STUDIA UNIVERSITATIS MOLDAVIAE, 2015, nr.11
Seria "Ştiinţe sociale" ISSN 1814-3199, ISSN online 2345-1017, p.120-125

SPECIFICUL ACTIVITĂŢII SPECIALE DE INVESTIGAŢIE ŞI ACŢIUNII DE URMĂRIRE PENALĂ ÎNTREPRINSE PENTRU ADMINISTRAREA PROBELOR LA CERCETAREA CRIMELOR CIBERNETICE

Svetlana PURICI

Universitatea de Stat din Moldova

Importanţa investigării „criminalităţii informatice" este dictată nu doar de progresul tehnic, dar în special de prezenta bază normativă în reglementările internaţionale şi în legile naţionale ale Republicii Moldova, precum: Legea cu privire la informatică, Legea privind accesul la informaţie etc., reguli ce trebuie aplicate şi care se vor reflecta în viaţa noastră, în special în procesul de apărare a drepturilor în judecată – moment în care importanţa şi influenţa „investigării criminalităţii cibernetice" este remarcată în procesul penal. Forma electronică a remiterii informaţiilor favorizează posibilitatea interceptării la distanţă a informaţiilor fără un oarecare transfer vizual al obiectelor materiale. Între activitatea specială de investigaţie în cadrul investigării crimelor cibernetice şi procesul penal există o legătură reciprocă, menirea primei fiind contribuţia nemijlocită la buna desfăşurare a procesului penal, prin cercetarea obiectivă, imparţială şi multilaterală a faptelor pasibile de pedeapsă penală, astfel asigurându-se aplicarea echitabilă a justiţiei.

Cuvinte-cheie: *activitate specială de investigaţie, corespondenţă, admisibilitatea probelor, interceptare, conservare.*

THE SPECIFICITY OF SPECIAL INVESTIGATIVE ACTIVITIES AND PROSECUTION ACTIONS TAKEN FOR THE ADMINISTRATION OF EVIDENCE ON RESEARCH OF CYBERCRIMES

The interest of the "cybercrime investigations" is given not only by the results of the technical progress, but especially by the existent, normative ground in the internaţional and especially national laws in Republic of Moldova, such as: The Law on informatics, The Law on access to information etc., rules that have to be applied and that will have effect on our life, in particular in the stage of defending the rights in the judicial way – the moment where the importance and the influence of "cybercrime investigations" in the penal procedural law is remarked. Electronic form of the information submission promotes distinctly to a possibility of distant interception of the information without any visual transfer of material objects. There is a reciprocity between special investigative activities in the investigation of cyber crimes and criminal procedure , the role of special investigative activites is the direct contribution to proper conduct of criminal proceedings, by objective, impartial and multilateral research of punishable criminal acts, thus ensuring equitable application of justice.

Keywords: *special investigative activities, correspondence, admissibility of proof, interception, conservation.*

Investigarea crimelor cibernetice necesită implicarea largă a specialiştilor din diverse domenii, care nu se regăsesc într-o unică instituţie de stat, precum ar fi [10]:

- domeniul tehnologiilor informaţionale (specialişti pentru colectarea probelor, asigurarea caracterului confidenţial în investigaţiile sub acoperire în reţelele de socializare, examinarea probelor digitale, administratorii de servicii etc.);
- domeniul securităţii sistemelor şi datelor informatice;
- domeniul telecomunicaţiilor (telefonie mobilă, fixă, VoIP);
- domeniul proprietăţii intelectuale;
- domeniul securităţii statului şi autorităţilor publice;
- domeniul protecţiei minorilor în mediul reţelelor de socializare, forumurilor, mesageriilor instantanee (chaturilor, skype etc.);
- domeniul protecţiei datelor cu caracter personal.

