UNIVERSITATEA NICOLAE TITULESCU BUCUREŞTI

TEZĂ
DE DOCTORAT

CRIMINALITATEA INFORMATICĂ

- REZUMAT -

CONDUCĂTOR ŞTIINŢIFIC
Prof.univ.dr. Vasile Dobrinoiu

DOCTORAND
Florin Encescu

2010

CUPRINS

CRIMINALITATEA INFORMATICĂ.
ASPECTE DE DREPT COMPARAT. EVOLUȚIA FENOMENULUI ȘI PROPUNERI DE REGLEMENTARE VIITOARE

CRIMINALITATEA INFORMATICĂ

- REZUMAT -

Infracţionalitatea informatică, generic, este nu numai un domeniu de maximă actualitate în materie penală, dar mai ales un domeniu ce oferă largi şi numeroase perspective cercetării viitoare, datorită fenomenalei dinamici tehnologice şi diversificării, dar şi sporirii gradului de rafinament al activităţilor antisociale, într-o lume electronică în care existenţa virtuală devine tot mai mult o a doua natură umană.

Complexitatea şi tehnicitatea domeniului, dar şi problemele tactice-criminalistice specifice au făcut ca evoluţia fenomenului infracţional să nu aibă un corespondent proporţional în activitatea de prevenire, descoperire şi tragere la răspundere a infractorilor, aceasta din urmă fiind de multe ori devansată de perspicacitatea autorilor şi tehnologiile din ce în ce mai avansate, de care aceştia dispun.

Locul infracţiunilor informatice în peisajul juridic penal a devenit în scurt timp la fel de important ca acela al infracţiunilor clasice deosebit de grave, gravitatea acestora fiind accentuată de uşurinţa comiterii şi camuflării lor, de caracterul preponderent transfrontalier datorat mediului Internet şi potenţialul devastator al efectelor acestor acţiuni.

Lucrarea își propune astfel, să semnaleze din perspectiva unui inventar de probleme, tehnici și tendințe, nevoia stringentă a reglementării globale și dezvoltării ramurii dreptului spațiului virtual, implicit să abordeze noi direcții în cercetarea fenomenului infracțional din acest mediu.

În acest context, criminalitatea specifică lumilor virtuale se înscrie ca o direcție de mare actualitate, fiind o zonă greu de explorat, dar propice fenomenului infracțional grav, aflat la adăpost datorită nivelului înalt de criptare și protocoalelor restrictive de acces.

Este un nivel de limitare a accesului similar sau superior celui reprezentat în cercurile cunoscătorilor de sistemul de comunicații Skipe, considerat o umbrelă confortabilă pentru comunicațiile grupărilor criminale.

Nevoia unui mecanism de raportare internaţional pentru furnizori de servicii Internet (ISP - Internet Service Provider: furnizorul serviciului Internet) în privința materialelor ilegale distribuite prin intermediul internetului este semnalată de mai bine de 10 ani. Aceasta ar însemna că oricine descoperă sau este sfătuit prin materiale ilegale, ar trebui să raporteze acest lucru la ISP-ul prin care materialul este distribuit, chiar şi în cazul în care prestatorul este în altă ţară. Furnizorul poate furniza apoi informaţii autorităţilor competente de anchetă.

Există, de asemenea, nevoia unei clasificări internaţionale şi a unui sistem de filtrare pentru materialele din Internet dăunătoare pentru tineri, ca de altfel şi a dezvoltării unui cod internaţional de conduită pentru comerţul electronic.

Realitatea este că cele mai multe ţări nu iau o poziţie coerentă, unitară privind modul în care legea poate fi aplicată pe Internet. În acest sens, măsurile trebuie să fie luate pentru a promova abilitarea forţelor la nivel internaţional.

Este încă o mare nevoie de noi norme internaţionale pentru a face mai uşoară investigarea şi urmărirea în justiţie a autorilor infracţiunilor săvârşite pe Internet. Cercetarea infracţiunilor va continua să fie reglementată de jurisdicţia binaţională: principiul că un act trebuie să fie pedepsit în ambele ţări va continua să se aplice pentru investigaţii penale internaţionale, iar autorităţile de anchetă nu vor fi autorizate să efectueze investigaţii la reţele de calculatoare în afara jurisdicţiei naţionale lor proprii.

Pe de altă parte, regulile care ar face posibilă exercitarea unui control total asupra membrilor publicului, cum ar fi obligaţiile internaţionale de a face decodabile materialele criptate, sunt respinse de către majoritatea ţărilor.

Ţara ”de origine” ar trebui să fie principalul factor în a decide care sistem de drept privat se aplică informaţiilor pe Internet. Acorduri de acest gen au fost deja efectuate în Europa în directiva privind comerţul electronic.

Principiul că ceea ce se aplică off-line ar trebui să se aplice, de asemenea, on-line, susţinând că natura specifică a Internetului, de exemplu, înseamnă că legislaţia specială pentru astfel de lucruri ca executarea, nu ar trebui exclusă.

Cu toate acestea, membrii publicului au dreptul să se aştepte că nivelul de protecţie juridică furnizată pe Internet nu este diferit de cel din Lumea Reală.

Este importantă astfel pe lângă auto-reglementare şi co-reglementarea (în parteneriat cu comunitatea de afaceri), ca o soluţie pentru problemele de pe Internet. Problema este în strânsă legătură cu interesele democraţiei constituţionale şi ale consumatorilor.

Lucrarea este structurată în trei părți principale, potrivit clasificării propuse de autor încă din debutul acesteia, și anume: ”Criminalitatea informatică”, ”Criminalitatea comerțului electronic”, respectiv ”Criminalitatea informatică. Aspecte de drept comparat. Evoluția fenomenului și propuneri de reglementare viitoare.”

I. Prima parte, denumită, așa cum am arătat, ”Criminalitatea informatică”, abordează după o scurtă introducere în *Capitolul I. Aspecte generale. Secţiunea 1-a*, o prezentare a reglementărilor din domeniu aplicabile, fiind efectuată o retrospectivă a reglementării europene, urmată de prezentarea reglementării interne, aici elementul de noutate reprezentându-l abordarea domeniului prin dispozițiile Noului Cod penal, fiind enumerate și formulate unele considerații asupra noutăților legislative.

Din aceeași perspectivă de actualitate, în *Secţiunea a 2-a. Înţelesul unor termeni. Noţiuni*, sunt prezentate comparativ și cuprinzător noțiunile specifice

definite atât de Noul Cod penal[1] cât și de Legea nr. 161/2003[2], norma specială în vigoare.

În continuare, sunt prezentate edificator pentru înțelegerea modului de structurare a lucrării o serie de clasificări ale infracțiunilor specifice, începând cu aceea a reputatului expert I.Vasiu, continuând cu clasificarea propusă de autor și finalizând cu o clasificare de actualitate schițată de expertul german Marco Gercke, care anticipează subdomenii și concepte noi pentru peisajul juridic românesc și european, cum ar fi acela al spălării de bani în spațiul virtual, dezvoltat în partea a treia a lucrării.

În Capitolul II, denumit ”Analiza principalelor infracţiuni informatice”, pe structura: conţinut legal; condiţii preexistente (obiectul infracţiunii; subiecţii infracţiunii); conţinutul constitutiv (latura obiectivă; latura subiectivă); forme, modalităţi, sancţiuni şi aspecte procesuale, din perspectiva noutăților teoretice și practice ale domeniului, sunt prezentate:

- ”Accesul ilegal la un sistem informatic” (Secţiunea 1-a);
- ”Interceptarea ilegală a unei transmisii de date informatice”, cu o subsecţiune denumită ”Consideraţii asupra disputei dintre teoreticienii şi

[1] Adoptat prin Legea nr. 286/2009 privind Codul penal publicată în Monitorul Oficial al Romaniei, Partea 1, Nr. 510 din 24 iulie 2009. Sub aspectul intrării în vigoare, TITLUL XIII, „Dispoziţii finale” prevede: Art. 446. - (1) Prezentul cod intră în vigoare la data care va fi stabilită în legea pentru punerea în aplicare a acestuia, cu excepţia dispoziţiilor alin. (2) si alin. (3), care intră în vigoare la 4 zile de la data publicării în Monitorul Oficial al României, Partea I, a prezentului cod. (2) Legea nr. 301/2004 - Codul penal, publicată în Monitorul Oficial al României, Partea I, nr. 575 din 29 iunie 2004, cu modificările ulterioare, și Legea nr. 294/2004 privind executarea pedepselor și a măsurilor dispuse de organele judiciare în cursul procesului penal, publicată în Monitorul Oficial al României, Partea I, nr. 591 din 1 iulie 2004, cu modificările ulterioare, se abrogă. (3) În termen de 12 luni de la data publicării prezentului cod în Monitorul Oficial al României, Partea I, Guvernul va supune Parlamentului spre adoptare proiectul de lege pentru punerea în aplicare a Codului penal. Această lege a fost adoptată la data de 25 iunie 2009, în temeiul prevederilor art. 114 alin. (3) din Constituția României, republicată, în urma angajării răspunderii Guvernului în fata Camerei Deputaților și a Senatului, în ședința comună din data de 22 iunie 2009.

[2] Legea nr. 161 din 19 aprilie 2003, privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei a fost publicată în MONITORUL OFICIAL nr. 279 din 21 aprilie 2003, fiind modificată şi completată de: ORDONANŢA DE URGENŢĂ nr. 40 din 20 mai 2003; LEGEA nr. 114 din 7 aprilie 2004; LEGEA nr. 171 din 14 mai 2004; LEGEA nr. 280 din 23 iunie 2004; LEGEA nr. 359 din 8 septembrie 2004; ORDONANŢA DE URGENŢĂ nr. 92 din 10 noiembrie 2004; ORDONANŢA DE URGENŢĂ nr. 14 din 3 martie 2005; ORDONANŢA DE URGENŢĂ nr. 31 din 19 aprilie 2006; LEGEA nr. 96 din 21 aprilie 2006; LEGEA nr. 251 din 23 iunie 2006; ORDONANŢA DE URGENŢĂ nr. 119 din 21 decembrie 2006; LEGEA nr. 144 din 21 mai 2007.

practicienii dreptului privind încadrarea juridică penală a Skimming-ului (Secţiunea 2-a);

- ”Alterarea integrităţii datelor informatice” (Secţiunea 3-a);
- ”Perturbarea funcţionării sistemelor informatice” (Secţiunea 4-a);
- ”Operaţiuni ilegale cu dispozitive sau programe informatice” (Secţiunea 5-a);
- ”Falsul informatic” (Secţiunea 6-a);
- ”Frauda informatică” (Secţiunea 7-a);
- ”Pornografia infantilă prin intermediul sistemelor informatice” (Secţiunea 8-a).

Prezentarea reprezintă implicit o radiografie a tuturor abordărilor doctrinare și practice, cu o valoare de actualitate dată de completările și opiniile personale aduse de autor aspectelor juridice sau tehnice descrise.

Capitolul III, denumit ”Aspecte procedurale prevăzute de Legea nr.161/2003” prezintă succint, din punct de vedere procesual, mijloacele de acțiune și conduita prescrisă organelor judiciare în instrucția infracțiunilor informatice.

În Capitolul IV, destinat prezentării aspectelor privind cooperarea internaţională, sunt trecute în revistă prevederile legii speciale în acest sens.

II. Cea de-a doua parte, denumită ”Criminalitatea comerțului electronic”, este bazată pe o a doua reglementare de maximă importanţă, preluată inclusiv de Noul Cod penal, cu cea mai largă acoperire, prin care legiuitorul român a abordat şi domeniile înrudite, într-un complex de acte normative speciale, menţionând aici în primul rând Legea nr. 365 din 7 iunie 2002, republicată, privind comerţul electronic şi Hotărârea de Guvern nr.1308/2002, privind aprobarea Normelor metodologice pentru aplicarea Legii nr.365/2002, privind comerţul electronic.

Vorbind despre raţiunile acestei reglementări, trebuie să spunem şi să acceptăm că noua civilizaţie informatică se bazează pe disponibilitatea şi accesibilitatea informaţiei, privită ca valoare strategică[3].

Tranziţia către societatea informaţională în România, ca o componentă relevantă a dezvoltării, nu presupune numai modernizarea infrastructurii informaţionale şi de comunicaţie, ci şi acoperirea lacunelor legislative cu privire la activităţile informatice, la procesul de informatizare şi, în general, la domeniul tehnologiei informaţiei.

Schimbarea, modernizarea şi adaptarea sistemului de drept al României la noul tip de societate se aliniază cerinţelor de reglementare europene şi internaţionale, reprezentând răspunsul ţării noastre la condiţiile de acceptare a României în structurile europene.

[3] Expunere de motive la proiectul Legii nr.365/2002 privind comerţul electronic

Dezvoltarea din ultimele decenii a tehnologiilor informaţionale determinate de necesitatea stocării şi a transmiterii rapide a informaţiilor cu cele mai mici costuri a revoluţionat comerţul global, comerţul direct sau cu amănuntul, redefinind principiile clasice ale marketingului, termenul de comerţ electronic devenind sinonim cu creşterea profitului.

Comerţul electronic, în concepţia Organizaţiei Economice de Cooperare şi Dezvoltare (OECD), reprezintă desfăşurarea unei afaceri prin intermediul reţelei Internet, vânzarea de bunuri şi servicii având loc off-line sau on-line.

