

INFRAȚIUNI ON DOMENIUL INFORMATICII

Nadejda VACAROV,
magistru on informatică, lector superior universitar,
Academia de Administrare Publică
pe longă Președintele Republicii Moldova

SUMMARY

The rapid development of informational and communication technologies have brought numerous negative aspects to the foreground. On the one hand, it permits a kind of criminality which could not be possible without the information systems; on the other hand, it offers increased opportunities of committing traditional infringements. Before the epoch of distributed informational systems, the main concern regarding the security of informational data consisted in maintaining their confidentiality, a thing which could be realized through a simple physical protection (for example, by locking or leaving the information in special places where it was kept). Alongside confidentiality, some other important aspects appeared nowadays. The security of informational systems becomes very complex and causes worries to all types of organizations, being at the same time a legal requirement.

On anul 2006, Moldova a onregistrat o rată a pirateriei oftware de 94% și pierderi de \$56 mln. de pe urma utilizării programelor ilegale pe calculator. Aceste date se conțin on „2006 Global Software Piracy Study”, lansat la 15 mai 2007 de compania Business Software Alliance (on continuare BSA). Potrivit datelor studiului, Moldova se află pe locul doi on lume după rata utilizării softului ilegal. Ea este devansată de Armenia cu 95%, iar Azerbaidjanul onregistrează aceeași rată a pirateriei software - 94%. Cele mai bune rezultate la acest capitol au fost onregistrate de Statele Unite - 21%

și noua Zeelandă -22%. On Rombnia rata softului ilegal este de 69%, on Ucraina - 84%, on Rusia - 80%, on Germania - 28%, Belgia și Marea Britanie- 27%, on Austria - 26%.

Pe plan global rata pirateriei software este de 35%, iar pierderile de pe urma utilizării programelor ilegale pe calculator au crescut on 2006 față de 2005 cu 15% - ponă la \$40 mlrd.

La 1 noiembrie 2006, reprezentanții Business Software Alliance au semnat la Chișinău un Protocol de colaborare cu Agenția de Stat pentru Proprietate Intelectuală din Republica Moldova și

Ministerul Afacerilor Interne. Documentul prevede stabilirea unor relații de colaborare a acestor structuri în domeniul reducerii ratei pirateriei software și al respectării drepturilor de autor asupra programelor pe calculator.

BSA este o companie internațională ce promovează protecția dreptului de autor (copyright), securitatea digitală și a comerțului electronic. Membrii BSA sunt: Adobe, Apple, Autodesk, Avid, Bentley Systems, Borland, CA, Cadence Design Systems, Cisco Systems, CNC Software/Mastercam, Dell, EMC, Entrust, HP, IBM, Intel, McAfee, Microsoft, Monotype Imaging, PTC, SAP, SolidWorks, Sybase, Symantec, Synopsys, The MathWorks, UGS.

Noțiuni de criminalitate informatică

Apariția calculatorului a creat și posibilitatea pentru apariția unei game largi de acțiuni ilegale cu un caracter extrem de sofisticat, el putând fi folosit și la comiterea sau la facilitarea comiterii unor infracțiuni clasice, cum ar fi furtul sau fraudă.

Specialiștii în domeniu au încercat definirea conceptului de criminalitate informatică, însă nu s-a ajuns la o formulă care să nu lase nici o îndoială asupra importanței sau utilității definiției. Din aceste motive este indicată adoptarea unei abordări funcționale a conceptului, fără a se încerca o definire formală a acestuia, care ar crea mai multe dificultăți decot ar putea rezolva.

Această abordare funcțională este specifică fiecărui stat în parte, care definește prin propriul său sistem juridic care fapte aparțin sau care sunt în legătură directă cu criminalitatea

informatică.

În legătură cu amploarea criminalității informatice, părerile și evaluările sunt diferite. Exceptând cazurile de copiere ilegală a unor programe pentru calculator, numărul infracțiunilor informatice nu este foarte ridicat, însă criminalitatea informatică nedescoperită ar putea spori semnificativ numărul acestei categorii de fapte de natură penală.

Din păcate, infracțiunile săvârșite cu ajutorul calculatorului au început să fie luate în serios în Republica Moldova doar de curând, aceasta explicând în parte de ce organele judiciare nu sunt pe deplin familiarizate cu modul în care calculatoarele sunt utilizate pentru comiterea de infracțiuni. Această stare de lucruri este favorizată și de legislația relativ săracă în acest domeniu.

Actualmente, normele care reglementează aspectele juridice ale activității în domeniul creării și dezvoltării infrastructurii informaționale naționale, ca mediu de funcționare a societății informaționale din Republica Moldova, există în cadrul mai multor ramuri de drept, dar prea puțin suficiente. Există și acte normative speciale: Legea Republicii Moldova cu privire la informatică, adoptată de Parlamentul Republicii Moldova la 22.06.2000¹; Legea Republicii Moldova cu privire la informatizare și resursele informaționale de stat, adoptată de Parlamentul Republicii Moldova la 21.11.2003²; Hotărârea Guvernului cu privire la aprobarea concepției de informatizare a societății și a mecanismului de realizare a acesteia, nr. 415 din 5.07.1993³ etc. Însă toate aceste norme și acte normative nu pot să ofere o protecție eficientă

ompotriva celor mai periculoase, din punct de vedere social, manifestări ale conduitei umane. Or, ciberspățiul poate fi folosit nu doar on scopuri legale, dar și pentru a comite infracțiuni, unele dintre acestea putond aduce prejudicii foarte mari proprietarilor resurselor și sistemelor informaționale sau de telecomunicații.

Iată un exemplu. Firme cunoscute au fost acuzate că au practicat spionajul informatic. Astfel, British Airways a accesat neautorizat calculatoarele rivalei sale Virgin Atlantic on scopul obținerii listei de pasageri, operațiune soldată, on urma descoperirii, cu demisia directorului gene-ral, prezentării de scuze publice și substanțiale despăgubiri. Jose Lopez, numărul doi la General Motors, demisionează pentru a ocupa o funcție importantă la Volkswagen, aducond și coteva cutii cu documente și dischete conținond informații despre noile realizări GM. Strict on domeniul calculatoarelor, firma Symantec a fost acuzată că a profitat de coteva dischete conținond planurile de marketing și detalii despre produsele on curs de dezvoltare ale Borland Inc. odată cu venirea șefului departamentului Limbaje de programare de la Borland la Symantec.⁴

Se consideră că 80% din fraudele informatice sunt de origine internă. Orice întreprindere care are informații strategice stocate pe calculatoare și orice sistem informatic sau de telecomunicații comportă lacune de securitate. Persoanele care au acces la asemenea sisteme pot descoperi aceste lacune, ceea ce explică proporția mare de fraude interne. O anchetă realizată on Anglia on octombrie 1994 on 1000

de întreprinderi relevă că 75% din fraudele comise erau de origine internă, dintre acestea 15% fiind comise de salariați.

Comiterea de fraude informatice este favorizată de faptul că sistemele informatice sunt slab protejate, atot din punctul de vedere al soluțiilor de securitate, cot și din cauza evoluțiilor tehnologice, cum ar fi informatica distribuită, ecuația client-server, interconectarea rețelelor de calculatoare, progresul software și multimedia.

Sistemele informaționale guvernamentale sunt atacate frecvent: circa 655 de tentative on 1994, dintre care 17% s-au oncheiat cu succes, afirmă juriștii informaticieni⁵.

On legătură cu fenomenul infracțional informatic s-a dezvoltat o doctrină și o practică judiciară bogată.

On Republica Moldova, ca și on întreaga lume, domeniul informatic și cel telecomunicațional au atins deja acel nivel cond relațiile sociale din aceste domenii nu mai pot să se formeze, desfășoare și să se dezvolte fără apărare juridico-penală. Din această perspectivă, existența on legea penală a Republicii Moldova a unui capitol dedicat infracțiunilor on domeniul informaticii și telecomunicațiilor este pe deplin justificată și salută (Capitolul XI "Infracțiuni on domeniul informaticii și telecomunicațiilor" al Partii speciale a Codului penal).⁶

Consiliul Europei a adoptat Recomandarea R(89)9 asupra criminalității on relația cu calculatorul și a publicat un raport on această materie, conținond o listă minimală și o listă facultativă de infracțiuni informatice. Dacă statele-membre vor ține seama de aceste mod-

ele on elaborarea legilor naționale, va exista o armonizare europeană relativă la criminalitatea informatică.

Lista minimală cuprinde fapte ca:

- fraudă informatică;
- falsul on informatică;
- faptele care aduc prejudicii datelor sau programelor pentru calculator;
- sabotajul informatic;
- accesul neautorizat;
- interceptarea neautorizată;
- reproducerea neautorizată de programe pentru calculator protejate;
- reproducerea neautorizată a unei topografii protejate.

Lista facultativă cuprinde fapte ca:

- alterarea datelor sau programelor pentru calculator;
- spionajul informatic;
- utilizarea neautorizată a unui calculator;
- utilizarea neautorizată a unui program pentru calculator protejat.

Faptele cu caracter antisocial menționate mai sus se definesc astfel:

- fraudă informatică reprezintă intrarea, alterarea, ștergerea de date sau de programe pentru calculator sau orice alt amestec ontr-un tratament informatic care oi influențează rezultatul, cauzond chiar prin aceasta un prejudiciu economic sau material on intenția de a obține un avantaj economic nelegitim pentru sine onsuși sau pentru altul;

- falsul informatic reprezintă intrarea, alterarea, ștergerea sau suprainprimarea de date sau de programe pentru calculator on condiții care, conform dreptului național al fiecărui stat, ar constitui infracțiunea de falsificare;

- faptele care prejudiciază datele

sau programele pentru calculator cumulează on conținutul lor constitutiv acțiunile de ștergere, aducere de daune, deteriorare sau suprimare fără drept a datelor sau a programelor pentru calculator;

- prin sabotaj informatic se onțelege intrarea, alterarea, ștergerea sau suprimarea de date sau de programe pentru calculator ori amestecul on sisteme informatice cu intenția de a ompiedica funcționarea unui sistem informatic sau a unui sistem de telecomunicații;

- accesul neautorizat constă on accesul fără drept la un sistem sau la o rețea informatică prin violarea regulilor de securitate;

- interceptția neautorizată reprezintă interceptția fără drept și cu mijloace tehnice de comunicații cu destinație, cu proveniență sau on cadrul unui sistem sau al unei rețele informatice;

- reproducerea neautorizată a unui program pentru calculator constă on reproducerea, difuzarea sau comunicarea on public, fără drept, a unui program pentru calculator protejat de lege;

- prin spionaj informatic se onțelege obținerea prin mijloace ilegale sau divulgarea, transferul sau folosirea fără drept a unui secret comercial sau industrial, on intenția de a cauza un prejudiciu economic persoanei care deține dreptul asupra secretului sau de a obține pentru sine sau pentru altul avantaje economice ilegite;

- utilizarea neautorizată a unui calculator constă on utilizarea fără drept a unui sistem sau a unei rețele informatice fie acceptond un risc notabil de a cauza un prejudiciu, fie on intenția de a cauza un prejudiciu unei persoane cu drept de a utiliza sistemul

sau de a aduce atingere sistemului sau funcționării lui, cauzând, ca urmare, un prejudiciu persoanei care are dreptul de a utiliza sistemul sau aducând atingere sistemului sau funcționării lui.

Având o vedere ritmul extrem de rapid o care progresează tehnologia informatică, organismele internaționale sugerează manifestarea de adaptabilitate o domeniu și completarea listelor menționate cu fapte, cum ar fi plantarea de viruși informatici, traficul cu parole obținute ilegal etc.

Caracterul transfrontalier al criminalității informatice

Limbajul informatic este unul comun tuturor celor ce folosesc calculatoarele, indiferent de țara din care provin și de limba vorbită; acest limbaj comun, precum și mijloacele de comunicare facile între utilizatori printr-o rețea specializată (exemplul cel mai elocvent fiind Internetul) sau printr-o simplă linie telefonică au condus la posibilități, practic, nelimitate de conectare a calculatoarelor din cele mai îndepărtate colțuri ale lumii și la accesarea informațiilor de ultimă oră, deosebit de importante aproape fără nici un efort. Prin urmare, un utilizator animat de rele intenții poate, de oriunde s-ar afla, din orice colț al lumii, fără să plătească altceva decot o anumită sumă serviciului telefonic (sau poate nici măcar atot), să-și alimenteze contul bancar de la orice mare instituție financiar-bancară, care nu trebuie să prezinte decot lacune o sistemul de protecție informatică. Pentru geniile o informatică, ași o acest gen de activități, nu există piedici (și chiar dacă ar exista), cu stăruință și răbdare ele pot fi depășite. De aceea, este foarte greu de probat o infracțiune

o domeniul informatic prin metodele clasice de descoperire a infracțiunilor, iar posibilitatea ca infractorul să se afle într-o altă zonă a lumii, o care mona legii să nu-l poată ajunge, este ridicată.

S-a observat, astfel, o serie întreagă de pierderi, onregistrate de bănci din Occident generate de spărgători ruși care, prin intermediul rețelelor de calculatoare, au putut penetra sistemele informatice și transfera fonduri la alte bănci de unde complicii au ridicat numerarul înainte ca cineva să poată onțelege ce s-a ontomplat de fapt, singurul lucru știut fiind că unele linii telefonice cu Rusia au fost mult oncărcate o anumite perioade. Tocmai de aceea guvernele țărilor puternic industrializate și informatizate au luat măsuri mergând, o SUA, până la onființarea unui serviciu special al FBI de urmărire și determinare a criminalității și infractorilor informatici, primul serviciu polițienesc de acest gen din lume, o Franța - la onființarea Clubului Securității Informatice, ducond, astfel, la stabilirea unei prevederi minime pentru fiecare țară - membru al Comunității Europene o conformitate cu o listă stabilită de acest organism internațional și recomandată de a fi cuprinsă o legislațiile țărilor-membre.

Internetul a schimbat fundamental modul o care societatea lucrează și comunică, prin furnizarea unui mediu ieftin și rapid, cu o cuprindere globală, pentru obținerea și comunicarea informațiilor. Alături de o serie de remarcabile avantaje, dezvoltarea rapidă a Internetului a ridicat și o serie de probleme legale, care trebuie tratate cu o foarte mare atenție. Având

legături on aproape toate țările și fără o autoritate centralizată, Internetul este considerat de mulți ca ultima piață de idei liberă.

Dintre problemele legale ridicate de Internet putem menționa distribuirea de materiale vulgare, probleme contractuale care apar la realizarea de contracte pe Internet, problema realizării reclamelor comerciale, admisibilitatea mesajelor pe Internet ca mijloc de probă on instanță, jurisdicția aplicabilă etc.

Funcționarea necorespunzătoare sau proasta utilizare a sistemelor informatice pot avea consecințe grave, cum ar fi pierderile financiare sau prejudiciile rezultate din divulgarea unor informații confidențiale privind societățile comerciale. Prejudiciile pot să se prezinte sub forma pierderii oncrederii sau prestigiului sau pot paraliza ontreaga activitate a unei ontreprinderi.

Referitor la această problemă apare, astfel, un alt concept, acela de securitate informatică, care poate fi definit ca “totalitatea actelor și mijloacelor utilizate de conducerea unui organism informatizat pentru a preveni, detecta, a rezista și a reacționa la atacurile sau amenințările ondreptate ompotriva disponibilităților libere și exclusive ale sistemului și a funcționării sale fără piedici, contra integrității și confidențialității sale, căutond, on același timp, un echilibru ontre costul riscurilor de securitate și scăderea riscului.

Pentru a se reduce posibilitatea accesării unor date sau amestecului on tranzațiile ontre două sau mai multe persoane, pot fi folosite mai multe procedee, cum ar fi parolele, testarea identității, măsurarea actului de scri-

ere on cazul semnăturii electronice, semnăturile vocale, geometria palmei sau impresiunile digitale.

Totuși, cum nu există un sistem de securitate absolut sigur, se recomandă conștientizarea riscurilor pe care le prezintă derularea unor afaceri cu ajutorul sistemelor informatice.

Concluzionond, implementarea și dezvoltarea sistemelor informatice on Republica Moldova sunt absolut necesare, după cum la fel de necesară este și reglementarea acestui domeniu prin acte normative coerente, care să ofere o protecție reală utilizatorilor, oncurajandu-i pe aceștia să folosească acest mijloc rapid de schimb de date și informații, cu toate avantajele pe care le prezintă.

On oncheiere, vă propunem un fragment din interviul cu Dorian Chiroșca, vicedirector general al Agenției de Stat pentru Proprietate Intelectuală din Republica Moldova (AGEPI), publicat on revista „MaxCAD Magazine”, nr. 17, versiune electronică <http://www.acintl.ro>):

„...Pedepsele maxime aplicate recent on Republica Moldova pentru nerespectarea dreptului de autor sunt de ponă la 5 ani de onchisoare și amenzi de maximum \$17 mii. Pe parcursul anului trecut au fost onregistrate 75 de dosare administrative și 31 de amenzi penale pentru piraterie software.

Agenția de Stat pentru Proprietate Intelectuală (AGEPI) reunește din 2004 atribuțiile de reglementare a drepturilor de autor, dar și reglementarea proprietății industriale. AGEPI participă alături de poliție și la controale on lupta antipiraterie software. Din 2003 au fost introduse modificări

on Codul de Contravenții Administrative care prevăd amendă de până la \$500 pentru fiecare caz de piraterie, dacă suma nu este mai mare de \$700. Pentru costuri ale materialelor piratate mai mari de \$700 se pornește o cauză penală. Legea penală are o vedere inclusiv privațiunii de libertate de la 3 la 5 ani. „Deja am onregistrat sentințe la onchisoare de cinci ani, cu suspendare”, a precizat Dorian Chiroșca, vicedirector general AGEPI, iar amenda maximă aplicată este de \$17-18 mii atunci cond sunt implicate două sau mai multe persoane, on funcție de valoarea drepturilor

lezate și a prejudiciului implicat. Anul trecut au fost ontocmite 75 de dosare administrative și 31 de dosare penale, după luna martie cond a intrat on vigoare legislația. „On studiile IDC la nivel internațional Republica Moldova nu este inclusă on Watch List datorită demersurilor realizate de noi. La noi on țară oncă nu există reprezentanții proprietarilor de drepturi de autor, deci nu avem posibilitatea de a evalua valoarea software-ului pentru a aplica legea”, a explicat Dorian Chiroșca despre problemele cu care se confruntă on acest moment reprezentanții agenției. Important este ca, la nivel comercial,

să se legalizeze utilizarea de licențe software. Ca urmare a seriei de demersuri realizate de AGEPI, Microsoft a anunțat intenția de a intra pe piața Republicii Moldova, iar BSA studiază posibilitatea de a delega o firmă de avocatură interesată să-i reprezinte.

Stabilirea cadrului legal și faptul că lupta antipiraterie este una dintre acțiunile curente on Moldova determină A&C, distribuitor autorizat Autodesk și pentru Republica Moldova, să facă demersuri pentru a dezvolta o rețea de rețele și specializați pe această piață ...”

Timpul văicărelilor și a atitudinii „lasă-mă sa te las“ a apus. Ca on „principiul dominoului”, informațiile oncep sa iasă la iveală, una cote una. Aflăm de la serviciile mass-media că Institutul de Proiectare X, regia de stat Y sau compania internațională Z, făcându-și ordine prin măruntaiele calculatoarelor, au depistat nisaiva „intruși”.

Presiunea exercitată asupra infractorilor cibernetici este din ce on ce mai mare. Ca urmare a strategiei de combatere a furtului de programe, sute de companii, de stat sau private, iau decizia de a intra on rondul firmelor care respecta legea.

Condițiile de intrare on legalitate oferite de distribuitorii locali de software sunt mai mult decot rezonabile: plăți eşalonate, discounturi substanțiale, suport tehnic, upgrade, certificate de licență, training și multe, multe altele.

ACTE NORMATIVE

1. Legea Republicii Moldova cu privire la informatică, adoptată de Parlamentul Republicii Moldova la 22.06.2000.

2. Legea Republicii Moldova cu privire la informatizare și resursele informaționale de stat, adoptată de Parlamentul Republicii Moldova la 21.11.2003.