Specificul investigaţiilor efectuate în cazul crimelor cibernetice:

1) particularităţile măsurilor speciale de investigaţie (website-urile, profilurile şi conturile agenţilor sub acoperire, preluarea identităţii infractorilor membri ai grupurilor criminale etc.);
2) particularităţile probatoriului cauzelor penale (probele digitale, conservarea probelor electronice, administrarea datelor informatice, interceptările comunicărilor efectuate prin reţelele Internet şi Intranet, sechestrarea corespondenţei poştelor electronice, supravegherea tehnică, audierea specialiştilor IT [16], datele informatice culese de la instituţiile de telecomunicaţii şi operatorii de telefonie mobilă, traficul

informatic preluat de la furnizorii de servicii, constatările tehnico-ştiinţifice, expertizele judiciare, examinarea sistemelor informatice etc.);

3) particularităţile componenţei de infracţiune (obiectul infracţiunii, metoda comiterii infracţiunii, mijloacele utilizate la săvârşirea crimelor, locul săvârşirii infracţiunii, caracterul transfrontalier, subiectul infracţiunii etc.);
4) conlucrarea cu organele competente din alte state (utilizarea punctului G8, OECD).

Potrivit art.273 alin.(3) CPP RM, în situaţia în care există indicii temeinice despre săvârşirea unei infracţiuni, organele de urmărire penală (OUP) pot efectua acte premergătoare în vederea începerii urmăririi penale (UP). În situaţii speciale, expres reglementate de lege, pot efectua acte premergătoare şi alte organe de constatare din cadrul MAI, CCCEC, SIS, SV (art.273 alin.(1) CPP RM) [2].

În doctrină există numeroase controverse cu privire la instituţia actelor premergătoare, întrucât legea nu defineşte, în concret, aria actelor procedurale care pot fi efectuate, ele având menirea de a ajuta OUP în completarea informaţiilor pe care le deţin sau pot contribui la verificarea informaţiilor pentru stabilirea existenţei unei activităţi infracţionale.

În faza actelor premergătoare se pot efectua diverse activităţi (de ex.: verificări, audieri de persoane etc.), dar nu se pot dispune măsuri care ar presupune calitatea de bănuit, învinuit sau inculpat a persoanei împotriva căreia se desfăşoară, întrucât o asemenea calitate implică începerea UP.

Precizăm că efectuarea actelor premergătoare nu este obligatorie în fiecare caz în parte, însă pot exista situaţii în care pentru buna desfăşurare a procesului penal (PP) cu privire la instrumentarea unui caz de criminalitate informatică ar fi necesară efectuarea de asemenea acte.

Problema privind afectarea drepturilor şi libertăţilor fundamentale, în cazul realizării investigaţiilor cibernetice, apare cu precădere în situaţia celor ce se efectuează în activitatea specială de investigaţie (ASI). În procesul efectuării interceptărilor comunicărilor, înregistrărilor de imagini şi a altor forme de înregistrare operativă sunt viciate câteva drepturi fundamentale ale persoanei [3]. Utilizarea acestora afectează în special dreptul la secretul corespondenţei, reglementat în art.12 al Declaraţiei Universale a Drepturilor Omului, de art.17 al Pactului internaţional cu privire la drepturile civile şi politice din 1966, de art.8 al Convenţiei europene pentru apărarea drepturilor şi libertăţilor fundamentale ale omului, de art.30 din Codul penal şi de art.14 din Codul de procedură penală ale Republicii Moldova.

Astfel, *Dreptul la secretul corespondenţei* presupune asigurarea unei protecţii corespunzătoare din partea statului împotriva oricărei acţiuni de cunoaştere a conţinutului scrisorilor, telegramelor, al altor trimiteri poştale, al convorbirilor telefonice şi al celorlalte mijloace de comunicare. Afectarea acestora este prezentă atunci când înregistrarea vizează anume conţinutul acestor comunicări, altfel spus – atunci când se procedează la interceptarea comunicărilor.