Această operaţiune constă în derularea unei afaceri, ca activitate generatoare de valoare, având ca suport reţeaua Internet şi utilizarea unor pachete de programe software specifice.

Accesibilitatea tehnologiilor informaţionale legate de Internet, costul scăzut al acestora, precum şi relativa independenţă de tehnologiile clasice, permit economiilor ţărilor dezvoltate sau în curs de dezvoltare, precum şi agenţilor economici din aceste ţări o integrare rapidă în acest nou domeniu de activitate.

Impactul economic al comerţului electronic are ca efecte principale transformarea pieţei, prin creşterea flexibilităţii şi adaptabilităţii furnizorilor şi consumatorilor, accelerarea schimbărilor din economie, respectiv realizarea rapidă a reformelor şi reglementărilor, realizarea legăturilor electronice între companii, globalizarea activităţii economice, cererea de personal de înaltă calificare, creşterea interactivităţii economice, prin eliminarea barierelor economice şi geografice, reducerea importanţei timpului, globalizarea.

Legea nr. 365 privind comerţul electronic, adoptată în anul 2002, inspirată din legislaţia europeană, oferă protecţie consumatorului în relaţia afacere-consumator (*business to consumer- eng.*). Existenţa cadrului legislativ adecvat a mărit încrederea consumatorilor şi viteza operaţiunilor interbancare, rezultatul fiind o creştere fără precedent a tranzacţiilor comerciale on-line.

În perspectiva continuării evoluţiei favorabile a acestui sector al economiei româneşti s-a impus ca Legea nr.365/2002 privind comerţul electronic să fie modificată şi completată - mai ales în ceea ce priveşte răspunderea şi principiul ţării de origine, în scopul alinierii complete a normelor acestei legi la dispoziţiile Directivei 2000/31/EC a PE şi a Consiliului din 8 iunie 2000 (referitoare la anumite aspecte juridice privind serviciile societăţii informaţionale, în special comerţul electronic în Piaţa Internă).

După ce în Capitolul I, denumit ”Aspecte generale” sunt prezentate raţiunile acestei reglementări specifice şi actele normative înrudite care completează cadrul complex al tranzacţiilor electronice, în Capitolul II, ”Reglementarea internaţională”, este prezentată perspectiva europeană, incluzând directivele Uniunii Europene destinate armonizării legislaţiilor naţionale la nivel european în ceea ce priveşte comerţul electronic (Directiva

Comerţului Electronic a Uniunii Europene şi Directiva vânzării la distanţă), dar şi perspectiva internaţională şi cea americană, de referinţă (modelul UNCITRAL pentru comerţul electronic şi reglementarea specifică din S.U.A. în ceea ce priveşte comerţul electronic şi semnătura electronică).

În continuare, în Capitolul III destinat reglementării interne, este prezentat cadrul legal general, adică dispoziţiile relevante ale Legii nr. 365/2002 privind comerţul electronic, urmat de normele metodologice, pentru aplicarea acestei legi şi, succint dispoziţiile Ordonanţei nr.130/2000, privind regimul juridic al contractelor la distanţă

Capitolul IV parcurge definiţiile comerţului electronic şi clasificarea tranzacţiilor electronice, pentru delimitarea neechivocă a domeniului şi înţelegerea complexităţii, dar şi limitelor acestuia.

Prin conţinutul său, Capitolul V, denumit ”Mijloace de plată în Internet”, abordează într-o manieră dezvoltată conceptul de plată electronică, prin definirea acestuia şi enumerarea explicativă a mijloacelor de plată folosite în Internet - mijloace de plată tradiţionale adaptate contextului reţelei, mecanisme noi de plată - dezvăluind în final o abordare particulară privind structura, mecanismele şi vulnerabilităţile activităţii de comerţ electronic.

În Capitolul VI sunt analizate, pe aceeaşi structură constitutivă ca în cazul celor informatice, infracţiunile la regimul comerţului electronic, în preliminarii fiind amintite potrivit Regulamentului Băncii Naţionale a României nr. 6/2006, definirile unor noţiuni esenţiale cum ar fi aceea de card, Cod de Identificare al Emitentului, Cod Personal de Identificare, procesator ș.a.

Analiza infracţiunilor prevăzute de Legea nr. 365/2002 parcurge infracţiunile de:

1. Falsificarea instrumentelor de plată electronică;
2. Deţinerea de echipamente în vederea falsificării instrumentelor de plată electronică;
3. Falsul în declaraţii în vederea emiterii sau utilizării instrumentelor de plată electronică;
4. Efectuarea de operaţiuni financiare în mod fraudulos;
5. Acceptarea operaţiunilor financiare efectuate în mod fraudulos.

III. Cea de-a treia parte a lucrării, denumită ”Criminalitatea informatică. Aspecte de drept comparat. Evoluţia fenomenului şi propuneri de reglementare viitoare”, dezvoltă în Secţiunea 1-a, ”Aspecte generale. Caracterul preponderent transfrontalier al fenomenului şi necesitatea unei reglementări globale”, tendinţa de universalizare a Convenţiei Consiliul Europei privind criminalitatea informatică, realizând şi o retrospectivă a eforturilor globale de cooperare împotriva terorismului cibernetic.

În Secţiunea a 2-a, ”Provocări ale domeniului. Actualităţi”, autorul conduce ideea lucrării spre un viitor devenit prezent, efectuând o incursiune în noile ”realităţi” sociale de genul Second life (”A doua viaţă”) şi Habbo Hotel

(Hotelul personajelor ”Habbo”) – lumi virtuale paralele care obligă la regândirea fundamentelor dreptului penal.

După prezentarea și relevarea trăsăturilor acestora, călătoria continuă în alte zone ce pot reprezenta tot atâtea provocări și pentru societatea noastră, fiind abordată problema așa-ziselor droguri virtuale, dar și a violenței proliferate prin mijloace informatice (Cyberbullyng, Happy Slapping).

Secţiunea a 3-a este destinată concluziilor şi implicit propunerilor de reglementare viitoare. Sunt prezentate abordările proprii asupra Furtului virtual, Furtului folosinţei unui terminal de comunicaţii, Spălării de bani în spațiul virtual.

Spațiul virtual, noile incriminări naționale specifice și viitoarele incriminări.

A. Furtul virtual.

Furtul virtual nu are un corespondent eficace în incriminarea legală națională. Aceasta este practic o situație similară furtului de semnal TV, asupra căruia disputele nu au încetat decât prin intervenția legiuitorului, prin recunoașterea potențialului criminal al acestui gen de fapte și a pericolului social generic reprezentat.

În cazul furtului virtual ar însemna să acceptăm în mod practic că obiectul imaterial, dar cu materialitate virtuală, are asociată o valoare economică, raționamentul juridic fiind similar celui atribuit de legiuitor în cazul furtului de energie, incriminat prin dispozițiile art. 208 alin.2 din Codul penal.

Implicit, raportându-ne la dispozițiile penale existente ar trebui să conferim obiectelor virtuale natura unei energii. În opinia noastră această interpretare nu este în măsură să complinească o lipsă reală a incriminării legale. Aici în contextul nevoii de reglementare, textul legal în vigoare ar trebui modificat prin includerea pe viitor a unui alineat care să prevadă și să sancționeze adecvat acest gen de furt, lucru aparent destul de dificil de realizat, în condițiile în care definirile acțiunilor din latura obiectivă a infracțiunii clasice vorbesc despre „luare”, „detenție”, „posesie”, „însușire”, atribute ale unor acțiuni materiale în deplin acord cu natura pur materială a unui „bun” sau „lucru”.

În spațiul virtual, corespondența atributelor nu este însă exclusă atâta vreme cât juridic și legal este acceptată materialitatea bunului în această lume la fel de reală senzorial ca aceea în care ne ducem existența fizică acceptată biologic.

Într-o formulare viitoare la încriminarea furtului virtual ar trebui arătat că bunul din lumea virtuală cu valoare economică asociată sau proprie este asimilat bunurilor materiale, supunându-se incriminării în aceleași condiții sau în condiții speciale, raportat pe de o parte la ușurința comiterii faptei și a camuflării identității autorului, dar pe de altă parte și la posibilitățile oarecum limitate în prezent de valorificare prin împosedare ale bunurilor virtuale.

Sub acest aspect, trebuie observat că faptul împosedării se limitează și în acest spațiu la mutarea bunului într-un alt loc și impiedicarea utilizatorului legal să dispună de acesta. Teoretic, urmărirea și găsirea bunului nu ar trebui să pună probleme, urmele fiind destul de facil de identificat.

Mai complexă este situația în care bunul este valorificat prin înstrăinare, infractorii însușindu-și sumele de bani virtuali și corelativ reali, ulterior făcându-se nevăzuți prin abandonarea echipamentelor și renunțarea la identitățile false preluate.

B. Furtul folosinței unui terminal de comunicaţii

Un reputat expert german în domeniul criminalității informatice, Marco Gercke, spunea cu ocazia Conferinței Taiex de la București din toamna anului 2009, cu admirație, dar și cu o doză de malițiozitate, că România s-a grăbit să implementeze toate normele specifice progresiste, referindu-se mai ales la cele europene. Prin încriminarea furtului folosinței unui terminal de comunicaţii al altuia sau folosirea unui terminal de comunicaţii racordat fără drept la o reţea, condiționate de producerea unei pagube, se pare că ne situăm, și de această dată, de partea țărilor care s-au grăbit să implementeze cele mai noi strategii de prevenire și combatere a criminalității informatice, regăsindu-ne totodată în mijlocul unor aprinse controverse legale și morale. Lucrarea noastră încearcă aici, cu modestie, un exercițiu mai profund de interpretare și imaginație, din dorința de a releva concepte noi, unele, deși enunțate, nedezvoltate și implicit neintegrate, în măsură să contribuie la regândirea fundamentelor dreptului penal în acord cu realități sociale situate dincolo de percepția fizică, așa cum este spațiul virtual.

a. Introducere. Ideea acestei prezentări ne-a venit plecând de la numeroasele întrebări rămase fără răspuns pe care practicienii, dar mai ales teoreticienii domeniului, au început să le pună în urma modificărilor legislative recente din domeniul penal în privința criminalității informatice.

Pe de altă parte, dintr-o perspectivă nouă pentru noi, dar deja deschisă de specialiști din alte țări preocupați de problematica infracționalității informatice, nevoia de a răspunde provocărilor pe care le implică reglementările noi, obligă la reafirmarea unor necesități de reconsiderare a fundamentelor dreptului penal, fiind bucuroși să constatăm că nevoia de reglementare adecvată este recunoscută din ce în ce mai mult.

Astfel, opinii generale de genul inutilității reglementării speciale a noilor modalități faptice de comitere a infracțiunilor informatice, denumite generic, cu motivarea că instituțiile de drept penal clasice pot asigura, prin opera judiciară de interpretare, tragerea la răspundere penală în toate situațiile, suferă de cel puțin două mari nejunsuri:

- nu au vocație universală, așa cum reclamă în mod firesc un spațiu fără frontiere cum, de altfel, este spațiul virtual; teritorialismul sistemelor judiciare tradiționale și diferențele conceptuale presupun ca, de exemplu, principiul legalității încriminării specific sistemului de drept romano-german, pozitivist, să

reprezinte un real impediment la activitatea de interpretare și tragere la răspundere a făptuitorilor, prin comparație cu sistemul precedentului judiciar sau anglo saxon (*common-law*);

- nu răspund unor cerințe minime de adaptare a textelor legale la noile realități sociale care implică și dezvoltarea tehnologică fără precedent.

Citându-l pe Daniel E.Greer jr., ”lumea digitală nu este lumea fizică”[4], aceasta fiind și în opinia noastră cheia întregii problematici. Bazându-ne pe intuiţia derivată din lumea fizică pentru a face alegeri de politică penală, nu vom face decât să avem de fiecare dată probleme.

În opinia aceluiași autor, legea digitala este şi trebuie să fie contraintuitivă. Deoarece intuiţia noastră despre sfera digitală poate fi atât de uşor greşită, este extrem de util ori de câte ori este posibil să ne bazăm alegerile politicilor noastre pe fapte solide.

Discutând în mai multe situații cu diverși specialiști implicați în activitatea practică de identificare și tragere la răspundere penală a infractorilor informatici, nu de puține ori aceștia remarcau că problemele de încadrare riguroasă a faptelor în textul legal adecvat sunt privite în alte sisteme judiciare mult mai larg, în contextul în care un text legal clasic prevede o infracțiune care în esență acoperă suficient nevoia de sancționare a unei fapte ce aduce atingere gravă relațiilor sociale ocrotite.

Cu alte cuvinte, legalitatea incriminării ar fi relativă prin raportare la diversele modalități normative ale aceleiași infracțiuni, câtă vreme faptele sunt mai presus de orice îndoială.

Același simț practic, transpus la nivel de principiu, face ca în condițiile în care fapta este fără importanță, și nu neapărat în mod vădit, sau cheltuiala cu investigațiile să fie estimată ca fiind prea mare în raport cu valoarea prejudiciului cauzat, cercetarea să nu fie declanșată de către organele judiciare, prezumându-se că acestea lucrează în mod eficient în numele statului.

O asemenea perspectivă poate părea îndepărtată celor mai mulți dintre practicienii noștri și poate păcătui prin aceea că autoritățile judiciare nu au ajuns încă la maturitatea de a acționa responsabil în toate cazurile, tributari uneori unor reglementări lacunare sau insuficient informați, mai ales în domeniile noi, preponderent tehnice. Pe de altă parte, legalitatea încriminării, ca principiu, constituie o garanție în plus a drepturilor cetățenilor față de abuzurile la care ar putea fi expuși cu știință sau prin gravă neglijență de autoritățile statului.

