MINISTERUL AFACERILOR INTERNE

ACADEMIA DE POLIȚIE „Alexandru Ioan Cuza”

TEZĂ DE DOCTORAT

(REZUMAT)

COOPERAREA INTERNAŢIONALĂ ÎN DOMENIUL COMBATERII CRIMINALITĂŢII INFORMATICE

CONDUCĂTOR DE DOCTORAT:

PROF.UNIV. DR. LUCA IAMANDI

DOCTORAND:

GROPENEANU (DRAGOMIR) TICUŢA - ANTONELA

Teză elaborată în vederea obţinerii titlului de DOCTOR în „Ordine publică şi siguranţă naţională”

Bucuresti

2016

INTRODUCERE

Civilizaţia informatică de generaţie nouă este bazată pe accesibilitatea şi disponibilitatea informaţiei. Informaţia în societatea actuală îşi asumă rolul de proprietate naţională cu adevărat vitală, având valoare strategică importantă: aceasta poate fi cucerită sau distrusă iar de aceea apare necesitatea de a fi protejată prin drept. Drept consecinţă, dreptul trebuie să sufere o schimbare întru totul radicală impusă de revoluţia informaţională dreptul trebuie să ţină pasul cu societatea informaţională ce îşi are bazele în cunoaştere şi să o reflecte tocmai datorită amplelor sale legături cu fenomenele economice şi sociale.

România are nevoie de o schimbare,respectiv de o adaptare a sistemului de drept ce poate raspunde pozitiv cerinţelor reglementărilor europene şi internaţionale precum şi cerinţelor Uniunii Europene şi NATO prezente în acest nou tip de societate. Această schimbare reprezintă răspunsul concret al statului ce nu se poate integra intr-o societate informaţională europeană şi globală in lipsa unui sistem de drept corespunzător. Dezvoltarea societăţii informaţionale a creat necesitatea existenţei unui drept specific, Cyberlaw.

Mediul internet prezintă societatea informaţională drept un domeniu foarte nou şi diferit incât nu oferă posibilitatea unui precedent. Soluţiile tehnice şi juridice prezente in acest domeniu se afla intr-o foarte strânsă legătură una de alta. Bazându-se pe cunoaştere, societatea informaţională necesită un singur drept şi anume dreptul informatic, care să ii semene prin esenţă.

Reţeaua internet, reprezentând atât de fidel societatea informaţională a reuşit să deschidă mai mult decât orice calea către indeplinirea acestor drepturi, tocmai pentru că obiectul de activitate al reţelei este insuşi traficul de informaţii ce este definit de comunicare, achiziţii, expunere şi distribuţie.

Cu toate acestea, există drepturi fundamentale ale omului precum drepul la viaţa intimă sau la secretul comunicaţiilor pe care societatea informaţională le poate incălca foarte uşor. Guvernele folosesc de cele mai multe ori scuze precum securitatea sau supravegherea statului pentru a justifica ingrădirea liberei comunicări umane.

Adevăratul secret al comunicaţiilor este reprezentat de toate tipurile de comunicaţii interpersonale prezente in societatea informaţională. Pentru o asigurare validă şi veridică a acestui deziderat este necesară existenţa in cadrul legislaţiei a normelor corespunzătoare in domeniu iar acestea sa fie asigurate sub imperiul sancţiunii.

Informatizarea este cunoscută ca nefiind o tehnică politică neutră, aceasta participând cu o dinamică proprie ce oferă posibilitatea de intărire a centrelor de putere precum marile intreprinderi, corporaţiile dar şi intituţiile statului.

O legislaţie adecvată poate stinge conflictul dintre libertatea de exprimare şi secretul comunicaţiilor dar şi intre libertatea de exprimare şi interesul public.

Diverse medii de afaceri vad această creştere exponenţială a internetului drept o oportunitate deosebită. Pe lângă oportunităţiule de afaceri deosebite, reţeaua internet permite existenţa unei serii de dezavantaje ce trebuie luate in considerare pentru a fi evitate pierderile, in prim plan fiind cele financiare.

In urma dezvoltarii vertiginoase a tehnologiei au aparut, pe lângă numeroasele beneficii şi un număr impresionant de infracţiuni cu un conţinut sofisticat, elevat.

Pentru comunitatea internaţională, România reprezintă o ţară periculoasă, in urma acestui fapt, statul a fost somat să işi completeze normativul juridic penal in domeniul informaticii.

Noul Cod penal care a intrat în vigoare, reglementează între art.360-365

infracţiunile contra siguranţei şi integrităţii sistemelor şi datelor informatice, astfel:

(1) Accesul ilegal la un sistem informatic

(2) Interceptarea ilegală a unei transmisii de date informatice

(3) Alterarea integrităţii datelor informatice

(4) Perturbarea funcţionării sistemelor informatice

(5) Transferul neautorizat de date informatice şi

(6) Operaţiuni ilegale cu dispozitive sau programe informatice

După cum societatea informaţională este reprezentată foarte specific de reţeaua Internet, deţine un caracter global iar din acesta rezultă că, in elaborarea legislaţiei aplicabile in România a trebuit să se ţină seama mai mult de reglementările SUA şi UE in domeniu.

Cifra neagră reprezintă un segment important in ceea ce priveşte faptele penale nedescoperite in cadrul criminalităţii generale, in ceea ce priveşte criminalitatea informatică, acest procent reprezintă in jur de 90%. Procentul foarte ridicat al infracţiunilor nedescoperite este o consecinţă directă a faptului că infracţiunea informatică, in general, reprezintă un act ilegal recent sancţionat şi se află deocamdată incriptat in spatele unor noi tehnologii, deseori inaccesibile chiar celor care ar trebui să combată fenomenul.

Unul din efectele informatizării tehnologice este impactul asupra evoluţiei tehnologiei telecomunicaţiilor[1]. Comunicarea clasică, prin intermediul telefoniei, a fost depăş ită de noile metode de transmitere la distanţă nu numai a vocii, ci şi a datelor, muzicii, fotografiilor ori filmelor. Aceste schimburi de informaţii nu mai apar numai între oameni, dar şi între oameni şi sisteme informatice ori numai între acestea din urmă.

Folosirea poştei electronice sau accesul la pagini web prin intermediul internetului constituie exemple ale acestei evoluţii, modificând profund societatea noastră.

Uşurinţa accesului la informaţii în sistemele informatice, combinată cu

[1] **V. Hanga**, *Dreptul şi calculatoarele*, Ed. Academiei Române, 1991

posibilităţile practic nelimitate de schimb sau diseminare a acestora, indiferent de graniţele geografice sau naţionale, a dus la o creştere explozivă a cantităţii de informaţie disponibilă şi a cunoştinţelor care pot fi extrase din aceasta[2].

Această evoluţie a dat naştere la schimbări economice şi sociale fără precedent, dar în acelaş i timp foloseşte şi scopurilor mai puţin legitime: apariţia unor noi infracţiuni, ori săvârşirea infracţiunilor tradiţionale prin intermediul noii tehnologii.

Dreptul trebuie să facă faţă noilor provocări ridicate de dezvoltă rile tehnologice. Iată de ce în ultimii ani legiuitorul român a fost preocupat de elaborarea unui cadru normativ care să reglementeze accesul şi desfăşurarea activităţii prin intermediul sistemelor informatice în diferite sectoare.

În ceea ce priveşte formalizarea criminalităţii informatice, statele membre ale Uniunii Europene au ajuns la un numitor comun, fiind identificate trei activităţi distincte :

- *activităţi care aduc atingere vieţii private: colectarea, stocarea, modificarea şi dezvăluirea datelor cu caracter personal* ;
- *activităţi de difuzare a materialelor cu conţinut obscen şi/sau xenofob: materiale cu caracter pornografic (în special cele legate de minori), materiale cu caracter rasist şi care incită la violenţă* ;
- *criminalitatea economică, accesul neautorizat şi sabotajul*: *activităţi prin se urmăreşte distribuirea de viruşi, spionajul şi frauda realizată prin calculator , distrugerea de date şi programe sau alte infrac ţiuni: programarea unui calculator de a "distruge" alt calculator.* Până în prezent, la nivelul UE nu există instrumente de combatere a acestui tip de criminalitate;

Internetul aduce o continuă schimbare în peisajul politic al zilelor noastre. Oferă noi şi ieftine metode de colectare şi publicare a informa ţiilor, de comunicare şi coordonare a acţiunilor la scară globală şi, nu în ultimul rând, de

[2] **Costică Voicu şi colaboratorii**, *Globalizarea şi criminalitatea economico-financiară*, Editura Universul Juridic, Bucureşti, 2005

ajungere la factorii de decizie[3]. De asemenea, oferă posibilităţi de comunicare atât deschise, cât şi private. Grupurile de sprijin politic ori cele de presiune, precum şi personalităţi din lumea întreagă folosesc din plin facilităţile Internetului în încercarea de a-şi atinge scopurile sau de a influenţa politica externă[4].

CAPITOLUL I
SISTEME INFORMATICE ŞI MEDII DE STOCARE

1.1. Date generale despre istoria calculatorului

Momentul incipient in istoria calculatoarelor poate fi considerat a fi legat de numele celebrului mathematician englez Charles Babbage. In anul 1830, acesta a propus o Maşină Analitică ce urma să anticipeze intr-un mod foarte precis structura mecanismelor de calcul actuale. Posibilităţile tehnologice din momentul respective au fost devansate cu peste 100 de ani de propriile idei. Pascal şi Leibnitz au mai avut incercări in acest domeniu chiar inainte de acesta, in secolul al XIII-lea. 5.

Anul 1937 reprezintă un alt moment de referinţă, atunci cand Howard Aiken din cadrul Universităţii Harvard, bazându-se pe ideile lui Babbage şi calculatoarele electromecanice produse de comania IBM, a produs Calculatorul cu secvenţă de Comandă Automată. Acest prim mecanism a fost denumit Mark I iar construcţia acestuia a fost începută in anul 1939 şi terminate mai apoi in anul 1944. Fiind alcătuit din comutatoare şi relee, Mark I a reprezentat primul calculator electromecanic.

---

[3] **I. Vasiu**, *Drept şi Informatică. Protecţia juridică a programelor*, Studii de drept românesc, Ed. Academiei Române, 1993

[4] **T. Amza**, **C.P. Amza**, *Criminalitatea Informatică*, Ed. Lumina Lex, 2003

Prima generaţie de calculatoare cuprinde sistemele construite între anii 1944-1956, fiind caracterizată de utilizarea tuburilor electronice în locul releelor electromagnetice. Cel mai cunoscut calculator din această perioadă a fost ENIAC, construit între anii 1943-1944 în Statele Unite. La fel ca toate sistemele de calcul din generaţia sa, ENIAC avea dimensiuni gigantice: ocupa un spaţiu de 150 mp şi cântarea 30 de tone; la construirea sa au fost folosite 18.000 de tuburi electronice, 70.000 de rezistenţe şi 6000 de comutatoare. Pentru a funcţiona, acest calculator uriaş avea nevoie de o putere de 150 de KW, iar capacitatea consta în efectuarea a circa 32.000 de operaţii pe secundă.

Generaţia a doua. Principalele tehnologii hard erau reprezentate de tranzistori (diode semiconductoare), inventat de W. Shockley (1947). Echipamentele periferice de introducere/extragere de date au evoluat şi ele; de exemplu, de la maşini de scris cu 10 caractere pe secundă s-a trecut la imprimante rapide (pentru acea perioadă) cu sute de linii pe minut. Programarea acestor calculatoare se putea face şi în limbaje de nivel înalt (Fortran, Cobol) prin existenţa unor programe care le traduc în limbaj maşina (compilatoare).

Generatia a treia (1964-1971). Principala tehnologie hard era reprezentată de circuitele integrate (circuite miniaturizate cu functii complexe), memoriile interne ale calculatoarelor fiind alcătuite din semiconductoare. Apar discurile magnetice ca suporturi de memorie externă, iar viteza de lucru creşte la 5 milioane de operaţii pe secundă. Cel mai cunoscut reprezentant al generaţiei este IBM 360, iar dintre calculatoarele româneşti - familia FELIX, calculatoare universale realizate sub licenţa franceză.

Calculatoarele din generaţia a patra (1982 – 1990) sunt caracterizate prin utilizarea pe scară largă a circuitelor integrate şi prin răspândirea computerelor personale (PC). Sistemele de calcul construite în această perioadă sunt mai performante decât cele din generaţia anterioară: viteza de lucru urcă la 30.000.000 de operaţii pe secundă, capacitatea de memorare ajunge la 8 MB, consumul de

energie şi dimensiunile aparatului devin din ce în ce mai reduse, iar utilizarea calculatoarelor devine din ce în ce mai accesibilă mai multor categorii de persoane[5].

Generaţia a cincea de calculatoare. Este reprezentată de sistemele construite din 1990 până in prezent. Acestea accentuează performanţele generaţiei anterioare prin utilizarea microcipurilor (circuite integrate pe o scară ultra largă), prin creşterea vitezei de operare şi a capacităţii de stocare (ajunge în prezent la ordinul Giga octetilor).

1.2. Reţele informatice

Conceptul de reţea de calculatoare

Reţeaua de calculatoare este un ansamblu de calculatoare (sisteme de calcul) interconectate prin intermediul unor medii de comunicaţie (cablu coaxial, fibră optică, linie telefonică, sateliţi de comunicaţie) în scopul utilizării în comun de către mai mulţi utilizatori a tuturor resurselor fizice**,** logice (software de bază şi aplicaţii) şi informaţionale (baze de date, fişiere), asociate calculatoarelor din reţea.

Reţeaua de calculatoare desemnează o colecţie interconectată de calculatoare autonome. Se spune despre două calculatoare că sunt interconectate dacă sunt capabile să schimbe informaţie între ele. Impunând calculatoarelor cerinţa de a fi autonome, dorim să excludem din definiţia noastră sistemele în care există o relaţie clară de tip master/slave. Dacă un calculator poate să pornească, să oprească sau să controleze în mod forţat un altul, atunci calculatoarele nu sunt autonome. Un sistem cu o unitate de control si mai multe unităţi aservite nu este o reţea; aşa cum nu este o reţea nici un calculator mare cu imprimante şi terminale aflate la distanţă[6].

În general, toate reţelele au anumite componente, funcţii şi caracteristici comune, printre acestea numărându-se următoarele:

- *servere* – calculatoare care oferă resurse partajate pentru

[5] **T. Amza**, **C.P. Amza**, *Criminalitatea Informatică*, Ed. Lumina Lex, 2003
[6] **W. Odom**, *Reţele de calculatoare*, Ed. Corint, 2004

utilizatorii reţelei;

- *clienţii* – calculatoare de lucru (terminale, staţii de lucru) care accesează resursele partajate în reţeaua de server;
- *mediu de comunicaţie* – modul şi elementele prin intermediul cărora comunică calculatoarele în reţea;
- *date partajate* – fişiere puse la dispoziţie de serverele din reţea;
- *imprimante* sau alte periferice partajate;
- *resurse* – fişiere, imprimante şi alte componente care pot fi folosite de utilizatorii reţelei.

Modele de referinţă

Odată cu puternica dezvoltare a echipamentelor de reţele au apărut diferite companii care îşi extindeau reţelele, dar care aveau probleme în a comunica cu alte companii deoarece nu foloseau aceleaşi standarde.

Modelul de referinţă OSI. Modelul OSI a fost elaborat pentru a furniza producătorilor de echipamente de comunicaţie un set de standarde, a căror respectare asigura compatibilitatea şi intercompatibilitatea între diverse tehnologii furnizate de firme diferite.

