CRIMINALITATEA INFORMATICĂ ÎN REPUBLICA MOLDOVA

Ion PASCARI,
Coordonator ştiinţific:Veronica ROŞCA

Universitatea Tehnică a Moldovei

Abstract*: Dezvoltarea tehnologiilor informaţionale a dus la schimbări fundamentale în societate şi economie fără precedent şi este probabil ca aceste schimbări profunde să se producă în continuare.Astfel apare un nou tip de infracţiuni,infracţiunile informatice sau tratarea infracţiunilor tradiţionale într-o manieră mai nou,informaţională.În zilele de astăzi un terorist cu un "keyboard" în mână poate crea mai multe pagube decît unul cu o bombă...Adesea locul săvîrşirii unei crime informatice diferă de locul unde se găseşte infractorul.Prin o simplă apăsare a unui buton acesta poate aduce încălcări de lege atât faţă de persoanele fizice şi juridice din toată lumea,cît şi faţă de state,producând prejudicii de miliarde de dolari,la mii de km depărtare.*

Cuvinte cheie*: criminalitate, informatică, infracţiune.*

I. Conceptul general de "criminalitate informatică"

O primă noţiune dată faptelor penale de natură informatică de către grupul de experţi ai OECD în 1983 este: *"Orice comportament ilegal, neetic sau neautorizat ce priveşte un tratament automat al datelor şi/sau o transmitere de date."*Aceasta definiţie, deşi formulată în urmă cu două decenii, îşi dovedeşte utilitatea în primul rând prin faptul că permite integrarea dezvoltărilor ulterioare ale tehnicii în domeniul informatic.În prezent funcţionează alte două definiţii formulate de UNAFEI.

Astfel, prin infracţiune informatică în sens larg se înţelege:*"Orice infracţiune în care un calculator sau o reţea de calculatoare este obiectul unei infracţiuni, sau în care un calculator sau o reţea de calculatoarea este instrumentul sau mediul de înfăptuire a unei infracţiuni."*

Prin infracţiune informatică în sens restrâns se înţelege:*"Orice infracţiune în care făptuitorul interferează, fără autorizare, cu procesele de prelucrare automată a datelor."*

II. Reglementarea juridică şi dezvoltarea strategiilor de combatere a criminalităţii informatice în Republica Moldova.

Ţara noastră în ultimii ani a întreprins o serie de măsuri în prevenirea şi combaterea criminalităţii informaţionale. Cel mai însemnat eveniment îl reprezintă cu siguranţă semnarea Convenţiei de la Budapesta din 2001, care a avut loc la 23 noiembrie 2001 şi care a fost ratificată prin Legea nr. nr. 6 din 02.02.2009. Convenţia a intrat în vigoare pentru Republica Moldova la 01.09.2009. Defapt îndată după ratificarea Conveţiei de la Budapesta, a fost adoptată Legea Nr. 20 din 03.02.2009 privind prevenirea şi combaterea criminalităţii informatice, care reglementează raporturile juridice privind:

a) prevenirea şi combaterea infracţiunilor informatice;
b) cadrul de asistenţă mutuală în prevenirea şi combaterea criminalităţii informatice, în protecţia şi acordarea de ajutor furnizorilor de servicii şi utilizatorilor de sisteme informatice;
c) colaborarea autorităţilor administraţiei publice cu organizaţii neguvernamentale şi cu alţi reprezentanţi ai societăţii civile în activitatea de prevenire şi de combatere a criminalităţii informatice;
d) cooperarea cu alte state, cu organizaţii internaţionale şi regionale avînd competenţe în domeniu.