Reglementarea riguroasă, științifică, actuală a noilor realități sociale reprezintă astfel soluția păstrării echilibrului între nevoia de asigurare a securității sociale și respectarea drepturilor și libertăților fundamentale ale cetățenilor.

---

[4] Daniel E.Greer jr., *The Physics of Digital Law: Searching for Counterintuitive Analogies,* în Cybercrime. Digital Cops and Laws in a Networked Enviroment; http://books.google.ro/books?id=JTF0xZlHZ2gC&printsec=frontcover&dq=related:ISBN1851096833#v=onepage&q&f=false

Într-un asemenea context se situează şi demersul de reglementare al legiuitorului român care, în noul Cod Penal, introduce furtul folosinţei unui terminal de comunicaţii al altuia sau folosirea unui terminal de comunicaţii racordat fără drept la o reţea, condiționat de producerea unei pagube, subiect care, cel puțin sub aspectul conectării la internet, este extrem de controversat, fiind supusă dezbaterii legalitatea și moralitatea unei astfel de încriminări.

b. Spațiul virtual și domiciliul informatic. În Partea specială a Noului Cod penal[5] se regăsesc incluse pentru a doua oară[6], prin opera de sistematizare şi codificare a legiuitorului român, infracţiunile informatice, acestora în raport de importanţa lor fiindu-le dedicat chiar un întreg capitol, denumit „Infracţiuni contra siguranţei şi integrităţii sistemelor şi datelor informatice", în cadrul Titlului VII destinat „Infracţiunilor contra siguranţei publice", infracţiunile specifice regăsindu-se însă şi în alte titluri, aşa cum vom vedea în continuarea prezentării. Astfel:

În Titlul II, destinat „Infracţiunilor contra patrimoniului", în Capitolul I, denumit „Furtul", este încriminat „Furtul în scop de folosinţă". Potrivit art. 229 alin.2, furtul care are ca obiect un vehicul, săvârşit în scopul de a-l folosi pe nedrept, se sancţionează cu pedeapsa prevăzută în art. 228 sau art. 229, după caz, ale cărei limite speciale se reduc cu o treime.

Cu pedeapsa prevăzută în alin. (1) se sancţionează *folosirea fără drept a unui terminal de comunicaţii al altuia sau folosirea unui terminal de comunicaţii racordat fără drept la o reţea, dacă s-a produs o pagubă.*

Deşi în capitolul destinat înţelesului unor termeni sau expresii Codul nu defineşte „terminalul de comunicaţii" este evident că acesta poate fi şi un sistem informatic, probabil cea mai mare parte a comunicaţilor moderne fiind facilitate de astfel de sisteme. Această interpretare este sugerată sistematic de expresia

---

[5] Adoptat prin Legea nr.286/2009 privind Codul penal publicată în Monitorul Oficial al României, Partea 1, Nr. 510 din 24 iulie 2009. Sub aspectul intrării în vigoare, Titlul XIII, „Dispoziţii finale" prevede: Art. 446. - Prezentul cod intră în vigoare la data care va fi stabilită în legea pentru punerea în aplicare a acestuia, cu excepţia dispoziţiilor alin. (2) şi alin. (3), care intră în vigoare la 4 zile de la data publicării în Monitorul Oficial al României, Partea I, a prezentului cod. Legea nr. 301/2004 - Codul penal, publicată în Monitorul Oficial al României, Partea I, nr. 575 din 29 iunie 2004, cu modificările ulterioare, şi Legea nr. 294/2004 privind executarea pedepselor şi a măsurilor dispuse de organele judiciare în cursul procesului penal, publicată în Monitorul Oficial al României, Partea I, nr. 591 din 1 iulie 2004, cu modificările ulterioare, se abrogă. În termen de 12 luni de la data publicării prezentului cod în Monitorul Oficial al României, Partea I, Guvernul va supune Parlamentului spre adoptare proiectul de lege pentru punerea în aplicare a Codului penal. Această lege a fost adoptată la data de 25 iunie 2009, în temeiul prevederilor art. 114 alin. (3) din Constituţia României, republicată, în urma angajării răspunderii Guvernului în fata Camerei Deputaţilor şi a Senatului, în şedinţa comună din data de 22 iunie 2009.

[6] În ceea ce priveşte criminalitatea informatică şi în Codul penal preconizat să intre în vigoare în septembrie 2006 a fost introdus un titlu distinct, Titlul X, denumit „Delicte contra datelor şi sistemelor informatice", în care de asemenea au fost preluate, cu unele modificări, infracţiunile din Legea 161/2003.

”racordat fără drept la o rețea”, termenul ”rețea” fiind elocvent pentru definirea nivelului tehnologic la care se referă.

Bogdan Manolea, un binecunoscut specialist în domeniul IT se întreba[7] nu cu mult timp în urmă dacă este un punct de acces Wi-Fi un terminal de comunicații, considerând mai degrabă că acesta nu ar avea o astfel de calitate, terminalul fiind calculatorul sau telefonul care se conectează la Internet. Întrebarea firească imediată a fost dacă se poate vorbi de racordare fără drept în cazul unui Wi-Fi neprotejat, răspunsul său fiind tot negativ.

Același autor se întreba la ce acțiuni se referă articolul de lege în acest context, făcând trimitere la opinia și argumentele unui alt specialist Maxim Dobrinoiu, legând discuția de noțiunile de wardriving sau piggybacking.

Maxim Dobrinoiu, susținea astfel[8] că folosirea sintagmei „accesarea rețelei Wi-Fi” este de natură să producă anumite confuzii, întrucât utilizatorii realizează doar o conectare la serviciile de Internet furnizate (prin unde radio) de către router și nicidecum o „intrare” (în tot sau doar într-o parte) în sistemul informatic reprezentat de router și restul dispozitivelor electronice echipate wireless aflate într-o relație similară de „conectare” cu punctul de acces.

Dacă, însă, nu conectarea la Internet, ci Punctul de Acces sau rețeaua Wi-Fi (protejată sau nu) reprezintă țintele persoanei interesate, pot exista incriminări în baza art. 42 din Legea 161/2003, cu condiția să existe probe relevante din care să rezulte intenția făptuitorului de a accesa setările sau fișierele routerului ori de a interacționa cu celelalte componente ale rețelei (computere, telefoane inteligente, PDA-uri etc.).

Autorul arăta că tehnic, acest lucru este posibil, dacă sunt efectuate anumite setări în sistemul de operare al dispozitivului „intrus” ori prin folosirea unor aplicații dedicate. Pe de altă parte, din punct de vedere strict tehnic, simpla conectare la semnalul Internet Wi-Fi se poate realiza adesea automat, în funcție de setările dispozitivului folosit de prezumtivul făptuitor, fără știrea acestuia, în acest caz fiind exclusă existența vinovăției, deci și a infracțiunii.

Opiniile exprimate de unii specialiști, potrivit cărora ne-am putea afla în condițiile *”interceptării fără drept a unei emisii electromagnetice provenită dintr-un sistem informatic ce conține date informatice care nu sunt publice…”* (art. 43 alin 2 din Legea 161/2003), în opinia aceluiași autor, nu sunt pertinente, întrucât datele informatice conținute în emisia electromagnetică (respectiv broadcast-ul radio) purtătoare a semnalului Internet sunt publice. În aceste condiții, singura posibilitate de încadrare juridică a conectării la serviciile de comunicații electronice furnizate de un punct de acces Wi-Fi ar putea-o reprezenta infracțiunea de furt (prevăzută si pedepsită de art. 208 alin 2 Cod Penal), în condițiile *„furtului unei energii care are valoare economic*ă*”*, întrucât

[7] B.Manolea, http://legi-internet.ro/blogs/index.php/2009/08/28/infractiuni-informatice-noul-cod-penal.

[8] Maxim Dobrinoiu, *Provocarea legislativă a rețelelor Wi-Fi*, în Revista Intelligence, Anul VI nr. 16, iulie 2009; http://e-crime.ro/ecrime/site/index.php/articole/.

semnalul Internet, respectiv accesul la serviciile societății informaționale, sunt obținute de proprietarul, deținătorul ori utilizatorul legal al Routerului IP de la un furnizor de servicii Internet (ISP) în schimbul unei sume de bani (abonament lunar etc.). În opinia sa, această încadrare este forțată și oarecum imorală, însă, până la o reglementare adecvată, poate fi practică – mai ales în cazul rețelelor (punctelor de acces) private.

Activitățile specifice de detectare și folosire a semnalului electromagnetic emis de punctele de acces legitime, sunt denumite și clasificate specific în literatura de specialitate sub denumirea de *wardriving* și *piggybacking*.

Wardriving[9] este definit ca fiind actul de căutare a rețelelor Wi-Fi de către o persoană aflată într-un vehicul aflat în mişcare, folosind un calculator portabil sau PDA. Software-ul pentru wardriving este disponibil gratuit pe internet, acoperind o gamă completă de dispozitive și aplicații. Sub aspect tehnic, dispozitivul folosit de persoana interesată captează semnalul radio emis de punctul de acces (routerul IP), iar printr-o interfață specializată, oferă informații despre acesta, cum ar fi: numele punctului (SSID), puterea de emisie (puterea semnalului radio), existența măsurilor de protecție și algoritmul de criptare utilizat (ex. WEP,WPA, WPA-2), adresa de IP alocată, adresa serverului DNS (Sistem Nume de Domeniu – care permite translatarea unui nume de domeniu într-o adresă IP în Internet).

Toate aceste date sunt consemnate electronic, o analiză ulterioară putând oferi informații clare despre situația punctelor de acces Wi-Fi care furnizează servicii de comunicații electronice (conectare la Internet) într-o anumită arie de interes. Trebuie subliniat faptul că echipamentul Wi-Fi al persoanei nu obține automat servicii de comunicații electronice, pentru aceasta fiind necesară lansarea unei comenzi de conectare.

Piggybacking[10] ar însemna într-o traducere liberă dedicată *accesul la internet "călărind pe spatele altuia"*, referindu-se la stabilirea unui conexiuni wireless la Internet folosind serviciul wireless de acces la internet al unui abonat, fără cunoștința sau permisiunea explicită a acelui abonat. Universal, este un punct de vedere legal şi etic controversat în practică, reglementările fiind foarte variate, fiind fie complet scos în afara legii în unele locuri, fie permis în altele.

---

[9] http://en.wikipedia.org/wiki/Wardriving; Softul este în special pentru Windows NetStumbler, Kismet sau SWScanner pentru Linux, FreeBSD, NetBSD, OpenBSD, DragonFly BSD, Solaris, şi KisMac pentru Macintosh. Există, de asemenea homebrew wardriving, cererile de joc pe console portabile cu suport Wi-Fi, cum ar fi sniff_jazzbox / wardive pentru Nintendo DS, Dog de parcurs pentru Sony PSP, WiFi. În cazul dispozitivelor telefonice gen iPhone cu sistem de operare Android avem wardrive G-MON, pentru cele gen Nokia, cu sistem de operare Symbian, având WlanPollution. De asemenea, exista un mod în Metal Gear Solid: Portable Ops pentru Sony PSP (în care jucătorul este capabil să găsească noi tovarăşi prin căutarea punctelor de acces fără fir), care pot fi utilizate în acest scop.

[10] http://en.wikipedia.org/wiki/Piggybacking

Astfel, un client al unei afaceri care furnizează hotspot de servicii, cum ar fi un hotel sau cafenea, în general nu este considerat a fi într-o situație de piggybacking, deşi non-clienţi sau cei care sunt pur şi simplu în afara spaţiilor ajung să fie în această situație. Multe astfel de locaţii oferă acces liber sau plătit la Internet fără fir, prin amabilitatea patronilor sau pur și simplu pentru a atrage oameni în zonă, putând avea acces și alte persoane situate în apropierea sediului. Procesul de transmitere a datelor, împreună cu confirmarea de primire este numit piggybacking.

Noțiunea de piggybacking este diferită de wardriving, acesta din urmă implicând numai logarea sau cartografierea punctelor de acces.

De semnalat este că, acest fenomen, piggybacking-ul, se manifestă din ce în ce mai frecvent în raport cu rețelele wireless particulare, indiferent că acestea aparțin unor persoane fizice sau juridice. În acest caz accesul la serviciul Internet depinde strict de măsurile de securitate asociate punctului de acces[11].

Se pare că răspunsul la întrebarea cât de legală sau de morală este însă o asemenea conectare la serviciile societății informaționale prin intermediul punctelor de acces wireless a fost oferit de legiutorul român prin încriminarea realizată prin textul art. 230 alin. 1, teza a II-a din Codul penal, ca furt, a *folosirii fără drept a unui terminal de comunicaţii al altuia sau folosirii unui terminal de comunicaţii racordat fără drept la o reţea, dacă s-a produs o pagubă.*

Amintim și de această dată că analogia cu furtul de energie este în opinia noastră nepotrivită, acest gen de energie, ca de altfel și semnalul TV distribuit prin cablu, nefiind cuantificabil sub aspect industrial, măsurarea fiind posibilă doar în condiții de laborator și nerelevantă sub aspectul valorii prejudiciului.