Acest model defineşte şapte nivele, împreuna cu standarde şi un set de protocoale pentru reţele. Este un model teoretic, construit pentru a schematiza comunicaţia într-o reţea de calculatoare şi pentru a explica traseul informaţie dintr-un capăt în altul al reţelei. Modelul OSI al Organizaţiei Internaţionale pentru Standardizare (ISO) este structurat pe şapte nivele: fizic, legătură de date, rețea, transport, sesiune, prezentare, aplicație.

Nivelul fizic. Nivelul fizic se ocupă de transmiterea biţilor printr-un canal de comunicaţie. Proiectarea trebuie să garanteze ca atunci când unul din capete trimite un bit 1, acesta e receptat în cealaltă parte ca un bit 1, nu ca un bit 0. Problemele tipice se referă la câţi volţi trebuie utilizaţi pentru a reprezenta un 1 şi câţi pentru un 0, dacă transmisia poate avea loc simultan în ambele sensuri, cum este stabilită conexiunea iniţială şi cum este întreruptă când au terminat de comunicat ambele părţi, câţi pini are conectorul de reţea şi la ce foloseşte fiecare pin.

Nivelul fizic defineşte specificaţii electrice, mecanice, procedurale şi funcţionale pentru activarea, menţinerea şi dezactivarea legăturilor fizice între sisteme. În această categorie de caracteristici se încadrează nivelurile de tensiune, sincronizarea schimbărilor acestor niveluri, ratele de transfer fizice, distanţele maxime la care se poate transmite şi alte atribute similare care sunt definite de specificaţii fizice.

Scopul nivelului fizic este de a transporta o secvenţă de biţi de la o maşină la alta. Pentru aceasta pot fi utilizate diverse medii fizice. Fiecare dintre ele este definit de lăţimea sa de bandă, întârziere, cost şi uşurinţă de instalare. Îl putem asocia cu termenii semnal şi medii de transmitere.

Conform principiilor ISO-OSI, dispozitivele de nivel fizic asigură legătura între două staţii de nivelul cel mai coborât. Singurul dispozitiv de nivel fizic care mai există astăzi este HUB-ul însă, din punct de vedere istoric primul dispozitiv de nivel 1 a fost repertorul.

Nivelul legătură de date. Sarcina principală a nivelului legătură de date este de a transforma un mijloc oarecare de transmisie într-o linie care să fie disponibilă nivelului reţea fără erori de transmisie nedetectate. Nivelul legătură de date realizează această sarcină obligând emiţătorul să descompună datele de intrare în cadre de date (în mod tipic, câteva sute sau mii de octeţi), să transmită cadrele secvenţial şi să prelucreze datele de confirmare trimise înapoi de receptor[7].

Deoarece nivelul fizic nu face decât să accepte şi să transmită un flux de biţi, fără să se preocupe de semnificaţia sau de structura lor, responsabilitatea pentru marcarea şi recunoaşterea delimitărilor între cadre îi revine nivelului legătură de date. Aceasta se poate realiza prin ataşarea unor şabloane speciale de biţi la începutul şi la sfârşitul cadrului. În cazul în care şabloanele respective de biţi pot apare accidental în datele propriu-zise, trebuie luate măsuri speciale de

[7] **V.V. Patriciu**, *Criptografia şi securitatea reţelelor de calculatoare*, Ed. Tehnică, 1994

precauţie pentru ca aceste şabloane să nu fie incorect interpretate ca delimitatori de cadre. Un zgomot apărut pe linie poate distruge un cadru în întregime. În acest caz, programele nivelului legătură de date de pe masina-sursă pot să retransmită cadrul.

Transmiterile multiple ale aceluiaşi cadru introduc posibilitatea cadrelor duplicate. Un cadru duplicat poate apare la transmisie în situaţia în care s-au pierdut cadrele de confirmare trimise de la receptor înapoi spre emiţător. Rezolvarea problemelor apărute datorată cadrelor deteriorate, pierdute sau duplicate cade în sarcina nivelului legătură de date. Acesta poate oferi nivelului reţea câteva clase de servicii diferite, fiecare de o calitate şi un preţ diferit. O alta problemă care apare la nivelul legătură de date (şi la majoritatea nivelurilor superioare) este evitarea inundării unui receptor lent cu date provenite de la un emiţător rapid. În acest scop sunt necesare mecanisme de reglare a traficului care să permită emiţătorului atât cât spaţiu-tampon deţine receptorul la un moment curent. Controlul traficului şi tratarea erorilor sunt deseori integrate.

Pe scurt, transmiterea sigură şi corectă a datelor folosindu-se o legătură fizică existentă formată intre două puncte direct conectate cu ajutorul acesteia este asigurată de nivelul legătură de date ce se preocupă in acelaşi timp li de controlul fluxului fizic(flow control), dar şi de detecţia şi anunţarea erorilor. Nivelul fizic este incapabil de a realiza acest lucru, tocmai pentru că in cazul nivelului fizic nu poate fi vorba despre niciun fel de cadre(frames) sau de date, ci doar despre biţi sau mai exact despre configuraţia fizică a acestora(intensitatea luminii, niveluri de tensiune etc).

Acest nivel se ocupă cu probleme de genul adresarea hardware, topologia reţelei şi felul în care computerele dintr-o reţea accesează mediul comun. Când datele din nivelul *Aplicaţie* circulă prin stivă pentru a ajunge până la nivelul Fizic aceste date sunt împărţite în unităţi mai mici care primesc informaţii adiţionale (headere şi trailere). Aceste unităţi au fiecare câte un nume, unul pentru fiecare nivel care încapsulează date. Datele încapsulate de nivelul 2 poarta numele de frames. Cu ajutorul biţilor primiţi din header şi trailer pot fi identificate sursa şi

destinaţia datelor transmise şi pot fi găsite pachetele de date care conţin erori, asigurând în acest mod fiabilitatea comunicării în reţea.

Acest produs seamănă foarte mult cu trimiterea unei scrisori unui prieten: se introduce scrisoarea (datele din nivele superioare) într-un plic şi pe plic se scrie adresa prietenului şi adresa proprie. Informaţiile scrise pe plic vor asigura că scrisoarea va fi transmisă în direcţia cea bună de serviciile poştale (dispozitivele din reţea) până când va ajunge în sfârşit în cutia poştală a prietenului[8].

Nivelul reţea. Nivelul reţea se ocupa de controlul funcţionarii subreţelei. O problema cheie în proiectare este determinarea modului în care pachetele sunt dirijate de la sursă la destinaţie. Dirijarea se poate baza pe tabelele statice care sunt „cablate" intern în reţea şi care sunt schimbate rar. Traseele pot fi stabilite la începutul fiecărei conversaţii, de exemplu la începutul unei sesiuni la terminal. În sfârşit, dirijarea poate fi foarte dinamică, traseele determinându-se pentru fiecare pachet în concordanţă cu traficul curent din reţea.

Multe probleme pot apare când un pachet trebuie să călătorească dintr-o reţea în alta ca să ajungă la destinaţie. Modul de adresare folosit de a doua reţea poate să difere de cel de prima. A doua reţea poate chiar să nu accepte de loc pachetul pentru că este prea mare sau protocoalele pot fi diferite. Rezolvarea acestor probleme în vederea interconectării reţelelor eterogene este sarcina nivelului reţea.

În reţelele cu difuzare problema dirijării este simplă, astfel că nivelul reţea este adeseori subţire sau chiar nu exista deloc. Dacă în reţea există prea multe pachete simultan, ele vor intra unul pe traseul celuilalt şi astfel se vor produce congestii. Controlul unor astfel de congestii îi revine tot nivelului reţea. Nivelul reţea este un nivel complex care oferă conectivitate şi selectează drumul de urmat între două sisteme gazde care pot fi localizate în reţele separate geografic. Acesta

[8] **W. Odom**, *Reţele de calculatoare*, Ed. Corint, 2004

este nivelul cel mai important în cadrul Internetului, asigurând posibilitatea interconectării diferitelor reţele. Tot la acest nivel se realizează adresarea logică a tuturor nodurilor din Internet. La nivelul reţea operează ruter-ele, dispozitivele cele mai importante în orice reţea de mari dimensiuni.

Nivelul transport. Rolul principal al nivelului transport este să accepte date de la nivelul sesiune, să le descompună dacă este cazul în unităţi mai mici, să transfere aceste unităţi nivelului reţea şi să se asigure că toate fragmentele sosesc corect la celalalt capăt. În plus, toate acestea trebuie făcute eficient şi într-un mod care izolează nivelurile de mai sus de inevitabilele modificări în tehnologia echipamentelor.

În condiţii normale nivelul transport creează o conexiune de reţea distinctă pentru fiecare conexiune de transport cerută de nivelul sesiune. În cazul în care conexiunea de transport necesită o productivitate mare, nivelul transport poate totuşi să creeze conexiuni de reţea multiple şi să dividă datele prin conexiunile de reţea, astfel încât productivitatea să crească. Pe de altă parte, în cazul în care crearea şi întreţinerea unei conexiuni de reţea este costisitoare, nivelul transport ar putea reduce costul prin multiplexarea câtorva conexiuni de transport pe aceeaşi conexiune de reţea. În oricare dintre cazuri, nivelului transport i se cere să facă multiplexarea transparentă pentru nivelul sesiune.

Nivelul transport determină, de asemenea, ce tip de serviciu să furnizeze nivelului sesiune, şi în final, utilizatorilor reţelei. Cel mai obişnuit tip de conexiune transport este un canal punct-la-punct fără erori care furnizează mesajele sau octeţii în ordinea în care au fost trimişi[9]. Alte tipuri posibile de servicii de transport sunt transportul mesajelor individuale – fără nici o garanţie în privinţa ordinii de livrare şi difuzarea mesajelor către destinaţii multiple. Tipul serviciului se determină când se realizează conexiunea.

[9] **V.V. Patriciu**, *Criptografia şi securitatea reţelelor de calculatoare*, Ed. Tehnică, 1994

Nivelul transport segmentează datele în sistemul sursă şi le reasamblează la destinaţie. Limita dintre nivelul transport şi nivelul sesiune poate fi văzută ca garanţia între protocoalele aplicaţie şi protocoalele de transfer de date. În timp ce nivelurile aplicaţie, prezentare şi sesiune se preocupă cu probleme legate de aplicaţii, cele patru niveluri inferioare se ocupă cu probleme legate de transportul datelor. Nivelul transport încearcă să ofere un serviciu de transport de date care să izoleze nivelurile superioare de orice lucruri legate de modul în care este executat transportul datelor. Mai specific, probleme cum ar fi siguranţa sunt responsabilitatea nivelului transport. În cadrul oferirii de servicii de comunicare, nivelul transport iniţiază, gestionează şi închide circuitele virtuale. Pentru a fi obţinută o comunicaţie sigură, servicii de detectare de erori sunt oferite tot la acest nivel. Tot aici este realizat controlul fluxului.

Nivelul sesiune. Nivelul sesiune permite utilizatorilor de pe maşini difere să stabilească între ei sesiuni. Ca şi nivelul transport, o sesiune permite transportul obişnuit de date, dar furnizează totodată şi servicii îmbunătăţite, utile în anumite aplicaţii. O sesiune poate fi utilizată pentru a permite unui utilizator să se conecteze la distanţă pe un sistem cu divizarea timpului sau să transfere un fişier între două maşini. Unul dintre serviciile nivelului sesiune se referă la controlul dialogului. Sesiunile pot permite să se realizeze trafic în ambele sensuri simultan sau numai într-un sens odată. Dacă este permis traficul într-un singur sens, nivelul sesiune poate ajuta să se ţină evidenţa emiţătorilor cărora le vine rândul să transmită. Un serviciu sesiune înrudit este gestionarea jetonului; în unele protocoale este esenţial ca cele două părţi să nu încerce să nu realizeze aceeaşi operaţie în acelaşi timp. Pentru a trata aceste situaţii nivelul sesiune dispune de jetoane care pot circula între maşini. Numai partea care deţine jetonul are voie să realizeze operaţia critică.

Un alt serviciu sesiune este sincronizarea. Să considerăm problemele care pot apare atunci când se încearcă transferarea unui fişier între două maşini, în

condiţiile în care transferul durează 2 ore, iar intervalul mediu de cădere a legăturii este de 1 oră. După fiecare eşec tot transferul va trebui iniţiat din nou şi nu va reuşi nici încercarea următoare. Pentru a elimina problema respectivă, nivelul sesiune prevede o modalitate de a introduce în flux de date puncte de control, astfel încât după un eşec trebuie să se reia numai transferul datelor de după ultimul punct de control.

Aşa cum implică şi numele său, nivelul sesiune se ocupă cu stabilirea, menţinerea, gestionarea şi terminarea sesiunilor în comunicarea dintre două maşini. Nivelul sesiune oferă servicii nivelului prezentare; el realizează sincronizarea între nivelurile prezentare ale celor doua staţii şi gestionează schimbul de date între acestea. În plus faţă de realizarea sesiunilor, nivelul sesiune oferă bazele pentru transferul eficient de date, pentru clase de servicii, pentru raportarea excepţiilor nivelurilor sesiune, prezentare şi aplicaţie.

Nivelul prezentare. Nivelul prezentare se asigură că informaţia transmisă de nivelul aplicaţie al unui sistem poate fi citită şi interpretată de către nivelul aplicaţie al sistemului cu care aceasta comunică. Daca este necesar, nivelul prezentare face traducerea între diverse formate de reprezentare, prin intermediul unui format comun. Tot nivelul prezentare este responsabil cu eventuala compresie/decompresie şi criptare/decriptare a datelor.

Nivelul fizic. Nivelul aplicaţie este cel care este situat cel mai aproape de utilizator; el oferă servicii de reţea aplicaţiilor utilizatorului. Diferă de celelalte niveluri OSI prin faptul că nu oferă servicii nici unui altui nivel, ci numai unor aplicaţii ce sunt situate în afara nivelului OSI. Nivelul aplicaţie stabileşte disponibilitatea unui calculator cu care se doreşte iniţierea unei conexiuni, stabileşte procedurile ce vor fi urmate în cazul unor erori şi verifică integritatea datelor. Nivelul aplicaţie conţine o varietate de protocoale frecvent utilizate. De exemplu, în lume există sute de tipuri de terminale incompatibile. Gândiţi-vă la impasul în care se afla un editor în mod ecran care trebuie să lucreze într-o reţea cu

multe tipuri diferite de terminale, fiecare cu un aspect diferit al ecranului şi cu secvenţe ESCAPE diferite pentru introducerea şi ştergerea textului, mutarea cursorului etc. O modalitate de a se rezolva problema este să se definească un terminal virtual de reţea abstract şi să se scrie editoare şi alte programe care ştiu să lucreze cu acesta. Pentru a putea lucra cu orice tip de terminal, este necesar un program care să pună în corespondenţă funcţiile teminalului virtual de reţea şi terminalul real. De exemplu, atunci când editorul mută cursorul din terminalul virtual în colţul din stânga sus al ecranului, programul trebuie să aplice secvenţa potrivită de comenzi pentru terminalul real, astfel încât să se mute şi cursorul acestuia. Toate programele terminalului virtual se află pe nivelul aplicaţie.