Afectarea *dreptului la viaţa intimă, familială şi privată* (art.12 al Declaraţiei Universale a Drepturilor Omului, art.17 al Pactului internaţional cu privire la drepturile civile şi politice, art.8 al Convenţiei europene pentru apărarea drepturilor şi libertăţilor fundamentale ale omului) are loc mai ales în cazul lezării dreptului la secretul corespondenţei, al cărui conţinut presupune, de regulă, informaţie de caracter intim, familial sau privat. În plus, viaţa intimă, familială şi privată devine obiect al nerespectării şi atunci când se efectuează înregistrările de imagini sau înregistrări audio nelegate de interceptări.

În esenţă, aceste două drepturi fundamentale au reuşit să dobândească, în special datorită ponderii ultimului, denumirea generică de „drept la intimitate" [9]. În contextul reglementărilor internaţionale, în special al celor ce ţin de activitatea normativă a Uniunii Europene, în doctrina actuală a statelor membre ale acestui organism internaţional conceptul dat este tot mai frecvent utilizat fără să cunoască însă o definire unanim acceptată şi universal valabilă termenului. Faptul dat s-a datorat practicii CEDO, care, examinând cauza *Van Oosterwijk contra Belgiei*, a determinat dreptul la respectarea vieţii private în sensul art.8 din Convenţie: „Dreptul la respectarea vieţii private este dreptul la intimitate, dreptul de a trăi aşa cum doreşti, protejat de publicitate".

Prin urmare, ceea ce justifică legalitatea afectării dreptului la intimitate este însăşi conduita subiectului lezat, iar afectarea dreptului este o măsură de protecţie întreprinsă de stat [14]. Doctrina americană de specialitate [6] susţine o poziţie similară în ceea ce priveşte dreptul la intimitate, afirmând în acelaşi context că un infractor se aşteaptă la mai puţină intimitate decât un non-infractor, ceea ce implică un grad mai înalt al inteligenţei acestuia în comunicările telefonice şi în altele de asemenea natură (telegrafice, electronice).

Afectarea intimităţii se realizează însă nu doar prin încălcarea secretului corespondenţei, al vieţii intime, familiale şi private, deşi acestea deţin ponderea majoră, ci şi prin atingerile aduse inviolabilităţii domiciliului, întrucât sursa informaţiei înregistrate audio/video [11] este nu de puţine ori domiciliul subiectului. De aceea, atunci când mijloacele tehnice de interceptare sau înregistrare audio/video sunt plasate în obiecte formând interiorul domiciliului, utilizarea acestora este imposibilă fără a pătrunde în el [3].

Prin urmare, deoarece nici legea nu distinge când urmează a fi exercitat dreptul la apărare în cazurile respective – în momentul încălcării sau după aceasta, respectiva prerogativă legală, în situaţia dată, nu apare ca fiind lezată, întrucât bănuitul, învinuitul, martorul, partea vătămată au oricând posibilitatea de a se adresa instanţei în legătură cu încălcarea acestui drept fundamental. În plus, atunci când este vorba de interceptare sau de o înregistrare operativă, anume pentru asigurarea dreptului la apărare a fost inclusă instituţia autorizării [5] judecătorului de instrucţie (JI), care ar apărea în calitate de garant al respectării legalităţii şi, implicit, al drepturilor fundamentale, atunci când confidenţialitatea este cerinţa principală a eficienţei actului procesual sau special respectiv.

Admisibilitatea probelor ridicate din sisteme informatice nu este importantă numai pentru utilizarea fişierelor informatizate cu ocazia procesului în materie penală. Într-adevăr, în majoritatea ţărilor, dispoziţiile procedurale cu caracter de constrângere nu se aplică decât elementelor care ar putea constitui mijloace de probă admisibile cu ocazia unui proces. În consecinţă, dacă anumite date informatizate sau anumite ieşiri pe imprimanta unui computer nu ar putea servi ca probe, ele nu ar mai putea să facă obiectul unei percheziţii ori vreunei confiscări[*].

