cu ajutorul unei variante modificate a virusului Ms Blast. 31

407 În acelaşi fel, un individ a blocat calculatorul unei alte persoane pe care nu o simpatiza, astfel încât după ce accesa programul Word, calculatorul se reseta, devenind inutilizabil. Aşadar, concluzionând,

transmiterea se poate realiza prin: ‣ transferul (copierea) în sistemul informatic vizat de fişiere sau programe infectate de pe suporţi externi; ‣ transmiterea de mesaje „e-mail" **având ca ataşament fişiere infectate; ‣ descărcarea de fişiere sau programe purtătoare de cod** malițios **din Internet.** Celelalte modalităţi **de** 1

săvârşire a infracţiunii de mai sus, cum ar fi:

„modificarea", „ştergerea" sau „deteriorarea" datelor informatice ori restricţionarea accesului la aceste date constituie şi modalităţi de comitere **a infracţiunii „de alterare a integrităţii datelor informatice",** facem **trimitere la explicaţiile date cu ocazia analizei acestei infracţiuni.** 1

Trebuie să mai precizam că pentru existenţa acestei infracţiuni în modalităţile enumerate mai sus condiţia este ca acţionarea să se facă

fără drept. Va acţiona îndreptăţit, spre exemplu, persoana fizică sau juridică, care, în baza unui contract specific încheiat cu proprietarul sau deţinătorul de drept al sistemului informatic, execută o operaţiune de „Ethical Hacking" - Penetrare cu Acord - prin care se determină vulnerabilităţile sistemului şi se propun mijloacele **adecvate de securitate, provocând o perturbare a funcţionării respectivului ansamblu informatic.** C2. **Urmarea imediată constă în alterarea datelor informatice, creându-se prin aceasta o stare de pericol asociată funcţionării defectuoase, haotice, de necontrolat a sistemului informatic în cauză, rezultând o perturbare gravă a funcţionării sistemului. Prin perturbarea funcţionării unui sistem informatic se înţelege alterarea totală sau parţială a parametrilor funcţionali ai acestuia, de natură să provoace un dezechilibru temporar sau** permanent408, **spre exemplu, virusarea sistemului informatic de gestiune a tranzacţiilor în cadrul unei burse de valori. Gravitatea perturbării este dată de importanţa obiectivului social sau economic controlat prin intermediul sistemului informatic afectat, dar mai ales de dimensiunea şi valoarea pagubelor materiale rezultate.** 1

C3. Legătura de cauzalitate Pentru realizarea acestei infracţiuni se impune a exista o

legătură de cauzalitate între activitatea făptuitorului şi urmarea produsă. D. **Latura subiectivă** 1
Infracţiunea de perturbare a funcţionării unui sistem informatic se poate comite cu intenţie directă sau indirectă. Adesea, diferenţa dintre cele două forme de vinovăţie este dată de natura datelor introduse, transmise, modificate, şterse, deteriorate **sau supuse restricţionării.**

E. Forme. Modalităţi. Sancţiuni. Aspecte procesuale E1.

Forme Actele pregătitoare, deşi posibile, nu sunt incriminate şi ca atare nu se pedepsesc. 1
Anumite acte pregătitoare sunt incriminate ca infracţiuni de sine stătătoare, cum ar fi: art. 42 - accesul ilegal la un sistem informatic, art. 43 - interceptarea ilegală a unei transmisii de date informatice ori art. 46 - operaţiuni ilegale cu dispozitive sau programe informatice. Tentativa se pedepseşte conform **art. 47 din lege. Infracţiunea se consideră consumată atunci când sistemul informatic vizat**

408 Hotca, M.A., Dobrinoiu, M., op. cit., p. 597

dă primul semn de funcţionare defectuoasă sau de blocare. 1

E2.

Modalităţi Infracţiunea analizată prezintă 6 **modalităţi normative în varianta tip, respectiv introducerea, transmiterea, modificarea, ştergerea, deteriorarea** sau **restricţionarea accesului la date informatice.** 1

E3.

Sancţiuni Pedeapsa prevăzută este închisoarea de la 3 la 15 ani. E4. **Aspecte procesuale** 3
Acţiunea penală se pune în mişcare din oficiu.

VI.3.3

.5. Operaţiuni ilegale cu dispozitive sau programe informatice - art. 46 38

Sediul materiei îl constituie

art. 46 din legea nr. 161/2003. „(l) Constituie infracţiune şi se pedepseşte cu închisoare de la l la 6 ani: a) fapta de a produce, vinde, importa, distribui sau pune la, dispoziţie, sub orice forma, fără drept, un dispozitiv sau program informatic, conceput sau adaptat în scopul săvârşirii uneia din infracţiunile prevăzute de art. 42-45; b) fapta de a produce, vinde, importa, distribui sau pune la dispoziţie, sub orice formă. fără drept, o parola, cod de acces sau alte asemenea date informatice care permit accesul total sau parţial la un sistem informatic în scopul săvârşirii uneia din infracţiunile prevăzute de art. 42-45; (2) cu aceeaşi pedeapsă se sancţionează şi deţinerea, fără drept, a unui dispozitiv, program informatic, parolă, cod de acces sau dată informatică, dintre cele prevăzute în alin. (l) în scopul săvârşirii uneia din infracţiunile prevăzute în art. 42-45”. 7

Prin incriminarea acestor fapte s-a urmărit să se

limiteze accesul la instrumente (dispozitive, programe, parole, coduri de acces) care permit săvârşirea de infracţiuni informatice. 4

A. Obiectul juridic ► Obiectul juridic special este reprezentat de relaţiile sociale referitoare la încrederea în datele, dispoziţiile şi programele informatice, în sensul utilizării corecte şi legale a acestora, precum şi în desfăşurarea corectă şi legală a operaţiunilor comerciale în legătură cu acestea. ► Obiectul material, se concretizează în: 1

‣

dispozitive; ‣ programe informatice; ‣ parolă; ‣ cod de acces, de natură a permite accesul total sau parţial la un sistem informatic. 4

Pentru a săvârşi această infracţiune autorul poate folosi anumite modalităţi de a

exploata vulnerabilitatea unui computer sau a unei reţele, 30

cum ar fi:

script sau program; agent independent; virus sau Troian; program integrat; unelte distribuite; sau interceptor de date. B. Subiecţii infracțiunii ‣ **Subiectul activ** 4

al acestei infracţiuni poate fi orice persoană fizică sau juridică **care îndeplineşte condiţiile de** 4

tragere la răspundere penală. Participaţia penală este posibilă sub cele trei forme:

coautorat, instigare si complicitate. ‣ Subiectul pasiv este persoana fizică sau juridică 11

care suferă vreun prejudiciu, deținătoare de drept a sistemului informatic,

dar şi proprietarul ori deţinătorul dreptului de autor pentru produsele „hardware” ori „software” modificate sau adaptate în scop infracţional. 1

C.

Latura obiectivă C1. **Elementul material este reprezentat de acţiunea de a produce, vinde, importa, distribui sau pune la dispoziţie unul sau mai multe dispozitive ori programe informatice, special concepute sau adaptate** cu **scopul săvârşirii uneia din infracţiunile informatice menţionate mai sus. Producerea** unul **dispozitiv informatic constă în efectuarea unor activităţi de ordin tehnic prin care anumite componente electronice sunt astfel îmbinate şi interconectate încât produsul obţinut să poată interacţiona** 1

cu un sistem informatic sau să devină o parte integrantă a acestuia. Spre exemplu, 1

mai multe persoane au fost trimise în judecată pentru că în cursul anului 2006 au constituit un grup infracţional organizat, care a achiziţionat aparatură electronică pentru a o folosi la bancomate în Olanda, în scopul obţinerii de beneficii materiale.

Echipamentele achiziţionate au fost montate la mai multe bancomate din Olanda şi în acest fel au obţinut date de pe cardurile bancare folosite de titularii acestora, iar mai apoi

au pus în circulaţie instrumente de plată electronică, 6

procedând la efectuarea de extrageri neautorizate. Din această activitate ilegală gruparea infracţională a obţinut in numai două luni peste 32.000 Euro, bani ce au fost împărţiţi în mod egal între membrii grupării.409

Crearea unui program informatic presupune elaborarea unei schiţe logice a programului în funcţie de scopul urmărit şi transcrierea instrucțiunilor **într-un limbaj de programare,** 7

pentru a fi înțelese **şi ulterior executate de către sistemul informatic vizat. Un exemplu în acest sens poate fi conceperea, cu ajutorul limbajului de programare de nivel înalt C++, a unui program care, pus în execuţie pe un computer, permite accesul unei persoane neautorizate la resursele sale ori la întregul sistem informatic la care este conectat, prin efectuarea unei operaţiuni de identificare a parolei ori codului de acces. Cele mai periculoase programe informatice sunt, însă, cele care generează viruşi informatici, cai troieni sau „bombe logice”** 410. **Legiuitorul** incriminează, **totodată, şi fapta aceluia care, deşi nu are nici o contribuţie la crearea dispozitivului sau programului informatic, îl** impută, **îl distribuie ori îl pune la dispoziţia persoanei care acţionează în mod nemijlocit asupra sistemului informatic. În acelaşi timp, vor fi sancţionate şi producerea, vânzarea, importul, distribuirea ori punerea la dispoziţia** peroanelor **neautorizate a parolelor, codurilor de acces sau oricăror alte date informatice care permit** 1

409 disponibilă pe site-ul

www.scj.ro 410 Hotca, **M. A.,** și colab. **op. cit., p.** 6

601 407

accesul, total sau parţial, la un sistem informatic. Parola ca şi codul de acces reprezintă o înşiruire cu lungime variabilă de cifre, litere şi sume **speciale rezultate în urma atingerii** unor 1

butoane ale tastaturii, ori generate aleatoriu, prin aplicarea unui algoritm matematic anumitor semnale electrice (sau de altă natură) în cadrul unui dispozitiv special fabricat în acest sens.

C2.