Modelul de referinţă TCP/IP. Deşi modelul OSI este universal recunoscut, iniţiatorul din punct de vedere istoric şi tehnic al standardelor pentru Internet este însă modelul de referinţă şi stiva de protocoale TCP/IP. Modelul de referinţă TCP/IP reprezintă cel mai flexibil mod de transport disponibil şi permite computerelor din întreaga lume, rulând sisteme de operare complet diferite, să comunice între ele. TCP/IP este prescurtarea de la Transmission Control Protocol / Internet Protocol. Dezvoltarea lui a început în anii 1960 sub forma unui proiect finanţat de SUA. Standardul TCP/IP este folosit în acest moment pentru transmisiile de date din cea mai mare reţea existenta - Internetul.

Modelul de referinţa TCP/IP a fost creat de Departamentul Apărării din SUA pentru a deveni reţeaua suprema care să supravieţuiască în orice condiţii. Agenţia ARPA a creat în anul 1975 protocolul TCP/IP pentru a interconecta reţelele militare, dar a furnizat pe gratis standardele de protocol agenţiilor guvernamentale şi universităţilor. La 1 ianuarie 1983, TCP/IP a devenit unicul protocol oficial. Practic toate calculatoarele conectate la Internet utilizează familia de protocoale TCP/IP. Punctele forte ale acestei stive sunt:

- este independentă de producător (vânzător);
- nu este protejată prin legea copyright-ului;
- se poate utiliza atât pentru reţele locale (LAN), cât şi pentru

reţele globale (WAN);

- se poate utiliza pe aproape orice tip de calculator.

TCP/IP este un set de protocoale stabil, bine definit şi complet care asigură transferul pachetelor de date cu o rată foarte mică de eroare printr-o reţea neomogenă de calculatoare. TCP/IP este o suită de protocoale, dintre care cele mai importante sunt TCP şi IP.

Din punct de vedere arhitectural protocoalele TCP/IP au patru niveluri în loc de şapte ca în modelul OSI. Cele patru nivele ale modelului TCP/IP sunt: nivelul aplicaţie, nivelul transport, nivelul Internet şi nivelul reţea.

Nivelul reţea. Numele acestui nivel e extrem de confuz. Se mai numeşte şi nivelul gazdă pentru reţea sau acces la reţea. Este nivelul ce se ocupă de problemele pe care le întâmpină un pachet IP pentru a realiza o conexiune fizică, şi apoi o altă conexiune fizică. Include detalii ale tehnologiei LAN şi WAN şi toate atributele caracteristice nivelului fizic şi legătură de date din modelul OSI.

Nivelul Internet. Acest nivel îşi propune transmiterea pachetelor de la sursă din orice reţea a interconexiunii şi sosirea lor la destinaţie independent de calea urmată. Protocolul specific acestui nivel e Internet protocol (IP). Determinarea căii optime se face la acest nivel . Este asemănător cu sistemul poştal - când se trimite o scrisoare, nu are importanţă cum ajunge la destinaţie (există multiple căi), dar ca ajunge sigur[10].

Nivelul transport. Nivelul transport se ocupa de problemele legate de performanţele sistemului, controlul fluxului şi corectarea greşelilor. Unul din protocoalele sale Transmission Control Protocol (TCP), propune modalităţi flexibile de comunicare, cu flux de date excelent, cât mai puţine erori. TCP este un protocol orientat pe conexiune. Propune dialogul dintre sursă şi destinaţie în timpul în care împachetează informaţia nivelului aplicaţie în unităţi numite segmente. Orientat pe conexiune nu înseamnă că există un circuit între calculatoarele

[10] **V.V. Patriciu**, *Criptografia şi securitatea reţelelor de calculatoare*, Ed. Tehnică, 1994

comunicante; presupune de fapt că segmentele nivelului 4 sunt retransmise după o anumită perioadă în caz că nu au ajuns la destinaţie în forma corectă.

Nivelul aplicaţie. Realizatorii modelului TCP/IP au considerat că protocoalele nivelului cel mai de sus trebuie să includă detalii ale nivelului sesiune şi prezentare, aşa că au creat nivelul aplicaţie ce tratează protocoalele de nivel înalt, probleme de reprezentare, codificare şi control al dialogului. TCP/IP combină toate problemele aflate în legătură cu nivelul aplicaţie într-un singur nivel, asigurându-se că aceste date sunt corect împachetate pentru următorul nivel.

1.3. Vulnerabilităţi ale sistemelor informatice

Vulnerabilitatea este o slăbiciune a unui sistem hardware sau software ce permite utilizatorilor neautorizaţi să obţină acces asupra sa **Error! Reference source not found.**. Principalele vulnerabilităţi în cadrul sistemelor informatice sunt de natură fizică, hardware, software sau umană.

Sistemele informatice sunt vulnerabile în primul rând la atacurile clasice, atunci când un atacator reuşeşte să pătrundă în incinta sistemelor de calcul şi să sustragă informaţii confidenţiale. Pentru a preîntâmpina acest lucru trebuie să se asigure securitatea fizică a echipamentelor de calcul prin plasarea acestora în zone sigure, restricţionate personalului neautorizat. Accesul la aceste zone trebuie făcut prin folosirea interfoanelor, cardurilor de acces sau dispozitivelor de scanare a datelor biometrice pentru autentificarea utilizatorilor cu permis de intrare. O altă vulnerabilitate a sistemelor informatice o reprezintă dezastrele naturale; cutremure, inundaţii, incendii sau accidentele precum căderile de tensiune sau supratensiunile ce pot duce la distrugerea fizică a echipamentelor de calcul. De aceea trebuie avute în vedere şi amplasarea echipamentelor pentru reducerea riscului faţă de ameninţările mediului înconjurător.

O atenţie deosebită trebuie acordată componentelor hardware pentru ca acestea să nu afecteze ulterior buna funcţionare a sistemelor informatice. În cazul serverelor ce furnizează servicii în Internet trebuie alese componente hardware tolerante la defectări pentru a oferi disponibilitate serviciilor şi datelor partajate în reţea şi pentru a reduce riscul vulnerabilităţilor de tip hardware. Aceste vulnerabilităţi sunt întâlnite cel mai des la sistemele de stocare a datelor, fiind cele mai sensibile componente hardware şi în cazul defectării lor pagubele fiind cele mai însemnate prin pierderea parţială sau totală a informaţiilor. Din acest punct de vedere se recomandă salvările de siguranţă atât la nivelul informaţiilor cât şi la nivelul sistemului de operare, pentru repunerea rapidă a acestuia şi a serviciilor configurate în caz de defecţiune.

Comunicaţiile în Internet sunt de asemenea nesigure. Oricine se poate conecta la linia de comunicaţie şi poate intercepta, altera sau chiar devia traficul de date. Pentru a înlătura aceste vulnerabilităţi se recomandă folosirea metodelor de criptare a datelor, ca în cazul în care acestea sunt interceptate, ele să nu poată fi decriptate.

Din punct de vedere software, există mai multe tipuri de vulnerabilităţi:

- care măresc privilegiile utilizatorilor locali fără autorizaţie;
- care permit utilizatorilor externi să acceseze sistemul în mod neautorizat;
- care permit implicarea sistemului într-un atac asupra unui terţ utilizator (exemplu atacul DDoS – Distributed Denial of Service).

O clasificare poate fi făcută după gradul de pericol pe care-l reprezintă vulnerabilităţile pentru sistemul informatic supus atacului. Astfel vulnerabilităţile prezintă 3 grade în funcţie de pericolul prezentat: A, B şi C.

Grad de vulnerabilitate A: Consecinţe – Permite utilizatorilor externi să acceseze în mod neautorizat sistemul informatic; Mod de atac – troieni, viermi.

Grad de vulnerabilitate B: Consecinţe – Permite utilizatorilor locali cu privilegii limitate să-şi mărească privilegiile fără autorizaţie; Mod de atac – buffer overflow.

Grad de vulnerabilitate C: Consecinţe – Permite utilizatorilor externi să altereze procesele sistemelor informatice – DoS, DDoS.

Vulnerabilităţile de clasă C, cele care permit atacuri prin refuzul serviciilor, sunt vulnerabilităţi ale sistemului de operare, în special al funcţiilor de reţea. Aceste vulnerabilităţi permit utilizatorilor externi să altereze serviciile de reţea ale unui sistem informatic, sau, în anumite cazuri, transformă sistemul victimă într-un sistem zombi ce va putea fi implicat ulterior într-un atac de tip DDoS. Aceste vulnerabilităţi, dacă sunt exploatate, duc la încetinirea sau la oprirea temporară a serviciilor de reţea oferite, ca de exemplu un server HTTP, FTP sau de e-mail.

CAPITOLUL II
REGLEMENTĂRI JURIDICE PRIVIND CRIMINALITATEA INFORMATICĂ

Reglementarea criminalităţii informatice

Limbajul informatic este comun tuturor celor care folosesc calculatoarele, indiferent de ţara de proveniență şi de limba vorbită; acest limbaj comun, precum şi mijloacele de comunicare facile între utilizatori, printr-o reţea specializată (exemplul cel mai elocvent fiind Internetul) sau printr-o simplă linie telefonică, au dus la posibilităţi practic nelimitate de conectare a calculatoarelor din cele mai îndepărtate colţuri ale lumii şi de accesare a informaţiilor de ultimă oră, deosebit

de importante, aproape fără nici un efort. Prin urmare, un utilizator animat de rele intenţii poate, de oriunde s-ar afla, din orice colţ al lumii, fără să plătească altceva decât, eventual, o anumită sumă operatorului telefonic, să-şi alimenteze contul bancar de la orice mare instituţie financiar-bancară care prezintă lacune în sistemul de protecţie informatică.

S-a observat, astfel, o serie de pierderi înregistrate de bănci din Occident, generate de spărgători ruşi care, prin intermediul reţelelor de calculatoare, au putut penetra sistemele informatice şi transfera fonduri la alte bănci, de unde complicii au ridicat numerarul, înainte ca cineva să poată înţelege ce s-a întâmplat, de fapt, singurul lucru ştiut, fiind acela că unele linii telefonice cu Rusia au fost mult încărcate în anumite perioade. Tocmai din acest motiv, guvernele ţărilor puternic industrializate şi informatizate au luat măsuri, ajungând, în SUA de pildă, până la înfiinţarea unui serviciu special al FBI, de urmărire şi detectare a criminalităţii şi a infractorilor informatici – primul serviciu poliţienesc de acest gen din lume – în Franţa, la înfiinţarea Clubului Securităţii Informatice, ducând, astfel, la stabilirea unei minime prevederi pentru fiecare ţară membră Comunităţii Europene, în conformitate cu o listă stabilită de acest organism internaţional şi recomandată a fi cuprinsă în legislaţiile ţărilor membre.

Datorită naturii calculatoarelor există posibilităţi crescânde de a înmagazina, transfera, utiliza şi manipula date prin contact de la mare distanţă, de a comunica şi transmite rapid şi la o calitate ridicată cantităţi practic nelimitate de date de la un sistem informatic la altul[11].

De obicei statele îşi stabilesc propria jurisdicţie exclusiv în baza teritoriului lor naţional[12].

Experţii susţin că reţelele informatice internaţionale sunt vulnerabile la criminalitatea informatică – sectorul bancar, de exemplu. La fel, lumea afacerilor a

[11] *I.Vasiu*, Criminalitatea informatică, Ed. Nemira, Bucureşti, 1998, p.47 şi urm;
[12] *M. Zainea, R. Simion*, Infracţiuni în domeniul informatic. Culegerea de practică judiciară, Ed. C.H.Beck, 2009, Bucureşti, p. 8;

recunoscut, ea însăşi, caracterul vulnerabil al afacerilor internaţionale. Pentru cazurile de criminalitate informatică cu caracter transfrontalier, Comitetul a apreciat că este necesar ca statele membre să-şi revadă criteriile de aplicare pentru a determina locul unde a fost săvârşită infracţiunea şi jurisdicţia care trebuie să o ancheteze şi să o urmărească. Când mai multe state sunt competente, poate exista conflict de jurisdicţie, în plus, în cursul instrumentării acestor infracţiuni, se poate dovedi necesar să se urmărească date stocate în alte ţări, să se recurgă la instrumente internaţionale de întrajutorare judiciară. În lumina situaţiilor transfrontaliere, trebuie să se determine dacă aplicarea acestor instrumente, mai exact a convenţiilor europene în domeniu, se poate face fără dificultăţi.[13]

Pentru a rezolva în mod eficient problema infracţiunilor informatice este nevoie de o cooperare internaţională concertată. Aceasta se poate întâmpla numai dacă există un cadru comun de înţelegere a problemei şi a soluţiilor care trebuie luate în considerare. În prezent armonizarea sistemelor legale şi a definiţiilor infracţiunilor informatice a fost propusă de către Naţiunile Unite, OECD şi Consiliul Europei.

a) Primele iniţiative ale OECD

Primele eforturi internaţionale privind confruntarea cu problemele penale ridicate de către infracţiunile informatice au fost depuse de către OECD. Din anul 1983 până în anul 1984, o comisie ad-hoc a OECD a pus în discuţie posibilitatea armonizării legislaţiei penale în domeniul infracţiunilor informatice. În septembrie 1984 comisia a recomandat ţărilor membre incriminarea de către legislaţia penală internă a fiecărei ţări a faptelor ilicite cunoscute deja până în acel moment.

b) Reglementările Consiliului Europei

Din anul 1984 până în anul 1989, Comitetul de experţi în probleme informatice al Consiliului Europei a pus în discuţie problemele legate de infracţiunile informatice. Aceasta a condus la adoptarea Recomandării numărul

[13] *I. Vasiu*, op. cit., p. 49;

R(89)9 care a fost adoptată de Consiliul Europei la 13 septembrie 1989. Acest document recomandă guvernelor statelor membre să ia în considerare, în momentul modificării legislaţiilor sau iniţierii unor noi proiecte de legi, raportul privind infracţiunile informatice şi, în principal, orientările propuse pentru completarea legislaţiilor naţionale. Acestea includ atât o listă minimă de fapte ilicite care reflectă consensul general la care a ajuns Comitetul privind infracţiunile informatice, cât şi o listă opţională care descrie faptele care au fost deja incriminate de către alte state, dar asupra cărora nu s-a ajuns la un consens internaţional[14].

Lista minimală a infracţiunilor pentru care s-a ajuns la consens conţine următoarele:

- Frauda informatică. Introducerea, alterarea, ştergerea sau suprimarea unor date sau programe sau alte interpuneri în procesarea datelor care influenţează rezultatul acestora astfel, cauzând pierderi economice unei alte persoane comisă cu intenţia procurării unui câştig ilegal pentru sine sau pentru altul.
- Falsul informatic. Introducerea, alterarea, ştergerea sau suprimarea unor date sau programe sau alte interpuneri în procesarea datelor în maniera sau condiţiile prezentate de legea naţională astfel încât să constituie infracţiunea de fals dacă ar fi fost comisă în condiţiile prezentate de respectiva lege.
- Deteriorarea datelor sau programelor. Ştergerea, alterarea sau suprimarea unor date sau programe, fără drept.
- Sabotajul informatic. Introducerea, alterarea, ştergerea sau suprimarea unor date sau programe sau alte interpuneri cu un sistem informatic cu intenţia de a stânjeni funcţionarea unui computer sau sistem de telecomunicaţii.
- Accesul neautorizat. Accesul fără drept la un sistem informatic sau reţea prin încălcarea măsurilor de securitate.
- Interceptarea neautorizată. Interceptarea realizată fără drept şi prin mijloace tehnice a comunicaţiilor la, de la sau prin intermediul unui sistem sau reţea.
- Reproducerea neautorizată a unor programe protejate. Reproducerea, distribuirea sau comunicarea către public, fără drept, a unor programe protejate de lege.