Plenul Curţii Supreme de Justiţie de asemenea explică posibilitatea folosirii probelor – înscrisurilor care au fost administrate cu ajutorul tehnicii electronice de calcul[**], cu condiţia ca:

- să fie acumulate, dobândite pe cale legală;
- să fie întocmite în corespundere cu ordinea stabilită (anume această ordine şi necesită a fi reglementată în mod detaliat şi expres pentru a evita abuzurile şi interpretările greşite);
- să se confirme prin alte mijloace doveditoare;
- să nu aibă o valoare prestabilită din timp, adică să se aprecieze conform regulilor generale.

Faţă de suporturile electronice de informaţie se înaintează suplimentar următoarele cerinţe, deduse din prevederile legislaţiei procesual penale:

- trebuie să fie prezentate în limba în care se desfăşoară procesul (conform prevederilor art.16 CPP RM „Limba în care se desfăşoară procesul penal şi dreptul la interpret");
- datele sau informaţia de pe acestea trebuie să fie prezentate în formă materializată (pe hârtie) şi anexate la dosar;
- datele prezentate să fie înţelese, perceptibile.

Unele aspecte cu privire la administrarea suporturilor electronice de informaţie ca mijloc de probaţie în procesul penal. În ceea ce priveşte administrarea suporturilor electronice de informaţie ca mijloc de probaţie în PP, menţionăm următoarele:

- cercetarea acestora poate avea loc în şedinţa de judecată sau într-o altă încăpere special amenajată, dacă aceasta o cere specificul mijlocului de probaţie prezentat pe suportul electronic;
- la cercetarea acestuia poate fi invitat specialistul (pentru a primi consultaţie sau ajutor în ceea ce priveşte gestionarea suporturilor electronice) sau, după caz, expertul (în caz că apare necesitatea de a da răspuns la întrebări care cer cunoştinţe speciale);
- părţile în proces au posibilitatea să dea explicaţii, lămuriri, să pună întrebări cu privire la autenticitatea, veridicitatea şi importanţa informaţiei prezentate cu ajutorul suporturilor electronice;
- mijlocul de probă prezentat cu ajutorul suportului electronic poate fi cercetat (vizionat, ascultat etc.) ori de câte ori este necesar acest lucru;
- suportul electronic de informaţie se anexează la dosar şi se păstrează la instanţa de judecată[***].

[*] În practică, diversele probleme juridice care se pun sunt cruciale, căci este uşor să manipulezi scoaterile pe imprimantă şi datele informatizate (fenomen care este bine descris făcând scoateri pe imprimanta de computer a „*produselor de mâna a doua*").

[**] Hotărârea Plenului Curţii Supreme de Justiţie cu privire la practica aplicării de către instanţele judecătoreşti a legislaţiei procesual civile la întocmirea hotărârii şi încheierii, nr.12 din 25.04.2000. În: Culegeri de hotărâri explicative (mai 1974 - iulie 2002). - Chişinău, 2002.

[***] Numai la cererea părţii acesteia i se poate face o copie de pe suportul electronic sau, în cazuri excepţionale, după ce hotărârea judecătorească rămâne definitivă şi irevocabilă, părţii interesate i se poate restitui suportul respectiv (ceea ce ridică însă întrebarea cu privire la dreptul de proprietate asupra suportului electronic de informaţie).

STUDIA UNIVERSITATIS MOLDAVIAE, 2015, nr.11
Seria "Ştiinţe sociale" ISSN 1814-3199, ISSN online 2345-1017, p.120-125

Lărgirea sferei de probare din contul mijloacelor tehnice pe calea modificării legii (procesuale) constituie un stimul pentru modernizarea şi perfecţionarea echipării tehnice a OUP şi a celor judecătoreşti, deoarece aceasta ar fi de acum o necesitate procesuală.

În această ordine de idei, dispoziţiile CPP RM în vigoare reglementează acest domeniu prevăzând o listă exhaustivă şi limitativă a suporturilor electronice de informaţie ce pot servi ca mijloc de probaţiune, astfel stabilindu-se o ordine. Menţionăm însă că nici aceste dispoziţii nu reflectă în totalitate posibilităţile progresului tehnico-ştiinţific. Se cere deci un cadru legislativ cel puţin de perspectivă pentru problema în cauză, în special în ceea ce priveşte elaborarea mecanismelor, regulilor procedurale de aplicare a conceptului.

