CZU 343.7:004.056

TIPURILE ŞI METODELE DE SĂVÂRŞIRE A INFRACȚIUNILOR INFORMAȚIONALE

Alexandru PARENIUC,
dr. în drept, conf. univ.

Andrei GHIMPU,
doctorand

Articolul cuprinde o analiză succintă a tipurilor şi metodele de săvârşire a infracțiunilor informaționale.

Cuvinte-cheie: Tehnologie, IT, infracțiuni informatice, infracțiuni în domeniul telecomunicațiilor, accesarea ilegală, frauda informatică, pătrunderea în sistemul informatic.

TYPES AND METHODS OF INFORMATION OFFENSES COMMITTING

Alexandru PARENIUC,
PhD, associate professor

Andrei GHIMPU,
PhD student

The article contains a brief analysis of the types and methods of committing information crimes.

Keywords: Technology, IT, computer offenses, telecommunications offenses, illegal access, computer fraud, entry into the computer system.

„Technology is the art of turning science into something practical." [1]

Introducere. Odată cu evoluția timpului, societatea îmbrățișează din ce în ce mai mult tehnologia informației. Informația care până nu de mult avea la bază hârtia îmbracă acum forma electronică. Informația pe suport de hârtie mai este încă rezervată documentelor oficiale, acolo unde este necesară o semnătură sau o ștampilă. Adoptarea semnăturii electronice deschide însă perspectiva digitizării complete a documentelor, cel puțin din punct de vedere funcțional.

Acest nou mod de lucru, în care calculatorul a devenit un instrument indispensabil și un mijloc de comunicare prin tehnologii precum poșta electronică sau Internetul, atrage după sine riscuri specifice. O gestiune corespunzătoare a documentelor în format electronic face necesară implementarea unor măsuri specifice. Măsurile ar trebui să asigure protecția informațiilor împotriva pierderii, distrugerii sau divulgării neautorizate. Cel mai sensibil aspect este acela de a asigura securitatea informației gestionată de sistemele informatice în noul context tehnologic.

Securitatea informației este un concept mai larg care se referă la asigurarea integrității, confidențialității și disponibilității informației. Dinamica tehnologiei informației induce noi riscuri pentru care organizațiile trebuie să implementeze noi măsuri de control. De exemplu, popularizarea unităților de inscripționat CD-uri sau a memoriilor portabile de capacitate mare induce riscuri de copiere neautorizată sau furt de date.

Lucrul în rețea și conectarea la Internet induc și ele riscuri suplimentare, de acces neautorizat la date sau chiar frauda.

Dezvoltarea tehnologică a fost acompaniată și de soluții de securitate, producătorii de echipamente și aplicații incluzând metode tehnice de protecție din ce în ce mai performante. Totuși în timp ce în domeniul tehnologiilor informaționale schimbarea este exponențială, componenta umană rămâne neschimbată. Asigurarea securității informațiilor nu se poate realiza exclusiv prin măsuri tehnice, fiind în principal o problemă umană. Majoritatea incidentelor de securitate sunt generate de o gestiune și organizare necorespunzătoare, și mai puțin din cauza unei deficiențe a mecanismelor de securitate. Este important ca organizațiile să conștientizeze riscurile asociate cu utilizarea tehnologiei și gestionarea informațiilor și să abordeze pozitiv acest subiect printr-o conștientizare în rândul angajaților a importanței securității informațiilor, înțelegerea tipologiei amenințărilor, riscurilor și vulnerabilităților specifice mediilor informatizate și aplicarea practicilor de control.

Materiale și metode de cercetare aplicate. În limitele de studiu al acestui articol, în calitate de metodă ce cercetare principală întru realizarea studiului de față a fost utilizat un spectru larg de surse sub formă de monografii, atât în domeniul tehnologiilor informaționale, cât și în materia protecției dezvoltării acestei tehnologii ireversibile. Studierea și analiza acestora nu ar fi fost posibile în mod eficient decât prin utilizarea metodelor de cercetare, de genul: observația, metoda deducției, metoda comparativă, metoda istorică, metoda logică, precum și cea sistemică.