[14] *I. Vasiu,i L. Vasiu*, Prevenirea criminalităţii informatice, Ed. Hamangiu, Bucureşti, 2006, p. 146;

- Reproducerea neautorizată a unor topografii. Reproducerea, fără drept, a unei topografii protejate de lege, a unui semiconductor sau exploatarea comercială ori importarea în acest scop realizată fără drept a unei topografii sau semiconductor confecţionat prin utilizarea unei topografii.

c) Rezoluţia Adunării Generale a O.N.U.

În anul 1990, aspectele juridice privind infracţiunile informatice au fost discutate şi de către Naţiunile Unite la al VIII-lea Congres privind prevenirea infracţionalităţii şi tratamentul infractorilor, desfăşurat la Havana, ca şi la Simpozionul privind infracţiunile informatice, organizat de Fundaţia pentru utilizarea responsabilă a computerului.

Cu prilejul celui de-al VIII-lea Congres al Naţiunilor Unite a fost adoptată o rezoluţie[15] referitoare la infracţiunile informatice. Această rezoluţie face referire la abordările internaţionale existente în lupta împotriva criminalităţii informatice. În baza acestei rezoluţii, O.N.U. a publicat „Manualul Naţiunilor Unite pentru Prevenirea şi Controlul Infracţiunilor Informatice", în anul 1994[16]. Ulterior, în Rezoluţia 44/121, Adunarea Generală a O.N.U. prezintă instrumentele şi rezoluţiile adoptate la congres şi invită guvernele să se ghideze după acestea în formularea legislaţiei corespunzătoare şi a politicilor penale în această materie, în acord cu interesele economice, politice, culturale şi juridice ale fiecărei ţări în parte.

d) Rezoluţia propusă de Asociaţia Internaţională de Drept Penal

Rezoluţia adoptată la Colocviul AIDP ţinut la Würzburg, în perioada 4-8 octombrie 1992, conţine un număr de recomandări printre care:

- În măsura în care legea penală tradiţională nu este suficientă, modificarea acesteia sau crearea unor noi infracţiuni ar trebui coroborată cu alte măsuri (principiul subsidiarităţii).
- În promulgarea unor noi amendamente sau prevederi legale accentul ar trebui să fie pus pe precizie şi claritate. În legile speciale care

[15] Rezoluţia nr. 44/121/14.12.1990, United Nations, General Assembly;
[16] International Telecommunication Union, Cybercrime Legislation Resources, Understanding Cybercrime: A Guide for Developing Countries, Aprilie, 2009, p. 91;

cuprind dispoziţiuni penale, cum ar fi legea dreptului de autor, această cerinţă ar trebui de asemenea aplicată.

- Pentru a evita dubla incriminare, ar trebui să se ţină cont de măsura în care legea penală se extinde şi asupra altor domenii înrudite. Extinderea care se întinde peste aceste limite necesită o examinare şi justificare atentă.

Mai mult, se sugerează ca unele definiţii prezentate în lista Consiliului Europei – cum ar fi cea a accesului neautorizat – să fie ulterior clarificate şi ajustate în lumina dezvoltării tehnologice a informaţiei şi a schimbărilor în domeniul criminalităţii informatice. Din anumite motive, alte tipuri de fapte care nu sunt incluse expres în listă, cum ar fi traficarea parolelor de computer obţinute în mod ilegal şi a altor informaţii despre mijloace de obţinere a accesului neautorizat la un sistem computerizat şi distribuirea de viruşi sau programe similare ar trebui, de asemenea, să fie luate în considerare de ţările candidate, în vederea incriminării lor în concordanţă cu tradiţia lor legislativă şi prin raportare la legile existente. O atenţie aparte ar trebui acordată şi în cazul în care infracţiunea finală ar putea fi privită ca o formă de sabotaj.

Rezoluţia recunoaşte eforturile depuse de OECD şi de Consiliul Europei şi promovează liniile de bază arătate de acest din urmă organism care a propus o listă minimă a actelor infracţionale ca şi o listă opţională a faptelor care ar trebui sancţionate de legile naţionale. Proiectul de rezoluţie a fost adoptat la Congresul AIDP ţinut la Rio de Janeiro, în anul 1994.

La nivel multistatal, Convenţia de la Budapesta[17] privind criminalitatea informatică constituie primul tratat internaţional în domeniul infracţiunilor penale comise contra reţelelor informatice sau cu ajutorul acestora.

Textul, semnat la 23 noiembrie 2001 de 30 de ţări dintre care Franţa şi Belgia, vizează armonizarea legislaţiilor naţionale pentru o lupta mai eficientă împotriva criminalităţii informatice, permiţând un tratament eficace cu privire la acţiunile autorilor infracţiunilor comise pe ascuns. Intrarea în vigoare a

[17] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

documentului internaţional a fost condiţionată de ratificarea acestuia de către parlamentele a 4 state semnatare, dintre care 3 membre ale Consiliului Europei, iniţiatoare ale textului.

În ceea ce priveşte conţinutul, Convenţia fixează dreptul comun în ceea ce priveşte măsurile de ancheta penală din domeniul reţelelor. Ea se bazează pe poziţia autorităţilor însărcinate cu lupta împotriva criminalităţii informatice care au o competenţă naţională exclusivă.

Raportat la elementele de noutate, Convenţia vine şi introduce noi proceduri în materia obţinerii şi colectării de date informatice necesare în cadrul anchetelor penale aflate în curs, permiţând obţinerea acestora.

Autorii Convenţiei au căzut de acord asupra a două cazuri în care agenţiilor de punere în aplicare a legii le este permis accesul la datele stocate în afara teritoriului lor: informaţiile disponibile publicului şi accesul având consimţământul persoanei legal autorizate.

Convenţia recunoaşte datelor numerice o valoare juridică şi efecte probatorii identice elementelor materiale existente în mediul extern.

Titlul 2 defineşte noţiunea de "conservare rapidă a datelor stocate". Modalităţile de punere în aplicare a acestei măsuri variază în funcţie de state.

Titlul 3, în cadrul articolului 18, prevede cazul de „încetare de producere de date". Această măsură trebuie să constituie fundamentul juridic care să permită reducerea anumitor date de către autorităţile competente[18].

Titlul 3, în cadrul articolului 19, vizează „căutările informatice de la distanţă". Datele căutate pot fi conservate pe un suport de stocare sau stocate într-un alt sistem informatic dacă acesta rămâne în limitele teritoriale ale statului „căutător". În revanşă, acest articol nu autorizează căutarea datelor stocate în străinătate, chiar dacă ele sunt accesibile prin intermediul reţelei.

[18] Pentru detalii, a se vedea *A. C. Moise*, Metodologia investigării criminalistice a infracţiunilor informatice, Ed. Universul Juridic, Bucureşti, 2011,p. 346;

Aceste dispoziţii sunt supuse condiţiilor legale ale statelor semnatare însă trebuie să respecte drepturile omului şi aplicarea principiului proporţionalităţii. Convenţia stabileşte şi anumite regulile de cooperare internaţională. Din punct de vedere al competenţei, fiecare ţară este competentă dacă infracţiunea este comisă: pe teritoriul său, la bordul vapoarelor sau avioanelor ce-i aparţin, sau când unul din resortisanţii săi este autorul acelei infracţiuni, dacă infracţiunea nu este de competenţa unui alt stat[19].

Autorii Convenţiei, căutând să răspundă provocărilor legate de combaterea criminalităţii informatice şi urmărind transmiterea rapidă şi continuă a datelor cu interes pentru statele membre, au aut ideea înfiinţării unei reţele de puncte de contact[20].

CAPITOLUL III
SECURITATEA CIBERNETICĂ

Securitatea cibernetică în Uniunea Europeană

Documentele prezente la nivelul Uniunii Europene ce privesc domeniul securităţii cibernetice privesc Strategia UE pentru Securitate Cibernetică(Concluziile Consiliului din iulie 2014 privind „Strategia Uniunii Europene pentru securitate cibernetică: un spaţiu cibernetic securizat, deschis şi sigur” şi Cadrul Strategic UE privind Drepturile Omului şi Democraţia. Comisia Europeană a publicat in februarie 2013, alături de Inaltul reprezentant pentru politică de securitate şi afaceri externe al Uniunii Europene, Strategia privind domeniul securităţii cibernetice, precum şi propunerea de Directivă a Comisiei in

[19] Idem, p. 341;
[20] Council of Europe. Economic Crime Division. Directorate General of Human Rights and Legal Affairs, The functioning of 24/7 points of contact for cybercrime, Strasbourg, France, April 2009, p. 4;

ceea ce priveşte Securitatea Informaţiei şi a Reţelelor (Directiva NIS), având articolul 114 din TFUE (Tratatul privind Funcţionarea Uniunii Europene) drept temei juridic.

Agenda europeană privind securitatea, reuşeşte să indeplinească un angajament insuşit in orientările politice enunţate de Jean-Claude Juncker, preşedintele Comisiei Europene, şi reuşeşte să inlocuiască strategia anterioară ce a fost adoptată in anul 2010(Strategia Uniunii Europene de securitate internă pentru perioada 2010-2014). Interesele aflate pe Agenda europeană, reuşesc stabilirea strategiei Uniunii, creată pentru a combate ameninţările la adresa securităţii Uniunii Europene in perioada 2015-2020. In ceea ce priveşte securitatea, UE şi statele membre se confruntă cu serioase provocări.

Criminalitatea organizată şi terorismul reprezintă reale probleme ce tind să devină din ce in ce mai serioase, societăţile din toate colţurile Europei devenind ţinte, de asemenea amploarea şi caracterul acestor probleme s-au schimbat. Europa suportă efectele create de instabilitatea politică din teritoriile din vecinătatea ei imediată, acestea reprezentând un pericol pentru securitatea Uniunii Europene.

Chiar daca este vorba de atacarea instituţiilor şi valorilor Europei, de recrutarea şi radicalizarea persoanelor în organizaţii teroriste sau de răspândirea urii, este absolut necesar să fie luate măsuri coordinate pentru combaterea de asemenea activităţi.

Principala responsabilitate pe care statele membre continua să o aibă este aceea de a asigura securitatea internă. Cu toate acestea, la adresa cetăţenilor Europei sunt din ce in ce mai multe ameninţări cu un caracter transfrontalier foarte pronunţat şi sunt foarte variate. Deşi statele membre răspund în primul rând de securitate , de cele mai multe ori nu reuşesc pe deplin dacă sunt pe cont propriu. Faptele de natură teroristă şi infracţională nu îşi limitează activitatea la frontierele Uniunii Europene şi nici la regiunile vecine.

Agenda europeană privind securitatea ar trebui să permită serviciilor de aplicare a legii şi serviciilor de poliţie din diferite state să realizeze un schimb eficient de date, dând dovadă de o bună cooperare în combaterea criminalităţii.Statele membre pot să conteze pe ajutorul oferit de agenţiile UE. În mare parte, agenta se concentrează pe constituirea de valoare adăugată la nivelul Uniunii prin:

Exemplul 1: Echipele comune pentru anchetă(JIT) vor aduna ofiţeri de poliţie din state membre pentru o perioadă de timp bine determinată, având scopul de a acheta diverse cazuri transfrontaliere. Va fi promovată de către Comisia Europeană utilizarea mai regulată a echipelor de anchetă comune a statelor membre şi va fi asigurat faptul că ţările terţe implicate în JIT vor fi incluse în cazurile ce au o dimensiune internaţională.

Exemplul 2: Agenţiile Uniunii, în special Eurojust şi Europol, au un rol crucial în realizarea anchetelor transfrontaliere şi a cooperării. Operaţiunea Arhimede, coordonată în septembrie 2014 de Europol pentru a aborda diferite grave infracţiuni comise în ţări terţe şi în 34 de state membre, a condus la arestarea a peste o mie de persoane pe întreg teritoriul European. Comisia Europeană garantează îmbunătăţirea coordonării activităţii agenţilor Uniunii Europene pentru se asigura că este valorificat potenţialul lor de cofinanţare, stimulare a formării şi sprijinire a statelor membre pentru asigurarea securităţii la nivelul UE:

Agenda pentru securitate reuşeşte să arate trei mari priorităţi de acţiune pentru Uniunea Europeană şi se concentrează asupra domeniilor în care poate fi observată o schimbare reală în cadrul Uniunii, acestea fiind:

1.Ameninţări importante la adresa securităţii UE sunt radicalizarea şi terorismul. Din cauza atacurilor recente din spaţiul European, a fost evidenţiată nevoia de a formula răspunsuri şi de a crea moduri de acţiune comune la nivelul UE pentru a combate asemenea evenimente şi pentru a răspunde de asemenea

pericolului creat de luptătorii din alte ţări ce se întorc în ţara de origine. Cu toate că acest fenomen nu este recent apărut, fluxul de luptători proveniţi din ţări precum Irak, Libia şi Siria şi amploarea, precum şi legătura evidentă dintre aceste conflicte sunt cu adevărat fără precedent.

2. Criminalitatea organizată are costuri economice, sociale şi umane semnificative, începând de la acţiuni precum traficul de persoane şi introducerea ilegală de imigranţi, traficul de ţigări, droguri sau arme de foc şi terminând la acţiuni precum infracţiunile de mediu, economice sau financiare.

3. Criminalitatea informatică prezintă un imens potential pentru infractori, astfel, pe măsură ce modul de viaţă al cetăţenilor şi activităţile acestora precum comerţul sau activitatea bancară se mută în mediul online, sunt oferite mai multe oportunităţi infractorilor. Având în vedere că din ce în ce mai multe date cu caracter personal sunt prezente şi stocate în mediul digital, dreptul la viaţa privată şi securitatea personală sunt în pericol. Abuzând de tehnicile moderne, infractorii beneficiază, reuşind să facă comerţ ilegal cu arme, droguri sau să realizeze alte activităţi ilegale. O importantă parte din lupta împotriva criminalităţii din mediul online vizează şi acţiunile elaborate pentru a combate infracţiuni precum exploatarea sexuală a minorilor.

Cele trei priorităţi relevate în cadrul agendei nu reprezintă fenomene noi, fiind deja prevăzute ca obiective strategice în Strategia de securitate internă a UE, în perioada 2010-2014. Datorită nivelului de complexitate al ameninţărilor, strategia europeană trebuie să se dezvolte în consecinţă. Pentru înfăptuirea acestui obiectiv, agenda îşi are baza în măsurile întreprinse în perioada recentă, reuşind să asigure o acţiune coerentă şi continuă.

La baza abordării Uniunii Europene în ceea ce priveşte combaterea ameninţărilor la adresa securităţii şi combaterea terorismului, trebuie să se afle valorile democratice comune însuşite de comunităţile europene deschise.

Respectarea drepturilor fundamentale şi securitatea nu reprezintă obiective care să se excludă reciproc ci mai degrabă reprezintă obiective complementare şi coerente. Comisia urmează să efectueze o evaluare pertinentă a instrumentelor de politică şi a celor legislative pentru a se asigura că aceste elemente respectă în deplinătate drepturile fundamentale şi asigură securitatea, precum şi că impactul eventual asupra protecţiei datelor cu caracter personal şi asupra libertăţii circulaţiei este în concordanţă deplină cu principiul proporţionalităţii. Abordarea Uniunii în ceea ce priveşte securitatea va promova şi va respecta drepturile fundamentale ale omului ce sunt prevăzute în Carta drepturilor fundamentale. Absolut toate instrumentele folosite trebuie să fie conforme cu principiile legalităţii, proporţionalităţii şi necesităţii, oferind garanţii menite să asigure răspunderea şi dreptul de a fi introduce căr de atac pe cale judiciară. Astfel, Comisia invită Consiliul şi Parlamentul European să accepte această agenda ca fiind Strategia reînnoită pentru securitate internă, în asociere cu apropiatul Consiliului European realizat în iunie 2015, şi să se implice active pentru punerea în aplicare, în cooperare strânsă cu absolut toţi actorii relevanţi.