Urmarea imediată constă în crearea unei stări de pericol, de ameninţare **la adresa datelor, dispozitivelor sau programelor informatice.** C3. **Legătura de cauzalitate** există între **activitatea făptuitorului şi urmarea** 2

produsă. Această legătură rezultă

din materialitatea faptei. D. **Latura subiectivă Operaţiunile ilegale cu dispozitive sau programe informatice se săvârşesc cu intenţie directă calificată** de **scop. Astfel, acţiunile descrise în alin.(** l) **şi (2) vor fi comise în scopul săvârşirii infracţiunilor prevăzute de art. 42-45 (accesul ilegal la un sistem** informatic, **interceptarea ilegală a unei transmisii de date informatice, alterarea integrităţii datelor informatice, perturbarea funcţionării sistemelor informatice).** E. **Forme.** Modalități. **Sancţiuni.** Aspecte procesuale E1. **Forme Actele pregătitoare, deşi posibile, nu sunt incriminate şi ca atare nu sunt pedepsite. Observăm** însă **că faptele incriminate la art. 46 lit. a) - c) constituie acte pregătitoare ale infracţiunilor prevăzute în art. 42 - 45, însă legiuitorul român a preferat să le incrimineze în mod** separat. **Tentativa se pedepseşte conform art. 47 din lege. Infracţiunea se consideră consumată în momentul producerii, comercializării, importului, distribuirii, punerii la dispoziţie ori deţinerii, fără drept, a unui dispozitiv, program** informatic, **parolă, cod de acces sau alt tip de date informatice în scopul săvârşirii infracţiunilor mai sus menţionate. Săvârşirea faptelor incriminate în art. 46 lit. a) - c), cu aceeaşi ocazie şi în mod neîntrerupt, realizează conţinutul constitutiv al unei singure infracţiuni (unitate naturală de infracţiune)** 411. E2. **Modalităţi Infracţiunea** prezentată are **şase modalităţi normative, respectiv producerea, vânzarea, punerea la dispoziţie sau deţinerea, fără drept, a unui dispozitiv, program informatic, parolă, cod de acces sau alte date informatice. Acestor modalităţi normative pot să le corespundă** o multitudine de **modalităţi** faptice **de** săvârşire. E3. **Sancţiuni Pedeapsa prevăzută este** închisoarea **de la** l an **la 6 ani.** E4. **Aspecte procesuale Acţiunea penală se pune în mişcare din oficiu.** 3

VI.3.3.6. Infracţiunea de fals informatic - art. 48 Sediul materiei îl constituie art. 48 din Legea nr. 161/2003.

„Fapta de a introduce, modifica sau şterge, fără drept, date informatice ori de a restricţiona, fără drept, accesul la aceste date, dacă fapta are ca rezultat obţinerea de date necorespunzătoare adevărului, în scopul de a fi utilizate în vederea producerii unei consecinţe juridice, constituie infracţiune şi se pedepseşte cu închisoare de la 2 la 7 ani”. 22

A. Obiectul juridic ► Obiectul juridic special constă în relaţiile sociale referitoare la încrederea publică în siguranţa şi fiabilitatea sistemelor informatice, la valabilitatea şi autenticitatea datelor informatice, a întregului proces modern de prelucrare, stocare şi tranzacţionare automată a datelor de interes oficial sau 2

411 Dobrinoiu, M. și colab. op. cit. p. 541

privat. Datele informatice au dobândit un rol important în societatea actuală. Ele contribuie la facilitarea contractelor sociale şi la o mai bună comunicare între persoane (fizice sau juridice, în conformitate cu exigenţele statului de drept şi interesele individuale ale cetăţenilor) 412 ► Obiectul material 1

al infracţiunii constă în suportul (listing, disc magnetic etc.) pe care se înscriu datele sau programele pentru calculator supuse activităţii infracţionale. B. Subiecţii infracţiunii ► Subiectul activ al infracţiunii poate fi orice persoană fizică sau juridică, responsabilă din punct de 4

vedere penal. Trebuie să precizăm însă că, cel mai adesea, manipulările frauduloase sunt efectuate de iniţiaţi şi, mai ales, de persoane

care au acces, prin natura serviciului lor, la date şi programe pentru calculator 4

(cei care fac parte din „criminalitatea gulerelor albe”), cei care efectuează îndeosebi tranzacţiile bancare, operaţii contabile şi plăţile413. ►

Subiectul pasiv poate **fi persoana fizică sau juridică prejudiciată în propriile interese şi faţă de care se produc consecinţe juridice (de ordin patrimonial, moral ori social) în urma contrafacerii datelor informatice.** 1

C.

Latura obiectivă C1. **Elementul material este dat de** una dintre acţiunile **de a: ‣ „introduce”; ‣ „modifica”; ‣ „şterge”; ‣ „restricţiona** 4

accesului la date informatice”. **Întrucât aceste modalităţi** alternative de săvârşire **au fost analizate în cadrul infracţiunii de alterare a integrităţii datelor informatice,** facem **trimitere la explicaţiile de la respectiva** 1

infracţiune. Pentru a exista această infracţiune, trebuie îndeplinită o cerinţă esenţială şi anume fapta trebuie să aibă ca rezultat obţinerea de date necorespunzătoare 412 Dobrinoiu, M. și colab. op. cit. p. 542 413 Vasiu, I., Criminalitatea informatică, Editura Nemira, București, 1998, p. 82. 410 adevărului. De asemenea, trebuie să se dovedească că aceste date au fost obţinute

în scopul de a fi utilizate în vederea producerii unei consecinţe juridice. 9

Actele prin care se realizează elementul material al infracţiunii implică efecte negative asupra stării datelor în ce priveşte capacitatea lor de a funcţiona şi atesta fapte ori situaţii de maniera prevăzută de persoana care dispune de ele, ajungându-se la o situaţie care corespunde fabricării unor documente false sau falsificării unor documente autentice414. **Cu titlu de exemplu, falsificarea datelor informatice s-ar putea realiza sub următoarele forme: ‣ înserarea, modificarea sau ştergerea de date în câmpurile unei baze de date existente la nivelul unui centru de evidenţă informatizată a persoanei,** a **unei bănci sau** societăți **de** asigurare ele. - **prin acţiunea directa 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.** 1

De pildă, comite infracţiunea de mai sus acela care intra în baza de date a unei universităţi şi îşi modifică situaţia şcolară, după care merge şi ridică diploma de studii ce va cuprinde date privind situaţia la învăţătură, necorespunzătoare realităţii415. C2.

Urmarea imediată constă în obţinerea de date necorespunzătoare adevărului şi, prin aceasta, 1

se creează o stare de

pericol pentru încrederea care se acordă datelor informatice şi, în general, prelucrării automate a acestora. C3. **Legătura de cauzalitate** dintre **activitatea făptuitorului şi urmarea produsă trebuie dovedită.** D. **Latura** obiectivă **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** 1

414 Vasiu, I., Vasiu, L., op. cit., p. 169. 415 Voicu, C., Boroi, A., op. cit., p.370 411

un scop „legitim" (de exemplu, pentru a crea proba unei situaţii juridice). 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. 416 E. **Forme. Modalităţi. Sancţiuni.** Aspecte procesuale E1. **Forme Actele pregătitoare, deşi posibile, nu sunt incriminate** de lege **şi ca atare nu** se pedepsesc. **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 restricţionat accesul la respectivele date dacă prin aceasta s-au produs alte date sau situaţii juridice** necorespunzătore **valorii de adevăr iniţiale.** E2. **Modalităţi Infracţiunea analizată prezintă patru modalităţi normative** de săvârşire, **respectiv: introducerea, modificarea, ştergerea de date informatice, precum şi restricţionarea accesului la aceste date. Acestor modalităţi normative pot să le corespundă** 3

o multitudine

de variante de fapt. E3. Sancţiuni Fapta este pedepsită cu închisoare de la 2 la 7 ani. 1
E4. Aspecte procesuale Acţiunea penală se pune în mişcare din oficiu.

416 Toader, T.,

Drept penal, Partea specială, Editura All Beck, București, 2002, 40

p. 386; Loghin, O., Filipaș, A.,

Drept penal român, Partea specială, Casa de Editura și Presă Șansa, București 1992, p. 27
269; Dobrinoiu, V.

și colab.,

op. cit., p. 618; Boroi, Al., Nistoreanu, Gh., Drept Penal, Partea specială, Editura All 1
Beck, București, 2004, p. 723.

412 VI.3.3.7. Frauda informatică - art. 49 Sediul materiei îl constituie art. 49 din Legea nr. 161/2003.

„Fapta de a cauza un prejudiciu patrimonial unei persoane prin introducerea, modificarea sau 2
ştergerea de date informatice, prin restricţionarea accesului la date informatice ori prin
împiedicarea, în orice mod, a funcţionării unui sistem informatic, în scopul de a obţine un beneficiu
material pentru sine sau pentru altul, constituie infracţiune şi se pedepseşte cu închisoare de la 3 la 12
ani”.

Cu alte cuvinte, frauda informatică presupune

intrarea, alterarea, ştergerea sau supraimprimarea de date sau de programe pentru calculator sau 2
orice altă

intruziune care ar putea sa genereze o influență a rezultatului, cauzând prin aceasta un prejudiciu material sau economic important, făptuitorul urmărind să obţină un avantaj patrimonial pentru sine ori pentru altul. A. Obiectul juridic ► Obiectai

juridic special îl constituie relaţiile sociale care protejează integritatea datelor informatice, 2

securitatea sistemelor informatice şi patrimoniul unei persoane. ► Obiectai

material este reprezentat atât de datele informatice (stocate în sistemele informatice vizate), cât şi de entităţile materiale care compun un sistem informatic 1

(precum CD-ul, discheta, hard-disck-ul etc. pe care pot fi înscrise datele şi programele protejate).