Și aici, legiuitorul a încercat să ofere protecție juridică împotriva unui fenomen cu tendințe dinamice, capabil să creeze prejudicii evidente deopotrivă furnizorilor și consumatorilor acestui gen de servicii, furnizarea accesului la Internet.

Dificultățile apar însă dacă ne raportăm numai la consumatorul care lasă un astfel de punct de acces public, din ignoranță sau neștiință, acesta fiind deja plătitor și beneficiar al unui astfel de serviciu, nefiind lipsit de folosința lui, fiind puțin probabil că în cazul unei utilizări în scop licit ar putea resimți vreo perturbare. Care ar fi prejudiciul cauzat acestuia? Dacă nu a fost cauzat un prejudiciu care ar fi modul de protejare al consumatorului devenit furnizor accidental de servicii internet?

[11] folosirea unui algoritm decriptare, de exemplu: WEP - Wired Equivalent Privacy, WPA - Wi-Fi Protected Access sau WPA2 și implicit parolarea; filtrarea MAC-rilor; adresă IP fixă; token-uri hardware sau software ș.a.

Opinia noastră este că rezolvarea legală ar fi poate alta, legată de noțiunea de *domiciliu informatic*[12] și implicit de dreptul la o viață privată neperturbată. De altfel, teoretizând, spațiul virtual, în abordarea noastră implică și noțiunea de domiciliu virtual, reclamând recunoașterea unor trăsături și aplicabilitatea sau necesitatea unei reglementări similare domiciliului real, așa cum este definit de legea penală.

Pornind de la o nepermisă, dar utilă analogie, amintim că potrivit art. 192 alin.1 din Codul penal în vigoare, pătrunderea fără drept, în orice mod, într-o locuință, încăpere dependință sau loc împrejmuit ținând de acestea, fără consimțământul persoanei care le folosește, sau refuzul de a le părăsi la cererea acesteia (modalitatea în care accesul a fost permis) se pedepsește cu închisoarea.

În cazul nostru, domiciliul informatic este reprezentat de calculatorul personal, toate emisiile electromagnetice ținând de acesta completând întinderea sa. Termenii clasici descriu însă o situație premisă, existența obligatorie a delimitării fizice. În mediul virtual, delimitarea fizică este aproape exclusă, singura limitare fiind aceea prin nume de utilizator și parolă, ceea ce în lumea fizică ar echivala cu a asigura locuința sau împrejmuirea cu sisteme de închidere.

Atunci de ce ar fi în primul rând moral și apoi legal ca oricine să se poată conecta fără permisiune la un serviciu internet al altuia fără consecințe? Dacă am gândi asemenea activiștilor Internet pentru liberalizare, adepții distribuirii gratuite a softurilor necesare utilizării neîngrădite a acestuia, explicația ar următoarea: pentru că așa este firesc în absența mijloacelor de securitate pe care utilizatorii le au la dispoziție și pentru că emisiile electromagnetice nu au în principiu bariere fizice și sunt prezumate publice, cu limitările legale legate de intercepție.

Suntem în prezența deopotrivă a mai multor raporturi juridice: unele licite, contractuale, dintre consumator și furnizorul serviciului, cu limitările ce decurg din convenție, altele de conflict, dintre furnizorul serviciului și consumator, respectiv utilizatorul nelegitim.

Este interesant aici de stabilit cine este subiectul pasiv al infracțiunii cauzatoare de prejudicii. În opinia noastră, subiectul pasiv principal va fi furnizorul serviciului de internet, reglementarea fiind în mod evident introdusă pentru protejarea acestui segment important din lumea afacerilor, subiect pasiv adiacent putând fi după caz și beneficiarul legitim al serviciului, dacă evident este dovedită și prejudicierea acestuia.

Obiectul juridic constituit din relațiile sociale patrimoniale care iau naștere și se dezvoltă în raporturile contractuale sau nu dintre furnizorul

[12] I.Vasiu, *Informatica juridică şi drept informatic*, Ed. Albastră, Cluj-Napoca, 2002, p.166; în același sens, dar în forma de ”spațiu informatic”, conceptul este reluat de M.Dobrinoiu, *Infracţiuni în domeniul informatic*, Ed.C.H.Beck, Bucureşti, 2006, p.147.

serviciilor societății informaționale și beneficiarii acestora, fiind dictat de scopul definit în verbum regens, cauzarea unui prejudiciu.

Evident în cazul subiectului pasiv principal, prejudiciul nu poate fi decât unul juridic, stabilit în baza legii prin estimare, similar furtului de energie electrică sau a celui de semnal TV distribuit prin cablu. Eventualul prejudiciu cauzat subiectului pasiv adiacent va trebui dovedit în condițiile Codului Civil, în acest caz, estimările legale neavând aplicabilitate.

Aspectele legate de subiectul infracțiunii relevă absența protecției juridice a consumatorului sub aspectul protecției spațiului său virtual privat și lasă deschisă discuția privind necesitatea unei astfel de intervenții de reglementare legală, într-o viitor al conexiunilor fără fir, devenit deja prezent. Este suficient să amintim cu titlu informativ că tendința devenită deja realitate este de a elimina inclusiv cablurile de alimentare electrică a dispozitivelor electronice, principiile inducției magnetice ale lui Tesla fiind cele care au făcut posibilă această tehnologie[13].

Interesul reglementării acestui aspect secundar generat de situația subiectului pasiv adiacent din noul Cod Penal este legat nu numai de necesitatea respectării vieții private a utilizatorului legitim al serviciului internet dar și de nevoia de intimidare a infractorilor care aleg să-și camufleze identitatea în acest mod, atacând sistemele și rețelele prin aceste portițe ideale care le asigură totodată scăparea și deplinul anonimat.

Cu alte cuvinte, în lupta cu un fenomen atât de greu de controlat, orice măsură de prevenire aduce mai multe avantaje celorlalți decât dezavantajele rezultând din incriminarea, tragerea la răspundere și sancționarea unor astfel de utilizatori nelegitimi, natura sancțiunii, procedibilitatea și procesibilitatea putând fi supuse unor condiții care să le facă flexibile, cum ar fi existența plângerii prealabile și posibilitatea împăcării părților.

Sub aspect profilactic, zonele de acces liber ar trebui semnalate atât în plan fizic cât și în spațiul virtual, cu denumirea punctului de acces, comunicațiile libere nefiind îngrădite între internauți care au posibilitatea să facă acest lucru securizat, în alte condiții aceștia devenind de fapt furnizori de servicii internet supuși reglementărilor legale.

c. Securitatea reţelelor wireless. **Noțiuni.**

Punctul de Acces *(*Access Point-*eng.)* este un dispozitiv electronic denumit router Wi-Fi (Wireless Fidelity - *eng*.), reprezentând un sistem informatic în accepțiunea art. 35 din Titlul III – prevenirea și combaterea criminalității informatice al Legii nr.161/2003, deoarece întrunește deopotrivă condițiile de a fi un dispozitiv electronic și de a funcționa în baza unui program informatic (firmware).

[13] A se vedea rezultatele cercetărilor Intel, Sony, Samsung în acestă privință, reflectate în media-internet.

Un ruter (sau *router-eng.*) este un dispozitiv hardware sau software care conectează două sau mai multe rețele de calculatoare bazate pe ”comutarea de pachete” (*packet switching - eng.*). Funcția îndeplinită de rutere se numește rutare. Diferențierea între rutere hardware și rutere software se face în funcție de locul unde se ia decizia de rutare a pachetelor de date. Ruterele software utilizează pentru decizie un modul al sistemului de operare, în timp ce ruterele hardware folosesc dispozitive specializate (de tip ASIC) ce permit mărirea vitezei de comutare a pachetelor.

Ruterele operează la nivelul 3 al modelului OSI (*Open Systems Interconnection)*[14]. Ele folosesc deci adresele IP[15] (Internet Protocol) ale pachetelor aflate în tranzit pentru a decide către care anume interfață de ieșire trebuie să trimită pachetul respectiv. Decizia este luată comparând adresa calculatorului destinație cu înregistrările (câmpurile) din tabela de rutare. Aceasta poate conține atât înregistrări statice (configurate/definite de către administratorul rețelei), cât și dinamice, aflate de la ruterele vecine prin intermediul unor protocoale de rutare.

Reţelele wireless sunt relativ mai puţin sigure decât cele cablate, datorită accesului mai facil la reţea al persoanelor neautorizate aflate în zonele de acoperire ale punctelor de acces. În implementarea reţelelor wireless, există

---

[14] **Modelul de Referință OSI** (engleză *Open Systems Interconnection - Reference Model*), pe scurt: OSI, este o structură de comunicare ierarhică foarte des folosită pentru a reprezenta o rețea. OSI este un standard al Organizației internaționale de standardizare, emis în 1984. Modelul de referință OSI propune niște criterii generale pentru realizarea comunicației sistemelor de calcul pentru ca acestea să poată schimba informații, indiferent de particularitățile constructive ale sistemelor (fabricant, sistem de operare, țară, etc). Acesta are aplicații în toate domeniile comunicațiilor de date, nu doar în cazul rețelelor de calculatoare. Modelul OSI divizează problema complexă a comunicării între două sau mai multe sisteme în 7 straturi (engleză *layers*) distincte, într-o arhitectură ierarhică. Fiecare strat are funcții bine determinate și comunică doar cu straturile adiacente. Aceste șapte niveluri formează o ierarhie plecînd de la nivelul superior 7 – aplicație (engleză *application*) și până la ultimul din partea de jos a stivei, nivelul 1 - fizic (engleză *physical*). Deși astăzi există și alte sisteme, cei mai mulți distribuitori de echipamente de comunicație folosesc OSI pentru a instrui utilizatorii în folosirea echipamentelor. Se consideră că OSI este cel mai bun mijloc prin care se poate face înțeles modul în care informația este trimisă și primită;
http://ro.wikipedia.org/wiki/Modelul_OSI

[15] **IP** (*Internet Protocol*) este un protocol care asigură un serviciu de transmitere a datelor, fără conexiune permanentă. Acesta identifică fiecare interfață logică a echipamentelor conectate printr-un număr numit ”adresă IP”. Versiunea de standard folosită în majoritatea cazurilor este IPv4. În IPv4, standardul curent pentru comunicarea în Internet, adresa IP este reprezentată pe 32 de biți (de ex. 192.168.0.1). Alocarea adreselor IP nu este arbitrară; ea se face de către organizații însărcinate cu distribuirea de spații de adrese. De exemplu, RIPE este responsabilă cu gestiunea spațiului de adrese atribuit Europei. Internetul este în proces de evoluție către versiunea următoare de IP, numită IPv6, care practic așteaptă un utilizator major, care să oblige folosirea acestei versiuni superioare și de către alții. Ramurile Ministerului Apărării al SUA (DoD) au anunțat ca în decursul anilor 2009 - 2011 vor înceta relațiile cu furnizorii de servicii Internet care nu folosesc IPv6.

diferite bariere care formează aşa numita securitate de bază a reţelelor wireless, care împiedică accesul neintenţionat al persoanelor străine de reţea, aflate în aria de acoperire a unui punct de acces. Pentru persoane rău intenţionate, cu bună pregătire în domeniu, de tipul hacker-ilor, securitatea acestor reţele, ca de altfel şi a altora, rămâne discutabilă.

Barierele de securitate (securitatea de bază) care au fost prevăzute în protocoalele reţelelor Wi-Fi asigură un nivel relativ scăzut al securităţii acestor reţele, ceea ce le-a frânat întrucâtva dezvoltarea. Securitatea de bază a reţelelor wireless este asigurată de următoarele funcţii implementate:

• SSID (Service Set Identifiers-*eng*.);
• WEP (Wired Equivalent Privacy-*eng*.);
• Verificarea adresei fizice MAC (Media Acces Control-*eng*.).

a) SSID este un cod care defineşte apartenenţa la un anumit punct de acces wireless. Toate dispozitivele wireless care vor să comunice într-o reţea trebuie să aibă SSID-ul propriu, setat la aceeaşi valoare cu valoarea SSID-ului punctului de acces pentru a se realiza conectivitatea. În mod normal un punct de acces îşi transmite SSID-ul la fiecare câteva secunde. Acest mod de lucru poate fi stopat, astfel încât o persoană neautorizată să nu poată descoperi automat SSID-ul şi punctul de acces. Dar, deoarece SSID-ul este inclus în beacon-ul (mici pachete de date transmise continuu de un punct de acces pentru a-şi face cunoscută prezenţa şi pentru a asigura managementul reţelei) oricărei secvenţe wireless, este uşor pentru un hacker dotat cu echipament de monitorizare să-i descopere valoarea şi să se lege în reţea.

b) WEP poate fi folosit pentru a ameliora problema transmiterii continue a SSID-ului prin criptarea traficului dintre clienţii wireless şi punctul de acces. Se realizează prin aceasta o autentificare printr-o cheie (shared-key authentication). Punctul de acces transmite clientului wireless o provocare pe care acesta trebuie s-o returneze criptată. Dacă punctul de acces poate decripta răspunsul clientului, are dovada că acesta posedă cheia validă şi are dreptul de a intra în reţea.