Conţinutul principal al activităţii ofiţerului de UP constă în culegerea probelor [4], documentarea, păstrarea, verificarea şi supunerea unei evaluări preliminare. Iar judecata cercetează aceste probe şi le apreciază în mod definitiv. Efectuând cercetările, ofiţerul de UP creează premise pentru examinările judiciare. Deşi OUP nu sunt în subordinea instanţei de judecată, activitatea lor are loc până la judecată şi pentru judecată.

Acţiunile procedurale de culegere, cercetare şi verificare a probelor, desfăşurate în faza urmăririi penale, se numesc acţiuni de UP.

Sintagma „acţiune de urmărire penală" [13] este răspândită în criminalistică şi utilizată de nenumărate ori în CPP RM.

Totalitatea acţiunilor de UP este inclusă în CPP RM şi serveşte drept temei juridic la efectuarea UP. Se ştie că direcţia principală a ofiţerului de UP este activitatea procedurală desfăşurată pentru cercetarea cauzei penale. Fiind o persoană oficială, el este împuternicit să ia personal hotărâri cu privire la efectuarea unor acţiuni de UP sau să poruncească efectuarea lor altor membri ai grupului de cercetare. În afară de aceasta, el este împuternicit să dirijeze în mod independent derularea cercetărilor, să trimită organului de investigaţie specială comisii rogatorii în scris, obligatorii pentru executare, pentru luarea unor măsuri de urmărire specială, pentru stabilirea unor circumstanţe pe cauza cercetată sau pentru efectuarea altor acţiuni de UP.

Cu certitudine, putem constata că prin acţiuni de UP se înţelege în mod tradiţional acţiuni cognitive şi identificative ale ofiţerului de UP sau ale procurorului care cercetează cauza concretă, ce constau în reflectarea pe baza percepţiei nemijlocite a urmelor evenimentului, în documentarea circumstanţelor, faptelor cuprinse în ele. Specifică este doar dispunerea interceptării comunicărilor sau dispunerea expertizei respective, care constituie un proces cognitiv mediat (de către operator, care nemijlocit înregistrează convorbirile, sau de către expert, care independent efectuează expertiza), însă şi aici are loc interacţiunea nemijlocită a ofiţerului de UP şi a operatorului, expertului. Nimic din toate acestea nu există în cazul controlului asupra convorbirilor telefonice şi acest lucru nu trebuie să ne mire, pentru că, de fapt, în acest caz de culegerea informaţiei se ocupă nu ofiţerul de UP sau procurorul, ci „instituţia însărcinată cu executarea tehnică a interceptării", în persoana operatorului tehnic. Ofiţerului de UP/procurorului nu-i rămâne decât să primească fonograma şi să o audieze, întocmind procesul-verbal respectiv.

Activitatea specială de investigaţie. Datele de fapt obţinute prin ASI pot fi admise ca probe numai în cazurile în care ele au fost administrate şi verificate prin intermediul mijloacelor prevăzute în legea procesuală [1]. Aceste date, care asigură soluţionarea cauzei penale, pot fi administrate în PP prin intermediul mijloacelor de probă. Noţiunea *mijloc de probă* trebuie delimitată de cea de *probă*[*]. Noţiunea *mijloc de probă* trebuie separată şi de noţiunea de *procedeu probatoriu*. Procedeele probatorii nu constituie o categorie a mijloacelor de probă, ci modul de a proceda în folosirea mijloacelor de probă [7]. Într-un sens general, mijloace de probă pot fi considerate căile prin intermediul cărora datele de fapt, care au o importanţă în soluţionarea unei cauze penale, ajung la cunoştinţa OUP[**]. Trebuie de asemenea delimitate noţiunile „act procesual" şi „act procedural". Primul este un act de dispoziţie al OUP, iar al doilea – un act prin care se aduce la îndeplinire actul procesual.