B. Subiecţii infracţiunii ► Subiectul activ poate fi orice persoană fizică sau juridică 2

aptă din punct de vedere penal de a săvârşi infracţiuni. În practică se constată că asemenea infracţiuni se comit cel mai adesea de persoane iniţiate

în domeniul informatic **ori de persoane care, prin natura serviciului, au acces la date şi sisteme** informatice417. **Participaţia** penală **este posibilă în toate formele sale: coautorat, instigare** 1

417 Vasiu, I., Vasiu, L., op. cit., p. 159. ori complicitate. ► Subiectul

pasiv poate fi orice persoană fizică sau juridică, afectată patrimonial prin acţiuni asupra sistemelor informatice pe care le deţin **sau pe care le utilizează.** C. **Latura obiectivă** C1. **Elementul material** 4

este realizat prin oricare dintre următoarele acţiuni: ‣

„introducerea de date informatice”; ‣ „modificarea de date informatice”; ‣ ştergere de date **informatice”; ‣ „restricţionarea accesului la date informatice”; ‣ „împiedicarea funcţionării unui sistem informatic”.** 25

Întrucât primele patru modalităţi de săvârşire

au fost deja analizate în cadrul infracţiunii de alterare a datelor informatice, facem **trimitere la explicaţiile date la acea infracţiune.** Prin **„împiedicarea funcţionării sistemului informatic”,** 3

ca a cincea modalitate de realizare a elementului material, trebuie să înţelegem realizarea oricărui act care are drept consecinţă

imposibilitatea utilizării, parţiale **sau** totale, **temporar sau permanent, a respectivului sistem.** 1

Împiedicarea funcţionării unui sistem informatic cuprinde atacuri fizice (spre exemplu,

tăierea de cabluri, întreruperea alimentării cu energie etc.) şi **atacuri logice,** care **împiedică pornirea normală a unui calculator** (spre exemplu, **prin modificarea setărilor iniţiale), atacuri de tip „refuz al serviciului”** (Devial **of service), blocarea sistemului** 2

prin folosirea de contaminanţi informatici,

blocarea tastaturii, consumarea memoriei sau a spaţiului de stocare de pe discuri. 2

Aceste acţiuni trebuie să fie efectuate de făptuitor în scopul de a obţine un beneficiu material pentru sine sau pentru altul, dar pentru existenţa infracţiunii **nu este necesar să îl** 2

obţină418 . 418 Vasiu, I., Vasiu, L., op. cit. p. 46

Frauda poate fi comisă cu ajutorul mai multor mijloace, însă în lucrarea de faţă vom aborda doar mediile electronice (poştă electronică, telefon, cablu, Internet). În mediul informatic, frauda poate avea mai multe forme şi adesea se poate confunda cu înşelăciunea tradiţională, mijlocul de realizare fiind computerul. 1

Din activitatea practică a rezultat că formele cele mai utilizate de comitere a infracţiunilor informatice în scopul obţinerii de foloase materiale injuste sunt vânzările şi cumpărăturile fictive prin intermediul platformelor comerciale on-line, precum şi efectuarea de licitaţii fictive on-line, inculpaţii folosind cel mai frecvent următoarele moduri de operare419 ‣ „Metoda Phishing” - este utilizată de inculpaţi în special pentru comiterea de infracţiuni informatice prin intermediul platformelor comerciale on-line (cum este de exemplu, platforma eBay). Acestea sunt portaluri de comerţ on-line, fără frontiere, unde se poate vinde sau cumpăra aproape orice şi oferă clienţilor săi şansa de a afişa produse spre vânzare pe site-urile sale prin licitaţie sau chiar vânzare directă şi, de asemenea, oferă posibilitatea să participe la asemenea licitaţii sau de a accede la produsele afişate spre vânzare pe site-uri. Persoana care intenţionează să vândă un produs postează o ofertă de vânzare cu un preţ minim de la care porneşte licitaţia on-line (de la antichităţi la autoturisme, articole sportive sau cărţi). Produsul este afişat pe site-ul platformei comerciale pentru o perioadă determinată (de exemplu, în cazul platformei comerciale eBay, produsul este afişat timp de 7 zile), în această perioadă, orice utilizator poate accesa produsul pe Internet. Persoana interesată de un anumit produs poate utiliza browser-ul de căutare pe categorii de produse, iar în ofertă găseşte informaţiile postate de vânzător referitoare la particularităţile produsului, fotografii ale acestuia. 419 Koveși, L.C., Finta, S, Încadrarea juridică a unor fapte de fraudă informatică, în Revista Dreptul, nr. 12/2006. 415 În scopul postării de licitaţii fictive pe platformele comerciale, inculpaţii îşi creează baze de date care conţin adrese valide de e-mail (useri şi parole) ale unor utilizatori ai platformei comerciale. În acest sens, se facilitează pagina de înregistrare „sign-in” a site-ului de licitaţii prin modificarea codului sursă, în sensul că se înlocuieşte adresa de contact a administratorului platformei comerciale cu o altă adresă de e-mail controlată de inculpaţi. Pagina falsă de înregistrare se transmite către adresele valide de e-mail din baza de date creată anterior (spam). O parte dintre utilizatorii care primesc mesajul nesolicitat de înregistrare (sau reconfirmare a datelor de înregistrare) sunt induşi în eroare de mesajul aparent autentic şi îşi introduc datele de înregistrare pe site-ul comercial. Datele de înregistrare ale utilizatorului legitim, introduse la rubrica „user ID” şi „password” (parola) sunt direcţionale fără ştirea utilizatorului, către adresa de e-mail specificată în codul sursă, odată cu efectuarea click-ului şi mail-urilor, pentru ca titularii legitimi să nu mai poată folosi aceste date şi apoi postează licitaţii fictive, în sensul că folosesc useri care nu le aparţin (deci nu poate fi verificată identitatea lor) şi oferă spre vânzare bunuri care în realitate nu le deţin, ştiind că, în cazul în care un potenţial client trimite banii pentru produsul oferit, acesta nu va primi niciodată bunul. Ulterior, inculpaţii iniţiază o corespondenţă prin e-mail cu persoana interesată şi, în cazul în care acesta este de acord cu încheierea tranzacţiei, încurajează potenţialul client să trimită contravaloarea produselor oferite (la preţuri avantajoase) sau a unui avans printr-un sistem rapid de transmitere a banilor (Western Union sau Money Gramm). Astfel, inculpaţii solicită o copie scanată a chitanţei din care rezultă că au fost trimişi banii, iar când se primeşte prin e-mail copia scanată a chitanţei de transmitere a banilor, aceştia se prezintă la instituţiile bancare şi ridică sumele de bani, fără a trimite vreodată bunul pentru care i s-au trimis banii. ‣ „Metoda Shipping” - este similară cu metoda phishing, respectându-se acelaşi mod de operare până în momentul participării la licitaţiile fictive, diferenţa constând în faptul că, în loc să primească banii, autorii primesc produsele, în 416 acest caz, inculpaţii participă la licitaţiile fictive nu în calitate de vânzători, ci în calitate de cumpărători şi propun potenţialei victime trimiterea produsului anterior efectuării plăţii. Bineînţeles că, după primirea produsului, inculpaţii nu trimit bunul licitat, înşelând în acest fel victima. ‣ „Metoda Escrow” - prin utilizarea acestei metode, inculpaţii postează licitaţii fictive pe diferite site-uri comerciale, în modurile descrise mai sus, iar atunci când potenţiala

victimă este interesată să cumpere produsul, inculpaţii propun potenţialului client intermedierea tranzacţiei printr-un site escrow falsificat şi controlat tot de ei. Această metodă este folosită în cazul clienţilor suspicioși sau reticenţi care nu doresc să trimită banii printr-un sistem rapid de transfer al sumelor de bani şi care folosesc în mod regulat site-uri de tip escrow, cunoscute pentru garantarea tranzacţiilor on-line. ‣ „Metoda carding” - utilizând aceasta metodă, inculpaţii urmăresc sustragerea şi folosirea datelor deţinătorilor de conturi pe site-urile comerciale. Pentru sustragerea datelor, inculpaţii transmit mesaje nesolicitate (spam), de actualizare a datelor deţinătorilor de conturi pe site-urile comerciale. Prin modificarea codului sursă a paginii originale, informaţiile introduse de utilizatorii legitimi sunt direcţionate spre o adresă de e-mail specificată de inculpaţi şi pentru sustragerea datelor aferente cărţilor de credit emise de instituţii bancare. După ce deţinătorii legitimi ai conturilor sau cardurilor îşi introduc datele, acestea sunt culese de autori din memoria căsuţei de e-mail specificata în codul sursă, după care sunt folosite la postarea de licitaţii fictive pe site-urile de comerţ on-line, la tranzacţii on-line la diverse magazine virtuale, pentru crearea de domenii pentru site-urile false sau la falsificarea unor carduri de tip blank. C2.

Urmarea imediată constă în crearea unui prejudiciu patrimoniului **unei persoane.** C3. **Legătura de cauzalitate** există **între activitatea făptuitorului şi urmarea produsă.** 1

417 D.

Latura subiectivă Frauda informatică se săvârşeşte numai cu intenţie directă, calificată prin scop. Fapta se săvârşeşte în scopul obţinerii unui **beneficiu material pentru sine sau pentru altul. Pentru existenţa** 1

acestei infracţiuni

nu este nevoie ca prejudiciul material să fi fost efectiv realizat, ci numai să fi existat ca o posibilitate urmărită de făptuitor. E. **Forme. Modalităţi. Sancţiuni.** Aspecte procesuale E1. **Forme Actele pregătitoare,** sunt **posibile,** dar **nu sunt** 1

pedepsite de lege. **Tentativa se pedepseşte conform art. 50 din lege. Infracţiunea se** 9

consumă

atunci când făptuitorul a introdus, modificat şters în vreun fel date informatice ori a restricţionat accesul la aceste date sau împiedicat în orice fel funcţionarea unui sistem informatic, cauzând prin aceasta un prejudiciu patrimonial unei persoane. E2. Modalităţi Infracţiunea analizată prezintă cinci modalităţi normative de realizare, respectiv introducerea, modificarea, ştergerea datelor informatice, restricţionarea accesului la aceste date ori împiedicarea în orice mod a funcţionării unui sistem de calcul. Acestor modalităţi normative pot să le corespundă variate modalităţi de fapt. E3. Sancţiuni Pedeapsa prevăzută este închisoarea de la 3 la 12 ani. E4. Aspecte procesuale Acţiunea penală se pune în mişcare din oficiu. 1

VI.3.3.8.