În ceea ce priveşte **strategia de securitate cibernetică** a Uniunii Europene care înca nu a intrunit acordul unanim al statelor membre, dar a fost elaborată ca directivă de către Comisia Europeană, își propune să prevină și să reacționeze rapid la atacurile care afectează rețeaua de telecomunicații a Europei.

Propunerea de directivă europeană impune un nivel minim de securitate pentru tehnologiile, rețelele și serviciile digitale în toate statele membre. Dar, un acord privind stabilirea normelor europene referitoare la securitatea cibernetică a fost amânat din cauza punctelor de vedere diferite ale statelor membre. Aceste amânări vin într-un moment nepotrivit în condiţiile în care Europa se confruntă cu conflicte la granițele sale externe, iar ***atacurile cibernetice*** sunt tot mai frecvente.

Directorul Europol Rob Wainwright declara recent ca cele mai multe atacuri cibernetice vin din Rusia si Ucraina. Sa nu uitam si incdentul recent de la siteului televiziunii francez TV5 atacat de hackeri jihadisti. Provocările de securitate la adresa Europei de Est, pe fondul conflictului din Ucraina şi al relaţiilor tensionate cu Rusia, dar şi din sud unde organizaţii jihadiste se infiltrează în Europa şi folosesc reţele de internet. De asemenea, statele membre vor fi obligate să adopte strategii de securitate a rețelelor și a informațiilor și să instituie echipe de răspuns la incidente. S-ar crea rețele de cooperare la nivelul UE.

Potrivit unor surse europene există la nivelul Europol ample rapoarte, potrivit cărora statele membre ascund detalii importante privind dezvoltarea capacităților ofensive privind securitatea cibernetică. Totodată, NATO anunța că, în contextul dependenței tot mai mare de tehnologie și de internet, Alianța avansează în eforturile sale de a se confrunta o gamă largă de amenințări cibernetice care vizează rețelele sale de telecomunicatii. Atacurile cibernetice tot mai sofisticate fac ca protecţia comunicaţiilor Alianţei să devină o prioritate, mai ales în contextul provocărilor de securitate actuale.

Ce reprezintă strategia de securitate cibernetică a UE?

Strategia de securitate cibernetică a UE stabilește strategia UE de prevenire și reacție la perturbările și atacurile care afectează rețeaua de telecomunicații a Europei. Propunerea de directivă ar impune un nivel minim de securitate pentru tehnologiile, rețelele și serviciile digitale în toate statele membre. Aceasta propune, de asemenea, ca anumite întreprinderi și organizații să aibă obligația să raporteze incidentele cibernetice semnificative. Lista include motoare de căutare, furnizori de servicii de tip „cloud”, rețele sociale, administrații publice, platforme de plăți online, cum ar fi PayPal, și site-urile de comerț electronic majore, cum ar fi Amazon.

CAPITOLUL IV
PARTICULARITĂŢI ALE MANAGEMENTULUI INVESTIGĂRII FRAUDELOR INFORMATICE

Principalele probleme de clarificat în investigarea infracţiunilor informatice

Principalele probleme care trebuie clarificate în cadrul investigării infracţiunilor informatice ce se referă, în special, la identificarea aparaturii sau altor mijloace de accesare care au fost folosite sau au fost destinate să servească la săvârşirea faptei, a informaţilor obţinute în urma acţiunii ilegale, a hardware-ului ca rezultat al delictului, identificarea autorului şi a eventualilor participanţi, stabilirea condiţiilor care au favorizat comiterea faptei, consecinţele faptei, ş.a.

Identificarea obiectelor ce au fost folosite sau au fost destinate să servească la săvârşirea infracţiunilor informatice

Făcând parte din categoria „corpurilor delicte", aceste mijloace materiale de probă reprezintă mijloace de săvârşire a infracţiunii, fie că au fost folosite în acest scop, fie că urmau să fie utilizate de infractor pentru comiterea faptei.

De regulă, astfel de obiecte constituie izvor de probe, căpătând calitatea de surse de date procesuale. Aceste mijloace - examinate cu ajutorul metodelor şi mijloacelor ştiinţifice - pot revela elemente informative de maximă importanţă. Cu

toate acestea, ele nu au o valoare probatorie dinainte stabilită, urmând a fi valorificate în coroborare cu celelalte mijloace de probă[21].

Identificarea informaţiilor obţinute ca rezultat al infracţiunilor informatice

Deoarece indivizii obţin copii de software, violând legea copyright-ului, acestea vor putea fi în mod normal sechestrate, la fel ca ori care altă documentaţie care este obţinută în mod ilegal. De aceea, în cadrul cercetării, trebuie avut în vedere de la început producătorul de soft care poate permite cumpărătorului crearea unei copii de rezervă, dar care nu poate fi comercializată sau răspândită ca urmare a legii proprietăţii intelectuale (Copyright). De asemenea, obţinerea listei codurilor de acces şi a parolelor pentru reţelele guvernamentale, obţinută neautorizat, este o faptă penală, ea putând să reprezinte un act de spionaj, sabotaj, terorism, diversiune ş.a. Totodată, trebuie identificate alte date obţinute neautorizat.

Identificarea hardware-ului ca rezultat al infracţiunilor informatice

Procedurile legale permit emiterea de mandate pentru sechestrarea oricăror date ce sunt produse ale unor infracţiuni de acest tip dar şi a altor lucruri asemănătoare. În conformitate cu definiţia americană, "fructele crimei" include bunuri provenite din activităţi criminale precum bijuterii sau sume de bani gheaţă ce au fost obţinute în urma folosirii unei cărţi de credit falsificate. Organul de urmărire penală urmează să examineze dacă situaţiile au condus în mod sigur şi cert la consecinţe ilegale, în aşa fel încât să fie convins că obiectul respectiv a reprezentat un fruc al crimei sau a fost posedat în mod ilegal. Având în vedere premisele prezentate, este evident faptul că accesul ilegal la software-ul şi la hardware-ul unui calculator este considerat în termenii S.U.A, fruct al crimei sau contrabandă, respectiv delict informatic.

[21] **I. Vasiu**, *Criminalitatea Informatică*, Ed. Nemira, 1998

Identificarea circumstanţelor şi a autorului ce au favorizat comiterea unor infracţiuni informatice

În cazul făptuitorului, va fi stabilită modalitatea prin care acesta a putut accesa informaţii securizate, având în vedere şi posibilitatea utilizării neautorizate a unui calculator. În ceea ce îi priveşte pe ceilalţi participanţi, fiindcă de cele mai multe ori sunt vinovate mai multe persoane de comiterea unei asemenea infrastructure, este necesară stabilirea dacă acestea pot fi considerare parte dintr-o reţea ce acţionază cu scopul accesării ilicite a unor conturi, prin metode şi programe proprii, ori fiind folosite site-uri ţintă sau aflate în legătură cu o crimă de natură cibernetică.

Mijloace materiale de probă

Urma electronică

Impunându-se ca o veritabilă amprentă, acest gen de urmă este una din cele mai importante ţinte ale investigaţiei criminalistice a infracţiunilor informatice.

În momentul conectării la Internet, fiecare utilizator primeşte o identitate unică, un IP ce poate fi stabil (în cazul conectării directe) sau dinamic (în cazul conectării prin modem). În cazul celui din urmă, experienţa demonstrează că pot fi întâlnite probleme, în momentul încercării de identificare, pe parcursul anchetei.

Este cunoscut faptul că ISP-urile (Internet Service Provider) au obligaţia de a menţine, pentru o anumită perioadă de timp, fişiere cu loguri care oferă informaţii utile anchetatorilor, mai ales în cazul IP-urilor dinamice, a căror identitate poate fi greu determinată după mai mult timp de la săvârşirea faptei. Acţiunea unui utilizator pe Internet lasă o urmă electronică care se înregistrează într-un fişier log. Perioada de timp în care se păstrează fişierele log la nivel de servere private este la latitudinea administratorului reţelei respective.

În practică, în vederea contracarării atacurilor, a scanărilor de porturi, s-au specializat soft-uri pentru analiza de fişiere de log de pe servere. Prin aceste analize se pot examina anumite elemente care se repetă.

Astfel, un fişier log de pe un server va conţine: data şi ora accesului, IP-ul utilizatorului, porturile folosite, porturile scanate, fişierele accesate, timpul petrecut în locaţie.

Mai trebuie, de asemenea, precizat că toate serverele au încorporate servicii interne care să descopere scanarea de porturi, acesta fiind primul şi cel mai important element în prevenirea infracţiunilor electronice prin care se urmăreşte accesul în sistem.

De regulă, majoritatea reţelelor au montate pe fiecare staţie de lucru (maşină) un dispozitiv de tip Firewall, destinat prevenirii accesului din exterior a reţelei. Prin acest sistem reţeaua devine practic inutilizabilă.[22]

Informaţia ca instrument al infracţiunilor informatice

Instrumentul infracţiunii poate include atât elemente tangibile, cât şi virtuale. Astfel, în anumite cazuri, documentele care conţin informaţii şi instrumentele financiare folosite în comiterea faptei, pot fi sechestrate ca instrumente ale crimei.

Este necesar să subliniem că trebuie acordată multă atenţie conservării acestor date, în accepţiunea lor largă. Astfel, sunt avute în vedere nu numai datele afişate, ci şi cele memorate sau salvate, inclusiv notele scrise de mână după care s-a condus făptuitorul în săvârşirea infracţiunii.

De asemenea, investigatorii pot sechestra obiectele ce sunt destinate sau urmează a fi folosite ca instrumente ale delictului. Uneori acestea se vor potrivi criteriilor generale (de exemplu, proiecte pentru a ajuta hacker-ul să spargă parolele sau să fure listele cu numerele de pe cărţile de credit), dar, în alte cazuri, acest lucru s-ar putea să nu fie atât de simplu.

---

[22] J.Dibbel, „*My Tiny life – Crime and Passion in a Virtual World”*, Ed. Owl Book, New York, S.U.A., 1999

În practică, dacă se cercetează natura unui bulletin-board ilegal şi se cunoaşte că respectivul *bulletin* operează într-un singur PC ca home-page, un al doilea computer care se află în aceea încăpere nu va fi considerat instrument al delictului; dar, dacă anchetatorul ştie, în mod sigur, că suspectul avea în plan extinderea operaţiilor într-o a doua locaţie, cel de-al doilea computer va fi considerat ca având aceeaşi destinaţie delictuală şi va fi sechestrat ca instrument adiţional, dacă suspectul şi-a modificat în mod substanţial configurarea PC-ului sau a acţionat pentru îmbunătăţirea capacităţii de utilizare a acestuia, în vederea comiterii unui anumit tip de infracţiune.

Hardware-ul ca probă

Un obiect fizic de acest tip este considerat probă în identificarea unei persoane care a comis, o infracţiune, tară ca aceasta să fie admisă în mod necesar la proces. Instanţele vor efectua o sechestrare a aparaturii, în funcţie de convingerea intimă a anchetatorului, în circumstanţele date, fără ca acestuia să i se impute, ulterior, irelevanţa probei. Computerele conţin probe materiale; de exemplu, dacă o persoană trimite o scrisoare de ameninţare, în care pot fi identificate caracterele specifice, (partea de sus de la „W" este ştearsă, atunci cartuşul şi imprimanta vor constitui probe).

Dacă un computer şi toate perifericele sale reprezintă instrumentele unei infracţiuni, mandatul ar trebui să autorizeze sechestrarea lor integrală. Dar dacă se cercetează computerul doar pe documentele pe care aceste le conţine, justificarea reţinerii şi sechestrării hardware-ului ar putea fi mai greu de dispus.

De exemplu, dacă un individ comite o fraudă, prin intermediul cablului, trăgând la imprimantă mii de facturi false. În acest caz, se va dispune sechestrarea computerului, a monitorului, a tastaturii şi a imprimantei. În cazul în care individul a transmis electronic facturile victimelor, se va dispune de asemenea, sechestrarea modemului extern. Dacă, în loc să folosească poşta electronică, ar fi utilizat un fax convenţional, acesta trebuie sechestrat, jucând un rol important în anchetă.

Efectuarea unor acte de urmărire penală

Percheziţia calculatoarelor

Dacă un computer reprezintă fruct al crimei (în terminologia nord americană), instrument al infracţiunii sau probă, mandatul de percheziţie trebuie să vizeze computerul în sine şi în subsidiar informaţiile pe care le deţine. Mandatul ar trebui să fie cât mai detaliat în ceea ce priveşte descrierea componentelor care vor fi ridicate. Se vor include, acolo unde este posibil, date privind fabricantul, modelul, alte informaţii care pot servi la identificare. Sub raport tactic criminalistic este indicat să fie detaliate în mandat următoarele:

a)Descrierea locului ce trebuie percheziţionat. De regulă, un mandat specifică locaţia în care trebuie să aibă loc o percheziţie, anchetatorii urmând să ridice obiectele aflate în locul pe care aceştia le puteau accesa. Computerele conţin însă o lume virtuală, în care datele există nu sub o formă materială.

Într-o reţea, locaţia fizică a informaţiei poate fi necunoscută; de exemplu, un informator indică o fraudă financiară la firma la care lucrează, acesta vizând registrele falsificate în terminalul dintr-o clădire sau dintr-un anumit oraş, însă server-ul se află într-o altă clădire, oraş, ţară. Practic, ne putem afla în trei situaţii:

- informaţiile se află într-o locaţie externă, iar aceasta se află în afara localităţii, zonei etc.;
- informaţiile se află într-o locaţie, iar anchetatorii ştiu că aceasta se află în aceeaşi zonă;
- informaţiile se află într-o locaţie externă, necunoscută.

b)Descrierea obiectelor/aparaturii care trebuie percheziţionate şi ridicate. În primul rând, trebuie pornit de la modalitatea şi capacitatea de stocare. Atunci când proba conţine informaţii dintr-un sistem computerizat, dar computerul însuşi nu este instrument al infracţiunii, hardware-ul este un simplu dispozitiv de stocare. O diferenţă importantă dintre mediul fizic de stocare şi mediile electronice este dată de capacitatea lor de stocare. Un hard-drive standard de 40 de megabiţi conţine aproximativ 20.000 de pagini de informaţii, iar astăzi un drive de 200 conţine 100.000 de pagini.

Pornind de la această analogie, dacă anchetatorii au mandat doar pentru documentele din computer şi nu pentru computerul însuşi, mandatul ar trebui

redactat cu precizie, concret. Ca şi în alte cazuri de percheziţie, aria de aplicare a autorităţii mandatului va fi condiţionată de gravitatea infracţiunii. Fiecare mandat trebuie redactat în funcţie de natura faptei. El va trebui să vizeze conţinutul documentelor relevante şi în subsidiar dispozitivele de stocare pe care ar putea să le conţină. Nici măcar argumentul privind volumul mic de probe nu poate justifica ridicarea tuturor dispozitivelor de stocare.

Constatarea infracţiunii flagrante

Este flagrantă infracţiunea descoperită în momentul comiterii sau imediat după săvârşire. Reprezentând o procedură specială, constatarea infracţiunii flagrante capătă caracter procesual penal, iar procesul-verbal în care se consemnează aceasta devine, ca orice înscris ce are legătură cu fapta, mijloc de probă. Infracţiunea flagrantă reprezintă şi în cazul delictelor informatice o a doua excepţie de la efectuarea percheziţiei cu autorizarea magistratului[23].