Tot în acea perioada au avut loc şi schimbări în Capitolul XI „Infracţiuni informatice şi infracţiuni din domeniul telecomunicaţiilor" din Codul Penal al Republicii Moldova. Astfel în Codul Penal al Republicii Moldova avem următoarele categorii de crime informaţionale ce constituie infracţiuni:

- Accesul ilegal la informaţia computerizată (art. 259);
- Producerea, importul, comercializarea sau punerea ilegală la dispoziţie a mijloacelor tehnice sau produselor program (art. 260);
- Interceptarea ilegală a unei transmisii de date informatice (art. 260^1);
- Alterarea integrităţii datelor informatice ţinute într-un sistem informatic (art. 260^2);
- Perturbarea funcţionării sistemului informatic (art. 260^3);
- Producerea, importul, comercializarea sau punerea ilegală la dispoziţie a parolelor, codurilor de acces sau a datelor similare (art. 260^4);

- Falsul informatic (art. 260^5);
- Frauda informatică (art. 260^6);
- Încălcarea regulilor de securitate a sistemului informatic (art. 261);
- Accesul neautorizat la reţelele şi serviciile de telecomunicaţii (art. 261^1).

Astfel în ultimii 4 ani de la intrarea în vigoare a Convenţiei de la Budapesta, Republica Moldova întreprinde o serie de acţiuni şi întrevederi destinate prevenirii şi combaterii criminalităţii informatice.

La data de **4 mai 2010** conform noii structuri a Procuraturii Generale, printre schimbările care au avut loc în instituţie, s-a materializat şi crearea în premieră a secţiei tehnologii informaţionale şi investigaţii ale infracţiunilor în domeniul informaticii - subdiviziune separată, controlată direct de Procurorul General.Aceasta a fost creată în scopul realizării Convenţiei Consiliului Europei privind promovarea cooperării cu celelalte state părţi la Convenţiei şi lupta eficientă împotriva criminalităţii informatice, măsura a vizat alocarea resurselor disponibile pentru a face faţă noilor „specializări" ale infractorilor.

La data de **13 decembrie 2012**, ministrul Afacerilor Interne, Dorin Recean, a avut o întrevedere cu experţii Consiliului Europei (CE), care s-a aflat într-o vizită de lucru în Republica Moldova, pentru elaborarea unui studiu de fezabilitate referitor la consolidarea structurilor specializate în investigarea crimelor cibernetice, precum şi desfăşurarea tratativelor cu instituţiile de resort în privinţa creării unui Centru naţional de investigare a crimelor cibernetice.

Dezvoltarea Centrului de Combatere a Crimelor Informatice în cadrul Inspectoratului Naţional de Investigaţii e una din priorităţile reformei MAI. La fel pentru Europol combaterea crimei electronice este o prioritate - începînd cu **1 ianuarie 2013** la nivel european a fost creat Centrul European de Combatere a Crimelor Informatice (European Cybercrime Center). Din obiectivele acestei instituţii noi sunt lupta cu fraudarea identităţii, a atacurilor cibernetice asupra sistemelor electronice guvernamentale, dar şi asupra companiilor private din ţările-membre.

În perioada **12 – 16 mai 2014** curent, în oraşul Haga, Olanda, delegaţia Ministerului Afacerilor Interne formată din reprezentanţi ai Centrului pentru combaterea crimelor informatice al Inspectoratului General de Poliţie şi Academiei "Ştefan cel Mare" a MAI, a participat în cadrul atelierului de lucru privind trainingul organelor de drept pentru combaterea crimelor cibernetice, eveniment organizat de Oficiul European de Poliţie (EUROPOL) cu susţinerea financiară a Consiliului Europei.

Preşedintele Republicii Moldova, Nicolae Timofti, a prezidat la **7 octombrie 2014**, Consiliul Suprem de Securitate.

În cadrul şedinţei au fost examinate două subiecte:

1. Securitatea informaţională a Republicii Moldova şi capacităţile de asigurare a securităţii informaţiei de către instituţiile abilitate.