Infracţiunea de pornografie infantilă prin intermediul sistemelor informatice 1

- art. 51 Sediul materiei îl constituie art. 51

din Legea nr. 161/2003. „(1) Constituie infracţiune şi se pedepseşte cu închisoare de la 3 la 12 ani 7

producerea în vederea răspândirii, oferirea sau punerea la dispoziţie, răspândirea sau transmiterea, procurarea pentru sine sau pentru altul, de materiale pornografice cu minori prin sisteme informatice ori deţinerea, fără drept, de materiale pornografice cu minori într-un sistem informatic sau mijloc de stocare a datelor informatice. (2) Tentativa se pedepseşte". A. 20

Obiectul juridic ►

Obiectul juridic special îl constituie relaţiile sociale ce urmăresc protejarea minorilor. ► Obiectul material îl reprezintă suporţi de stocare a datelor din sistemele informatice ce conţin materiale pornografice cu minori. Astfel, potrivit art. 35 alin.(l) lit. i) din Legea nr. 161/2003, prin materiale pornografice cu minori se înţelege orice material care prezintă un minor având un comportament sexual explicit sau o persoana majoră care este prezentata ca un minor având un comportament sexual explicit, ori imagini care, deşi nu prezintă o persoana reală, simulează în mod credibil un minor având un 3

comportament sexual explicit. În art. 35 se foloseşte şi termenul de „imagini" care, deşi nu prezintă o persoană reală, simulează în mod credibil un minor având un comportament sexual explicit. Ca urmare, înregistrările audio nu pot constitui „materiale pornografice cu minori" decât în corelaţie cu înregistrările

video420. În

definirea materialelor pornografice cu minori se face referire la un comportament sexual explicit. 2 **Acest comportament poate însemna şi o poziţie sexuală, tot atât de bine cum poate prezenta un act sexual sau orice atitudine care poate fi considerată un comportament sexual; acesta trebuie să fie de asemenea** explicit421, **iar nu implicit, şi anume să reiasă în mod direct din imaginile prezentate, să nu fie simple sugerări. Comportamentul sexual al minorului trebuie să fie evident cuprins pe**

420 Hotca, M. A., Dobrinoiu, M., op. cit., p.611. 421 Breban, V.,

Dicţionar al Limbii române contemporane de uz curent, Editura ştiinţifică şi Enciclopedică, Bucureşti, 1980, p. **196.** 1

419

respectivul material pornografic422. **Trebuie subliniat însă că un tablou, un film, o scriere ori o fotografie vor avea caracterul de pornografie dacă detaliile lascive sunt folosite anume pentru a pune în lumină acest caracter obscen şi pentru a deschide drum pornografiei şi pornirilor către** imoralitate **sexuală.** 9

B. Subiecţii infracţiunii ► Subiect activ poate fi orice persoană fizică sau juridică **responsabilă penal. În cazul „producerii în vederea răspândirii" sunt consideraţi subiecţi ai** acestei infracţiuni **toate persoanele care iau parte la diferite stadii ale procesului de elaborare sau producere a materialelor pornografice cu minori, chiar şi cele care au servit de model (la fotografiere, filmare etc.).** 3

Participaţia penală

este posibilă sub toate formele sale: coautorat, instigare ori complicitate. ► Subiectul pasiv va fi minorul ale cărui ipostaze pornografice au fost înregistrate, stocate ori transmise prin sisteme informatice. A. Latura obiectivă C1. Elementul material este constituit din mai multe modalităţi alternative de executare, şi anume: „producerea în vederea răspândirii"; „oferirea"; „punerea la dispoziţie"; „răspândirea"; „transmiterea"; „procurarea pentru sine sau pentru altul de materiale pornografice cu minori"; „deţinerea, fără drept, de materiale pornografice cu minori într-un sistem informatic sau un mijloc de stocare a datelor informatice". Producerea în vederea răspândirii a materialelor pornografice cu minori presupune fabricarea, extragerea, combinarea acelor materiale. Pentru existenţa infracţiunii în această modalitate este necesar ca aceste materiale să fi fost produse în vederea răspândirii lor. Dacă producerea materialelor nu s-a făcut în vederea răspândirii lor, ci pentru sine, acţiunile respective nu vor constitui elementul material al infracţiunii. Va 1

exista totuşi faptă penală în 422 Pătrăuș, M., Uzvat,

C.Fl., Pornografia infantilă în reglementările actuale, Revista Dreptul, nr. 4/2003, pp .38-52 1

420 varianta

deţinerii fără drept de materiale pornografice cu minori. Oferirea materialelor pornografice cu minori înseamnă acţiunea de a prezenta cuiva aceste materiale. Prin acţiunea de a pune la dispoziţie, se înţelege asigurarea pe orice căi a accesului, fie contra cost, fie gratuit, la materiale pornografice cu minori, posibilitatea unor persoane de a dispune, de a folosi materiale cu caracter pornografic. Acţiunea de răspândire de materiale pornografice cu minori are loc de câte ori asemenea materiale sunt difuzate sau transmise persoanei care trebuie să le difuzeze sau unor amatori. Nu are importantă 3

din punct de vedere al existenţei faptei penale

dacă cel care răspândeşte materialele pornografice cu minori este chiar persoana care le-a confecţionat sau o altă persoană. Este de precizat că intră în noţiunea de răspândire şi expunerea publică cu sau fără scop de vânzare a materialelor respective, în cazul răspândirii considerăm că este vorba de o pluralitate de acte de transmitere care pot fi concomitente sau succesive. Acţiunea de transmitere a materialelor prevăzute în textul incriminator presupune trimiterea, predarea obiectelor în 1

care sunt materializate imagini cu caracter pornografic cu minori. Procurarea pentru sine sau pentru altul reprezintă orice acţiune prin care se intră în posesia materialelor pornografice cu minori (cumpărare, închiriere, primire etc.). Deţinerea fără drept a materialelor pornografice cu minori constă în simplul fapt de a le avea în stăpânire contrar dispoziţiilor legale. Prin urmare, deţinerea legitimă a acestora exclude răspunderea penală. Pentru existenţa infracţiunii analizate **este necesar ca activităţile incriminate să se refere la materialele pornografice cu minori.**

C2. Urmarea imediată Aceasta este reprezentată de

starea de pericol la adresa minorilor. Ea are loc în momentul declanşării acţiunii de producere, oferire, punere la dispoziţie, răspândire, transmitere, procurare sau deţinere de materiale pornografice cu minori. C3. **Legătura de cauzalitate** 1

trebuie să existe între acţiunea făptuitorului şi urmarea socialmente periculoasă produsă. D. Latura subiectivă Latura subiectivă este caracterizată atât de intenţie directă, cât şi de intenţie indirectă. E. Forme. Modalităţi. Sancţiuni. Aspecte procesuale E1.

Forme Actele pregătitoare, deşi posibile, nu sunt incriminate şi ca atare nu sunt pedepsite de lege. **Tentativa se pedepseşte conform alin.(2) din acest articol. Infracţiunea se consideră consumată atunci când făptuitorul a produs, oferit, pus la dispoziţie, răspândit, transmis, procurat pentru sine sau pentru altul ori** a **deţinut materiale pornografice cu minori într-un sistem informatic sau mijloc de stocare a datelor.** E2. **Modalităţi Infracţiunea analizată prezintă şapte modalităţi normative** de realizare, **respectiv cele enunţate în** textele **articolului. Acestor modalităţi normative pot să le corespundă variate modalităţi** faptice. E3. **Sancţiuni Pedeapsa prevăzută este închisoarea de la 3 la 12 ani.** E4. **Aspecte** 1

procesuale Acţiunea penală se pune în mişcare din oficiu. În 1

prezent, în România, există în vigoare mai multe prevederi legale, cuprinse în legi speciale, care incriminează **diferite fapte în legătură cu sistemele informatice ori societatea informaţională în ansamblul ei. Ca** 1

atare, se poate

trage concluzia că există **un cadru coerent şi conform cu ultimele dispoziţii internaţionale în domeniu.** 1

Coerenţa reglementării va deveni deplină

odată cu intrarea în vigoare a noului Cod 25

penal, care reglementează în Capitolul al VI-lea al titlului VII

„Infracţiuni contra siguranţei şi integrităţii sistemelor şi datelor informatice”. 17

Cu toate acestea, nu înseamnă că lucrurile sunt perfecte şi nu este loc de mai bine şi de aceea facem unele propuneri de lege ferenda:423 ‣ Potrivit

art. 8 din cadrul Convenţiei Consiliului Europei privind criminalitatea informatică, ratificată prin Legea nr. 64/2004, România se obligă ‣ să adopte măsurile legislative şi alte măsuri care se dovedesc necesare pentru a incrimina ca infracţiune fapta intenţionată săvârşită **„fără drept”, de** natură **a cauza un prejudiciu patrimonial unei persoane prin introducere, alterare, ştergere sau suprimare a datelor informatice ori prin orice formă care aduce atingere funcţionării unui sistem informatic, cu intenţia frauduloasă de a obţine fără drept un beneficiu economic pentru el însuşi sau pentru o altă persoană. În mod** cu totul inexplicabil, **legiuitorul român a incriminat** atât **în** 1

art. 49 din Legea nr. 161/2003, cât şi **în** 1

noul Cod penal (art. 249), infracţiunea de fraudă informatică, omiţând

referirile la cauzarea „fără drept” a unui prejudiciu patrimonial ori la obţinerea „fără drept” a unui beneficiu economic, aşa cum se prevede **în** 1

Convenţia Consiliului Europei privind criminalitatea informatică. ‣ Consider oportun a se incrimina şi săvârşirea infracţiunilor informatice din culpă de către persoanele răspunzătoare pentru aplicarea dispoziţiilor legale în materie, prin neglijenţă. Prin această incriminare s-ar crea

o infracţiune obstacol în calea săvârşirii unor alte infracţiuni mai grave. 1

‣ Posibilitatea descoperirii

faptelor îndreptate contra integrităţii şi securităţii datelor şi sistemelor informatice ar putea creşte dacă 1

şi în cazul acestor infracţiuni

ar fi reglementată o cauză de nepedepsire sau de reducere a pedepsei care să încurajeze denunţarea acestor fapte. Ar putea fi luat exemplul altor domenii în care operează asemenea instituţii **de drept** 1

penale: art. 15-16 din 423 Pentru amănunte, a se vedea Dobrinoiu, Maxim, op. cit., pp. 378 -381. 423 Legea nr. 143/2006, art. 10 din Legea nr. 241/2005, art. 9 din Legea nr. 39/2003. CONCLUZII ŞI PROPUNERI Pericolele - omniprezente şi ameninţările - omnidirecţionale pot schimba complet direcţia de evoluţie a sistemelor şi proceselor, determinând adevărate catastrofe în ceea ce priveşte relaţiile internaţionale. Privind în acest sens, criminalitatea transfrontalieră se constituie într-o sursă de generare şi regenerare a conflictualităţii, a instabilităţii şi insecurităţii. Începând cu ultimul deceniu al secolului al XX-lea, dimensiunea transfrontalieră a devenit esenţială în redefinirea criminalităţii organizate. Constituirea spaţiului Schengen, departe de a diminua această nouă caracteristică, a accentuat-o şi mai mult, astfel încât putem afirma că dimensiunea transfrontalieră a criminalităţii organizate a devenit dominantă la acest început de mileniu. De cele mai multe ori, crima organizată se întrepătrunde cu terorismul şi conţine un nucleu dur, reprezentat de criminalitatea economico-financiară, la care se adaugă corupţia, fenomen ce tinde să erodeze baza sistemului economic şi având ca finalitate afectarea instituţiilor fundamentale ale statului de drept.