Desigur, WEP nu asigură o securitate prea mare. Hackerul dotat cu echipament de monitorizare poate recepţiona şi înregistra întâi provocarea plecată de la punctul de acces apoi răspunsul criptat al clientului şi, pe baza unor procesări se poate determina cheia pe care apoi o poate folosi pentru a intra în reţea.

c) Verificarea adresei MAC. Se poate spori securitatea reţelei dacă administratorul de reţea utilizează filtrarea adreselor MAC, adică punctul de acces este configurat cu adresele MAC ale clienţilor cărora le este permis accesul în reţea. Din nefericire, nici această metodă nu asigură o securitate prea mare. Un hacker poate să înregistreze secvenţe din trafic şi, în urma unor analize, poate să extragă o adresă MAC pe care ulterior o poate folosi pentru a intra în reţea.

O discuţie interesantă ar fi legată de definirea expresiei ”*terminal de comunicaţii*”, pe care Codul Penal nu o acoperă. Aici trebuie să amintim

Ordonanţa nr. 130/2000 privind regimul juridic al contractelor la distanţă[16], defineşte la rândul său o serie de termeni utili în găsirea definirii căutate, şi anume:

- *tehnică de comunicaţie la distanţă* - orice mijloc ce poate fi utilizat pentru încheierea unui contract între comerciant şi consumator şi care nu necesită prezenţa fizică simultană a celor două părţi;
- *operator de comunicaţie* - orice persoană fizică sau juridică a cărei activitate profesională constă în a pune la dispoziţie comerciantului una sau mai multe tehnici de comunicaţie la distanţă.

Tehnicile de comunicaţie la distanţă sunt prevăzute în anexa care face parte integrantă din ordonanţă, acestea fiind după cum urmează: a) imprimat neadresat; b) imprimat adresat; c) scrisoare tipizată; d) publicitate tipărită cu bon de comandă; e) catalog; f) telefon cu intervenţie umană; g) telefon fără intervenţie umană (automat de apel, audiotext); h) radio; i) videofon (telefon cu imagine); j) videotext (microordinator, ecran Tv cu tastatură sau ecran tactil); k) poştă electronică (e-mail); l) telecopiator (fax); m) televiziune (teleshopping).

Amintim aici, de asemenea, termenii specifici definiți de Legea nr. 365 din 7 iunie 2002 (republicată) privind comerţul electronic, potrivit dispozițiilor căreia:

1) *serviciu al societăţii informaţionale* – este orice serviciu care se efectuează utilizându-se mijloace electronice şi prezintă următoarele caracteristici:

a) este efectuat în considerarea unui folos patrimonial, procurat ofertantului în mod obişnuit de către destinatar;

b) nu este necesar ca ofertantul şi destinatarul sa fie fizic prezenţi simultan în acelaşi loc;

c) este efectuat prin transmiterea informaţiei la cererea individuală a destinatarului;

[16] Ordonanţa de Guvern nr. 130 din 31 august 2000 (republicată), privind protecţia consumatorilor la încheierea şi executarea contractelor la distanţă). Publicată în MONITORUL OFICIAL nr. 177 din 7 martie 2008. Republicată în temeiul art. V lit. a) din titlul III „Dispoziţii finale" al Legii nr. 363/2007 privind combaterea practicilor incorecte ale comercianţilor în relaţia cu consumatorii şi armonizarea reglementărilor cu legislaţia europeană privind protecţia consumatorilor, publicată în Monitorul Oficial al României, Partea I, nr. 899 din 28 decembrie 2007, dându-se textelor o nouă numerotare. Ordonanţa Guvernului nr. 130/2000 privind protecţia consumatorilor la încheierea şi executarea contractelor la distanţă, publicată în Monitorul Oficial al României, Partea I, nr. 431 din 2 septembrie 2000, a fost aprobată cu modificări şi completări prin Legea nr. 51/2003, publicată în Monitorul Oficial al României, Partea I, nr. 57 din 31 ianuarie 2003, şi a fost modificată prin Legea nr. 365/2002 privind comerţul electronic, publicată în Monitorul Oficial al României, Partea I, nr. 483 din 5 iulie 2002 şi republicată în Monitorul Oficial al României, Partea I, nr. 959 din 29 noiembrie 2006. Data intrării în vigoare : 07/03/2008

2. *mijloace electronice* - echipamente electronice şi reţele de cablu, fibra optică, radio, satelit şi altele asemenea, utilizate pentru prelucrarea, stocarea sau transmiterea informaţiei;
3. *furnizor de servicii* - orice persoana fizică sau juridică ce pune la dispoziţie unui număr determinat sau nedeterminat de persoane un serviciu al societăţii informaţionale;
4. *destinatar al serviciului sau destinatar* - orice persoana fizică sau juridică ce utilizează, în scopuri comerciale, profesionale sau de alta natură, un serviciu al societăţii informaţionale, în special în scopul căutării de informaţii sau al furnizării accesului la acestea;
5. *consumator* - orice persoană fizică ce acţionează în alte scopuri decât cele ale activităţii sale comerciale sau profesionale.

Totodată, trebuie spus că din perspectiva art. 35 din Legea nr. 161/2003, Titlul III - prevenirea şi combaterea criminalităţii informatice:
a) prin *„furnizor de servicii”* se înţelege:
- orice persoană fizică sau juridică ce oferă utilizatorilor posibilitatea de a comunica prin intermediul sistemelor informatice;
- orice altă persoană fizică sau juridică ce prelucrează sau stochează date informatice pentru persoanele prevăzute la pct. 1 şi pentru utilizatorii serviciilor oferite de acestea;
b) prin *„date referitoare la traficul informaţional”* se înţelege orice date informatice referitoare la o comunicare realizată printr-un sistem informatic şi produse de acesta, care reprezintă o parte din lanţul de comunicare, indicând originea, destinaţia, ruta, ora, data, mărimea, volumul şi durata comunicării, precum şi tipul serviciului utilizat pentru comunicare;
c) 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 orice alte date care pot conduce la identificarea utilizatorului.

Coroborând aceste dispoziţii legale, expresia ”terminal de comunicaţii” include în mod evident şi sistemele informatice, ca echipamente electronice, dar şi reţele de cablu, fibra optică, radio, satelit şi altele asemenea, utilizate pentru prelucrarea, stocarea sau transmiterea informaţiei.

În privința definirii punctului terminal al rețelei, găsim o astfel de prevedere în Legea nr. 304/2003 pentru serviciul universal și drepturile utilizatorilor cu privire la rețelele și serviciile de comunicații electronice, republicată[17], care în art.2 litera f), precizează că acesta este punctul fizic la care

[17] Republicată în Monitorul Oficial, Partea I nr. 343 din 5 mai 2008. Republicată în temeiul prevederilor art. IX din Ordonanța de urgentă a Guvernului nr. 70/2006, privind modificarea și completarea unor acte normative din domeniul comunicațiilor electronice și serviciilor poștale, publicată în Monitorul Oficial al României, Partea I, nr. 810 din 2 octombrie 2006, dându-se textelor o noua numerotare. Ordonanța de urgentă a Guvernului nr. 70/2006 a fost

unui abonat i se furnizează accesul la o rețea publică de comunicații; în cazul rețelelor care utilizează comutarea sau rutarea, punctul terminal este identificat prin intermediul unei adrese specifice de rețea (IP), care poate fi asociată numărului sau numelui unui abonat.

Definirea punctuală specifică a terminalului de comunicații o regăsim însă în Hotărârea Guvernului nr. 88/2003, privind echipamentele radio şi echipamentele terminale de telecomunicaţii şi recunoaşterea mutuală a conformităţii acestora, republicată[18], care în art. 5 litera d), arată că *echipamentul terminal de telecomunicaţii* este un produs sau o parte componentă relevantă din acesta, care permite comunicaţia şi care este destinat să fie conectat direct ori indirect prin orice mijloace la interfeţele reţelelor publice de comunicaţii. Același articol mai definește astfel termenii asociați de:

a) *aparat* - orice echipament care este fie echipament radio, fie echipament terminal de telecomunicaţii sau amândouă;

b) *reţea de comunicaţii electronice* - sistemele de transmisie şi, acolo unde este cazul, echipamentele de comutare sau rutare, precum şi orice alte resurse, care permit transportul semnalelor prin fir, radio, fibră optică sau orice alte mijloace electromagnetice, incluzând reţelele de comunicaţii prin satelit, reţelele fixe, cu comutare de circuite sau de pachete, inclusiv internet şi reţelele mobile terestre, sistemele de transport al energiei electrice, în măsura în care sunt utilizate în scopul transmiterii de semnale, reţelele utilizate pentru transmiterea comunicaţiei audiovizuale şi reţelele de cablu TV, indiferent de tipul informaţiei transportate;

e) *echipament radio* - un produs sau o parte componentă relevantă a acestuia, capabil să comunice prin intermediul emisiei şi/sau recepţiei undelor radio utilizând spectrul alocat radiocomunicaţiilor terestre/spaţiale;

f) *unde radio* - unde electromagnetice cu frecvenţe cuprinse între 9 kHz şi 3.000 GHz, care se propagă în spaţiu fără ghidare artificială;

g*) interfaţă* - punct terminal al reţelei, care este punctul de conexiune fizică la nivelul căruia utilizatorului îi este asigurat accesul la reţeaua publică de comunicaţii, sau o interfaţă radio specificând calea radio între echipamente.

---

rectificată în Monitorul Oficial al Romaniei, Partea I, nr. 899 din 6 noiembrie 2006 și aprobată cu modificări și completări prin Legea nr. 133/2007, publicată în Monitorul Oficial al României, Partea I, nr. 355 din 24 mai 2007. Legea nr. 304/2003 pentru serviciul universal și drepturile utilizatorilor cu privire la rețelele și serviciile de comunicații electronice a fost publicată în Monitorul Oficial al Romaniei, Partea I, nr. 551 din 31 iulie 2003.

[18] Republicată în temeiul art. II din Hotărârea Guvernului nr. 236/2004 pentru modificarea şi completarea Hotărârii Guvernului nr. 88/2003 privind echipamentele radio şi echipamentele terminale de telecomunicaţii şi recunoaşterea mutuală a conformităţii acestora, publicată în Monitorul Oficial al României, Partea I, nr. 191 din martie 2004, dându-se articolelor o nouă numerotare. Hotărârea Guvernului nr. 88/2003 a fost publicată în Monitorul Oficial al României, Partea I, nr. 94 din 14 februarie 2003.

Articolul 5 litera k), defineşte şi termenul de *interferenţă prejudiciabilă*, ca fiind interferenţa care pune în pericol funcţionarea unui serviciu de radionavigaţie sau a altor servicii de siguranţă ori care degradează serios, împiedică sau întrerupe repetat un serviciu de radiocomunicaţii ce funcţionează potrivit legislaţiei în vigoare.

Extrem de important din perspectiva întrebărilor ridicate de fenomenul wardriving, în art.2 din Hotărâre se arată că aceasta se aplică şi *aparatului* definit la art. 5 lit. a), care include, ca o parte integrantă sau ca un accesoriu, un dispozitiv de uz medical, inclusiv un dispozitiv de uz medical activ, implantabil, în înţelesul prevederilor Legii nr. 176/2000 privind dispozitivele medicale, republicată.

Hotărârea transpune Directiva 1999/5/CE a Parlamentului European şi a Consiliului privind echipamentele radio şi echipamentele terminale de telecomunicaţii şi recunoaşterea mutuală a conformităţii acestora.

Deci, în sensul legii, terminalul de comunicații poate fi definit ca un echipament electronic sau o componentă a unui echipament electronic care funcțional asigură comunicaţia şi care sunt destinate conectării directe ori indirecte, prin orice mijloace, la interfeţele reţelelor de comunicaţii.

Sub aspect informatic, echipamentul electronic trebuie să asigure prelucrarea automată a datelor, cu ajutorul unui program informatic[19].

d. Concluzii. Prin cele arătate mai sus am încercat astfel să găsim raţiunile şi să întrevedem sensurile unei reglementări penale noi, depăşind într-o oarecare măsură, scepticismul unora dintre specialiştii din domeniu la apariția textului de lege.

Reglementarea ne situează şi de această dată de partea ţărilor care s-au grăbit să implementeze cele mai noi strategii de prevenire și combatere a criminalității informatice.

Pe de altă parte, aşa cum am mai arătat, lucrarea noastră încearcă un exercițiu mai profund de imaginație, prin dorința de a releva concepte noi, unele deși enunțate nedezvoltate și implicit neintegrate, în măsură să contribuie la regândirea fundamentelor dreptului penal în acord cu realități sociale situate dincolo de percepția fizică, așa cum este spațiul virtual.

Violarea domiciliului virtual poate fi astfel la fel de justificată la reglementare cum legiuitorul a făcut posibilă încriminarea furtului folosinței unui terminal de comunicații sau folosința unui astfel de terminal racordat fără drept la o rețea, când aceasta a cauzat o pagubă.

Acoperă dispozițiile art. 42 din Legea nr.161/2003 care incriminează accesul ilegal la un sistem informatic situația de fapt descrisă în teza a II-a a textului încriminator? Amintim aici că, potrivit acestui articol, accesul, fără drept, la un sistem informatic constituie infracţiune, iar dacă fapta este săvârşită

[19] Exemple: computer personal (PC), două sau mai multe calculatoare conectate prin cablu fără fir (wireless), reţea de calculatoare ansamblu de tip calculator-periferice (imprimantă, dispozitive de stocare externe, scannere etc).

în scopul obţinerii de date informatice, se pedepseşte cu mai grav. De asemenea, dacă faptele sunt săvârşite prin încălcarea măsurilor de securitate, pedeapsa este şi mai gravă.