Rezultate obținute și discuții. Totodată, dezvoltarea tehnologiilor informaționale a sporit considerabil eficiența afacerilor în cele mai diferite sfere de activitate (economie, medicină, drept etc.), rețelele de telecomunicații permit efectuarea tranzacțiilor în regim real de timp, viteza de procesare a sporit considerabil, iar companiile sunt capabile să păstreze și să prelucreze masive enorme de date.

Însă, pe lângă aspectele pozitive, a apărut un șir de fenomene negative – infracțiunile informatice, adică realizarea unor acțiuni directe sau indirecte, fizice sau logice, premeditate sau nepremeditate, ce au scop modificarea uneia sau mai multor stări (confidențialitate, integritate, accesibilitate, non-repudiere) ale unui sistem sau subsistem informațional.

Potrivit raportului cu privire la Indicele Global Cybersecurity (GCI v3) realizat și analizat de către Uniunea Internațională a Telecomunicațiilor din anul 2019, Republica Moldova s-a clasat pe locul 31 la nivel regional și pe locul 53 la nivel global, aceasta fiind printre țările care au dezvoltat angajamente complexe și se angajează în securitatea informatică, programe și inițiative.

Acest indice este axat pe politicile guvernamentale și structurile legislative ale UE și reprezintă o referință de încredere ce măsoară angajamentul țărilor pentru securitatea cibernetică la nivel global cu scopul de a crește gradul de conștientizare cu privire la importanța și dimensiunile diferite ale problemelor existente [2].

Criminalitatea în mediul virtual, generic denumită e-crime sau cybercrime, a avut o evoluție dramatică, acest fenomen cunoscând patru etape, și anume:

– prima (specifică anilor ’80), care a fost caracterizată de banalizarea informaticii, piratarea programelor, falsificarea cărților de credit;

– a doua (specifică sfârşitului anilor ’80), a fost favorizată de apariţia reţelelor locale şi extinse, precum şi a punţilor de legătură, şi caracterizată de importante deturnări de fonduri şi „isprăvile” hacker-ilor care accesau calculatoarele NASA, CIA şi oricare altă ţintă care reprezenta un simbol politico-tehnologic sau un element al puternicului complex militaro-industrial american;
– a treia (specifică anilor ’90), care a coincis cu proliferarea sistemelor informatice şi reţelelor de comunicaţii (Internet-ului, în special) şi a fost caracterizată de specializarea infractorilor, apariţia unor „veritabili” profesionişti ai pirateriei, deturnărilor de fonduri, sabotajelor informatice;
– a patra (în prezent), favorizată de faptul că sistemele informatice au pătruns în toate sectoarele vieţii sociale şi le controlează pe cele mai importante dintre ele (transporturi, apărare etc.), şi care este caracterizată de conturarea de noi şi grave ameninţări ca terorismul informatic, războiul informatic etc. [3, p.53].

Scopul principal al studiului este de a evidenţia acţiunile necesare de a fi întreprinse, care sunt aspectele-cheie la care este nevoie să se acorde atenţia pentru a fi siguri că nu au fost distruse dovezile şi, nu în ultimul rând, necesitatea pregătirii cadrelor capabile să efectueze o expertiză juridică calitativă.

Infracţiunile informatice, la fel ca şi în cazul infracţiunilor obişnuite, au un subiect şi obiect al infracţiunii.

Subiectul infracţiunii informatice poate fi definit ca persoana care, motivată de anumiţi factori (necunoaştere, curiozitate, interes material etc.), realizează acţiuni ce contravin normelor legale sau etice.