Organizaţiile criminale profită de contradicţiile generate de permisivitatea sau chiar lipsa unor legi, de neaplicarea legilor existente, de relaţiile neadecvate dintre sferele politice, economice şi administrative, precum şi de ineficienta ori slaba colaborare dintre **structurile interne** sau internaţionale **abilitate în combaterea fenomenului infracţional.** 5

Una din caracteristicile organizaţiilor criminale ale acestui început de mileniu este menţinerea şi dezvoltarea relaţiilor mult mai eficient, cu un sistem de cooperare şi de lucru în timp real, pentru realizarea scopului şi produsului infracţional, coroborat cu spălarea banilor şi introducerea lor în circuitul legal statal sau multinaţional. Mai mult decât atât, organizaţiile criminale reuşesc să se adapteze imediat pentru a scăpa de măsurile întreprinse împotriva lor de către poliţie şi justiţie, ceea ce denotă că există un anumit „model criminal" ce cuprinde elemente de tactică, căi şi mijloace de acţiune, foarte sofisticate şi deosebit de periculoase.

Experienţa a demonstrat că nu există o singură abordare în combaterea crimei organizate care să fie cu adevărat eficientă, succesul putând **fi asigurat de o gamă largă de strategii care acţionează în mod concertat.** 5

În contextul în care forurile continentale şi mondiale îşi canalizează eforturile pe direcţia identificării soluţiilor adecvate pentru ţinerea fenomenului criminalităţii organizate sub control, România şi-a amplificat eforturile de contracarare a acestui flagel, atât în plan intern, cât şi internaţional. Aceste eforturi vizează alăturarea României la efortul internaţional, prin punerea la dispoziţie a potenţialului naţional de combatere şi intensificarea măsurilor de actualizare a cadrului legislativ, cu preponderenţă cel penal.

Dacă în domeniul clasic al asistenţei **judiciare penale** internaţionale, **reglementată prin** convenţii, **uniformizarea** legislaţiilor **penale ale** ţărilor **membre ale UE întâmpină inerente** dificultăţi **cauzate de specificul** naţional tradiţional **al acestora, apreciem că în** privinţa **noilor forme ale crimei organizate** transnaţionale **cum ar fi criminalitatea informatică, această uniformizare va fi mult mai uşor de realizat, întrucât în acest domeniu nu există o** tradiţie **juridică a** ţărilor **europene, iar o reglementare unitară la nivel continental va fi convenabilă tuturor şi va fi uşor de pus în aplicare la nivel** naţional, **cât şi** internaţional. **Mergând pe această linie, sunt de actualitate cuvintele vizionarului politician francez Robert Schumann, care în 1950 spunea: „Europa nu se va face dintr-o dată, nici într-o** construcţie **de ansamblu, ci prin realizări concrete care să creeze mai întâi** 426 **solidaritate de fapt."** 5

Prin urmare, abordarea sistemică a problematicii privind criminalitatea organizată implică în

mod obligatoriu luarea în calcul a două elemente inseparabile, **respectiv obiectivele urmărite şi metodele folosite.** 33

În acest sens, obiectivele ce trebuie avute în vedere la elaborarea strategiilor de prevenire şi reprimare a crimei organizate ar putea fi: reducerea vulnerabilităţii societăţii **la infiltrarea** organizaţiilor **criminale; reducerea** posibilităţilor **de acumulare şi folosire a profiturilor** obţinute **din** activităţi **ilicite; identificarea, dezmembrarea şi lichidarea** organizaţiilor **criminale prin urmărirea şi condamnarea membrilor acestora, confiscarea bunurilor** obţinute **din** infracţiuni **şi a celor folosite în astfel de scopuri.** 5

Pentru realizarea acestor obiective, este nevoie de elaborarea, adoptarea şi aplicarea unor strategii de prevenire şi reprimare adecvate, prin metode şi mijloace eficiente, motiv pentru care considerăm că se impune ca reglementarea tehnicilor speciale de investigare424 în legislaţia română să fie îmbunătăţită. Practica organelor judiciare a demonstrat că pe parcursul urmăririi penale a unor infracţiuni de criminalitate organizată pot fi necesare procedee probatorii care presupun limitări ale drepturilor fundamentale ale persoanelor vizate şi pentru care nu există în prezent o procedură legală care să prevadă condiţiile de autorizare într-o manieră care să garanteze respectarea drepturilor fundamentale ale persoanelor.

Legea nr. 135/2010 privind Codul de procedură penală 12

prevede o reglementare nouă a tehnicilor speciale de investigare, însă nu răspunde tuturor provocărilor pe care le presupune crima organizată, omiţând reglementarea unor instrumente esenţiale în probarea unei activităţi infracţionale. În acest scop, propun lărgirea sferei tehnicilor speciale de supraveghere 424 Potrivit Recomandării (2005) 10 a Comitetului de Miniştri al Consiliului Europei, prin noţiunea de tehnici speciale de investigare se înţelege tehnicile folosite de autorităţile judiciare în cadrul anchetelor penale, urmărind depistarea unor infracţiuni grave, astfel încât persoanele în cauză sa nu aibă cunoştinţa de acest lucru. 427 prin reglementarea utilizării persoanei juridice sub acoperire, precum şi a posibilităţii folosirii colaboratorului investigatorului sub acoperire în cazul investigării infracţiunilor prevăzute de Legea nr.39/2003. Aceste procedee probatorii sunt utilizate în majoritatea statelor din Europa şi reprezintă elemente esenţiale pentru a asigura succesul misiunilor, conspirativitatea acţiunilor şi protejarea identităţii reale a investigatorilor sub acoperire. Evoluţia infracţionalităţii a determinat ca în anumite situaţii organele de urmărire penală să nu poată pătrunde în mediul unor persoane suspectate de săvârşirea de infracţiuni decât folosind acoperirea unei persoane juridice, prin intermediul cărora să desfăşoare anumite activităţi, sau prin intermediul unei persoane care este deja cunoscută de membrii grupului infracţional şi care beneficiază de încrederea acestora. Astfel, persoana juridică de acoperire este forma de asociere sau organizare cu sau fără personalitate juridică, înfiinţată în condiţiile legii, care este folosită în scopul derulării activităţilor specifice ale investigatorilor sub acoperire, în cadrul activităţilor de legendare. În Germania, spre exemplu, aceste persoane juridice sunt folosite în cadrul unor investigaţii de mare amploare, procedura de înfiinţare fiind cea obişnuită pentru toate societăţile comerciale, iar cheltuielile de funcţionare fiind avansate de către stat. Reglementarea persoanei juridice sub acoperire prezintă o dificultate suplimentară prin aceea că în acest mod se naşte un subiect de drepturi şi

obligaţii, atât de natură patrimonială cât şi nepatrimonială. Pe parcursul existenţei, persoana juridică poate avea angajaţi, poate încheia contracte cu executare succesivă în timp sau poate acumula obligaţii fiscale, iar legea trebuie să prevadă soarta acestor raporturi juridice în momentul în care societatea şi-a îndeplinit scopul în vederea căreia a fost creată şi îşi încetează existenţa. Colaboratorul este persoana care nu face parte din autorităţile judiciare şi care, în baza şi limitele autorizării date de organul competent, efectuează anumite acte şi activităţi, în scopul stabilirii existenţei infracţiunii şi identificării membrilor unui grup de crimă organizată sau a unor persoane care au legături 428 infracţionale cu un astfel de grup. Legislaţia britanică425, spre exemplu, prevede posibilitatea de a autoriza în cadrul unei investigaţii „surse umane acoperite de informaţii", criteriul esenţial pentru stabilirea acestei calităţi fiind relaţia existentă între sursă şi persoana investigată, şi nu apartenenţa sursei la organul judiciar. Potrivit acestei norme, pot fi autorizaţi pentru obţinerea de informaţii şi mijloace de probă în procesul penal atât investigatori sub acoperire, cât şi colaboratori ai poliţiei fără calitate specială. De asemenea, legislaţia olandeză426 prevede că atunci când folosirea unui investigator sub acoperire este imposibilă, poate fi folosit un civil pentru realizarea unei operaţiuni acoperite. Pentru a garanta protejarea drepturilor fundamentale ale persoanelor vizate de aceste procedee probatorii, condiţiile şi procedura de autorizare a persoanei juridice sub acoperire şi a colaboratorilor trebuie să fie similare celor de autorizare a investigatorilor sub acoperire, atât sub aspectul testului de proporţionalitate, cât şi din perspectiva organului competent să autorizeze activitatea. Practica organelor judiciare a demonstrat, totodată, că reglementarea actuală a instituţiei investigatorilor sub acoperire nu acoperă toate ipotezele în care activităţile desfăşurate de investigator implică o atingere adusă dreptului persoanei la respectarea vieţii private şi a domiciliului. Astfel, nu există dispoziţii exprese referitoare la situaţia în care investigatorul pătrunde în locuinţa unei persoane în vederea obţinerii de informaţii sau de mijloace de probă. Potrivit art. 27 din Constituţie, nimeni nu poate pătrunde în domiciliul sau reşedinţa unei persoane fără învoirea acesteia, iar excepţiile trebuie să fie prevăzute de lege. Dispoziţii similare se regăsesc în Articolul 8

al Convenţiei Europene a Drepturilor Omului, care prevede 12

în plus condiţia proporţionalităţii ingerinţei cu importanţa interesului legitim protejat. În ipoteza unui investigator sub acoperire care pătrunde în locuinţa unei persoane pentru a cumpăra droguri, spre exemplu, se poate argumenta că acordul persoanei care foloseşte locuinţa este suficient pentru a conferi legalitate 425 Regulation of Investigatory Powers Act 2000 426 Special Power of Investigation Act (Wet Bijzondere opsporingsbevoegdheden) din 2000 429 activităţii sale. Pe de altă parte, se poate susţine şi că în această situaţie acordul nu este valabil exprimat, având în vedere că persoana care 1-a exprimat nu cunoştea adevărata calitate a investigatorului, şi că viaţa privată a persoanei cercetate a suferit o atingere care nu este prevăzută de lege. Astfel, există posibilitatea de a contesta legalitatea mijloacelor de probă administrate în această modalitate. Specificul activităţii desfăşurate de un investigator sub acoperire presupune ca acestea să aibă un comportament normal în mediul în care încearcă să se integreze, ceea ce poate presupune accesul în locuinţele membrilor unui grup infracţional. În asemenea situaţii este imposibilă determinarea în prealabil a tuturor locuinţelor în care investigatorul va fi nevoit să pătrundă, astfel încât nu se poate obţine o autorizaţie individuală pentru accesul în fiecare imobil. Totodată, într-o asemenea situaţie intensitatea ingerinţei este în mod vădit mai mică decât în cazul unei percheziţii

domiciliare, astfel încât nu se justifică o procedură de autorizare similare percheziţiei. Pentru a evita riscul unor interpretări neunitare în practică şi jurisprudenţă, soluţia pe care o propun este ca reglementarea instituţiei investigatorului sub acoperire să cuprindă referiri exprese la posibilitatea ca acesta sa pătrundă în locuinţe pentru a obţine informaţii în baza autorizaţiei emise de către organul judiciar competent. O asemenea dispoziţie se regăseşte în legislaţia landului german Baden Wurtemberg427, care prevede în mod expres ca acordul persoanei care foloseşte o locuinţă este suficient pentru accesul în imobil al investigatorului. Reglementările actuale în materia investigatorului sub acoperire nu cuprind dispoziţii referitoare la situaţia în care activităţile de integrare în mediul infracţional presupun

săvârşirea unei fapte prevăzute de legea penală pentru 19

427

Joubert, C., Bevers, H., Schengen investigated. A Comparative Interpretation of the Schengen Provisions on mInternational **Police Cooperation in the light of the European Convention on Human Rights,** Ed. **Kluwer Law International,** 24