În constatarea infracţiunilor cibernetice flagrante este esenţial să se manifeste aceeaşi atenţie în modul de acţiune, ca şi în cazul percheziţiilor, pentru conservarea urmelor electronice, a tuturor datelor în legătură cu delictul săvârşit.

CAPITOLUL V
CONCLUZII ŞI PROPUNERI

Concluzii privind cooperarea poliţienească internaţională în domeniul combaterii criminalităţii informatice

[23] **V. Dobrinoiu**, **N. Conea**, **C.R. Romi ţan**, **M. Dobrinoiu**, **N. Neagu**, **C. Tănăsescu**, *Drept Penal – Partea Specială vol. II*, Ed. Lumina Lex, 2004

Domeniul crminalităţii informatice a cunoscut o evolutie foarte rapidă de la începutul cooperării între state, stând la baza fondării sistemelor de asistenţă judiciară şi de cooperare în cadrul UE.

În plan normativ, convenţiile sunt foarte numeroase şi complicate (cuprinzând preambuluri, clauze finale, protocoale adiţionale etc.), în timp ce numărul de ratificări la nivel global este redus.

Guvernele europene colaborează oficial şi desfăşoară acţiuni comune pentru combaterea criminalităţii informatice, încă de la înfiinţarea Interpol-ului, în anul 1923. Cu toate acestea, nu s-a reuşit atingerea gradului de cooperare internaţională obţinut în activitatea grupărilor criminale transfrontaliere. Poliţia a obstrucţionat activitatea acestor reţele infracţionale, dar nu a reuşit să le destructureze definitiv. În acelaşi timp, procurorii s-au mulţumit cu obţinerea unor condamnări individuale, fără a afecta semnificativ ameninţarea pe care aceste reţele o reprezintă pentru economie şi societate privite ca întreg.

Problema cooperării poliţieneşti la nivel european în vederea prevenirii şi combaterii criminalităţii informatice trebuie abordată atât din perspectiva convenţiilor şi actelor comunitare existente şi a reglementărilor naţionale, cât şi din perspectiva elaborării unor noi instrumente de cooperare poliţienească şi a principiilor care trebuie să guverneze utilizarea concretă a acestor instrumente.

Combaterea fenomenelor infracţionale specifice transnaţionale constituie primul obiectiv al cooperării poliţieneşti. La acest nivel UE poate demonstra valoarea adăugată a intervenţiei sale. Modelul european de informare va permite în acest sens facilitarea activităţii serviciilor operative, clarificând diferitele canale de schimburi de date existente.

Principalul obiectiv al cooperării la nivelul UE în materie de respectare a aplicării legii este combaterea formelor de criminalitate informatică, care au în general o dimensiune transfrontalieră.

Este important ca posibilităţile de care dispun autorităţile de aplicare a legii de a obţine de la celelalte state membre informaţii şi date operative privind criminalitatea informatică să poată fi percepute într-o manieră orizontală şi nu din perspectiva diferenţelor în ceea ce priveşte tipul de infracţiuni sau repartizarea competenţelor între autorităţile de aplicare a legii şi autorităţile judiciare.

Personalul din unităţile de cooperare, precum şi din cele care beneficiază de cooperarea internaţională operativă, trebuie să înveţe să rezolve problemele în parteneriat cu unităţile similare la nivel internaţional, iar pentru rezolvarea acestui deziderat este nevoie de timp în scopul adaptării activităţilor la noul concept. De asemenea, trebuie să accepte ideea că *noua cultură şi valorile tradiţionale ale sistemului poliţienesc vor fi orientate, intersectate şi chiar influenţate de politicile comunităţii*[24].

Domeniile cooperării poliţieneşti în care managementul resurselor umane interculturale poate fi deosebit de util sunt reprezentate de instruirea comună a ofiţerilor de poliţie din diverse ţări şi cooperarea transfrontalieră a grupurilor de lucru şi a grupurilor operative. În aceste domenii, orientarea managerială combinată cu o conştientizare a diferenţelor culturale pot îmbunătăţi strategiile prin crearea sinergiilor interculturale. Elementele schimbării pot fi introduse la agenţiile de poliţie, atât în est, cât şi în vest, mai ales dacă acestea au de luptat cu inerţia unei culturi poliţieneşti statice[25].

Responsabilitatea asigurării de către România a cerinţelor UE la graniţa noastră externă ne obligă să gestionăm eficient schimbul de date şi informaţii derulate de ţara noastră pentru a nu permite creşterea actelor infracţionale, inclusiv pe domeniul criminalităţii informatice. Aceste cerinţe implică prevenţia, descoperirea şi combaterea modurilor de manifestare a fenomenului criminalităţii

[24] Platon, Sabin, *op.cit.*, pag. 239, 2014

[25] *O perspectivă europeană asupra activităţii de poliţie (sinteză documentară)*, Ministerul Internelor şi Reformei Administrative, 2007.

informatice, ceea ce generează permanent creşterea volumului schimbului de date şi de informaţii, atât între instituţiile statului nostru, cât şi cu altele similare din statele UE.

În urma cercetării efectuate în cuprinsul lucrării, am identificat trei obstacole majore în calea cooperării poliţieneşti internaţionale:

- o reticenţă naturală cu privire la schimbul de informaţii în domeniul criminalităţii informatice;

- coexistenţa în statele membre a diferitelor servicii de poliţie;

- faptul că întărirea cooperării poliţieneşti este tributară ameliorării cooperării judiciare în materie penală.

Căutarea şi schimbul de informaţii sunt o parte esenţială a muncii de poliţie, în special pentru prevenirea şi combaterea infracţiunilor. Succesul anchetelor şi combaterea consecutivă a infracţiunilor depind de calitatea informaţiilor obţinute, de analiza lor şi, mai ales de protecţia acestor informaţii faţă de persoanele sau organizaţiile care nu au dreptul să aibă cunoştinţă despre acestea. Din acest motiv există o reticenţă firească în a face schimb de informaţii, în special cu serviciile sau persoanele cu care nu există nicio relaţie de încredere reciprocă.

Cooperarea internaţională este complicată încă de coexistenţa, în numeroase ţări, a diferitelor corpuri de poliţie: poliţie civilă, poliţie militară, poliţii naţionale, regionale şi/sau locale, sau poliţie statală. În plan organizaţional, această coexistenţă a mai multor corpuri distincte de poliţie complică activitatea de cooperare, mai ales atunci când este vorba de schimbul de informaţii. De aceea, statele membre ale UE desemnează un singur serviciu care va fi competent pentru toate contactele internaţionale. Este indispensabil ca fiecare stat membru al UE să-şi organizeze cadrul intern, în aşa măsură încât toate serviciile implicate să poată lua parte la cooperarea internaţională.

Schimbul internaţional de informaţii nu se poate îmbunătăţi fără ca statele membre ale UE să dispună de anumite sisteme de cooperare, atât la nivel naţional

cât şi internaţional. În plan intern, trebuie să existe un sistem electronic de schimb de informaţii care să permită tuturor serviciilor de aplicare a legii să-şi transmită în mod rapid şi în siguranţă datele şi informaţiile de care au nevoie. Sistemul trebuie să cuprindă o funcţie de analiză a infracţiunilor, care să poată fi alimentată şi consultată de toate serviciile, pe întreg teritoriul ţării.

Al treilea factor se referă la cooperarea poliţienească internaţională în anchetele propriu-zise. Marea majoritate a tehnicilor de anchetă utilizate de către poliţie trebuie să fie autorizate în prealabil de către autorităţile judiciare, în acord cu reglementările procedural-penale naţionale. Convenţia privind asistenţa judiciară în materie penală din anul 2000 vizează simplificarea procedurilor generale de cooperare judiciară şi favorizează cooperarea privind tehnicile speciale de anchetă.

Un alt obiectiv prioritar la nivel european îl constituie acela de a împiedica utilizarea de către infractori a spaţiului fără frontiere pentru a scăpa de anchete şi urmăriri. Cercetarea eficienţei operative trebuie să fie criteriul care determină nivelul de cooperare, fie el regional, naţional, european sau internaţional.

Într-un mod mai general, eficienţa cooperării poliţieneşti presupune dezvoltarea unor relaţii strânse cu ţările terţe. UE va trebui să încheie, atunci când este necesar, acorduri de cooperare poliţienească. În acest cadru, trebuie luate măsuri pentru consolidarea complementarităţii între acţiunea Uniunii şi cea a statelor membre.

De asemenea, este primordial pentru UE să fie în măsură *să consolideze prevenirea criminalităţii informatice.* Pentru a evalua impactul acţiunii sale, Uniunea trebuie să dispună de *instrumente statistice de măsurare a activităţilor infracţionale.* În plus, este necesară elaborarea unei *abordări comune* care să ofere un cadru de intervenţie a actorilor locali şi naţionali (atât din partea autorităţilor de aplicare a legii, cât şi din partea societăţii civile).

În combaterea criminalității informatice, care se caracterizează prin lipsa frontierelor și prin enorm de multe posibilități pentru infractori de a se ascunde,

avem nevoie de un răspuns flexibil și adecvat. Centrul european de combatere a criminalității informatice este menit să ofere această expertiză în calitate de centru de fuzionare, de centru pentru investigații operaționale și asistență în domeniul criminalisticii, dar și prin abilitatea sa de a mobiliza toate resursele relevante din statele membre UE pentru a atenua și reduce amenințarea pe care o reprezintă infractorii informatici, indiferent de locul de unde aceștia acționează" a declarat Troels Oerting, șeful Centrului de combatere a criminalității informatice.[26]

Documentarea, în cadrul procesului de elaborare a tezei de doctorat, s-a dovedit a fi o operaţiune deosebit de complexă. În concret, referitor la baza bibliografică, am procedat la: consultarea specialiştilor în domeniul cooperării poliţieneşti şi judiciare internaţionale în materie penală din cadrul Poliţiei Române şi Ministerului Public; parcurgerea lucrărilor de referinţă teoretice şi de specialitate din ţară şi străinătate şi actualizarea şi completarea operativă a volumului de surse informaţionale prin intermediul internetului.

Cercetarea a vizat atât aspectele de ordin teoretic, cât şi cele de ordin practic şi procedural referitoare la cooperarea poliţienească internaţională în domeniul combaterii criminalităţii informatice.

Elementele de noutate şi contribuţiile personale aduse în domeniul supus cercetării ştiinţifice sunt, în opinia noastră, următoarele:

a) *Tratarea într-o viziune integrată, a cooperării poliţieneşti internaţionale în domeniul combaterii criminalităţii informatice.* Deşi în trecut au mai fost publicate lucrări de referinţă în domeniul cooperării poliţieneşti internaţionale în domeniul combaterii criminalităţii informatice, acestea au abordat în mod fragmentar, neunitar problematica supusă cercetării. Lucrarea de faţă propune cititorului, în mod unitar, abordarea fenomenului.

[26] Centrul european de combatere a criminalității informatice (EC3), ianuarie 2013

b) *Un alt element de noutate îl constituie radiografierea în detaliu a tuturor instituţiilor implicate în cooperarea poliţienească şi judiciară în context european*.

c)*Îmbunătăţirea eficientiă a managementului juridic, instituţional şi procedural în domeniul supus analizei şi cercetării*. Aceste propuneri sunt motivate şi prezentate pe larg în ultima secţiune a tezei.

Propuneri privind îmbunătăţirea cadrului juridic, instituţional şi procedural circumscris cooperării poliţieneşti internaţionale în domeniul combaterii criminalităţii informatice

Faţă de cele afirmate în lucrare şi în concluzii apreciem pertinente unele propuneri, şi anume:

1. O propunere se referă la coordonarea sistemelor penale naţionale în scop represiv. Fiecare dintre sistemele penale naţionale incriminează infracţiuni informatice, potrivit politicii penale a statului respectiv, ori pericolul regional, continental sau global ce îi reprezintă criminalitatea informatică prin extinderea şi diversificarea unor categorii de infracţiuni, impune ca o necesitate actuală cooperarea între aceste sisteme naţionale penale.
2. Iniţierea unor măsuri eficiente atât sub aspect poliţienesc cât şi normativ la toate nivelele şi în toate ţările pentru prevenirea şi lupta împotriva criminalităţii informatice. Este nevoie şi de măsuri legislative de redefinire a acestei infracţiuni deoarece nu există o definiţie internaţională comună, pentru criminalitatea informatică, conţinutul acestei noţiuni variind de la o ţară la alta.
3. Efectuarea unei analize asupra posibilităţilor de asigurare a individualităţii şi personalităţii fiecărei structuri conform legislaţiei interne şi internaţionale, prin servicii separate (Punctul Naţional Focal, S.E.C.I., Unitatea Naţională Europol, Serviciul de Informaţii Suplimentare Schengen, ataşaţii de afaceri interne şi ofiţerii români şi cei străini de legătură) iar Biroul Naţional Interpol să fie transferat din cadrul Inspectoratului General al Poliţiei Române la Centrul de Cooperare Poliţienească Internaţională.
4. Consider necesară apariţia unui „*Drept al Internetului*” sau un „*Cod al legislaţiei societăţii informaţionale*” pentru următoarele considerente:

– sistemele electronice de comunicaţie neputând fi secretizate perfect devin vulnerabile în faţa acţiunilor ilegale comise prin intermediul computerelor;

- nevoia de reglementare juridică a internetului rezidă şi din aceea că unele fapte comise în această reţea, cad deja sub incidenţa unor legi existente;
- adoptarea acestor legi este absolut necesară în condiţiile integrării României în structurile Uniunii Europene, în plus pericolul criminalităţii informatice pentru societatea românească este unul real, motiv pentru care consider că va impulsiona interesul acestora pentru luarea unor măsuri de securitate.

Progresul cooperării poliţieneşti este frânat de punerea în aplicare prea lentă şi insuficientă a instrumentelor juridice adoptate la nivel comunitar. De aceea, suntem de părere că este necesară transpunerea rapidă în dreptul intern a deciziilor luate de către UE. De asemenea, este necesară ratificarea urgentă de către toate statele membre a convenţiilor internaţionale cu incidenţă în domeniu.

În aceşti ultimi ani, diverse sisteme de comunicaţii şi baze de date au fost puse în aplicare în cadrul UE, la dispoziţia serviciilor de prevenire şi combatere a criminalităţii. Printre cele mai importante, menţionăm Sistemul de informaţii al Europol-ului, SIS, Sistemul de informaţii criminale Interpol, Sistemul de informaţii vamale etc.

În vederea evitării suprapunerii şi înregistrării aceleiaşi informaţii în mai multe sisteme de date, opinăm faptul că există trei soluţii posibile:

a) Fuzionarea sistemelor existente într-un singur sistem de informaţii al UE, care va evolua prin integrarea sistemelor care vor deveni necesare în toate domeniile de activitate. De exemplu, o soluţie ar putea fi fuzionarea SIS cu Sistemul de informaţii al Europol-ului şi plasarea Birourilor Sirene sub managementul Europol.

b) Menţinerea sistemelor existente şi autorizarea creării de noi sisteme, în funcţie de necesităţile viitoare ale serviciilor de aplicare a legii.

c) Soluţia intermediară o constituie armonizarea formatelor de date şi informaţii şi a regulilor de acces între diferitele sisteme, permiţând actualelor sisteme să evolueze pentru a asigura interoperabilitatea.

În prezent, soluţia intermediară este opţiunea cea mai viabilă, însă în viitor se impune cu stringenţă crearea unui sistem unic de informaţii privind criminalitatea la nivelul UE.