Unele măsuri speciale de investigaţii posedă trăsături comune cu acţiunile de UP. Aceasta se explică prin faptul că scopul ambelor tipuri de activităţi este obţinerea informaţiilor despre fapte; acestea se obţin din una şi aceeaşi primă sursă, sunt folosite aceleaşi metode de cunoaştere analogice: chestionarea, urmărirea, compararea ş.a.

[*] Împrejurarea de fapt, care conduce la o concluzie de vinovăţie sau nevinovăţie, nu poate fi confundată cu mijlocul prin care această împrejurare este cunoscută sau demonstrată.

[**] Legea procesual penală determină nu doar mijlocul de provenienţă a probelor, dar şi procedeele prin care aceste mijloace de probă pot fi obţinute. Unele mijloace de probă pot fi obţinute prin diferite procedee probatorii. Spre exemplu, mijloacele materiale de probă pot fi obţinute atât în cadrul cercetării la faţa locului, cât şi al percheziţiei sau ridicării.

STUDIA UNIVERSITATIS MOLDAVIAE, 2015, nr.11
Seria "Ştiinţe sociale" ISSN 1814-3199, ISSN online 2345-1017, p.120-125

Rezultatele ASI [12] sunt informaţiile speciale de investigaţii, conţinute în rapoarte, în notele colaboratorului special care a efectuat nemijlocit măsura specială de investigaţii (MSI), în comunicările confidenţilor, în concluziile experţilor, specialiştilor, în materialele foto şi video, în diferite obiecte materiale obţinute public sau confidenţial ca urmare a realizării MSI.

În concluzie, menţionăm că între ASI în cadrul investigării crimelor cibernetice şi procesul penal există o legătură reciprocă, menirea primei fiind contribuţia nemijlocită la buna desfăşurare a PP, prin cercetarea obiectivă, imparţială şi multilaterală a faptelor pasibile de pedeapsă penală, astfel asigurându-se aplicarea echitabilă a justiţiei.

Interceptarea comunicărilor telefonice şi de altă natură şi intercalarea cu ASI. Conform art.132[2] CPP RM, interceptarea comunicărilor (convorbirilor telefonice prin radio sau altor convorbiri, cu utilizarea mijloacelor tehnice) se efectuează de către OUP, cu autorizaţia JI, în baza ordonanţei motivate a procurorului.

Reglementarea interceptării şi înregistrării comunicărilor telefonice şi de altă natură prin norme de PP confirmă că aceasta este o acţiune procedurală. Acest fapt a fost menţionat şi de L.Carneeva, A.Davletov, L.Canevschi şi alţii, care, subliniind că interceptarea convorbirilor telefonice şi de altă natură este o nouă măsură procedurală, deoarece este reglementată ca acţiune de anchetă în Codul de procedură penală, au remarcat că poartă un caracter neobişnuit şi se efectuează vădit ascuns [15].

Esenţa acestei acţiuni de UP constă în faptul că, în baza hotărârii ofiţerului de UP sau a procurorului respectiv, organul tehnic împuternicit interceptează şi înregistrează, cu ajutorul mijloacelor tehnice, conţinutul comunicărilor telefonice şi de altă natură, care apoi sunt prezentate comandatarului (ofiţerului de UP sau procurorului)[*]. Această activitate este asemănătoare, într-o măsură oarecare, cu ASI. Caracterul specific al acestei acţiuni de UP constă şi în îmbinarea măsurilor de urmărire specială cu acţiunile procedurale. În afară de aceasta, natura specifică a acestei acţiuni constă şi în faptul că posibilitatea efectuării ei este legată de gravitatea infracţiunii săvârşite, precum şi de limitele neobişnuite de timp, care uneori sunt mai mari decât termenul de cercetare iniţial al infracţiunii, stabilit de legiuitor.