Reglementarea infracţiunilor informatice în legislaţia naţională a venit ca o adaptare firească a legislaţiei la realităţi ce nu puteau fi ignorate. Astfel, în Codul penal al Republicii Moldova, adoptat prin Legea nr. 985 din 18.04.2002, în vigoare din 12.06.2003 în premieră a fost introdus capitolul „Infracţiuni informatice şi Infracţiuni în domeniul telecomunicaţiilor”, care cuprindea iniţial trei articole: art.259 – Accesul ilegal la informaţia computerizată; art.260 – Producerea, importul, comercializarea sau punerea ilegală la dispoziţie a mijloacelor tehnice sau produselor program şi art.261 – Încălcarea regulilor de securitate a sistemului informatic.

După ratificarea Convenţiei Consiliului Europei privind criminalitatea informatică, adoptată la Budapesta la 23.11.2001, prin Legea nr. 6 din 02.02.2009, Codul penal al R. Moldova, fiind armonizat în conformitate cu prevederile Convenţiei prin Legea nr 278 din 18.12.2008, ambele publicate în MO la 20.02.2009, a fost suplinit cu articole noi 260^1-260^6, care prevedeau noi tipuri de infracţiuni cum ar fi interceptarea ilegală a unei transmisii de date, perturbarea funcţionării sistemului informatic, falsul informatic, frauda informatică etc. [4].

Potrivit Convenţiei Consiliului Europei privind criminalitatea informatică *I* (adoptată la Strasbourg la 28 ianuarie 2003), printre momentele-cheie se constată categoriile infracţiunilor din domeniul informatic:

– accesarea ilegală;
– interceptarea ilegală;
– afectarea integrităţii datelor;
– afectarea integrităţii sistemului;
– abuzurile asupra dispozitivelor;
– falsificarea informatică;
– infracţiuni referitoare la pornografia infantilă;
– infracţiuni referitoare la atingerile aduse proprietăţii intelectuale şi drepturilor conexe.

Prevederile Convenţiei vizează primordial armonizarea dispoziţiile de drept material în domeniul infracţiunilor informatice, la fel introduce dispoziţii procedurale indispensabile în procesul investigării şi urmăririi unor asemenea categorii de infracţiuni şi pune pe rol un proces rapid şi eficient de cooperare internaţională. Convenţia deci se referă atât la

incriminarea unor fapte ca infracțiuni, cât și la alte aspecte de drept material, referitoare la răspunderea penală, participație și sancțiuni. Așadar, potrivit enumerării enunțate mai sus, se definesc nouă infracțiuni grupate în patru categorii diferite.

Astfel, sunt considerate infracțiuni următoarele tipuri:

1. aducând atingere confidențialității, integrității și disponibilității datelor și sistemelor informatice: accesarea ilegală (art.2), interceptarea ilegală (art.3), alterarea integrității datelor (art.4), alterarea integrității sistemului (art.5) și abuzurile asupra dispozitivelor (art.6);

2. privind mediul informatic: falsificarea informatică (art.7) și frauda informatică (art.8);
3. privind minorii: pornografia infantilă (art.9);

4. aducând atingere proprietății intelectuale și drepturilor conexe: încălcarea drepturilor proprietății intelectuale și a drepturilor conexe (art.10). [5].

Așadar, infracțiunile informatice pot fi separate în două categorii: infracțiuni a căror săvârșire a fost facilitată de tehnologiile informaționale, și infracțiunile unde calculatoarele și rețelele de calculatoare reprezintă ținta atacului.

Atunci când un calculator este utilizat pentru săvârșirea unei infracțiuni, pe suportul de date pot fi găsite înregistrări despre frauda comisă care include informație despre identificarea falsă, reproducerea și distribuirea informației, informație-subiect al proprietății intelectuale, colectarea și distribuirea pornografiei și multe altele (acces nesancționat la resurse, instrumente de ocolire/ înlăturare a protecției logice etc.).

Infracțiunile la care calculatoarele și rețelele de calculatoare reprezintă *obiectul* infracțiunii constă, de obicei, în distrugeri de date și resurse tehnice. Adesea, calculatoarele compromise sunt utilizate pentru compromiterea altor calculatoare și/sau rețele-obiect al infracțiunii (aplicații malefice – viruși, instrumente de organizare a atacurilor direcționate DDoS etc.)