Având în vedere aspectele expuse anterior, suntem de părere că pot fi instituite noi forme de cooperare în context european. *Propunerea noastră care prezintă un interes special este aceea de înfiinţare a unor grupuri de lucru, a grupurilor de investigaţii sau a grupurilor operative pe o mai mică bază formală.* Cooperarea ar putea fi limitată în termenii competenţelor, ai perioadelor de timp implicate sau ai graniţelor geografice. Acest fapt ar prezenta două avantaje: în primul rând, acest tip de cooperare la nivel inferior nu vine în conflict cu principiul suveranităţii naţionale; în al doilea rând, ea intensifică interacţiunea personală directă dintre poliţiştii din aceste ţări, având în spate fonduri culturale diferite. Pe această cale, grupurile bilaterale sau multinaţionale îşi pot dezvolta propriile strategii noi.

În prezent, există deja o cooperare extinsă între ofiţerii de legătură trimişi de statele membre, în funcţie de nevoile lor naţionale, în ţări terţe şi la organizaţii internaţionale. *Cu toate acestea, este necesar să fie consolidate anumite aspecte ale cooperării între ofiţerii de legătură, în scopul unei utilizări cât mai bune a resurselor statelor membre.* De aceea, este necesar să se consolideze cooperarea dintre statele membre în acest domeniu, pentru a facilita schimbul de informaţii, în vederea combaterii formelor grave ale infracţionalităţii informatice.

Viitorul este legat de permanenta îmbunătăţire a schimbului de informaţii. Libera circulaţie a persoanelor, a bunurilor şi a serviciilor impune o cooperare deosebită în schimbul de informaţii. *Propunerile noastre în vederea îmbunătăţirii schimbului de date şi informaţii în cadrul cooperării poliţieneşti la nivel european,* sunt următoarele:

- reducerea timpului de primire a răspunsurilor solicitate prin OIPC-Interpol, SECI etc.

- Continuarea si realizarea în mod operativ a schimbului de informaţii;
- simplificarea modului de transmitere a informaţiilor şi a cererilor de asistenţă prin imbunataitrea sistemelor deja existente;
- schimbul de experienţă pentru cunoaşterea reciprocă a cerinţelor din activitatea curentă şi a sistemului juridic;
- acord direct cu ofiţerii de legătură şi ataşaţii de afaceri interne, cu cei de la Europol şi Interpol;
- operativitate mai mare din partea ofiţerilor de legătură români, crearea unor modalităţi concrete de cooperare cu ofiţerii de legătură, fără intermediere din partea SECI;
- sa se faca progrese mai mari in ceea ce priveste armonizarea legislaţiilor şi procedurilor de lucru;
- crearea unui sistem standard pentru schimbul de date şi informaţii între România şi statele Uniunii Europene, care sunt vizate din ce in ce mai mult de către cetăţeni români pentru locuri de muncă (Spania, Italia, Germania, Franţa etc.).

Libera circulaţie a persoanelor în cadrul spaţiului de libertate, securitate şi justiţie necesită măsuri destinate compensării deficitelor de securitate create prin suprimarea controalelor la frontiere, infractorii fiind în măsură să se deplaseze la fel de liber precum cetăţenii care respectă legea. Faţă de situaţia actuală şi experienţa acumulată, *este necesară legiferarea principiilor fundamentale comune, ameliorarea mecanismelor existente şi reglementarea structurilor care să permită progresul cooperării.*

În acest sens, *considerăm necesară adoptarea la nivel european a unei Directive a Consiliului UE privind îmbunătăţirea cooperării poliţieneşti între statele membre ale UE, în special la frontierele interne, şi de modificare a Convenţiei de punere în aplicare a Acordului Schengen.*

Suntem de părere că trebuie acordată o importanţă deosebită promovării unor măsuri de natură practică, abordărilor inovative, inclusiv prin analiza fezabilităţii mecanismelor internaţionale structurate, şi bunelor practici pentru stimularea cooperării internaţionale în domeniul combaterii criminaltăţii organizate şi întărirea eficienţei mecanismelor existente în acest domeniu. Astfel de *măsuri şi bune practici* pot include următoarele:

- În domeniul cooperării internaţionale privind produsele infracţiunilor, adoptarea de măsuri pentru facilitarea la cel mai extins mod posibil a asistenţei acordate celorlalte state pentru identificarea, urmărirea, indisponibilizarea[27] şi confiscarea unor astfel de produse;
- Utilizarea mijloacelor moderne de comunicare pentru a transmite şi răspunde solicitărilor urgente de asistenţă judiciară reciprocă, precum şi a celor mai moderne mecanisme de furnizare a asistenţei, în special utilizarea videoconferinţei ca modalitate de audiere a martorilor şi experţilor;
- Măsuri practice pentru facilitarea, creşterea eficienţei echipelor comune de anchetă atunci când infracţiunea sau infracţiunile cercetate prezintă elemente transnaţionale;
- Utilizarea extinsă şi consistentă a reţelelor judiciare în scopul eficientizării activităţii de investigaţie şi urmărire penală;
- Promovarea în continuare a practicii de detaşare în străinătate a magistraţilor de legătură în vederea facilitării comunicării şi soluţionării eventualelor interpretări eronate a diferitelor sisteme de drept.

Dezvoltarea criminalităţii la nivel internaţional a dus la o creştere considerabilă a numărului de cazuri în care mai multe state membre au jurisdicţie, conform normelor interne de procedură din fiecare stat, în ceea ce priveşte urmărirea penală şi judecarea infracţiunilor informatice. De aceea, *este necesară facilitarea rezolvării pretenţiilor conflictuale legate de jurisdicţie între statele membre şi, atunci când este posibil, evitarea multiplei urmăriri penale*[28].

În domeniul anchetelor penale privind infracţiuni informatice, probele pot fi obţinute pe două căi: pe baza cooperării poliţieneşti sau judiciare. Riscul obţinerii probei în baza unei cereri de asistenţă poliţienească adresată altui stat, constă în faptul că proba obţinută pe această cale nu poate fi folosită în procesul penal (reprezintă doar un indiciu). De aceea, trebuie îmbunătăţită cooperarea poliţienească

[27] În ceea ce priveşte procedura, este nevoie de o îmbunătăţire a procedurii de transmitere directă a mandatelor de indisponibilizare între autorităţile judiciare. În prezent, în multe state membre se cere transmiterea prin intermediul unei autorităţi centrale. Cu toate acestea, aproape toate statele membre dispun de reglementări privind imediata executare a deciziilor, precum şi privind termenele de indisponibilizare. De asemenea, este nevoie de o îmbunătăţire semnificativă a implementării prevederilor privind motivele de nerecunoaştere şi de neexecutare. Statele membre au transpus majoritatea motivelor, însă acestea au fost aplicate ca fiind motive obligatorii.

[28] Hester, Judith; Klackl, Michael; Mucha, Gabriele; Reich, Roman; Schneider, Birgit; Tiegs, Harald; Tolstiuk, Michael; Zainea, Mariana, *op.cit.*, pag. 16, 2014

în domeniul combaterii criminalităţii informatice, pentru că actele astfel obţinute pot fi folosite imediat de organul judiciar în actul de acuzare.

În viitor ar trebui să fie realizată o evaluare amănunţită a instrumentelor legislative în vigoare şi a raporturilor dintre acestea, incluzând nu numai deciziile-cadru, dar şi raporturile dintre aceste decizii-cadru şi instrumentele multilaterale în vigoare. Procesul început cu mandatul european de arestare ar trebui să continue.

BIBLIOGRAFIE

I. Legislaţie

1. Constitutia României, din 21 noiembrie 1991, republicată, publicată în Monitorul Oficial Partea I, nr. 767 din 31 octombrie 2003- modificată şi completată prin Legea de revizuire a Constituţiei României nr. 429/2003 publicată în Monitorul Oficial Partea I, nr. 758/29.10.2003
2. Codul Penal Român, adoptat prin Legea 286/2009 actualizata, emitent: Parlamentul;
3. Lege 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; emitent: Parlamentul; (aplicabilă cu data de 25 noiembrie 2007;
4. Lege nr. 64 din 24 martie 2004 pentru ratificarea Convenţiei Consiliului Europei privind criminalitatea informatică adoptată la Budapesta la 23 noiembrie 2001; emitent: Parlamentul; publicat în: Monitorul Oficial nr. 343 din 20 aprilie 2004;
5. Lege nr. 365 din 7 iunie 2002 privind comerţul electronic, emitent: Parlamentul; publicat în: Monitorul Oficial nr. 483 din 5 iulie 2002;
6. Hotărâre nr. 1.308 din 20 noiembrie 2002 privind aprobarea Normelor metodologice pentru aplicarea Legii nr. 365/2002 privind comerţul electronic; emitent: Guvernul; publicat în: Monitorul Oficial nr. 877 din 5 decembrie 2002;
7. Lege Nr. 8 din 14 martie 1996 privind dreptul de autor şi drepturile conexe; emitent: Parlamentul; publicat în: Monitorul Oficial NR. 60 din 26 martie 1996, modificată de Legea nr. 285 din 23 iunie 2004 pentru modificarea si completarea Legii nr. 8/1996 privind dreptul de autor şi drepturile conexe; emitent: Parlamentul; publicat în: Monitorul Oficial nr. 587 din 30 iunie 2004;

Ordonanţa urgenţă a Guvernului nr. 123 din 1 septembrie 2005 pentru modificarea şi completarea Legii nr. 8/1996 privind dreptul de autor şi drepturile conexe; emitent: Guvernul; publicat în: Monitorul Oficial nr. 843 din 19 septembrie 2005

8.Lege nr. 196 din 13 mai 2003 privind prevenirea şi combaterea pornografiei; emitent: Parlamentul; publicat în: Monitorul Oficial nr. 342 din 20mai 2003; modificată de Legea nr. 496 din 12 noiembrie 2004. Parlamentul; publicat în: Monitorul Oficial nr. 1.070 din 18 noiembrie 2004;

9.Ordonanţa nr. 130 din 31 august 2000, privind regimul juridic al contractelor la distanţă; emitent: Guvernul; publicat în: Monitorul Oficial nr. 431 din 2 septembrie 2000, modificată de Legea nr. 51 din 21 ianuarie 2003 pentru aprobarea Ordonanţei Guvernului nr. 130/2000 privind regimul juridic al contractelor la distanţă; emitent: Parlamentul; publicat în: Monitorul Oficial nr. 57 din 31 ianuarie 2003;

10. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică; emitent: Parlamentul; publicat în: Monitorul Oficial nr. 429 din 31 iulie 2001;

11.Ordin nr. 389 din 27 iunie 2007 privind procedura de avizare a instrumentelor de plata cu acces la distanta, de tipul aplicaţiilor Internet-banking, home-banking sau mobile-banking; emitent: Ministerul Comunicaţiilor ŞI Tehnologiei Informaţiei; publicat în: Monitorul Oficial nr. 485 din 19 iulie 2007;

12.Regulament nr. 4 din 13 iunie 2002 privind tranzacţiile efectuate prin intermediul instrumentelor de plată electronică şi relaţiile dintre participanţii la aceste tranzacţii; emitent: Banca Naţională a României; publicat în: Monitorul Oficial în. 503 din 12 iulie 2002;

13. Lege nr. 677 din 21 noiembrie 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date; emitent: Parlamentul; publicat în: Monitorul Oficial nr. 790 din 12 decembrie 2001;

14. Lege nr. 506 din 17 noiembrie 2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice; emitent: Parlamentul; publicat în: Monitorul Oficial nr. 1.101 din 25 noiembrie 2004;

15. Lege nr. 102 din 3 mai 2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal; emitent: Parlamentul; publicat în: Monitorul Oficial nr. 391 din 9 mai 2005;

16.Lege nr. 451 din 1 noiembrie 2004 privind marca temporală; emitent: Parlamentul; publicat în: Monitorul Oficial nr. 1.021 din 5 decembrie 2004 activităţii electronice notariale; emitent: Parlamentul; publicat în: Monitorul Oficial nr. 1.227 din 20 decembrie 2004;

Hotărârea nr.271 din 15.05.2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, publicată în Monitorul Oficial, Partea I nr. 296 din 23.05.2013;
Hotarare Nr.494 din 11.05.2011 privind înfiinţarea Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică - CERT-RO
Decizia Curtii Constitutionale nr. 17 / ianuarie 2015 asupra obiectiei de neconstitutionalitate a dispozitiilor legii privind securitatea cibernetica;
Declaratia Summit-ului NATO de la Lisabona (paragraful 40) ;
Legea de functionare si organizare a DIICOT nr. 508/2004;
Legea de functionare si organizare a Politiei Romane nr. 218/2002;
Ghidul de legislatie si proceduri privind cooperarea judiciara internationala in materie penala;
Ghid de cooperare judiciara internationala in materie penala;
Legea 300/2013 pentru modificarea si completarea Legii nr. 302/2004 privind cooperarea judiciara internationala in materie penala. Lege nr. 300/2013

II. Tratate, cursuri, monografii, articole româneşti

1. G.Rătescu, L. Ionescu-Dolj, I.Gr. Perieteanu, V. Dongoroz, HL.Asnavorian, M. Papadopolu, N. Pavalescu, Codul penal adnotat, vol. I (partea generală), vol.II şi III (partea specială), Editura Librăriei, Socec, Bucureşti, 1937;
2. L.Vasiliu, D. Pavel, G. Antoniu, D. Lucinescu, V. Papadopol, V. Rămureanu, codul penal comentat şi adnotat, partea generală, Editura Ştiinţifică şi enciclopedică, Bucureşti, 1972;
3. L. Vasiliu şi colaboratorii, Codul penal comentat şi adnotat, partea specială, VoI. I, Editura Ştiinţifică şi Enciclopedică, Bucureşti, 1975;
4. L. Vasiliu şi colaboratorii, Codul penal comentat şi adnotat, partea specială, VoI II, Editura Ştiinţifică şi Enciclopedică, Bucureşti, 1977;
5. Costică Voicu, Florin Sandu, Ion Dascălu – Frauda în domeniul financiar-bancar şi al pieţei de capital;Editura Trei – Bucureşti 1998;
6. Costică Voicu, Florin Sandu – Managementul organizaţional în domeniul ordinii publice, editura M.A.I. – 2000;
7. Costică Voicu, Ştefan Prună, - Managementul organizaţional al poliţiei; editura Mediuna – Bucureşti 2007;
8. Costică Voicu şi colaboratorii, Globalizarea şi criminalitatea economico-lanciară, Editura Universul Juridic, Bucureşti, 2005;
9. Ion Neagu, Drept procesual penal. Tratat, Editura Global Lex, Bucureşti, 2002;
10. Al. Boroi, Ghe. Nistoreanu, Drept penal, partea generală, Editura AllBeck Bucureşti, 2004;