Din momentul adoptării hotărârii cu privire la interceptarea comunicărilor, „întocmirea demersului respectiv, primirea acceptului JI" şi până la însărcinarea organului tehnic cu sarcina concretă se scurge etapa de pregătire a acestei acţiuni de UP, apoi urmează nemijlocit interceptarea comunicărilor ca realizare a MSI – etapă de lucru, iar la primirea rezultatelor interceptării şi la întocmirea în scris a procesului-verbal are loc etapa de documentare a acţiunii respective de UP.

În această procedură lipseşte semnul determinant al acţiunii sus-numite: obţinerea nemijlocită de către persoana care investighează cauza a informaţiei probatorii de la purtătorul acesteia. Pentru că în acest caz rolul ofiţerului de UP sau al procurorului se reduce doar la înaintarea demersului (ordonanţei) respectiv, la obţinerea din instanţă a permisiunii pentru interceptare, iar apoi la primirea, audierea şi examinarea înregistrării (fonogramei), care i s-a prezentat, cu întocmirea unui proces-verbal de consemnare a acestui fapt.

În acest caz, ofiţerul de UP sau procurorul nu trebuie să înregistreze mecanic datele obţinute de la organele tehnice respective, dar să le perceapă şi să le evalueze în totalitatea lor, confruntându-le cu cealaltă informaţie (probe) atât din dosarul penal, cât şi din cel de urmărire specială, ţinând cont de faptul că aceste date pot să servească în calitate de probe în cauza respectivă.

În concluzie, putem constata că interceptarea comunicărilor telefonice şi de altă natură, prevăzută în CPP RM, fiind un mijloc eficient de descoperire a infracţiunilor, este o acţiune de UP complexă şi specifică, care pe bună dreptate şi-a găsit locul său în sistemul acţiunilor procesuale.

Conservarea datelor [8] reprezintă o nouă metodă de investigare a infracţiunilor săvârşite prin intermediul sistemelor informatice, în special a infracţiunilor comise prin intermediul internetului, datorită volatilităţii datelor informatice acestea putând fi foarte uşor alterate sau şterse. Conservarea datelor informatice reprezintă una dintre metodele prezervării integrităţii datelor informatice pentru a putea permite autorităţilor competente percheziţionarea sistemului informatic şi ridicarea obiectelor care conţin date informatice în vederea copierii acestora. Această măsură poate fi dispusă atunci când furnizorul de servicii care are sarcina administrării

[*] Acţiunea de interceptare corespunde tuturor cerinţelor prevăzute de lege pentru acţiunile de urmărire penală, numai că se efectuează într-un mod specific. Acest specific constă în faptul că ofiţerul de urmărire penală sau procurorul care cercetează cauza nu interceptează nemijlocit convorbirile. Ei numai organizează acest lucru (fac demers, obţin acceptul JI şi însărcinează subdiviziunea tehnică respectivă cu interceptarea anumitor convorbiri). Apoi urmează interceptarea nemijlocită a convorbirilor interesate pentru OUP şi înregistrarea lor de către personalul tehnic.

respectivelor date este o persoană de încredere. În această situaţie, conservarea datelor poate asigura într-un mod mai rapid securizarea integrităţii acestora decât prin percheziţie sau alte metode similare de acces, care pot afecta activitatea furnizorului de servicii şi dăuna reputaţiei acestuia.

Consolidarea capacităţilor profesionale individuale şi instituţionale de investigare a infracţiunilor informatice. Capacităţile insuficiente ale OUP, inclusiv lipsa unor abilităţi şi a unei instruiri corespunzătoare, constituie unul din motivele investigării şi UP eficiente. Organele de drept şi cele ale procuraturii, precum şi sistemul justiţiei penale din Republica Moldova în general, întâmpină dificultăţi în aplicarea tehnicilor speciale de investigare, care sunt utilizate în contracararea infracţiunilor cibernetice. Acest fapt este determinat de practica netransparentă de punere în aplicare a legii. Drept consecinţă, activităţile speciale de investigare subminează sistemul justiţiei penale, reducându-i vădit eficienţa şi capacitatea de a respecta standardele relevante în domeniul drepturilor omului, cum ar fi exigenţa clarităţii şi predictibilităţii cadrului de reglementare (*cazul Iordache şi alţii vs. Moldova*).