Un atac asupra unui sistem informatic se realizează prin următorii pași:

1. Cercetarea sistemului informatic în vederea obținerii de informații.

Primul pas în cadrul unui atac informatic îl reprezintă cercetarea sistemului informatic pentru a obține informații importante care pot fi utilizate în atac. Așadar, este important să se obțină informații, cum ar fi de exemplu tipul hardware-ului utilizat, versiunea software, informații personale ale utilizatorilor, care pot fi utilizate în următorul pas. Acțiuni utile în obținerea informațiilor includ: „ping sweeps" (metodă de a scana rețeaua) pentru a determina dacă sistemul informatic țintă răspunde; scanarea porturilor pentru a observa care porturi pot fi deschise; întrebări care trimit mesaje de avariere înapoi la sistem, când o problemă de transmitere a fost detectată; ghicirea parolelor.

2. Pătrunderea în sistemul informatic

Imediat ce sistemul informatic țintă a fost identificat, iar informațiile despre el au fost adunate, următorul pas este de a lansa atacul în scopul pătrunderii în sistem.

3. Modificarea setărilor sistemului informatic

Modificarea setărilor sistemului informatic reprezintă următorul pas după ce s-a pătruns în sistemul informatic. Acest pas permite atacatorului să reintre în sistemul informatic compromis mult mai ușor.

4. Comunicarea cu alte sisteme

Odată ce rețeaua sau sistemul informatic au fost compromise, atacatorul le utilizează în scopul de a ataca alte rețele și computere. Aceleași instrumente care sunt utilizate în pasul nr.1 sunt acum îndreptate spre alte sisteme.

5. Afectarea rețelelor și a dispozitivelor

Acest pas include ștergerea sau modificarea fișierelor, furtul datelor valoroase, distrugerea computerelor, sau atacurile DOS

(Denial of service attacks) [6, p.142].

În concluzie, apariția noilor tehnologii a adus și aduce beneficii extraordinare omenirii, dar poate să conducă și la distrugerea ei dacă nu se acționează pentru crearea unui cadru legal național care să răspundă cerințelor locale, dar în corelație cu cadrul regional și internațional.

1. Astfel, consider că succesul creării unei societăți informatice depinde, în mare parte, de soluționarea unui spectru de probleme juridice, economice și organizaționale, cum ar fi:

• Elaborarea și definirea unei terminologii unice în domeniul securității informatice și al dreptului informatic;

• Analiza practicilor moderne și armonizarea actelor normative în vigoare cu practicile internaționale și anume armonizarea în materie de documentare a dovezilor și în chestiunile de reproducere a înregistrărilor informatice – Societatea Informațională are nevoie de un drept specific evoluat;

• Reglementarea tranzacțiilor electronice. Elaborarea unui cadru legal adecvat pentru afaceri, care să reglementeze nu numai comerțul electronic și semnătura electronică, ci și aspectele referitoare la banii electronici, fiscalitatea și modul de încheiere a contractelor în Internet;

• Elaborarea tehnicilor și metodologiilor de cercetare a infracțiunilor informatice. Datorită caracterului transfrontalier al criminalității informatice, armonizarea legislației cu cea internațională trebuie să vizeze, în principal: dreptul de autor, confidențialitatea datelor, prevenirea și combaterea criminalității informatice, precum și promovarea standardelor tehnice care să asigure intercomunicarea noilor rețele de comunicații.

• Crearea programelor de studiu și pregătirea specialiștilor în domeniul securității informatice;

• Crearea în structurile de stat a funcțiilor, responsabile pentru implementarea și administrarea mecanismelor de securitate informațională;

• Organizarea seminarelor de aprofundare a cunoștințelor și de schimb de experiență cu specialiștii în domeniu din alte țări [7].