1996, p. 222 430 care nu există o autorizare expresă prealabilă din partea organului judiciar competent. Infiltrarea unui agent sub acoperire într-o grupare de criminalitate organizată poate presupune ca acesta să adopte comportamentul celorlalţi membri ai grupării, inclusiv săvârşirea unor fapte prevăzute de legea penală. Pentru aceste situaţii, regula ar fi ca procurorul care autorizează folosirea investigatorului sub acoperire să poată autoriza si comiterea acestor fapte după realizarea unui test de proporţionalitate. Această ipoteză este reglementată în legislaţia română cu privire la cumpărarea de droguri în articolul 22 din Legea nr. 143/2000, iar de noul Cod de procedură penală în articolul 150, care acoperă şi alte fapte prevăzute de legea penală ce pot fi autorizate. Prevederi similare se regăsesc în legislaţiile din majoritatea statelor europene. În practică au apărut situaţii în care activitatea grupării de crimă organizată s-a desfăşurat într-o modalitate diferită de cea prefigurată la momentul autorizării, astfel încât investigatorul a fost pus în situaţia de a săvârşi o fapta pentru care nu fusese autorizat, riscând ca astfel să fie deconspirat. Având în vedere că prevederile referitoare la stare de necesitate nu sunt întotdeauna deplin aplicabile în aceste situaţii, în legislaţia altor state s-a simţit nevoia unei reglementări exprese a acestor situaţii. Astfel, legislaţia olandeză prevede că în situaţii urgente investigatorul poate fi autorizat verbal

să săvârşească o faptă prevăzută de legea penală, 42

urmând ca procurorul să emită ulterior o autorizaţie scrisă în termen de 3 zile. Consider că se impune adoptarea unei reglementări similare şi în legislaţia română pentru a răspunde problemelor care apar în practica organelor judiciare.

Practica organelor judiciare a demonstrat că o altă lipsă a legislaţiei actuale în materia tehnicilor de supraveghere, care este reluată în noul Cod de procedură penală, este omisiunea unei reglementări legale a supravegherii operative. Acest procedeu probatoriu constă în monitorizarea activităţilor unei persoane de către un lucrător de poliţie, în scopul obţinerii de informaţii. În situaţiile în care supravegherea nu este însoţită de realizarea de înregistrări de imagini şi sunete, lucrătorul de poliţie consemnează constatările personale într- un proces verbal, care constituie mijloc de probă428, iar în aceste situaţii reglementarea în vigoare nu prevede necesitatea obţinerii unei autorizaţii. Având în vedere că supravegherea sistematică a unei persoane reprezintă o ingerinţă în viaţa privată a acesteia429, exigenţele

articolului 8 din Convenţia Europeană a Drepturilor Omului 11

presupun ca aceasta să fie prevăzută într-o lege care să definească atât infracţiunile pentru care poate fi dispusă măsura, cât si procedura de autorizare. Totodată, decizia de a folosi un asemenea procedeu trebuie luată numai în urma efectuării unui test de proporţionalitate. Din acest motiv, propun ca reglementările referitoare la tehnicile de supraveghere să fie modificate, astfel să fie reglementată o procedură legală de autorizare şi condiţii de administrare pentru orice activitate a organelor judiciare care presupune o ingerinţă în viaţa privată. În viziunea noastră, criteriul după care o activitate trebuie sau nu să fie autorizată trebuie să fie existenţa unei ingerinţe, şi nu modalitatea practică în care se realizează activitatea sau modul în care se consemnează rezultatele. Considerăm că nu se justifică situaţia actuală, în care realizarea unei supravegheri, ale cărei constatări se regăsesc într- o înregistrare de imagini, presupune o autorizaţie emisă de un judecător, pe când o supraveghere ale cărei rezultate sunt consemnate în scris de lucrătorul de poliţie nu are o reglementare legală care să cuprindă suficiente garanţii. Un exemplu poate fi legislaţia adoptată în Marea Britanie în cursul anului 2000430, care reglementează detaliat procedura de autorizare a supravegherii operative, distingând, totodată, între metodele de supraveghere obişnuite şi cele intruzive, care vizează activităţi efectuate în interiorul unei locuinţe sau presupun prezenţa unei persoane sau a unui dispozitiv în interiorul unei locuinţe 428

Udroiu, M., Predescu, O., Proiecţia **europeană a drepturilor omului şi procesul penal român, Editura C.H. Beck,** 12

2008, p.858 429 A se vedea CEDO, hotărârea din 26 martie 1987 în cauza Leander contra Suediei 430 Articolul 26 din Regulation of Investigatory Powers Act 432 şi care implică exigenţe sporite şi un grad mai înalt de autorizare. Totodată, în Olanda431, supravegherea sistematică a unei persoane, care permite obţinerea unei imagini de ansamblu asupra vieţii private a unei persoane, poate fi realizată numai cu autorizarea procurorului, pe când supravegherea obişnuită, a unei activităţi individuale sau întâmplătoare, se poate realiza fără o autorizare specială. O altă propunere, vizează reglementarea în legislaţia procesual penală a unor instituţii care să permită organelor judiciare accesul într-un loc,

ridicarea şi repunerea la loc a unui obiect sau 15

instalarea de obiecte. Aceste tehnici de investigare sunt reglementate în prezent în

Legea nr. 535/2004 privind prevenirea și combaterea terorismului 1

şi pot fi folosite doar de

către organele de stat cu atribuţii în domeniul securităţii naţionale. 15

Astfel, pe parcursul unei investigaţii poate fi necesar ca organele de urmărire penală să pătrundă în locuinţa unei persoane pentru a instala un dispozitiv de înregistrare cu ajutorul căruia să se realizeze o înregistrare de convorbiri autorizată de judecător, în condiţiile în care nu există o autorizare expresă a acestui tip de ingerinţă în viaţa privată a persoanei şi nicio o prevedere legală expresă din care să rezulte că autorizaţia de interceptare presupune şi dreptul de acces în locuinţa persoanei vizate, reglementarea actuală nu permite folosirea acestei tehnici de investigare. De asemenea, pentru a asigura conspirativitatea unei investigaţii, poate fi necesar ca un obiect să poată fi studiat fără cunoştinţa celui care îl deţine, activitate care nu poate fi efectuată în baza dispoziţiilor în vigoare referitoare la condiţiile de efectuare a percheziţiilor domiciliare. Prin reglementarea unei proceduri de autorizare pentru aceste tehnici de investigare similare procedurii aplicabile pentru interceptarea şi înregistrarea 431 Special Power of Investigalion Act (Wet Bijzondere opsporingsbevoegdhcdun) din 2000 433 convorbirilor, soluţia pe care o propun asigură suficiente garanţii pentru a respecta exigenţele Convenţiei Europene a Drepturilor Omului şi asigură un instrument eficient în combaterea criminalităţii organizate. În ciuda dificultăţii de a identifica un echilibru între interesul statului de a combate criminalitatea organizată şi drepturile fundamentale ale persoanelor vizate de tehnicile speciale de investigare, importanţa acestor instituţii determină necesitatea reglementării lor. Totodată, trebuie avută

în vedere necesitatea **ca** în **statele membre ale Uniunii Europene** 15

să existe principii standard ale procedurilor de executare a acţiunilor sub acoperire, iar legislaţia să fie adaptată la aceste principii. În acest sens, trebuie avută în vedere propunerea de Directivă a Uniunii Europene privind Ordinul European de Investigaţie432, aflată în curs de adoptare care reglementează punerea în executarea a procedeelor probatorii dispuse de un organ judiciar dintr-un alt stat membru, inclusiv a tehnicilor de investigare sub acoperire, astfel încât este esenţial ca legislaţia română sa prevadă instrumente similare celor din statele europene. Preocuparea de standardizare a

instrumentelor de combatere a crimei organizate se manifestă la un nivel mai larg decât cel al Uniunii Europene, reprezentând o prioritate a tuturor agenţiilor de aplicare a legii.

Summit-ul Mondial al Procurorilor Generali şi Procurorilor Şefi desfăşurat în 2009 **la** 36

Bucureşti a remarcat că răspândirea tehnologiilor moderne de informare şi comunicare, precum şi crescânda trans-naţionalitate a activităţilor infracţionale aferente creează o vastă gamă de noi oportunităţi pentru comiterea de infracţiuni, iar evoluţia constantă a mediului social, cultural şi economic ridică noi şi schimbă dramatic modul de abordare a şi impactul infracţionalităţii tradiţionale şi convenţionale. Din acest motiv, summit-ul a recomandat ca, pentru combaterea noilor şi sofisticatelor forme de infracţionalitate, să se dezvolte o reacţie mai eficientă din partea justiţiei penale, inclusiv o 432 http://register.consilium.europe.eu/pdf/en/10/st09/st09288-ad0l.en10.pdf 434 reconsiderare şi actualizare a standardelor şi normelor, în mod corespunzător şi conform necesităţilor, pentru a se asigura un răspuns adecvat nevoilor actuale ale tuturor statelor.433 O altă modificare legislativă pe care noi o considerăm necesară este preluarea poliţiei judiciare de către Ministerul Public şi înfiinţarea poliţiei judiciare a DIICOT. În concordanţă cu dispoziţiile constituţionale, care situează Ministerul Public în rândul Autorităţii Judecătoreşti, o eventuală organizare a poliţiei judiciare în cadrul Ministerului Public ar putea reprezenta una dintre soluţiile de eficientizare a combaterii fenomenului infracţional în general şi al crimei organizate în special. Constituţia României, republicată, menţionează în Titlul 111, la cap.6, secţiunea a 2-a (Autoritatea judecătorească) faptul că în

activitatea judiciară, Ministerul Public reprezintă interesele generale ale societăţii şi apără ordinea de drept, precum şi drepturile şi libertăţile cetăţenilor. Ministerul Public îşi exercită atribuţiile prin procurori constituiţi în parchete, în condiţiile legii. Parchetele funcţionează pe lângă instanţele de judecată, conduc şi supraveghează activitatea de cercetare penală a poliţiei judiciare, în condiţiile legii (art.131). 21