În ultima perioadă s-a ameliorat situaţia în acest domeniu. Astfel, au fost operate unele intervenţii specifice pentru implementarea unor metode moderne de investigare şi UP, a fost modificată legislaţia şi a fost instituită instruirea corespunzătoare a personalului implicat în aceste procese. Măsuri graţie cărora a devenit posibilă specializarea actorilor fazei prejudiciare şi efectuarea UP în cadrul unor grupuri interdepartamentale ("task force group"), precum şi consolidarea (s-a observat deja) capacităţilor centrelor de expertiză judiciară.

Bibliografie:

1. CARLAŞUC, I. Corelaţia dintre activitatea operativă de investigaţii şi procesul penal. În: *Legea şi Viaţa*, 2007, nr.9, p.39.
2. Codul de procedură penală al Republicii Moldova. În: *Monitorul Oficial al Republicii Moldova*, nr.104-110.
3. CROITOR, E. Argumentarea admisibilităţii înregistrărilor audio/video în procedura penală, din perspectiva drepturilor fundamentale. În: *Revista Naţională de Drept*, 2006, nr.6/73.
4. DINU, D. Interceptarea şi înregistrarea comunicărilor în sistemul acţiunilor de urmărire penală. În: *Legea şi Viaţa*, 2009, nr.11, p.51.
5. LASCU, L.-C. Autorizarea accesului la sistemele de telecomunicaţii sau informatice. În: *Dreptul*, 2003, nr.1, p.182.
6. WALLISER, B. *Systemes et Modeles.Introduction critique a l'analyse de systemes"*. Seuil, 1977, p.89-90.
7. БАЧИЛА, В. Оперативно-розыскное мероприятие „прослушивание телефонных переговоров": теория и практика. В: *Судовы вестнік*, 2008, №4, с.49.
8. БЫРГЭУ, М., КОГАМОВ, М., БАСЕЦКИЙ, И., КАРПОВ, Н. Фундаментальное исследование проблем функционального назначения оперативно-розыскной деятельности в уголовном судопроизводстве. В: *Закон и Жизнь*, 2009, №10, с.54.
9. ВОРОБЬЕВА, Ю., ЖЕРЕБЯТЬЕВ, И. Система носителей информации о доказательствах в условиях реализации принципа оценки доказательств по внутреннему убеждению. В: *Российский судья,* 2005, №6, с.28.
10. ИВАНОВ, А., СИЛАНТЬЕВ, Д. Предварительная проверка сообщений о неправомерном доступе к компьютерной информации. В: *Уголовное право,* 2003, №4, p.117.
11. МУХИН, Г., ЛОГВИН, В. Фиксация доказательственной информации с использованием цифровой фотосъемки. В: *Судовы веснік,* 2007, №3, с.63.
12. ПИВОВАРЧИК, А. К вопросу о соотношении понятия «доказательство» и фактических данных, получаемых в ходе осуществления оперативно-розыскных мероприятий. В: *Судовы веснік*, 2006, №2, с.59.
13. ПОЛЯКОВ, М., РЫЖОВ, Р. О модели правового института использования результатов оперативно-розыскной деятельности в уголовном процессе. В: *Уголовное право*, 2005, №1, с.88.
14. СИВИЦКАЯ, Н. Признаки объективной стороны несанкционированного доступа к компьютерной информации. В: *Судовы веснік,* 2007, №3, с.69.
15. СКЛЯРОВ, Д.В. *Искусство защиты и взлома информации.* Петербург: БХВ, 2004, с.97; ВЕХОВ, В.Б. *Компьютерные преступления. Способы совершения, методики расследования*. Москва, 1996, с.175.
16. ЧЕРЕПИЦА, Л. Защита информации в компьютерных системах. В: *Судовы веснік,* 2003, №4, с.22.

Prezentat la 24.04.2015