2. Impactul evoluţiilor din regiune asupra Republicii Moldova.

Consiliul Suprem de Securitate a decis să asigure:

- executarea Planului de acţiuni privind implementarea Strategiei Naţionale de dezvoltare a societăţii informaţionale "Moldova Digitală 2020";
- crearea CERT-ului Naţional (centrul de reacţie la incidentele de securitate), care, suplimentar la funcţiile de bază, va defini un instrument comun în efectuarea campaniilor de informare a statului, a companiilor şi a cetăţenilor cu privire la crimele informatice, ameninţările şi căile de prevenire ale acestora;
- elaborarea şi aprobarea unui program naţional de educaţie continuă a funcţionarilor publici, a angajaţilor din sectorul privat şi a populaţiei privind posibilele vulnerabilităţi, riscuri şi pericole cibernetice de la utilizarea necorespunzătoare a aplicaţiilor, tehnologiilor informaţiei şi comunicaţiilor electronice, precum şi despre impactul nefast de la atacurile, ameninţările şi incidentele cibernetice.

III. Crime informatice în Republica Moldova

Un studiu recent realizat de FBI zugrăveşte gravitatea crimelor informatice prin faptul că circa 69 % din cei interogaţi sunt mult mai îngrijoraţi de atacurile informatice decît de furturi sau fraude obişnuite. Cercetările criminologice asupra infracţiunilor realizate prin sistemele informatice se află încă în la o etapă fragilă.

Este important de menţionat faptul că doar o mică parte din faptele penale legate de utilizarea sistemelor informatice ajung la cunoştinţa organelor de cercetare penală, fiindcă este foarte dificil de monitorizat infracţiunile informatice. Chiar şi dacă este posibil să se efectueze o descriere certă a tipurilor de fapte penale în domeniul sistemului informatic, este foarte dificilă prezentarea unei sinteze asupra întinderii pierderilor cauzate de acestea, precum şi a numărului real de infracţiuni comise. Numărul cazurilor de infracţiuni informatice este în continuă creştere. O companie independentă de sondaje GO-Gulf arată că în anul 2013 s-au înregistrat circa 2,402,722 de crime informatice în Rusia, 907,102 in Taiwan, 780,425 în

Germania, 566,531 în Ucraina etc. Dar cum rămîne cu prejudiciile cauzate de crimele informatice? Ultimul sondaj efectuat Internet Crime Complaint Center (IC3) şi Federal Bureau of Investigation (FBI) în 2013 indică pierderi de circa 781 de milioane dolari SUA din cauza crimelor cibernetice,în 2001 fiind doar 17 milioane dolari SUA.

Conform Global Security Map Moldova se clasează pe locul 9 dintre alte 219 state în dependenţă de indicele de gravitate a securităţii în domeniul informatic, pe o scară de la 0 la 1000 Republica Moldova obţine 225.5.

Potrivit studiului Business Software Alliance din 2013 cu privire la pirateria software pentru computere personale, Republica Moldova face parte din grupul de state cu cea mai mare rată a pirateriei. Se constată că, ponderea produselor program ilegale din totalul software-ului utilizat este de 91%, ceea ce constituie, în opinia BSA, 57 milioane de dolari SUA, şi, totodată, cel puţin 140 milioane de lei venit naţional (reieşind din achitarea TVA şi a taxelor de import).

Cea mai recentă şi răsunătoare crimă informatică este cea că începînd cu anul 2011, 5 persoane suspecte comercializau prin reţeaua Internet softul maliţios „CITADEL", destinat infectării sistemelor informatice şi culegerii datelor despre conturile bancare şi a datelor cu caracter personal. Astfel, procurorii au constatat că, prin acţiunile lor, suspecţii au infectat peste 5 milioane de computere la nivel mondial, cauzînd instituţiilor financiare din SUA şi Europa daune materiale, estimate la mai bine de 10 milioane USD.