În prezent, dubla subordonare a lucrătorilor de poliţie judiciară, funcţional faţă de parchete, iar administrativ faţă de Ministerul Administraţiei şi Internelor duce în unele situaţii la o scădere a eficienţei. Cele două instituţii pot avea la un moment dat priorităţi diferite, astfel încât aceiaşi lucrători pot fi implicaţi administrativ într-un anumit tip de activităţi, urmărind combaterea unui anumit fenomen, iar din punct de vedere al cercetării penale priorităţile parchetului pot viza combaterea unui alt fenomen. Această abordare implică irosirea resurselor investigative, iar preluarea poliţiei judiciare de către Ministerul Public ar înlătura acest impediment. Este esenţială, din această perspectivă, diferenţierea între poliţia administrativă şi poliţia judiciară, cea din urmă structură având sarcina de a 433 www.http://www.summitgp2009.ro/upload/Raport_final_Summit_PG_2009.doc 435 constata şi urmări orice infracţiune, conformându-se regulilor de procedură penală şi de a executa măsurile dispuse de către procurori. Totodată, apreciem că este absolut necesar

ca structura specializată în combaterea crimei **organizate şi terorismului** 43

să aibă propria poliţie judiciară, formată din ofiţeri de poliţie specializaţi, care să acţioneze sub autoritatea exclusivă a procurorilor DIICOT. Evident, opţiunea către un asemenea mod de organizare ar presupune detaşarea unui număr de ofiţeri şi agenţi de poliţie judiciară, stabilit în funcţie de evoluţia anumitor indicatori ai criminalităţii iar evaluarea profesională a lucrătorilor de poliţie judiciară ar urma să fie în competenta procurorilor, care de altfel exercită atât coordonarea, controlul, cât si conducerea activităţilor de cercetare penală. De aceea, structura de poliţie judiciară trebuie să fie complet şi clar diferenţiată de structura de poliţie administrativă, cea de menţinere a ordinii publice. O altă măsură legislativă care apreciem că ar trebui introdusă este cea privind confiscarea extinsă şi modificarea reglementărilor referitoare la prezumţia dobândirii licite a averii. Dispoziţiile din Legea nr.39/2003 au adus o modificare esenţială în activitatea organelor judiciare în ceea ce priveşte instituirea măsurilor asigurătorii şi confiscarea specială întrucât se poate confisca şi echivalentul bunurilor supuse confiscării. Cu toate acestea, în activitatea practică s-au ridicat numeroase probleme privind instituirea măsurilor asigurătorii în cazurile de criminalitate organizată, fiind numeroase situaţiile în care membrii grupurilor infracţionale, deşi realizau beneficii materiale serioase din activitatea ilicită, nu deţineau bunuri în proprietate sau venituri care să poată fi indisponibilizate. De multe ori, imobilele ori terenurile dobândite cu venituri din activitatea ilicită au fost transferate pe numele unor membrii ai familiei sau prieteni, astfel că indisponibilizarea acestora a fost de multe ori dificilă. Principalele impedimente practice sunt generate de modul în care este reglementată instituirea măsurii asigurătorii în art.163 alin.2 („măsurile asigurătorii în vederea reparării pagubei se pot lua asupra bunurilor învinuitului sau inculpatului”), dar mai ales datorită modului în care sunt interpretate normele Constituţiei României, care în art.44 alineatul 8 prevede prezumţia dobândirii licite a averii. În practica organelor judiciare, acest text este interpretat, pornind şi de la deciziile Curţii Constituţionale, ca instituind o obligaţie pentru autorităţi de a stabili cu exactitate infracţiunea din care provine un bun supus confiscării. De aceea, apreciem că introducerea confiscării extinse este necesară în legislaţia noastră şi se impune chiar şi o modificare a Constituţiei cu privire la această prezumţie, astfel încât, în situaţia în care organele judiciare dovedesc că veniturile unei persoane condamnate nu justifică bunurile pe care le deţine, acea persoană să aibă obligaţia de a le dovedi provenienţa licită, iar în caz contrar bunurile să fie confiscate. Un sistem eficient de recuperare a sumelor obţinute prin infracţiuni presupune ca, în anumite situaţii, legislaţia naţională să permită răsturnarea sarcinii probei cu privire la provenienţa bunurilor. Această afirmaţie porneşte de la premisa că în orice sistem juridic este imposibil ca statul să stabilească cu precizie provenienţa infracţională a tuturor bunurilor dobândite de un inculpat, la acelaşi standard de probă necesar pentru condamnarea unei persoane.

Se întâmplă de multe ori, ca unui traficant de droguri să i se poată confisca doar sumele obţinute la ultima tranzacţie sau unui funcţionar corupt să i se confişte doar ultima mită şi să nu fie posibilă confiscarea averii pe care, în mod vădit nu o putea obţine din venituri 18

legale434. În aceste situaţii, statul nu îşi poate permite ca persoanele condamnate să păstreze bunurile dobândite de persoanele condamnate şi care nu pot fi justificate. La această concluzie au ajuns majoritatea statelor europene, iar răspunsul 434 http://www.mpublic.ro/presa/2011/discurs_bilant_2010.pdf 437 pe care l-au oferit a fost reglementarea unor instituţii în baza cărora în cazuri limitativ prevăzute de lege o persoană trebuie să dovedească originea bunurilor pe care le-a dobândit, în caz contrar acestea fiind confiscate. Soluţiile sunt diverse. Spre exemplu, în Anglia435, prezumţia este răsturnată pentru persoanele condamnate pentru infracţiuni grave sau condamnate de mai multe ori într-un anumit interval. După dispunerea unei asemenea condamnări, aceste persoane trebuie să facă dovada faptului că toate bunurile pe care le-au dobândit în ultimii 6 ani şi toate cheltuielile pe care le-au efectuat în această perioadă provin din surse licite, în caz contrar dispunându-se confiscarea. Mai mult, dacă persoana condamnată nu achită suma la care este obligat, pedeapsa îi poate fi majorată. Tot în Anglia, este reglementată aşa numita confiscare civilă436, în baza căreia se poate dispune confiscarea bunurilor provenite din infracţiuni chiar în lipsa unei condamnări. În această situaţie, statul poate demara o procedură civilă îndreptată împotriva bunurilor, în care trebuie să dovedească doar că este probabil că bunurile provin dintr-o infracţiune, invocând, spre exemplu, prezenţa unor urme de droguri pe bancnote, un standard sensibil mai scăzut decât pentru a obţine o condamnare. O altă reglementare437 din acelaşi sistem de drept permite confiscarea sumelor în numerar mai mari de 10.000 de lire sterline identificate asupra persoanelor şi care nu pot fi justificate. Poliţia este îndreptăţită să reţină aceste sume, urmând ca proprietarul să conteste măsura într-un termen determinat şi să facă dovada provenienţei licite a banilor, iar dacă acest lucru nu se întâmplă, sumele sunt confiscate. În Spania, a fost adoptată o altă metodă, care duce în final la acelaşi rezultat. În practica organelor judiciare infracţiunea de spălare de bani este interpretată în sens extensiv, astfel încât acoperă orice tranzacţie cu bunuri a căror provenienţă nu poate fi justificată şi cu privire la care există suspiciunea că provin din 435 Art.6 din Proceeds of Crime Act, adoplat în 2002. 436 Art.240 din Proceeds of Crime Act, adoptat în 2002. 437 Art.249 din Proceeds of Crime Act, adoptat în 2002. 438 infracţiuni. Astfel, orice bun a cărui provenienţă licită nu poate fi stabilită este prezumat ca provenind dintr-o infracţiune, astfel încât devine obiect material al infracţiunii de spălare de bani şi implicit supus confiscării. Din momentul în care autorităţile demonstrează că veniturile legale ale unei persoane nu justifică bunurile pe care le deţine şi că există o legătură de orice natură cu o activitate infracţională, devine obligaţia deţinătorului de a indica provenienţa exactă a acestor bunuri pentru a evita confiscarea lor. În Franţa, s-a ales soluţia adoptări unei incriminări speciale. Astfel, fapta de a justifica originea bunurilor deţinute sau a cheltuielilor efectuate constituie o infracţiune autonomă, care atrage atât condamnarea autorului cu

o pedeapsă de până la 3 **ani de închisoare,**	1

cât şi confiscarea bunurilor. Asemenea instituţii au fost adoptate în ultimii ani în majoritatea statelor europene - Anglia, Franţa, Olanda, Belgia, Spania şi, de curând, Bulgaria. Unele dintre aceste prevederi au fost examinate de Curtea Europeana a Drepturilor Omului438, care a concluzionat că o asemenea procedură conţine suficiente garanţii şi nu încalcă drepturile fundamentale la un proces echitabil sau la garantarea proprietăţii. Mai mult, Consiliul European a impus tuturor statelor membre ale Uniunii, prin Decizia Cadru 212, din 2005, să prevadă în legislaţia lor confiscarea extinsă, care să permită răsturnarea sarcinii probei în legătură cu provenienţa bunurilor persoanelor condamnate pentru infracţiuni. România

are nevoie, la rândul său, de asemenea instituţii şi trebuie să îşi îndeplinească şi obligaţiile care îi revin ca stat membru. În ultima perioadă au existat numeroase cazuri puternic mediatizate de persoane implicate în activităţi de crimă organizată sau de corupţie, care, deşi au fost condamnate, şi-au păstrat averea care nu ar fi putut fi justificată prin surse legale de venit. Este nevoie de instrumente care să permită ca aceste persoane să răspundă integral pentru 438 Philips contra Regatului Unit, 2001; Grayson şi Barnham contra Regatului Unit, 2008. 439 activităţile ilicite, însă, în prezent, adoptarea unor asemenea instrumente este împiedicată de prevederile Constituţiei referitoare la prezumţia caracterului licit al averii. Aceste prevederi nu permit răsturnarea sarcinii probei şi, implicit, nu permit ca România să adopte una sau mai multe dintre soluţiile identificate deja de celelalte state membre. Modificarea Constituţiei ar crea astfel o oportunitate pentru a elimina o situaţie de inechitate socială şi ar aduce, în acelaşi timp, sume semnificative la buget.