Noul Cod Penal prevede, la rândul său, în dispoziţiile art. 360(1) că accesul, fără drept, la un sistem informatic se pedepseşte cu închisoarea sau cu amenda. Dacă fapta este săvârşită în scopul obţinerii de date informatice, se pedepseşte cu închisoarea.

De asemenea, dacă fapta a fost săvârşită cu privire la un sistem informatic la care, prin intermediul unor proceduri, dispozitive sau programe specializate, accesul este restricţionat sau interzis pentru anumite categorii de utilizatori, pedeapsa este închisoarea mai gravă.

Ambele texte din lege încriminează fapta de acces ilegal la un sistem informatic într-o variantă tip şi două variante agravate, atunci când accesul este săvârşit în scopul obţinerii de date informatice, respectiv când fapta a fost săvârşită prin încălcarea măsurilor de securitate.

Cu referire la teza I din art 299 alin.2, suntem în mod evident în fața unui concurs de infracțiuni. Dar, este evident că prin acțiunea de folosire a unui terminal de comunicații racordat fără drept la rețea, terminal care poate fi propriu, deținut în mod licit, nu are loc un acces ilegal al sistemul informatic și implicit la datele informatice stocate în acesta.

Reamintim că *accesul*, presupune intrarea în tot sau numai într-o parte a sistemului informatic, metoda de comunicare fiind fără relevanță. Într-o formă simplă, accesul fără drept la un sistem informatic presupune un contact al făptuitorului cu tehnica de calcul prin intermediul echipamentelor sau diverselor componente ale sistemului. Utilizarea acestor dispozitive se transpune în solicitări către unitatea centrală a sistemului, care va procesa date ori va rula programe de aplicaţii în beneficiul intrusului.

Va exista acces ilegal şi în cazul în care intrusul, utilizând de la distanţă propriile echipamente periferice, va găsi şi va utiliza o cale externă de intrare într-un alt sistem de calcul, vorbind astfel de accesarea unei alte staţii de lucru aflate într-o reţea.

Mai nuanţat[20], prin „acces” se înţelege intrarea în tot sau într-o parte a unui sistem informatic, capacitatea de a lansa comenzi, de a accesa date informatice sau de a efectua alte operaţiuni informatice, fie direct de la o tastatură, fie prin intermediul unei reţele informatice.

Subliniem şi de această dată că, potrivit Convenţiei europene privind criminalitatea informatică, simpla trimitere a unui mesaj electronic sau fişier către un sistem informatic nu poate fi considerată „acces”. De asemenea, metoda folosită pentru realizarea accesului ilegal nu prezintă relevanţă pentru existenţa infracţiunii.

---

[20] I.Vasiu, L.Vasiu, *Prevenirea criminalităţii informatice*, Ed.Hamangiu, Bucureşti 2006, p.78.

Într-o altă accepţiune[21], prin „acces" înţelegem „a programa, a executa un program, a intercepta, a instrui, a comunica, a depozita/arhiva/stoca în a recupera date din sau în oricare altă folosinţă a unei surse oferită de computere, incluzând date sau programe pentru computere, sisteme de computere, reţele de computere sau baze de date".

Accesul poate fi prezentat într-o manieră foarte largă prin stabilirea unei comunicaţii cu sistemul, cel mai adesea sub o formă activă, ca fiind acţiunea prin care se permite penetrarea sistemului.[22]

Este penetrat sistemul în raţiunea legii penale examinate? Este stabilită o comunicaţie cu sistemul. În opinia noastră nu, astfel că demersul nostru este justificat, iar soluţia propusă posibilă.

C. Spălarea de bani în spaţiul virtual.

Definită succint, spălarea de bani este o modalitatea prin care infractorii ascund originea şi posesia reală a veniturilor ce provin din activităţile lor ilegale.

Potrivit art. 23 din Legea nr. 656/2002 pentru prevenirea şi sancţionarea spălării banilor, precum şi pentru instituirea unor măsuri de prevenire şi combatere a finanţării actelor de terorism,[23] prin spălarea banilor se înţelege:

" a) schimbarea sau transferul de bunuri, cunoscând că provin din săvârşirea de infracţiuni, în scopul ascunderii sau al disimulării originii ilicite a acestor bunuri sau în scopul de a ajuta persoana care a săvârşit infracţiunea din care provin bunurile să se sustragă de la urmărire, judecată sau executarea pedepsei;

b) ascunderea sau disimularea adevăratei naturi a provenienţei, a situării, a dispoziţiei, a circulaţiei sau a proprietăţii bunurilor ori a drepturilor asupra acestora, cunoscând că bunurile provin din săvârşirea de infracţiuni;

c) dobândirea, deţinerea sau folosirea de bunuri, cunoscând că acestea provin din săvârşirea de infracţiuni".

Spălarea de bani este un proces adesea complex, prin care se dă o aparenţă de legalitate unor profituri obţinute ilegal de către infractori, care fără a fi compromişi, beneficiază ulterior de veniturile respective.

Procesul presupune practic trei etape esenţiale, incluzând *plasarea* banilor iliciţi, *stratificarea* sau ascunderea şi *integrarea*, adică introducerea banilor în circuitul licit.

O deosebită importanţă prezintă astfel, faza intermediară, de anonimizare, secretul operaţiunilor fiind foarte important.

Secretul bancar asigură sub acest aspect un anumit nivel de securitate al beneficiarilor acestui tip de serviciu, dar paradisurile fiscale prin natura lor fizică

---

[21] T. Amza, C. Amza, *Criminalitatea informatică*, Ed. Lumina Lex, Bucureşti, 2003, p.14.

[22] A. Lucas, J. Deveze, J. Frayssinet, *Droit de l'informatique et de l'Internet*, Ed. Themis, Paris, 2001, p. 681, citaţi în D.Gărăiman, *op.cit*., p.305.

[23] Publicată în Monitorul Oficial, Partea I nr. 904 din 12 decembrie 2002.

și posibilitatea de monitorizare a comunicațiilor nu sunt lipsite de vulnerabilități din perspectiva unei anchete judiciare.

Există totuși, mai nou, un loc unde investigatorii pot ajunge foarte greu, unde comunicațiile sunt aproape imposibil de interceptat, iar stratificarea banilor poate avea loc cu ușurință: lumile virtuale.

Așa cum arătam în cuprinsul acestui capitol, printre trăsăturile definitorii ale acestor lumi se numără avatarul, corespondentul digital al utilizatorului, o entitate virtuală a cărei înfățișare poate fi ușor schimbată, dar și moneda proprie, respectiv convertibilitatea acesteia.

Aceleași lumi virtuale sunt deja locuri unde comerțul, afacerile, în general sunt la fel de intense și profitabile ca în lumea reală.

Aici, banii obținuți ilicit pot fi utilizați prin schimb valutar pentru a cumpăra spații, bunuri, servicii, pe care, în aceeași lume le poți tranzacționa, valuta obținută convertită în bani reali echivalând în final cu un venit licit, ușor integrabil, posibilitatea de urmărire a provenienței acestora, cel puțin în prezent, fiind aproape exclusă.

Acest lucru ne-a fost confirmat cu ocazia mai multor prezentări la care am participat în cursul anilor 2009-2010 alături de investigatori specializați ai U.S. Secret Service, aceștia descriind dificultățile tehnice insurmontabile pe care le implică o investigație judiciară în acest mediu.

În contextul celor deja spuse despre lumea virtuală, trebuie specificat că ofițerii sub acoperire în acest caz nu pot fi decât avataruri ale investigatorilor, care după un scenariu aproape identic celui din lumea reală trebuie să găsească indicii și să meargă pe firul acestora, lipsiți de cele mai multe ori de posibilitățile tehnice de interceptare a comunicațiilor, amintind exemplificativ, deplina confidențialitate prin nivelul excesiv de criptare de care se bucură, cel puțin, utilizatorii rețelei Skipe[24].

---

[24] **Skype** este un cuvânt artificial care desemnează un software gratuit, ce permite utilizatorilor să efectueze convorbiri telefonice prin Internet, utilizând tehnici de tip *Voice over IP* (*VoIP*). Apelurile spre alți utilizatori Skype sunt gratuite, indiferent de orașele și țările de unde se vorbește, în vreme ce apelurile la telefoanele obișnuite analoage din rețeaua clasică (fixă) sunt de obicei contra cost. Calitatea acustică și video a convorbirii este de obicei foarte bună. Funcționalități adiționale gratuite: telefonie video, mesagerie instantă de tip *chat*, transfer de fișiere, conferințe telefonice și videoconferințe. Skype a fost inițial scris de specialiștii estonieni Ahti Heinla, Priit Kasesalu și Jaan Tallinn. Acesta din urmă este și autorul sistemului de *File sharing* numit Kazaa. În 2003 suedezul Niklas Zennström și danezul Janus Friis au întemeiat compania Skype Group cu sediul la Luxemburg. Actualmente compania are filiale în Londra, Tallinn, Tartu, Stockholm, Praga și San José, California, SUA. După inaugurarea service-ului pentru Skype, software-ul a cunoscut o răspândire rapidă în aproape toată lumea. În septembrie 2005 compania Skype a fost achiziționată de către compania americană eBay la prețul de 2,6 miliarde USD

Economia unei lumi virtuale de genul SecondLife nu are regulile fiscale din economia reală. Libertatea de acțiune este practic neîngrădită, iar formalismul documentelor inexistent, garanțiile tranzacțiilor fiind asigurate prin aceleași metode pe care comerțul on-line le utilizează deja în lumea reală.

Fenomenul există, gradul de pericol social este indiscutabil, dar avem oare asigurată încriminarea specifică a acestuia?

Legea vorbește în toate modalitățile infracționale ale spălării de bani despre bunuri. În înțelesul obișnuit, acestea sunt corporale, materiale, având o existență fizică, perceptibilă prin simțurile noastre vizual, tactil. Acestora se pot adăuga bunurile incorporale tranzacționabile, dar și bunurile virtuale, care prin trăsăturilor lor deja enunțate, deși perceptibile senzorial nu au o existență fizică reclamând însă, prin corespondența real-virtual, trăsăturile bunurilor corporale, cu existență fizică.

În acest sens, datorită progresului tehnologic, bunurile virtuale corporale au posibilitatea de a fi percepute tridimensional, putând fi mutate, schimbate sau, mai general, utilizate asemenea bunurilor fizice. Mai mult, prin asocierea unei valori, cum de altfel se întâmplă în realitate pe site-urile de vânzare a acestor bunuri, devin valori patrimoniale, unele extrem de importante prin designul realizat de celebritățile domeniului[25].

Ca în cazul furtului de bunuri din spațiul virtual, legea nu asigură corespondența trăsăturilor și nu asociază valoare economică acestei categorii noi de bunuri.

Rămâne o zonă în care legiuitorul trebuie să intervină și să adapteze, în opinia noastră, textul legal, făcându-l aplicabil și spațiului virtual, prin simpla definire extensivă a bunurilor sau precizarea faptului întinderii reglementării și asupra activităților ilicite din spațiul virtual.

Aceasta este însă partea simplă, ușor de obiectivat a lucrurilor. Lumea virtuală oferă posibilități încă neexplorate de absorbție, stratificare și chiar integrare inițială a banilor spălați, putând reprezenta o interfață ideală în acest scop.

Atractivitatea domeniului și a mediului Internet în general este dată de accesul facil la acesta, caracterul impersonal al comunicării și rapiditatea tranzacțiiilor, sau, altfel spus, ușurința de acțiune, posibilitatea de camuflare, ascundere a identității reale și finalizarea operațiunii într-un timp atât de scurt, astfel încât ștergerea urmelor și pierderea în anonimat pot avea loc, exagerând puțin, aproape concomitent cu inițierea acesteia.

Amintim, totodată, că aceste trăsături oferă posibilitatea ca Internetul să poată fi folosit ca o umbrelă confortabilă pentru tranzacții și în afara lumilor virtuale, posibilitățile de transfer a banilor fără posibilitatea de monitorizare

[25] A se vedea de exemplu https://marketplace.secondlife.com/p/Switcheroo-Gold-Edition-Bedroom-Furniture-On-Introductory-Sale-Low-Prim-Bed/1232545?id=1232545&slug=Switcheroo-Gold-Edition-Bedroom-Furniture-On-Introductory-Sale-Low-Prim-Bed.

fiind nenumărate, necesitând încriminarea și sancționarea mai gravă a faptelor comise în această modalitate, măsura fiind benefică și sub aspectul asigurării securității sociale în acest spațiu virtual.

Legalitatea încriminării necesită o astfel de măsură, viitorul despre care ar părea că vorbim, fiind deja prezentul erei Internet, iar a preveni prin încriminări adecvate un fenomen cu o dinamică greu de transpus în statistici, este mai ușor decât a combate sau utopic spus, a eradica acel fenomen.

Să nu uităm totodată că spălarea de bani este poate cea mai importantă sursă de finanțare a terorismului, flagel care în contextul indiscutabil al globalizării a devenit cea mai gravă amenințare a vremurilor de pace.

În spațiul normativ național, noțiunile de ”spălare de bani informatică” (“Cybermoneylaundering”-*eng.*) sau de ”terorism informatic” (Cyberterrorism”-*eng.*) nu au în prezent nici un ecou, subiectul nefiind studiat şi tratat în consecință, pierzându-se în conceptele generale uzuale, care dau substanță domeniului criminalității informatice, prin intermediul practicii judiciare.