Un alt caz a fost în sectorul bancar, inculpaţii au fost învinuiţi de procurori că, în decursul anului 2013, au favorizat suplinirea conturilor numerelor de telefon ale operatorilor de telefonie mobilă din Republica Moldova la un preţ redus, şi anume, în valoare de 50-70% din valoarea tranzacţiei. De asemenea, inculpaţii au favorizat procurarea echipamentelor GSM, a sistemelor informatice, precum şi altor mijloace electronice la preţ redus, de pe unele website-uri care prestează servicii de vînzări on-line. La efectuarea respectivelor tranzacţii au fost utilizate datele cardurilor bancare străine, fără ştirea şi acordul titularilor acestora, efectuînd operaţiuni de plată online în suma de peste 250 mii lei moldoveneşti.

IV. **Concluzie**

Gradul de dezvoltare a tehnologiilor informaţionale depinde direct de dezvoltarea resurselor informaţionale, de cultura informaţională a membrilor societăţii, de competenţa cadrelor corespunzătoare ce activează în domeniul dat . Paralel cu dezvoltarea tehnologiilor informaţionale se dezvoltă infracţiunile în acest domeniu, iar succesul depistării infractorului şi aducerea acestuia la răspundere juridică în instanţă nu depinde de oamenii care utilizează sistemele informatice,asta este datoria primară a statului. Într-u cît Republica Moldova se află la o etapă fragilă de dezvoltare a ramurii respective şi întâmpină mari greutăţi în prevenirea şi combaterea crimelor de genul dat.

De asemenea, lipseşte o abordare de sistem şi o politică de stat în domeniul securităţii informaţionale, care ar unifica măsurile juridice, organizatorice, tehnice, tehnologice şi fizice de protecţie a spaţiului cibernetic al Republicii Moldova, precum şi reglementarea clară a rolurilor şi competenţelor autorităţilor de resort.

Prin urmare, pentru a construi o societate informaţională sănătoasă, statul, în primul rând, trebuie să ia toate măsurile necesare pentru a asigura securitatea subiecţilor participanţi la relaţiile informaţionale şi acestea ar fi:

1. Reglementarea tranzacţiilor electronice. Elaborarea unui cadru legal adecvat pentru afaceri, care să reglementeze nu numai comerţul electronic şi semnătura electronică, ci şi aspectele referitoare la banii electronici, fiscalitatea şi modul de încheiere a contractelor în Internet;
2. Elaborarea tehnicilor şi metodologiilor de cercetare a infracţiunilor informatice. Datorită caracterului transfrontalier al criminalităţii informatice, armonizarea legislaţiei cu cea internaţională trebuie să vizeze, în principal: dreptul de autor, confidenţialitatea datelor, prevenirea şi combaterea criminalităţii informatice, precum şi promovarea standardelor tehnice care să asigure intercomunicarea noilor reţele de comunicaţii.
3. Crearea programelor de studiu şi pregătirea specialiştilor în domeniul securităţii informatice.

Bibliografie:

1. http://www.securitatea-informatica.ro/criminalitatea-informatica/infractiunile-informationale-si-mijloace-de-combatere-a-lor/
2. http://www.riti-internews.ro/Capitolul%2005%20-%20Reglementarea%20criminalitatii%20informatice.pdf
3. http://www.lex.justice.md/index.php?action=view&view=doc&lang=1&id=333508
4. http://www.lex.justice.md/index.php?action=view&view=doc&id=331268

5. http://www.mai.gov.md/content/23594
6. http://www.mai.gov.md/content/27595
7. http://www.mai.gov.md/content/21080
8. http://www.itmoldova.com/2014/10/07/consiliul-suprem-de-securitate-examinat-chestiuni-legate-de-securitatea-informationala-republicii-moldova/
9. http://www.procuratura.md/md/newslst/1211/1/3596/
10. http://www.itmoldova.com/2014/10/06/cetateni-ai-republicii-moldova-implicati-comercializarea-si-utilizarea-softului-malitios-citadel/
11. http://www.security.ase.md/publ/ro/pubro28.html
12. http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf
13. http://www.go-gulf.com/blog/cyber-crime/
14. http://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/
15. http://globalsecuritymap.com/#md
16. http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf