STUDIA UNIVERSITATIS MOLDAVIAE, 2015, nr.3(83)
Seria "Ştiinţe sociale" ISSN 1814-3199, ISSN online 2345-1017, p.162-166

BUNE PRACTICI INTERNAŢIONALE CU PRIVIRE LA INVESTIGAREA INFRACŢIUNILOR INFORMATICE

Svetlana PURICI

Universitatea de Stat din Moldova

În prezent, relevanţa problemelor legate de protecţia informaţiilor a crescut în special datorită sporirii bruşte a rolului şi importanţei informaţiei în viaţa modernă a societăţii, în general, şi în domeniul economiei, în particular. Un nou tip de încălcare a legii – criminalitatea cibernetică – s-a răspândit pe scară largă. De menţionat că actuala legislaţie europeană privind informaţiile se află încă în stadiul de dezvoltare; din acest motiv, trebuie îndeplinit un mare volum de lucru pentru eliminarea neajunsurilor şi defectelor. Protecţia legală a furnizării informaţiilor depinde de tipul şi caracterul purtătorilor de informaţii.

Cuvinte-cheie: *cooperare internaţională, criminalitate informatică, investigare, asistenţă mutuală, reţea de calculatoare, confidenţialitate.*

BEST INTERNATIONAL PRACTICES REGARDING THE INVESTIGATION OF CYBERCRIME

Presently the information protection issues relevance has increased particularly due to a sharp increase of the role and importance of information in the life of modern society as a whole and economics in particular. A new type of law infringement – cybercrime – has spread widely. It is worth to mention that the present European legislation on information is still at the development stage; for this reason much work should be accomplished to eliminate the shortcomings and defects. The legal protection of information provision depends on the type and character of the information carriers.

Keywords: *international cooperation, cybercrime, investigation, mutual assistance, network, confidentiality/privacy.*

Expansiunea transnaţională extraordinar de rapidă a reţelelor de calculatoare şi extinderea accesului la aceste reţele prin intermediul telefoniei mobile au dus la creşterea vulnerabilităţii acestor sisteme şi la crearea de oportunităţi pentru săvârşirea infracţiunilor. Tehnologia informaţională atinge fiecare aspect al vieţii cotidiene a unei persoane fără a se ţine cont de poziţionarea geografică a acesteia. Activitatea zilnică a unei persoane este afectată în formă, conţinut şi timp de calculator. Tot mai multe activităţi comerciale, industriale, economice sau guvernamentale sunt dependente de reţelele informatice. Calculatoarele nu sunt utilizate doar pentru creşterea performanţelor economice şi industriale ale unei ţări, acestea au devenit parte integrantă a vieţii personale a individului. Calculatoarele sunt utilizate pentru stocarea şi transmiterea datelor confidenţiale de natură politică, socială, economică sau pur personale[*]. Calculatoarele asistă şi întreţin chiar şi confortul locurilor de muncă sau al locuinţelor personale.

Legislaţia statelor lumii este în continuă schimbare datorită dezvoltării tot mai accelerate a tehnologiei informatice, iar cooperarea internaţională este pusă în faţa unei provocări continue produse de creşterea criminalităţii informatice transnaţionale. Din ce în ce mai multe state au procedat la armonizarea propriilor legislaţii în vederea combaterii fenomenului în discuţie, însă rezultatele sunt doar mulţumitoare şi nu se va putea vorbi despre o eradicare a fenomenului. Problemele ridicate în cadrul reuniunilor internaţionale privind combaterea criminalităţii informatice sunt următoarele [2, p.80]:

- ✓ lipsa unui consens global privind definiţia noţiunii *criminalitate informatică*;
- ✓ lipsa unui consens global privind motivaţia realizării acestor fapte;
- ✓ lipsa expertizelor din partea persoanelor autorizate aparţinând unor instituţii cu atribuţii de control în domeniu;
- ✓ inexistenţa unor norme legale adecvate privind accesul şi investigaţia sistemelor informatice, inclusiv lipsa normelor prin care pot fi confiscate bazele de date computerizate;
- ✓ lipsa armonizării legislative privind investigaţiile în domeniu;
- ✓ caracterul transnaţional al acestui tip de infracţiune;
- ✓ existenţa unui număr redus de tratate internaţionale privind extrădarea şi asistenţa mutuală în domeniu.

[*] Date de volum impresionant pot fi comprimate şi stocate compact pe discuri de densitate mare. Viteza de lucru a cunoscut o creştere exponenţială, cele mai complicate calcule fiind realizate într-un interval de timp de ordinul milisecundelor. Miniaturizarea procesoarelor a permis realizarea conexiunilor şi a comunicaţiilor în timp real la nivelul globului.

STUDIA UNIVERSITATIS MOLDAVIAE, 2015, nr.3(83)
Seria "Ştiinţe sociale" ISSN 1814-3199, ISSN online 2345-1017, p.162-166

În acest sens, la nivel internaţional, Consiliul Europei a iniţiat o serie de reglementări cu privire la criminalitatea informatică. Astfel, dacă în 1995 a fost adoptată Recomandarea nr. R (95) 13 cu privire la problemele de procedură penală legate de tehnologiile informaţionale, atunci la 23 noiembrie 2001 a fost semnată, la Budapesta, Convenţia privind criminalitatea informatică [1][*]. Drept puncte de pornire pentru elaborarea Convenţiei au servit un şir de alte acte normative internaţionale, precum:

- ✓ Convenţia Consiliului Europei pentru protejarea persoanelor faţă de prelucrarea automatizată a datelor cu caracter personal (1981);
- ✓ Convenţia Naţiunilor Unite privind drepturile copilului (1989);
- ✓ Convenţia Organizaţiei Internaţionale a Muncii privind interzicerea celor mai grave forme ale muncii copiilor (1999);
- ✓ Recomandările Comitetului de Miniştri al Consiliului Europei[**].

Astfel, fiecare stat, parte contractantă a Convenţiei, adoptă măsuri legislative şi alte măsuri care se dovedesc a fi necesare pentru a obliga un furnizor de servicii în domeniul informaticii să păstreze confidenţialitatea oricărei informaţii în legătură cu acest subiect.

De asemenea, Convenţia prevede că, în caz de urgenţă, fiecare parte poate formula o cerere de asistenţă mutuală prin mijloace rapide de comunicare, precum faxul sau poşta electronică, cu condiţia ca aceste mijloace să ofere condiţii suficiente de securitate şi de autentificare (inclusiv folosirea codării, atunci când este necesar), cu o confirmare oficială ulterioară dacă partea solicitată va revendica acest lucru. Partea solicitată va accepta cererea şi va răspunde prin oricare dintre mijloacele sale rapide de comunicare.

O altă poziţie interesantă, pe care o oferă Convenţia, se remarcă prin faptul că o parte poate, în limitele dreptului său intern şi în absenţa unei cereri prealabile, să comunice unei alte părţi informaţii obţinute în cadrul propriilor anchete (investigaţii), în cazul în care consideră că acest lucru ar putea ajuta partea destinatară la începerea sau finalizarea cu succes a procedurilor având ca obiect infracţiuni stabilite în domeniul tehnologiilor informaţionale. În acest sens, un punct şi mai interesant este că orice cerere sau comunicare formulată în baza celor expuse mai sus poate fi avansată prin intermediul Organizaţiei Internaţionale de Poliţie Criminală (Interpol), ceea ce sporeşte considerabil operativitatea investigării.

Din punctul nostru de vedere, conservarea rapidă a datelor informatice, stocate în rezultatul efectuării acţiunilor de urmărire penală, reprezintă o lecţie bine însuşită de părţile contractante la Convenţia privind criminalitatea informatică. Astfel, o cerere de conservare va trebui să precizeze:

a) autoritatea care solicită conservarea;
b) infracţiunea care va face obiectul urmăririi penale, precum şi o scurtă expunere a faptelor care au legătură cu aceasta;
c) datele informatice stocate care vor trebui conservate şi natura legăturii lor cu infracţiunea;
d) toate informaţiile disponibile care vor permite identificarea posesorului datelor informatice stocate sau locaţia sistemului informatic;
e) necesitatea măsurii conservării;
f) faptul că partea are intenţia de a formula o cerere de asistenţă mutuală în vederea percheziţiei ori accesării printr-un mijloc similar sechestrului sau obţinerii ori divulgării datelor informatice în cauză.

Un aspect plauzibil este faptul că Convenţia prevede ca fiecare parte contractantă să desemneze un punct de contact disponibil 24 de ore din 24, 7 zile din 7, în scopul asigurării unei asistenţe imediate pentru investigaţiile referitoare la infracţiunile privind sisteme sau date informatice, sau pentru a strânge dovezile unei infracţiuni în format electronic [3].

---

[*] Convenţia îşi propune să prevină actele îndreptate împotriva confidenţialităţii, integrităţii şi disponibilităţii sistemelor informatice, a reţelelor şi a datelor, precum şi a utilizării frauduloase a unor asemenea sisteme, reţele şi date, prin asigurarea incriminării unor asemenea conduite şi prin încurajarea adoptării unor măsuri de natură să permită combaterea eficace a acestor tipuri de infracţiuni, menite să faciliteze descoperirea, investigarea şi urmărirea penală a acestora.

[**] Recomandările: nr. R (85) 10 privind aplicarea în practică a Convenţiei Europene de asistenţă judiciară în materie penală, referitoare la comisiile rogatorii pentru supravegherea telecomunicaţiilor; nr. R (88) 2 privind măsurile vizând combaterea pirateriei în domeniul drepturilor de autor şi al drepturilor conexe; nr. R (87) 15 vizând reglementarea utilizării datelor cu caracter personal în sectorul poliţiei; nr. R (95) 4 privind protecţia datelor cu caracter personal în domeniul serviciilor de telecomunicaţii, cu referire specială la serviciile de telefonie; nr. R (89) 9 referitoare la criminalitatea în legătură cu utilizarea calculatorului, care indică structurilor legiuitoare naţionale principiile directoare pentru definirea anumitor infracţiuni; nr. R (95) 13 privind problemele de procedură penală în legătură cu tehnologia informaţiei.

Ca model [2, p.89], Convenţia are aspecte deopotrivă pozitive şi negative. Abordarea este largă şi chiar uneori depăşeşte „graniţele" conceptului de criminalitate informatică. De exemplu, luând în considerare problema accesului guvernamental la datele informatice pentru toate infracţiunile, Convenţia lasă de dorit în ceea ce priveşte protejarea vieţii personale şi a drepturilor indivizilor.

Având în vedere dezvoltarea fără precedent a tehnologiei informatice şi aplicarea acesteia în toate sectoarele vieţii moderne, precum şi ofensiva infracţiunilor asupra sistemelor informatice, Consiliul Europei a aprobat ***Recomandarea R(95)13*** *privind probleme legate de procedura judiciară a cazurilor legate de tehnologia informatică şi de crearea de autorităţi cu atribuţii în acest domeniu*. Principalele norme statuate de Recomandarea menţionată, care au stat la baza modificării codurilor de procedură penală ale statelor europene, sunt următoarele:

Căutarea şi copierea datelor:

- trebuie făcută distincţie între activităţile de căutare şi copiere a datelor dintr-un calculator şi cea de interceptare a transmiterii datelor;
- Codul de procedură penală trebuie să permită autorităţilor competente să controleze sistemele de calculatoare în condiţii similare celor care au permis scanarea şi furtul datelor;
- pe parcursul realizării oricărui tip de investigaţii, autorităţilor specializate trebuie să li se permită, atunci când este necesar, extinderea cercetărilor şi asupra altor sisteme de calculatoare legate în reţea cu cel aflat sub investigaţie şi care se află în zona de jurisdicţie.

Tehnica de supraveghere:

- din punctul de vedere al convergenţei dintre tehnologia informatică şi telecomunicaţii, legislaţia trebuie să permită introducerea tehnicii de interceptare şi supraveghere a sistemului de telecomunicaţii în scopul combaterii criminalităţii informatice;
- legislaţia trebuie să permită autorităţilor abilitate să utilizeze întreaga tehnică disponibilă pentru a putea să monitorizeze traficul dintr-o reţea în cazul unei investigaţii;
- datele obţinute prin monitorizarea traficului, precum şi rezultatele obţinute prin prelucrarea acestora trebuie protejate conform legislaţiei în vigoare;
- codurile de procedură penală trebuie revizuite pentru a se facilita procedurile oficiale de interceptare, supraveghere şi monitorizare, în scopul evitării aducerii unor atingeri confidenţialităţii, integrităţii şi validităţii sistemului de telecomunicaţii sau al reţelelor de calculatoare.

Obligativitatea cooperării cu autorităţile abilitate:

- multe dintre reglementările legale ale statelor lumii permit autorităţilor abilitate să solicite de la persoanele care se bucură de un anumit tip de imunitate sau sunt protejate de lege punerea la dispoziţie a materialului probator. În paralel, prevederile legale trebuie să oblige persoanele implicate să prezinte orice tip de material necesar investigaţiilor unui sistem de calculatoare;
- pentru persoanele care se bucură de un anumit tip de imunitate sau sunt protejate de lege, autorităţile abilitate trebuie să aibă puterea şi competenţa de a le solicita orice material, aflat sub controlul acestora, necesar investigaţiilor. Codul de procedură penală trebuie să prevadă acelaşi lucru şi pentru alte persoane care au cunoştinţe privind funcţionarea unei reţele de calculatoare şi care aplică măsurile de securitate asupra acestora;
- operatorilor reţelelor publice sau private de calculatoare care deservesc sistemele de telecomunicaţii trebuie să li se impună obligaţii specifice care să le permită interceptarea comunicaţiilor la solicitarea organismelor abilitate;
- aceleaşi obligaţii specifice trebuie impuse şi administratorilor de reţele ale serviciilor de telecomunicaţii pentru identificarea unui utilizator, la solicitarea autorităţilor în drept.

Evidenţa electronică:

- activităţile de stocare, protejare şi expediere a evidenţelor electronice trebuie să se reflecte prin autenticitatea şi integritatea materialelor atât pentru necesităţile private, cât şi pentru cele oficiale;
- procedurile şi metodele tehnice de manipulare a evidenţelor electronice trebuie dezvoltate, asigurându-se compatibilitatea lor între statele membre;
- prevederile Codului de procedură penală aplicabile documentelor obişnuite pe suport de hârtie trebuie aplicate şi documentelor stocate electronic.

STUDIA UNIVERSITATIS MOLDAVIAE, 2015, nr.3(83)
Seria "Ştiinţe sociale" ISSN 1814-3199, ISSN online 2345-1017, p.162-166

Utilizarea criptării [*] [4]:

– trebuie luate măsuri prin care să se prevadă limitarea efectelor negative ale criptografiei în cazul aplicării acesteia în investigaţii oficiale, fără a afecta legitimitatea utilizării acestei metode mai mult decât este necesar.

Cercetare, statistică, instruire:

– riscul impunerii noilor aplicaţii tehnologice în raport cu comiterea infracţiunilor informatice trebuie studiat continuu. Pentru a se permite autorităţilor cu atribuţii în combaterea acestui fenomen să ţină pasul cu nivelul tehnic al cazurilor pe care le investighează, trebuie să se realizeze o bază de date care să cuprindă şi să analizeze cazurile cunoscute de criminalitate informatică: modul de operare, aspecte tehnice şi încadrări juridice;
– trebuie creat un corp de specialişti pregătiţi şi instruiţi continuu în domeniul expertizelor impuse de fenomenul analizat.

Cooperarea internaţională:

– trebuie impuse competenţe care să permită instituţiilor abilitate să desfăşoare investigaţii şi în afara zonei de jurisdicţie, dacă este necesară o intervenţie rapidă[**];
– trebuie realizată îmbunătăţirea acordului mutual de asistenţă, care este în vigoare, pentru clarificarea tuturor problemelor ce pot să apară în cadrul unei investigaţii privind autorizarea verificării unei anumite reţele informatice, confiscarea unor anumite tipuri de date necesare anchetei, interceptarea telecomunicaţiilor specifice sau monitorizarea traficului.

***Principii*:**

✓ nu trebuie să existe niciun loc sigur pentru cei care comit abuzuri prin intermediul tehnologiei informatice;
✓ investigaţiile şi pedepsele aplicate acestor infracţiuni trebuie coordonate cu sprijinul tuturor statelor, chiar dacă nu se produce niciun fel de pagubă;
✓ legea trebuie să combată explicit fiecare infracţiune de acest tip;
✓ legea trebuie să protejeze confidenţialitatea, integritatea şi utilitatea bazelor de date informatice, precum şi să sancţioneze pătrunderea neautorizată în sistemele informatice;
✓ legea trebuie să permită apărarea şi conservarea bazelor de date cu acces rapid, cele mai expuse atacurilor din exterior;
✓ regimul de asistenţă mutuală a statelor trebuie să permită informarea periodică şi, în caz de necesitate, în situaţiile unor infracţiuni transcontinentale;
✓ accesul la baze de date electronice deschise trebuie să se poată realiza liber, fără acordul statului pe al cărui teritoriu se află acestea;
✓ regimul juridic privind trimiterea şi autentificarea datelor electronice utilizate în cazul investigaţiilor informatice trebuie dezvoltat;
✓ extinderea unui sistem de telecomunicaţii practic şi sigur trebuie cumulată cu implementarea unor mijloace de detecţie şi prevenire a abuzurilor; activitatea în acest domeniu trebuie coordonată de instituţii şi foruri internaţionale specializate în domeniul informatic.

Planul comun de acţiune al Consiliului Europei în domeniul prevenirii şi combaterii infracţiunilor informatice cuprinde următoarele direcţii:

- utilizarea reţelei proprii de calculatoare şi a cunoştinţelor acumulate în domeniu pentru a asigura o comunicare exactă şi eficientă privind cazurile de criminalitate ce apar în reţele mondiale;
- realizarea paşilor necesari creării unui sistem legislativ modern şi eficace pentru combaterea fenomenului, care să fie pus la dispoziţia statelor membre;
- revizuirea legislaţiei naţionale a ţărilor membre şi armonizarea acesteia cu legislaţia penală necesară combaterii criminalităţii informatice;
- negocierea unor noi acorduri de asistenţă şi cooperare;

[*] ***Criptarea*** este procesul de ascundere a informaţiei pentru a o face ilizibilă fără cunoştinţe speciale.

[**] Pentru a se evita posibilele încălcări ale suveranităţii unui stat sau ale legilor internaţionale, cadrul legal existent în momentul de faţă trebuie modificat şi completat corespunzător pentru eliminarea ambiguităţilor. Trebuie să se negocieze rapid la nivel internaţional pentru obţinerea unui acord care să precizeze cum, când şi ce este permis în efectuarea unei investigaţii.

- dezvoltarea soluțiilor tehnologice care să permită căutarea transfrontalieră şi realizarea unor investigații de la distanță;
- dezvoltarea procedurilor prin care se pot obține date de interes de la responsabilii sistemelor de telecomunicații;
- colaborarea, inclusiv, cu ramurile industriale pentru obținerea celor mai noi tehnologii utilizabile în combaterea criminalității informatice;
- asigurarea de asistență în cazul unor solicitări urgente prin întregul sistem tehnologic propriu;
- încurajarea organizațiilor internaționale din sistemul informatic şi a celor din telecomunicații pentru creşterea standardelor şi măsurilor de protecție oferite sectorului privat;
- realizarea unor standarde unice privind transmiterea datelor electronice utilizate în cazul investigațiilor oficiale sau private.

Bibliografie:

1. Convenție privind criminalitatea informatică din 23 noiembrie 2001, Budapesta. În: *Monitorul Oficial al Republicii Moldova*, Partea I, 2004, nr.343. Seria „Tratate Europene nr.185; ratificată prin Legea Parlamentului Republicii Moldova nr.6-XVl din 02.02.2009.
2. DOBRINOIU, M. *Infracțiuni în domeniul informatic*. Bucureşti: C.H. Beck, 2006, p.80-89.
3. DUŞA, S., GHEORGHIȚĂ, M. Criminalitatea cibernetică – cu un pas înainte. Metodici de investigare. În: *Studia Universitatis. Seria „Ştiinţe Sociale"*, Anul V, nr.3(43). Chişinău: CEP USM, 2011, p.194.
4. http://ro.wikipedia.org/wiki/Criptare

Prezentat la 24.04.2015