Legiuitorul urmează să instituie reguli procesuale general-valabile cu privire la examinarea sistemelor informatice și a suporturilor de stocare a datelor informatice, efectuată în cadrul acțiunii de urmărire penală, la orice etapă procesuală – fie în cadrul urmăririi penale, fie la etapa judiciară. Din aceste considerente, este oportună introducerea unui articol nou în CPP privind reglementarea acțiunilor de urmărire penală efectuate asupra datelor informatice, în redacția: „**Articolul 130[1]** . *Percheziția informatică*" [8, p. 124,150].

2. Este necesară transpunerea în CPP al RM, dar și în Legea cu privire la asistența juridică internațională în materie penală, a instituției conservării datelor informatice, prevăzută în Legea privind prevenirea și combaterea criminalității informatice, în vederea asigurării protejării probelor electronice volatile. Astfel, este necesară completarea CPP cu art.130[2] având următorul conținut: „**Articolul 130[2]** . *Conservarea imediată a datelor informatice*" [8, p. 151].

În acest context, urmează a fi completată și Legea cu privire la asistența juridică internațională în materie penală, după cum urmează: la art.1 alin. (3) cu lit. a[1]) având următorul cuprins: „a[1]) conservarea imediată a datelor informatice;"; - cu articolul 13[1] în următoarea redacție: „ **Articolul 13[1]** *Conservarea imediată a datelor informatice*"

4. Conținutul art.134[1] CPP („*Monitorizarea conexiunilor comunicațiilor telegrafice și electronice*") urmează a fi racordat la denumirea acestuia, așa încât să reglementeze doar ridicarea datelor referitoare la traficul informatic. Totodată, colectarea informațiilor cu privire la conținutul comunicării informatice urmează să fie expusă într-un articol nou („*Interceptarea informatică*") [8, p. 133].

5. Este necesară eliminarea lacunei legislative de la art.133 CPP („*Reținerea, cercetarea, predarea, percheziționarea sau ridicarea trimiterilor poștale”*) și art.134[1] CPP *(„Monitorizarea conexiunilor comunicațiilor telegrafice și electronice”*) , prin care ambele reglementează modul de ridicare a comunicărilor electronice: „*comunicări prin poșta electronică*”, „*comunicații electronice*”, „*corespondență electronică*”. Astfel, propunem modificarea alin.(2) al art.133 CPP, prin excluderea cuvintelor „*și prin poșta electronică*”, iar după îmbinarea „scrisori de orice gen,” să fie introduse cuvintele „*cu excepția celor electronice*” [8, p. 134].

6. În vederea identificării conexiunilor dintre infracțiunile săvârșite în diferite locuri, a stabilirii legăturilor dintre diferite persoane, fapte și circumstanțe, a punerii în aplicare a tuturor activităților criminalistice la un nivel tehnologic avansat, se impune crearea unei baze de date centralizate pentru organele de drept, cu informație operativă pe cauzele de criminalitate informatică, care să conțină date cu privire la [8, p. 154]:

- toate operațiunile de plată electronică frauduloase (reușite și nereușite);
- conturile (bancare, telefonice, electronice) care au avut legătură directă cu infracțiunile informatice, inclusiv ale victimelor, de buffer și pentru lichefierea mijloacelor bănești;
- persoanele care au fost implicate direct în aceste infracțiuni;
- adresele IP prin intermediul cărora au fost efectuate conexiunile în procesul de pregătire, săvârșire și ascundere a infracțiunii (și anume, ale serverelor și sistemelor informatice utilizate la: gestionarea centrelor de control al botnetului, răspândirea virușilor, accesarea neautorizată a informației computerizate și altele);
- numele de domeniu ale site-urilor utilizate în pregătirea și comiterea infracțiunii;
- numerele de telefon, adresele poștelor electronice, conturile din softurile de comunicare rapidă, adresele MAC ale dispozitivelor ș.a., având legătură directă; viruși, botneturi etc.;
- subdiviziunile organelor de drept care au efectuat investigațiile, instituțiile de expertiză care au examinat sistemele și rețelele informatice.