România trebuie să implementeze decizia cadru nr.212 a Consiliului Uniunii Europene referitoare la confiscarea extinsă nu doar pentru a ne îndeplini obligaţiile asumate ca stat comunitar, ci în primul rând, pentru a răspunde unei nevoi sociale presante. 18

Credem că ar fi necesară adoptarea unei legislaţii privind confiscarea extinsă. Prevederile constituţionale se referă la averea tuturor cetăţenilor, însă confiscarea extinsă priveşte doar persoanele care sunt condamnate pentru fapte penale şi nu îşi pot justifica averea. O măsură la nivel instituţional, care apreciem noi că ar trebui implementată, este organizarea completelor specializate la instanţele care judecă cauzele de criminalitate organizată. Apreciem că judecarea acestor cauze de către judecători specializaţi în domeniul crimei organizate ar duce la creşterea gradului de combatere al acestui flagel, dar şi la prevenirea lui. Completele specializate ar putea contribui la aplicarea unitară şi uniformă a dispoziţiilor din legile speciale şi mai ales a dispoziţiilor privind tehnicile speciale de investigaţie, precum şi la aplicarea unor pedepse cu grad ridicat disuasiv. Mai mult, crearea acestor complete ar permite magistraţilor o specializare pe diverse domenii - criminalitatea informatică, trafic de droguri, trafic de persoane, etc. — elaborarea unor ghiduri de bune practici în judecarea acestui gen de cauze, precum şi o creştere a celerităţii în judecarea cauzelor. Adoptarea propunerilor prezentate mai sus s-ar înscrie în principiile şi orientările strategice ale UE, definite în

„Strategia de securitate internă a Uniunii Europene: Către un model european de securitate”. 8

Strategia consideră că

„principalele riscuri şi ameninţări infracţionale cu care se confruntă în prezent Europa, şi anume terorismul, formele grave de criminalitate, criminalitatea organizată, traficul de droguri, criminalitatea informatică, traficul de fiinţe umane, exploatarea sexuală a minorilor şi pornografia infantilă, infracţionalitatea economică şi corupţia, traficul de armament şi criminalitatea transfrontalieră, 16

se adaptează extrem de rapid la schimbările ştiinţifice şi tehnologice, în încercarea lor de a exploata în mod ilegal şi de a submina valorile şi prosperitatea societăţilor noastre deschise.” 439 Astfel, Uniunea Europeană stabileşte ca

principiu faptul că

„cetăţenii europeni vor să trăiască în condiţii de securitate şi să se bucure de libertăţile lor: securitatea constituie, în sine, un drept fundamental. Valorile şi principiile stabilite în tratatele Uniunii şi enunţate în Carta drepturilor fundamentale au inspirat Strategia de securitate internă a UE.” 440 În 8

ceea ce priveşte prezentul demers ştiinţific, de o deosebită importanţă este principiul politicilor în

materie de justiţie, libertate şi securitate care se consolidează reciproc, respectând totodată drepturile fundamentale, protecţia internaţională, statul de drept şi viaţa privată. 8

Pe baza principiilor sunt stabilite zece

orientări pentru acţiune în vederea garantării securităţii interne a UE în următorii ani: ‣ abordarea vastă şi globală a securităţii interne; ‣ asigurarea supravegherii democratice şi judiciare efective a activităţilor de securitate; ‣ prevenirea şi anticiparea: o abordare pro-activă şi fondată pe informaţii; 16

‣

elaborarea unui model global pentru schimbul de informaţii; 8

439

Secretariatul General al Consiliului European, Strategia de securitate internă a Uniunii Europene: Către un model european de securitate. Luxemburg: Oficiul pentru Publicaţii al Uniunii Europene. 8

ISBN 978-92-824-2690-6, p.7. 440

Strategia de securitate internă a Uniunii Europene: Către un model european de securitate, 8

op. cit., p. 19. 441 ‣ cooperarea operaţională; ‣

cooperarea judiciară în materie penală, care stabileşte pentru **„autorităţile judiciare ale statelor** 8 **membre să coopereze mai îndeaproape, după cum este necesar ca Eurojust să îşi pună în valoare** întregul potenţial **în cadrul legislaţiei aplicabile. La nivelul UE, operaţiunile şi anchetele în materie penală care s-au desfăşurat cu succes trebuie să ne permită să conştientizăm sinergiile potenţiale dintre serviciile de aplicare a legii şi cele de gestionare a frontierelor şi autorităţile judiciare, în scopul prevenirii criminalităţii transfrontaliere”** 441; ‣ **gestionarea integrată a frontierelor;**

‣ angajamentul

în favoarea inovării şi a formării; ‣ dimensiunea externă a securităţii interne/cooperarea cu ţările 28 **terţe; ‣ flexibilitatea în vederea adaptării la dificultăţile viitoare.**

„Riscul zero nu există, dar în ciuda acestui fapt, Uniunea trebuie să creeze un mediu sigur în care 8 **oamenii să se simtă protejaţi.** În acest sens, **trebuie instituite mecanismele necesare pentru menţinerea unui nivel ridicat de securitate, nu numai pe teritoriul UE, ci şi, într-o măsură cât mai mare, atunci când cetăţenii călătoresc în ţări terţe sau se află în medii virtuale, precum Internetul”**

442. 441

Strategia de securitale **internă a Uniunii Europene: Către un model european de securitate,** 8

op. cit., p. 26. 442

Strategia de securitale internă a Uniunii Europene: Către un model european de securitate, 8

op. cit., pp. 11. 442 357 360 362 363 364 367 369 370 371 372 380 381 383 389 393 394 398 399 400 401 407 disponibilă pe site-ul www.scj.ro 403 404 405 406 408 409 413 414 418 421 422 424 425 431 436 440

sources:

1 7,311 words / 31% - Internet from 03-Mar-2016 12:00AM
e-crime.ro

2 1,399 words / 6% - Internet from 06-Sep-2016 12:00AM
documents.tips

3 1,262 words / 5% - Internet from 21-Jun-2016 12:00AM
www.rasfoiesc.com

4 467 words / 2% - Internet from 19-Apr-2016 12:00AM
www.rasfoiesc.com

5 419 words / 2% - Internet from 04-Jun-2016 12:00AM
revistablogurilor.ro

6 340 words / 1% - Internet from 26-Aug-2015 12:00AM
ijc.rau.ro

7 307 words / 1% - Internet from 21-Sep-2016 12:00AM
www.avocatmarta.ro

8 285 words / 1% - Internet from 30-Jun-2015 12:00AM
www.consilium.europa.eu

9 250 words / 1% - Internet from 19-Mar-2014 12:00AM
www.slideshare.net

10 220 words / 1% - Internet from 02-Jul-2016 12:00AM
www.legi-internet.ro

11 170 words / 1% - Internet from 23-Jun-2011 12:00AM
www.euroavocatura.ro

12 166 words / 1% - Internet from 12-Jun-2014 12:00AM
www.propatrialex.ro

13 155 words / 1% - Internet from 21-Jul-2016 12:00AM
documents.tips

14 135 words / 1% - Internet from 06-Oct-2011 12:00AM
bistritaexpress.ro

15 122 words / 1% - Internet from 26-Aug-2015 12:00AM
ijc.rau.ro

16 114 words / < 1% match - Internet from 22-May-2014 12:00AM
m-securitynews.ro

17 103 words / < 1% match - Internet from 14-May-2016 12:00AM
rria.ici.ro

18 88 words / < 1% match - Internet from 26-Sep-2011 12:00AM
www.legalis.ro

19 72 words / < 1% match - Internet from 20-Mar-2014 12:00AM
www.avocat-bucuresti.info

20 63 words / < 1% match - Internet from 14-Jan-2013 12:00AM
www.itmsuceava.ro

21 55 words / < 1% match - Internet from 16-Feb-2012 12:00AM
www.justitia-romana.org

22 54 words / < 1% match - Internet from 27-Jan-2004 12:00AM
www.internet-magazin.ro

23 36 words / < 1% match - Internet from 18-Jan-2013 12:00AM
ccihr.ro

24 29 words / < 1% match - Crossref
Minas Samatas. "Greece in 'Schengenland': blessing or anathema for citizens' and foreigners' rights?", Journal of Ethnic and Migration Studies, 1/1/2003

25 27 words / < 1% match - Internet from 16-Feb-2012 12:00AM
procuratura.md

26 27 words / < 1% match - Internet from 04-Nov-2011 12:00AM
www.univath.ro

27 27 words / < 1% match - Publications
Roxana, Popoviciu Laura. "SIMILAR ASPECTS REGARDING THE INFRACTIONS WITHIN THE REGIME THAT IS ESTABLISHED FOR CERTAIN ECONOMIC ACTIVITIES", Annals of the University of Oradea, Economic Science Series/15825450, 20080601

28 22 words / < 1% match - Internet from 22-Jun-2013 12:00AM
detectiviparticulari.com.ro

29 21 words / < 1% match - Internet from 12-Nov-2011 12:00AM
legi-internet.ro

30 16 words / < 1% match - Internet from 27-Jan-2014 12:00AM
andrei.clubcisco.ro

31 16 words / < 1% match - Internet from 03-Jul-2015 12:00AM
www.uab.ro

32 14 words / < 1% match - Internet from 24-Jun-2013 12:00AM
www.avocatulroman.ro

33 14 words / < 1% match - Internet from 18-Apr-2013 12:00AM
www.scritube.com

34 14 words / < 1% match - Publications
Gheorghe, Carmen. "Egalitatea de gen în politicile publice pentru romi", Social Work Review / Revista de Asistenta Sociala/15830608, 20110601

35 13 words / < 1% match - Internet from 11-Feb-2008 12:00AM
www.dreptonline.ro

36 11 words / < 1% match - Internet from 17-Sep-2011 12:00AM
www.stiricentrale.ro

37 10 words / < 1% match - Internet from 02-May-2008 12:00AM
www.infarom.ro

38 10 words / < 1% match - Internet from 31-May-2013 12:00AM
www.carti-juridice.ro

39 9 words / < 1% match - Internet from 09-Jan-2016 12:00AM
www.hsph.harvard.edu

40 9 words / < 1% match - Internet from 10-Aug-2013 12:00AM
ro.wikipedia.org

41 8 words / < 1% match - Internet from 01-Jul-2016 12:00AM
lege5.ro

42 8 words / < 1% match - Internet from 07-Nov-2008 12:00AM
www.raa.ro

43 8 words / < 1% match - Internet from 23-Oct-2011 12:00AM
www.costelgilca.ro

44 8 words / < 1% match - Crossref
Marins, Paulo CÃ©sar Garcez. "O Parque do Ibirapuera e a construÃ§Ã£o da identidade paulista", Anais do Museu Paulista HistÃ³ria e Cultura Material, 1999.

45 6 words / < 1% match - Publications
Medar, Sergiu. "The Security of the Dynamic Systems", Theoretical & Applied Economics/18418678, 20091201