***

La o simplă trecere în revistă a reglementările penale naționale, se poate observa cu ușurință că infracţiunile îndreptate împotriva datelor şi sistemelor informatice ori comise prin intermediul acestora sunt abordate diferit, neunitar, folosind o terminologie diversificată de la stat la stat.

Sunt necesare prevederi comune care să reglementeze acest domeniu de activitate, Convenţia Consiliului Europei asupra Criminalităţii Informatice, semnată la Budapesta la 23 noiembrie 2001, fiind un astfel de instrument.

La fel de importante, datorită caracterului transfrontalier al acestui tip de criminalitate, sunt dispoziţiile procedurale şi de asistenţă judiciară, care prezintă instrumente specifice combaterii acestui tip de infracţiuni, aspecte neacoperite de acordurilor existente.

În ceea ce priveşte reglementările de drept substanţial, majoritatea statelor incriminează ca infracţiuni îndreptate împotriva confidenţialităţii, integrităţii şi securităţii datelor şi sistemelor informatice accesul ilegal la un sistem informatic şi alterarea integrităţii datelor. Foarte puţine ţări sunt cele care incriminează distinct interceptarea ilegală a unei transmisii de date informatice, frauda informatică sau falsul informatic, acestea fiind prevăzute printre infracţiunile de drept comun.

Aspectele prezentate reprezintă tot atâtea provocări pentru procesul legislativ, prin specificitatea lor unele dintre împrejurările arătate necesitând o reglementare distinctă viitoare, în acord cu evoluția fenomenului criminalității informatice.

De lege ferenda, furtul de bunuri din spațiul virtual, furtul de identitate în spațiul virtual, violarea domiciliului informatic, violența virtuală, spălarea de bani informatică și terorismul cibernetic, ar trebui încriminate, fie distinct, fie prin modificarea corespunzătoare a textelor legale clasice.

Abordarea domeniului ar trebui să aibă un caracter profund anticipativ și progresist, plecând de la premisa că într-un sistem social integrat, complet computerizat, poți comite chiar și crime de la distanță.

Reacția sistemului ar trebui să însemne și pedepse substanțiale, pe măsură, amintind aici, în final, replica acidă, dar corectă a unui investigator șef al US Secret Service care, informat cu ocazia unui seminar asupra politicii de reducere drastică a limitelor speciale de pedeapsă pentru infracțiunile informatice încriminate de legea românească, spunea că nepăsarea transmisă de politicile penale se datorează poate și faptului că victimele nu sunt, de regulă, concetățenii noștri și sistemul nostru comercial, ci alții, mai ales cetățenii americani sau din alte țări dezvoltate, pentru care tehnologiile prezentului sunt ceea ce pentru noi reprezintă tehnologiile viitorului.

Bibliografie:

I. Tratate, cursuri, monografii, articole româneşti:

[1]T. Amza, CP. Amza, *Criminalitatea Informatică*, Ed. Lumina Lex, Bucureşti, 2003
[2]G. Antoniu, *Noul cod penal. Codul penal anterior. Studiu comparativ*, Ed. AII Beck, Bucureşti, 2004
[3]G. Antoniu, *Vinovăţia penală*, Ed. Academiei Române, Bucureşti, 1995
[4]G. Antoniu, C. Bulai, *Practica judiciară penală*, vol. I, Partea generală, Ed. Academiei, Bucureşti, 1988
[5]G. Antoniu, C. Bulai, *Practica judiciară penală*, voi. II, Partea generală, Ed. Academiei, Bucureşti, 1990
[6]G. Antoniu, C. Bulai, *Practica judiciară penală*, vol. III, Partea specială, Ed. Academiei, Bucureşti, 1992
[7]G. Antoniu, E. Dobrescu, T. Dianu, G. Stroe, T. Avrigeanu, *Reforma legislaţiei penale*, Ed. Academiei, Bucureşti, 2003
[8]C. Balaban, *Infracţiuni prevăzute în legi speciale care reglementează domeniul comerţului*, Ed. Rosetti, Bucureşti, 2005
[9]C. Barbu, *Aplicarea legii penale în spaţiu şi timp*, Ed. Ştiinţifică, Bucureşti, 1972
[10]L. Bird, *Internet. Ghid complet de utilizare*, Ed. Corint, 2008
[11]L. Klander, *Anti-Hacker*, Ed. All Educaţional, Bucureşti, 1998
[12]Al. Boroi, Ghe. Nistoreanu, *Drept penal. Partea generală*, Ed. All Beck, Bucureşti, 2004
[13]Al. Boroi, Ghe. Nistoreanu, *Drept penal. Partea specială*, Ed. All Beck, Bucureşti, 2004
[14]C. Bulai, *Manual de drept penal, partea generală*, Ed. All Beck, Bucureşti, 1997
[15]M.Dobrinoiu, *Infracţiuni în domeniul informatic*, Ed.C.H.Beck, Bucureşti, 2006
[16]M.A.Hotca, M. Dobrinoiu, *Infracţiuni prevăzute în legi speciale.Comentarii şi explicaţii*, Ed. C.H.Beck, Bucureşti, 2008
[17]M.A.Hotca, M.Dobrinoiu, *Elemente de drept penal al afacerilor*, Ed.C.H. Beck, Bucureşti,2009
[18]T. Dima, *Drept penal. Partea generală*, vol. I - 2004, vol. II -2005, Ed. Lumina Lex, Bucureşti
[19]V. Dobrinoiu, *Drept Penal. Partea Specială. Teorie şi Practică Judiciară*, Ed. Lumina Lex, Bucureşti, 2002
[20]V. Dobrinoiu, N. Conea, C.R. Romiţan, N. Neagu, C. Tănăsescu, M. Dobrinoiu*, Drept Penal. Partea specială*, vol. II, Ed. Lumina Lex, 2004,
[21]V. Dobrinoiu, Ghe. Nistoreanu şi colab., *Drept penal. Partea specială*, Ed. Europa Nova,

1997
[23]D. Oprea, *Protecţia şi securitatea informaţiilor*, Ed.Polirom, Iaşi, 2003
[24]D.Gărăiman, *Dreptul şi informatica*, Ed.All Beck, Bucureşti, 2003
[25]I.Georgescu, *Infracţiunile informatice prevăzute de Legea nr.161/2003*, Buletin documentar nr.3/2005 al P.N.A./D.N.A., http://www.pna.ro/text_doctrina.jsp?id=46
[26]I.Vasiu, L.Vasiu, *Prevenirea criminalităţii informatice*, Ed. Hamangiu, 2006
[27]I.Vasiu, *Informatica juridică şi drept informatic*, Ed. Albastră, Cluj-Napoca, 2002
[28]I. Vasiu şi L. Vasiu, *Totul despre hackeri*, Ed. Nemira, 2001
[29]L. Vasiu şi I. Vasiu, *Internet - Ghid de navigare*, Ed. Albastră, Cluj-Napoca, 1996.
[30]C.Voicu, A.Boroi, I.Molnar, M.Gorunescu, S.Corlăţeanu, *Dreptul penal al afacerilor*, ediţia a 4-a, Ed.C.H.Beck, Bucureşti, 2008
[31]B. Predescu, A. Duşcă, *Dreptul comunitar al afacerilor,* Ed. Universitaria, Craiova, 2002.
[32]V.V. Patriciu, *Criptografia şi securitatea reţelelor de calculatoare*, Ed. Tehnică, Bucureşti, 1994
[33]V. V. Patriciu*, Sisteme electronice de plăţi*, http://www.afaceri.net
[34]V.V.Patriciu, I.Vasiu, S.G.Vasiu, *Informatică juridică*, vol.I, Ed.All Beck, 1999
[35]M.Cioată*, Plăţi electronice*, http://www.afaceri.net.
[36]M. Sauca, *Infracţiuni privind comerţul electronic*, Ed. Mirton, Timişoara, 2005,
[37]M. Pătrăuş, C.F.Uzvat, *Pornografia infantilă în reglementările actuale*, în Dreptul nr. 4/2003
[38]T. Vasiliu şi colab., *Codul penal comentat şi adnotat*, Ed. Didactică şi Enciclopedică, Bucureşti, 1975,
[39]D. Vasilache*, Comerţul electronic, eComerţ*, Revista Română de dreptul afacerilor nr. 1/2005
[40]I. Dogaru, *Drept civil român*, Tratat, vol.I, Ed.Europa, Craiova, 1996,
[41]I.Dogaru, P. Drăghici, *Drept civil. Teoria generală a obligaţiilor*, Ed.Themis, 2000*,* p. 411.
[42]C.Stătescu, C. Bîrsan, *Tratat de drept civil. Teoria generală a obligaţiilor,* Ed. Academiei Republicii Socialiste România, Bucureşti, 1981, p. 309-310.
[43]M.Zainea, R.Simion, *Infracţiuni în domeniul informatic. Culegere de practică judiciară*., Ed.C.H.Beck, Bucureşti, 2009.
[44]T. Dima, A.G. Păun, *Droguri ilicite (Legea 143/2000, jurisprudenţă şi comentarii)*, Ed. Universul Juridic, Bucureşti, 2010
[45]I.Gârbuleţ, *Traficul şi consumul ilicit de droguri. Studiu de legislaţie, doctrină şi jurisprudenţă*, Ed.Hamangiu, Bucureşti, 2008
[46]V. Dongoroz, S. Kahane, I. Oancea, I. Fodor, N. Iliescu, C. Bulai, R. Stănoiu, V. Roşca, *Explicaţii teoretice ale Codului Penal român*, vol. IV, Ed. Academiei Române, Bucureşti*,* 1972, reeditare 2003
[47]V. Breban, *Dicţionar al limbii române contemporane de uz curent*, Ed. Ştiinţifică şi Enciclopedică. Bucureşti, 1980.

II. Tratate, cursuri, monografii, articole străine:

[1]A. Lucas, J. Deveze, J. Frayssinet, *Droit de l'informatique et de l'Internet*, Ed. Themis, Paris, 2001
[2]L.Vasiu, *A conceptual framework for e-fraud control in an integrated supply chain, proceedings of the european conference on information systems*, Turku, Finland, 2004
[3]S. Philippsohn, S. Thomas, *E-Fraud - What companies face today*, Computer Fraud & Security, 2003
[4]E. Barbry, *Le droit du commerce electronique de la protection…a la confiance*,

http://.club-internet,fr/cyberlexnet VeriSign Inc., www.verisign.com/products *A What Every Merchant Should Know About Internet Fraud*, 2003
[4]Cristian Radu, *Implementing Electronic Card Payment Systems*, Artech House, Computer Security Series, 2003, www.artechhouse.com
[5]B.Brun, *Les mecanismes de paiement sur Internet,* 20 octombrie 1999, http://www.juriscom.net/universite/doctrine/article5.htm
[6]J.Leprâtre, *Le contrat dans le commerce electronique*, http://jullep.free.fr/computer/MemoireComputer.htm
[7]J. Arquilla, D. Ronfeldt, M. Zanini, *Networks, Netwar, and Information-Age Terrorism, Countering the New Terrorism*, RAND, 1999
[8]P. Bak, How Nature Works: *The Science of Self-Organizcd Critically*, Springer, Berlin, 1996
[9]D.I. Bainbridge, *Computers and the Law*, Ed. Pitman, Londra, 1990
[10]A. Bertrand, *Les contracts informatiques*, Ed. Les Paques, Paris, 1983
[11]M. Veron, *Droit penal special*, Armând Colin, Paris, 1998
[12]R. Vonin, *Precis de droit penal special*, Ed. Dalloz, Paris, 1953
[13]Auestad G. & Roland, E. (2005). Mobbing og mobiltelefon. *Spesialpedagogik, 4*, 4-11.
Balding, J. (2005). *Young People in 2004: the health-related behaviour questionnaire results for 40,430 young people between the ages of 10 and 15*. Schools Health Education Unit: Exeter.
[14]Barnfield, G. (2005). *Happy Slaps: fact and fiction. Rumours of an epidemic of videophone violence have been greatly exaggerated*. http://www.spiked-online.com/Articles/0000000CAAD3.htm (20/12/2006).
[15]Beran, T. & Li, Q. (2005). Cyber-Harassment: A new method for an old behavior. *Journal of Educational Computing Research, 32(3),* 265–277.
[16]Besley, B. (2005). *Cyberbullying: An emerging threat to the always on generation*. http://www.cyberbullying.ca (20/12/2006).
[17]Burgess-Proctor, A., Patchin, J.W. & Hinduja, S. (2006). *Cyberbullying: The victimization of adolescent girls*.
http://www.cyberbullying.us/cyberbullying_girls_victimization.pdf (20/12/2006).
[18]Cascardi, M., Avery Leaf, S., O'Leary, K. D. & Slep, A. M. S. (1999). Factor structure and convergent validity of the Conflict Tactics Scale in high school students. *Psychological Assessment, 14*, 546-555.
[19] Prados, M.A. & Solano Fernández, M.I. (2005). *Sociedad de la información y su impacto en la familia*. Paper presented at Conference "Interrelación entre familias y educación. Su contribución a la sociedad actual". Oviedo.
[20]Hernández Prados, M.A. & Solano, M.I. (2006). *Acoso escolar en la red. Cyberbullying*. Paper presented at Virtual Educa Conference (http://www.virtualeduca.org). Bilbao.
Howard, D.E. & Wang, M.Q. (2003).
[21]Katz, J. E. (2006). *Magic in the air: Mobile communication and the transformation of social life***.** New Brunswick, NJ: Transaction Publishers.
[22]Li, Q. (2005). *New Bottle But Old Wine: A Research on Cyberbullying in Schools*. http://www.ucalgary.ca/~qinli/publication/cyber_chb2005.pdf (20/12/2007).
[23]Li, Q. (2006). Cyberbullying in schools: A research of gender differences. *School Psychology International, Vol. 27(2),* 157–170.
[24]Manke, B. (2005). *The Impact of Cyberbullying*. http://www.mindoh.com (1/12/2005).
[25]MNet (2001). *Young Canadians in a Wired World.* http://www.media-awareness.ca/english/special_initiatives/surveys/index.cfm (20/12/2006).
[26]MSN.uk (2006). *MSN cyberbullying report*. http://www.msn.co.uk/cyberbullying (20/12/2006).