11. Dobrinoiu, G.Nistoreanu, I.Pascu, Al.Boroi, LMolnar, V.Lazăr, Drept penal, partea generală, Editura Europa Nova, Bucureşti, 1997;
12. I. Luca – Cooperarea poliţienească internaţională – editura Fundaţia universitară Dunărea de jos, Galaţi 2006;
13. C. Bulai, Manual de drept penal, partea generală, Editura All, Bucureşti, 1997;
14. Tudor Amza, Cosmin-Petronel Amza, Criminalitatea informatică, Ed. Lumina Lex, bucureşti, 2003;
15. Maxim Dobrinoiu, Infracţiuni în domeniul informatic, Editura C.H. Beck, Bucureşti, 2006 22. Ioana Vasiu, Criminalitatea informatică, Editura Nemira, Bucureşti, 1998;
16. Ioana Vasiu, Criminalitatea informatică, Ed. Nemira, Bucureşti, 2001;
17. Ioana Vasiu, Totul despre hackeri, Ed. Nemira, Bucureşti, 2001;
18. Ioana Vasiu, Lucian Vasiu, Prevenirea criminalităţii informatice, Editura Hamangiu, Bucureşti, 2006;
19. T. Dima, Drept penal, partea generală, vol.I 2004, vol.II 2005, Editura Lumina Lex, Bucureşti;
20. V. Dobrinoiu, W. Brânză, Drept penal, partea generală, Editura Lumina Lex, Bucureşti, 2003;
21. F.Streteanu, Drept penal, partea generală, Editura Rosetti, Bucureşti, 2005;
22. AI. Boroi, Ghe. Nistoreanu, Drept penal, partea specială, Editura AllBeck, Bucureşti, 2004;
23. V. Dobrinoiu, Drept penal, partea specială, vol.I, Editura Lumina Lex, Bucureşti, 2004;
24. V. Dobrinoiu, N. Conea, C.R. Romiţan, M. Dobrinoiu, N.
25. Tănăsescu, Drept Penal Partea Specială vol. II, Ed. Lumina Lex, 2004;
26. V. Dobrinoiu, Drept Penal - Partea Specială. Teorie şi Practică Judiciară, Ed. Lumina Lex, 2002
27. Toader, Drept penal, partea specială, Editura AllBeck, Bucureşti, 2002;
28. V. Lazăr, Drept penal, partea specială, Editura AllBeck, Bucureşti ;
29. Antoniu, C. Bulai, Practica judiciară penală, vol.I, partea generală, Editura Academiei, Bucureşti, 1988;
30. Antoniu. C. Bulai, Practica judiciară penală, vol.II, partea generală, Editura Academiei, Bucureşti, 1990;
31. Antoniu, C. Bulai, Practica judiciară penală, vol.III, partea specială, Editura Academiei, Bucureşti, 1992;
32. Dobrinoiu şi colaboratorii, Cauze penale comentate, partea specială, Bucureşti, 2003;
33. Toader, Drept penal, partea specială, culegere de probleme din

practica judiciară, Editura All Beck, Bucureşti, 2003;
34. Antoniu, E. Dobrescu, T. Dianu, G. Stroe, T. Avrigeanu, Reforma legislaţiei , Editura Academiei, Bucureşti, 2003;
35. I.Vasiu, Criminalitatea Informatică, Ed. Nemira, 1998 Albastră, 2002;
36. I.Vasiu, Drept şi Informatică. Protecţia juridică a programelor, Studii
37. de drept Românesc, Ed. Academiei Române, 1993;
38. Amza, CP. Amza, Criminalitatea Informatică, Ed. Lumina Lex, 2003;
39. I.Vasiu, Totul despre Hackeri, Ed. Nemira, 2001;
40. L. Vasiu, 1. Vasiu, INTERNET-Ghid de navigare, Ed. Albastră, 1996;
41. D. Oprea, Protecţia si Securitatea Informaţiilor, Ed. Polirom, 2003;
42. C. Troncotă, Neliniştile Insecurităţii, Ed. Tritonic, 2005;
43. V. Haga, Dreptul şi calculatoarele, Ed. Academiei Române, 1991;
44. L. Bir, Internet. Ghid complet de utilizare, Ed. Corint, 2004;
45. W. dom, Reţele de calculatoare, Ed. Corint, 2004
46. V.V. Patriciu, Criptografia şi securitatea reţelelor de calculatoare, Ed.
47. Tehnică, 1994;
48. G. Antoniu, Vinovăţia penală, Editura Academiei Române, Bucureşti, 1995;
49. V. Papadopol, D. Pavel, Formele unităţii infracţionale în dreptul penal român, Editura Şansa, Bucureşti, 1992;
50. Balaban, Infracţiuni prevăzute în legi speciale care reglementează domeniul Comerţului, Editura Rosetti, Bucureşti, 2005;
51. Ioana Vasiu, Unele aspecte de procedură penală privind mediul informatizat, în Revista de Drept Penal nr.1/2001;
52. Laura Codruţa Kovesi, Accesul şi supravegherea sistemelor de telecomunicaţii sau informatice, în Revista PRO LEGE nr.2/2003
53. Laura Codiuţa Lascu, Autorizarea accesului la sistemele de telecomunicaţii sau informatice, Dreptul nr. 1 din 2003;
54. Costică Păun, Unele consideraţii privind conceptele juridice şi reglementările existente pe plan internaţional în domeniul criminalităţii informatice, Pro Lege nr.3 din 2002;
55. Dorin Ciuncan, Înşelăciunea în contractele informatice prin intermediul Internetului, Revista de drept penal nr.3 din 1999;
56. Costică Păun, Unele consideraţii privind conceptele juridice şi reglementările existente pe plan internaţional în domeniul criminalităţii informatice, Pro Lege nr.3 din 2002;
57. Sorin Corlăţeanu, Costel Căşuneanu: Delicte contra datelor şi sistemelor informatice, Dreptul nr. 11 din 2004;
58. Laura Codruţa Kovesi, Sorin Finta, Încadrarea juridică a unor fapte de fraudă informatică, Dreptul nr. 12 din 2006 ;
59. Ioana Vasiu, Lucian Vasiu, Frauda informatică, Revista de Drept Penal nr. 1 din 2005;

60. Vasile Pătulea, Informaticajuridică, Dreptul nr. din 2006;
61. Ioana Vasiu, Lucian Vasiu, Contaminanţii informaţiei ca vector al accesului ilegal, Revista de drept penal nr.2 din 2006;
62. Ioana Vasiu, Prevenirea infracţiunilor informatice. Criptografia, Revista de Drept Penal nr. 2 din 1997;
63. Ioana Vasiu, Noi infracţiuni generate de tehnologia informaţiei, Revista de drept penal nr. 2 din 2000;
64. Dorin Ciuncan, Înşelăciunea în contractele informatice prin intermediul Internetului, Revista de drept penal nr.3 din 1999;
65. Laura Codruţa Kovesi, Augustin Lazăr, Accesul şi supravegherea sistemelor de telecomunicaţii sau informatice. Mijloace de probă, Dreptul nr. 7 din 2003;
66. Raluca Bercea: Documentul care reproduce datele unui contract înscris pe un suport informatic reglementat prin Proiectul Codului civil român constituie un mijloc de probă? Dreptul nr. 5/2005;
67. Ioana Vasiu, Cyberterorismul în discuţia specialiştilor, Revista de drept penal nr. 4 din 1999;
68. Ioana Vasiu, Modalităţi de comitere a infracţiunilor informatice. Programe distructive, Revista de Drept Penal, nr. 3 din 1997;
69. Alexandru Codescu, Dorina Davidescu. Infracţionalitatea informatică.
70. Eduard Bişceanu – Evaluarea riscurilor la care este supusă România prin terorismul cybernetic;

III. Tratate, cursuri, monografii, articole străine

1. Veron, Droit penal special, Armand Colin, Paris, 1998;
2. Bainbridge, Computers and the Law, Ed. Pitman, Londra, 1990;
3. Bertrand, Les contracts informatiques, Ed. Les Paques, Paris, 1983 ;
4. Bertrand, Protection juridique du logiciel, Ed. Les Paques, paris, 1984;
5. L. Le Moigne, La Modelisation des Systemes Complexes, Ed.
6. Dunod,1990;
7. L. Le Moigne, Systemique et Complexite, Revue Internationale de Systemique, 1990;
8. L. Le Moigne, Traduction de Sciences des Systenmes, Sciences de lartificie1, Ed. Dunod, 1991;
9. C. Lugan, La systemique sociale, Ed. PUF, 1993;
10. L von Bertalanffy, General System Theory: Foundations, Development, Applications, New York, 1998;
11. L. von Bertalanffy, The Organismic Psychology and Systems Theory, Worcester, 1998;
12. L. von Bertalanffy, Theorie des Systemes, Ed. Dunod, 1993;

13. L. von Bertalanffy, Perspectives on General Systems Theory;
14. Scientific-Philosophical Studies, New York, 1975;
15. de Rosnay, Le macroscope vers un vision globale, Paris, Seuil, 1975;
16. E. Morin, La metode, Ed. Dunod, 2001;
17. B. Walliser, Systemes et Modeles. Introduction critique a l'analyse de systemes, Seuil, 2007;
18. Y. Barel, Prospective et analyse de systeme, Documentation francaise, 1971;
19. E. Friedberg, Politiques urbaines et strategies corporatives, Ed. Sociologie du Travai1, 2008;
20. E. Friedberg, L 'acteur et le systeme, Paris, Seui1, 2001;
21. E.F. Codd, A Relaţional Model of Data for Large Shared Data Banks, 2007;
22. M. Eigen, P. Schuster, The Hypercycle: A Principie of natural self-organization, Springer, Berlin, 1979;
23. M. Mirapaul, Kosovo Conflict Inspires Digital Art Projects, New York Times Cybertimes, Apri115, 1999;
24. McShane, Yugoslavs Condemn Bombs Over E-mail to U.S. media, Nando Times, Apri1 17, 1999;
25. J. Pollock, A. Petersen, Unsolicited E-Mail Hits Targets in America in First Cyberwar, Wall Street Joumal, April8, 1999;
26. Montgomery, Enemy in Site - Time to Join the Cyberwar, Daily Telegraph, Australia, April 19, 1999;
27. Verton, Net Service Shields Web Users in Kosovo, Federal Computer Week, Apri1 19, 1999;
28. V. Rodger, Online Hiiman-Rights Crusaders, USA Today, August 25, 1999;
29. Lohr, Go Ahead, Be Paranoid: Hackers Are Out to Get you, New York Times, March 17, 1997;
30. Arquilla, D. Ronfeldt, M. Zanini, Networks, Netwar, and Information-Age Terorism, Countering the New Terrorism, 1999;
31. L. Staten, Testimony before the Subcommittee on Technology, Terrorism and Govemment Information, U.S. Senate Judiciary Committee, February 24, 1998;
32. Whitelaw, Terrorists on the Web: Electronic Safe Haven, U.S. News & World Report, June 22, 1998;
33. Oaks, Every Web Site a Chat Room, Wired News, June 14, 1999.
34. Stone, Profto BuildArchive of Insurgency Groups, Newsbytes, March 3, 1999;
35. Harris, Web Becomes a Cybertool for Politica/ Activists, Wall Street Journal, August 5, 1999;
36. Wall Street Journal, August 5, 1999;

37. D,Renfeldt, 1. Arquilla, Graham E. Fuller, M. Fuller, The Zapatista A Social Netvor, Report MR-994-A, 1998;
38. N.McKay, Pentagon Deflects Web Assault, Wired News, September 10,1998;
39. R.Alison, Belgrade Hackers Bombard MoD Website in First Internet War, PA New,March31, 1999;
40. E-Mail Attack on SriLanka omputers. omputer ecurity lert.No. 83, Computer Security Institute, June 1998;
41. 1.Wolf, First Terrorist Cyber-AttackReportedby D.S., Reuters, May 5, 1998;
42. P.Rey, E-Strikes and Cyber-Sabotage: Civilian Hackers Go Online to Fight, Fox News, April15, 1999;
43. R.Wesly, Controversial Basque Web Site Resurfaces, Wired News, August 28;
44. Y.Brides, The Zorros of the Net, Le Monde, November 16,1997;
45. Anti Terrorist Squad Orders Political Censorship of the Internet, press release from Internet Freedom, September 1997;
46. L.Murdoch, Computer Chaos Threat to Jakarta, Sydney Morning Herald, 18.08.1999;
47. .Williams, Federal Web Sites Dnder Attack After Embassy Bombing Newsbytes, May 10,1999
48. Barr, Anti-NATO Hackers Sabotage 3 Web Sites, Washington Post 12.05.1999;
49. Elton, Hacking in the Name of Democracy in China, The Toronto
50. Star, July 4 1999;
51. Taylor, CDC Says Hackers Are the Threat, IT Daily, August 26, 1999;
52. Glave, Confusion Over Cyberwar, Wired News, January 12, 1999;
53. Huang, Hackers War Erupts Between Taiwan, China, Associated Press, Taipei, Taiwan, August 9, 1999;
54. Beijing Tries to Hack D.S. Web Sites, Associated Press, July 30,1999;
55. Bridis, Hackers Become An Increasing Threat, Associated Press, July 7, 1999;
56. Gross, Israeli Claims to Have Hacked Saddam Off the Net, London Sunday Telegraph, February 7, 1999;
57. Colin, The Future of Cyberterrorism, Crime and Justice International, March 1997;
58. National Information Systems Security Conference, October 1997;
59. Computers at Risk, National Academy Press, 1991;
60. Church, Information Warfare Threat Analysis for the United States of America, Part Two: How Many Terrorists Fit on a Computer Keyboard'? Journal Infrastructural Warfare, Summer 1997;

61. Soo Hoo, S. Goodman, L. Greenberg, Information Technology and the Terrorist Threat, Survival, No. 3, Autumn 1997;
62. Critical Foundations: Protecting America 's Infrastructures, The Report of the President's Commission on Critic ai Infrastructure Protection, October 1997,Report Summary, http://www.pccip.gov.;
63. Protecting America 's Critical Infrastructures: PDD 63, The White House, May 22.1998 ;
64. CIW ARS Intelligence Report, Centre for Infrastructural Warfare Studies, June 21,1998 ;
65. Pentagon Computer Systems Hacked, Info Security News, June 1998;
66. D.Paternak, B. B. Auster, Terrorism at the Touch of a Keyboard, U.S.;
67. News & World Report, July 13,1998;

IV. Resurse Internet

1. http://www.crime-reasearch. org
2. http://cvberpo1ice. over-blog. corn
3. http://foldoc.doc.ic.ac.uk
4. http://w ww .mir. es/policia
5. http://www.efrauda.ro
6. http://www.europol.eu
7. http://www.eurojust.eu
8. http://www.interpol.eu
9. http://www.cepol.eu
10. http://www.frontex.eu
11. http://www.ic3. gov Internet Crime Complaint Centre
12. http://www.intemetcrimeforum.org.uk
13. http://ifccfbi.gov . Internet Fraud Complaint Centre
14. http://www. internetidentitv. corn Anti-phishing Consultancy la. http://www. interpol. int/Public/Technolo gyCrime
15. Il. http://www.nhtcu.org National High Tech Crime Unit (UK)
16. http://www . webopedia. corn Webopedia
17. http://www.netintercept. corn Computer Forensics
18. http://www. forensicon. corn E-discovery Specialists
19. http://www.world-check.com Terrorist Profite
20. http://www. centrex.police.uk Central Police Training and
21. Development Authority
22. http://www.hightechcrimeinstitute.com http://www.wikien.info
23. http://www.legalmountain.com Computer Crime Legislation
24. http://www .ncalt.com National Centre for Applied Leaming
25. Technologies
26. http://www.govtsecuritv.com

27. http://www.federalcrimes.com
28. http://www.scams.net
29. http://www.anti-spy.info
30. http://www.acunefix.com
31. http://rhizome.org/camivore
32. http://wvvw.pewintemet.org
33. http://www.kindercam.com
34. http://www.epic,org Centru de Informare pentru Confidenţialitate
35. Electronică
36. http://www. eff.org/Pri vacy Electronic Frontier Foundation
37. http://www privacyalliance.org Online Privacy Alliance
38. http://www.fbi.or g/hq/lab/Camivore Diagnostic