Pe lângă datele textuale formalizate, baza de date ar trebui să prevadă și posibilitatea de a salva date-media indexate: texte, imagini, înregistrări video și audio, documente electronice [8].

Referințe bibliografice

1. Citat de Marcio Barrios (http://subiecte.citatepedia.ro/despre.php?s=tehnologie);
2. https://stisc.gov.md/ro/content/republica-moldova-clasata-pe-locul-53-raportul-indicele-global-cybersecurity-2018 (vizitat la 10.02.2020);
3. Gheorghe-Iulian Ioniță, Infracțiuni din sfera criminalității informatice. București, Ed.Pro Universitaria, 2013;
4. Codul penal al Republicii Moldova, nr. 985-XV din 18.04.2002. În: Monitorul Oficial al Republicii Moldova nr.128-129/1012 din 13.09.2002. Republicat în: Monitorul Oficial al Republicii Moldova nr.72-74/195 din 14.04.2009;
5. Convenția Consiliului Europei privind criminalitatea informatică, (adoptată la Strasbourg la 28 ianuarie 2003), p.153;
6. Adrian Cristian Moise, Metodologia investigării criminalistice a infracțiunilor informatice, Editura Universul Juridic, București 2011., p.142;
7. Valeriu Cernei, Probleme de cercetare a infracțiunilor informatice,
8. http://www.security.ase.md/publ/ro/pub-ro28.html;
9. Purici S., Metodica cercetării infracțiunilor din domeniul informaticii. Monografie. Chișinău: CEP USM. 2018, p. 124,150, 151,

153, 133, 134, 154;

Literatura consultată

10. Codul de procedură penală al Republicii Moldova, nr. 122-XV din 14.03.2003. În: Monitorul Oficial al Republicii Moldova, nr.104-110/447 din 2003. Republicat în: Monitorul Oficial al Republicii Moldova nr. 248-251/699 din 05.11.2013;
11. Lege cu privire la informatică, nr. 1069-XIV din 22.06.2000. În: Monitorul Oficial al Republicii Moldova nr.73-74/547 din 05.07.2001;
12. Lege privind prevenirea și combaterea criminalității informatice, nr. 20-XVI din 03.02.2009. În: Monitorul Oficial nr.11-12/17 din 26.01.2010;
13. Adrian-Cristian Moise, Dimensiunea criminologică a criminalității din cyberspațiu, București, Editura C.H.Beck, 2015.
14. Metodologia investigării criminalistice a infracțiunilor informatice, Editura Universul Juridic, București, 2011.
15. Dumitru Oprea, Premisele si consecințele informatizării contabilității. Iași, Editura GRAEIX, 1994.
16. Conf. dr. Ioana VASIU, Lucian VASIU, Probleme juridice ale societății informatice, http://www.racai.ro/INFOSOC-Project/.
17. Dicționar de informatică. Editura Științifica și enciclopedică. București, 1981.
18. Parsons, M. (1998). Crime Prevention and the Electronic Frontier, FBI Law Enforcement Bulletin, www.fbi.org;
19. Андрей Белоусов, Уголовное право и информационные технологии, http://www.crime-research.ru/analytics/1928/, 2005.
20. Беломеря М.Н., "Научно-методические аспекты подготовки специалистов в области информационной безопасности", http://www.crime-research.ru/analytics/Belom/, 2005.

Despre autori:

Alexandru PARENIUC,
doctor în drept, conferențiar universitar,
prodecan al Facultății ,,Drept, ordine publică și securitate civilă"
a Academiei ,,Ștefan cel Mare" a MAI al RM,
e-mail:alexandru.pareniuc@mai.gov.md
tel.:(+373)079402970

Andrei GHIMPU,
doctorand, anul I de studii,
Școala doctorală ,,Științe penale și drept public"
a Academiei ,,Ștefan cel Mare" a MAI al RM,
e-mail:andrei.ghimpu@igp.gov.md
tel.:(+373)060033442