[27]National Children's Home (2005). *Putting U in the picture-Mobile phone bullying survey 2005*. http://www.nch.org.uk (20/12/2006).
[28]Oliver, C. & Candappa, M. (2003). *Tackling bullying: listening to the views of children and young people*. Department for Education and Skills/ChildLine, Nottingham.
[29]Olweus, D. (1993). *Bullying at school: What we know and what we can do*. Oxford: Blackwell.
[30]Ortega, R. & Martín-Ortega, O. (2005). Convivencia. A positive approach to prevent violence through training for citizenship in Spain. In VV.AA. (eds.): *Bullying-Ijime* (pp154-174). Tokyo: Minerva Shobo.
[31]Patchin, J. W. & Hinduja, S. (2006). Bullies Move beyond the Schoolyard: A Preliminary Look at Cyberbullying. *Youth Violence and Juvenile Justice, 4(2),* 148-169.
[32]Phrases.com.uk (2006). *Happy slapping*. Phrases.com.uk (20/12/2006).
Poitras, M. & Lavoie, F. (1995).
[33]Smith, P., Mahdavi, J., Carvalho, M. & Tippet, N. (2006). *An investigation into cyberbullying, its forms, awareness and impact, and the relationship between age and gender in cyberbullying*. London: Anti-Bullying Alliance. http://www.anti-bullyingalliance.org.uk/downloads/pdf/cyberbullyingreportfinal230106_000.pdf (20/12/2006).
[34]Smith, P.K., Morita, Y., Junger-Tas, J., Olweus, D., Catalano, R. & Slee, P. (eds.) (1999). *The nature of school bullying: A cross-cultural perspective*. London: Routledge.
[35]Thorp, D. (2004). *Cyberbullies on The Prowl in Schoolyard*. http://australianit.news.com.au/articles/0,7204,9980900^15322^^nbv^15306,00.html (15/07/2004).
[36]Wikipedia (2006) *Happy slapping*. http://en.wikipedia.org/wiki/Happy_slapping (20/12/2006).
[37]Willard, N. (2004). *An Educator's Guide to Cyberbullying and Cyberthreats*. http://cyberbully.org/docs/cbcteducator.pdf (6/10/2005).
[38]Ybarra, M. L., & Mitchell, J. K. (2004). Online aggressor/targets, aggressors and targets: A comparison of associated youth characteristics. *Journal of Child Psychology and Psychiatry*, *45*, 1308-1316.

III. Legislaţie:

[1]Constituţia României (M. Of. nr. 767 din 31 octombrie 2003)
[2]Codul penal al României, republicat .
[3]Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei (M. Of. nr. 279 din 21 aprilie 2003)
[4]Legea nr. 64/2004 pentru ratificarea Convenţiei Consiliului Europei privind criminalitatea informatică (M. Of. nr. 343 din 20 aprilie 2004)
[5]Legea nr. 365/2002 privind comerţul electronic (M. Of. nr. 483 din 5 iulie 2002)
[6]Legea nr. 8/1996 privind dreptul de autor şi drepturile conexe (M. Of. nr. 60 din 26 martie 1996) modificată de Legea nr. 285/2004 pentru modificarea şi completarea Legii nr. 8/1996 privind dreptul de autor şi drepturile conexe (M. Of. nr. 587 din 30 iunie 2004) şi O.U.G. nr. 123/2005 pentru modificarea şi completarea Legii nr. 8/1996 privind dreptul de autor şi drepturile conexe (M. Of. nr. 843 din 19 septembrie 2005)
[7]Legea nr. 196/2003 privind prevenirea şi combaterea pornografiei (M. Of. nr. 342 din 20 mai 2003) modificată prin Legea nr. 496/2004 pentru modificarea şi completarea Legii nr. 196/2003 privind prevenirea şi combaterea pornografiei (M. Of. nr. 1070 din 18 noiembrie 2004)
[8]Legea nr. 455/2001 privind semnătura electronică (M. Of. nr. 429 din 31 iulie 2001)

[9]Ordinul ministrului comunicaţiilor şi tehnologiei informaţiei nr. 218/2004 privind procedura de avizare a instrumentelor de plata cu acces la distanta, de tipul aplicaţiilor Internet-banking, home-banking sau mobile-banking (M. Of. nr. 579 din 30 iunie 2004)
[10]Regulamentul Băncii Naţionale a României nr. 4/2002 privind tranzacţiile efectuate prin intermediul instrumentelor de plată electronică şi relaţiile dintre participanţii la aceste tranzacţii (M. Of. nr. 503 din 12 iulie 2002)
[11]Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date (M. Of. nr. 790 din 12 decembrie 2001)
[12]Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice (M. Of. nr. 1101 din 25 noiembrie 2004)
[13]Legea nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal (M. Of. nr. 391 din 9 mai 2005)
[14]Legea nr. 451/2004 privind marca temporală (M. Of. nr. 1021 din 5 noiembrie 2004)
[15]Legea nr. 589/2004 privind regimul juridic al activităţii electronice notariale (M. Of. nr. 1227 din 20 decembrie 2004)

IV. Resurse Internet:

1. http://www.crime-reasearch.org
2. http://cyberpolice.over-blog.com
3. http://foldoc.doc.ic.ac.uk
4. http://www.mir.es/policia
5. http://www.efrauda.ro
6. http://www.ic3.gov Internet Crime Complaint Centre
7. http://www.internetcrimeforum.org.uk
8. http://ifccfbi.gov Internet Fraud Complaint Centre
9. http://www.internetidentity.com Anti-phishing Consultancy
10. http://www.interpol.int/Public/TechnologyCrime
11. http://www.nhtcu.org National High Tech Crime Unit (UK)
12. http://www.webopedia.com Webopedia
13. http://www.netintercept.com Computer Forensics
14. http://www.forensicon.com E-discovery Specialists 15.http://www.world-check.com Terrorist Profile
16.http://www.centrex.police.uk Central Police Training and Development Authority
17. http://www.hightechcrimeinstitute.com
18. http://www.computerworld.com/security
19. http://www.wikien.info
20. http://www.legalmountain.com Computer Crime Legislation
21. http://www.ncalt.com National Centre for Applied Learning Technologies
22. http://www.govtsecurity.com 23.http://www.federalcrimes.com
24. http://www.scams.net
25. http://www.anti-spy.info
26. http://www.acunefix.com
27. http://rhizome.org/carni vore
28. http://www.pewinternet.org
29. http://www.kindercam.com
30. http://www.epic.org Centru de Informare pentru Confidenţialitate Electronică
31. http://www.eff.org/Privacy Electronic Frontier Foundation
32.http://www.privacyalliance.org Online Privacy Alliance
33. http://www.fbi.org/hq/lab/Carnivore Carnivore DiagnosticTool
34. http://www.cdt.org Centrul pentru Democraţie si Tehnologie

35. http://www.stopcarnivore.org
36. http://www.privacyfoundation.org/workplace
37. http://www.indentix.com
38. http://www.digitalpersona.com
39. http://www.viisage.com
40. http://www.gcn.com
41. http ://www.anonymizer.com
42. http://www.linuxsecurity.com
43. http://www.w3.org/P3P Proiect Platforma pentru Preferinţe de Confidenţialitate
44. http://dlis.gseis.ucla.edu/people/pagre/baccode.html
45. http://www.baselinemag.com Projects Security Cybercrime
46. http://www.fieldassociates.co.uk Computer Forensics
47. http://www.compendianet.com Computer Forensics
48. http://www.idefense.com iDEFENSE
49. http://www.gmu.edii/security/practices George Mason University
50. http://www.cert.org Computer Emergency Response Team
51. http://www.gocsi.com Institutul pentru Securitatea Calculatoarelor
52. http://www.safedwelling.com Jd Theft Solutions
53. http://www.infosyssec.org Security Portal for Information
System Security
54. http://www.zybex.org
55. http://www.iss.net Internet Security Solutions
56. http://www.securityfocus.com
57. http://www.spidynamics.com
58. http://www.isec.pl iSec Security Research
59. http://www.globaldirectsvcs.com
60. http://www.accessdata.com
61. http://www.es. georgetown.edu/~denning
62. http://www.cyberspacelaw.org
63. http://mobile.f-secure.com
64. http://www.bitpipe.com/rlist/term/cyberterrorism.html
65. http://enterprisesecurity.symantec.com/solutionfinder
66. http://www.psywarrior.com
67. http://www.nps.navy.mil/ctiw Centre on Terrorism and
Irregular Warfare
68. http://www.homelandsecurityx.com
69. http://cisr.nps.navy.mil Centre for information Systems
Security Studies and Research
70. http://www.infowarrior.org
71. http://www.terrorism.com
72. http://www.thehacktivist.com
73. http://www.csis.org
74. http://www.nsa.gov
75. http://www.thing.net/-rdom/ecd/EDTECD.html
76. http://www.gn.apc.org/pmhp/ehippies
77. http://www.telediritto.it
78. http://www.cirsfid.unibo.it/cirsfid
79. http://www.ciberspazioediritto.org
80. http://62.110.105.159/alsiud
81. http://www.giustizia.it

82. http://www.alfa-redi.org
83. http://www.frammella.it
84. http://www.interlex.it
85. http://www.ordineavocatimilano.it
86. http://www.slentopoli.com
87. http://www.delitosinformaticos.eom
88. http://www.cyberlawsa.co.za
89. http://www.lexinformatica.org/cybercrime
90. http://www.41aw.co.il
91. http://www.wittys.com/files/mab Firewall Penetration Testing
92. http://is-it-tiue.org Hackers Tricks
93. http://www.cs.princeton.edU/.sip/pub/spooling.htrnl
94. http://ori.careerexpo.com/pub/docsoftl 97/spoof.soft.htm
95. http://www.engarde.com/software/ipwatcheiTisks/overview.htm
96. http://gradeswwvv.acns.nvvu.edu/ist/snap/doc/sniffing.htm
97. http://www.cytechsys.com/detect.htm
98. http://www.kimsoft.com/Korea/usa-nel .htm
99. http://www.usdoj.gov/crime/cybercrime
100. http://microassist.com.mx/noticias/inteniet
101. http://www.observatoriodigital.net
102. http://www.itu.int/itut/studygroups/coml7/cssecurity.htm
103. http://www.learnsecurityonline.com
104. http://www.edu-central.com
105. http://www.techlawed.org/page.php?v=24&c=28page=cri me
106. http://www.acunetix.com
107. http://www.ssppyy.com
108. http://www.isfsecuritystandard.com/pdf/standard.pdf
109. http://www.tiac.net/users/smiths/anon/anonprob.html
110. http://www.iwf.org.uk Internet Watch Foundation
111. http://www.spamhaus.org/cyberattacks
112. http://www.govexec.com/story_page. cfm?articleid=32415&dcn=e_tcmg
113. http://www.fcw.com/article88417-O3-28-05
114. http://conventions.coe.int/Treaty/en
115. http://www.privacyinternational.org/issues/cybercrime
116. http://www.infinisource.com/features/cybercrime.html Premier Resource Center
117. http://www.cybercrime.admin.ch Switzerland Cyhercrime Coordonation Unit
118. http://www.nctp.org National Cybercrime Training Part-nership
119. http://www.jislegal.ac.uk/cybercrime/cybercrime.html
120. http://www.bespacific.com/mt/archives/cat_cybercrime.html
121. http://www.forensics.nl
122. http://www.southeastcybercrimesummit.com
123. http://www.lib.msu.edu/harris23/crimjust/cybercrim.html
124. http://www.icc-ccs.org/main International Chamber of Commerce Crime Services
125. http://cyber-rights.org/cybercrime
126. http://www.efa.org.au/Issues/Security Electronic Frontiers Australia
127. http://www.iwar.org.ulc/ecoespionage Information Warfare Site
128. http://www.digital-law.net/lJCLP/CyJ2004
129. http://www.internetpolicy.net/cybercrime Global Internet Policy Inițiative
130. http://www.wgig.org/docs/WP__cybersec.pdf
131. http://www.aph.gov.au

132. http://faculty.ncwc.edu/toconnor/315
133. http://www.iia.net.au/cybercrimecode.htm
134. http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeCommEN. htm
135. http://europa.eu.int/information_society/topics/telecomms/ internet/crime
136. http://www.cybertelecom.org/security/crime.htm
137. http://www.vaonline/doc_internet.html
138. http://www.cybercrimelaw.net Legislaţie internaţională în domeniul criminalităţii informatice
139. http://www.legi-internet.ro.
140. http://www.cybercash.com
141. http://www.firstvirtual.com
142. http://www.fstc.org
143. http://www.netchex.com
144. http://www.echeck.org
145. http://mondex.com