Acta Univ. Sapientiae, Legal Studies, **6**, 2 (2017) 249–258

Rolul percheziției informatice în probarea infracțiunilor contra drepturilor de proprietate intelectuală

Crişan Eugen Gheorghe
Universitatea Sapientia
Departamentul de Ştiințe Juridice
E-mail: eugengcrisan@yahoo.com

Rezumat. Ca multe altele drepturi ale omului şi drepturile de proprietate intelectuală sunt lezate prin comiterea de infracțiuni. Dacă în urmă cu ceva vreme săvârşirea infracțiunilor se realiza prin modalități obişnuite a căror existență putea fi demonstrată prin intermediul unor probe consacrate, ca spre exemplu depozițiile unor persoane, în prezent, odată cu dezvoltarea tehnologiei şi cu folosirea acesteia atât în folosul omului, cât şi împotriva lui, adică în vederea comiterii de infracțiuni îndreptate împotriva omului, în general, şi a celor privind drepturile acestuia de proprietate intelectuală, în special, se pune problema eficienței probelor în demonstrarea existenței acestor infracțiuni. Cum orice activitate a omului, oriunde s-ar desfăşura, lasă urme, şi utilizarea mijloacelor tehnologice cum sunt sistemele informatice, ca şi componente ale tehnologiei avansate, lasă urme. Specialiştii în tehnologia informatică au arătat, însă, că prin utilizarea unor proceduri tehnologice, aceste urme pot fi căutate şi descoperite, respectiv transformate în probe uşor de perceput, motiv pentru care legiuitorul a transpus procedurile menționate în haină legislativă, pe care noi o putem numi astăzi percheziția informatică. Pentru că această probă este la început de drum, procesul penal prezintă aspecte pozitive ca reglementare, dar şi unele neajunsuri, care ar putea influența negativ bunul mers al procesului penal spre atingerea scopului acestuia şi anume stabilirea existenței infracțiunilor, identificarea autorilor şi stabilirea vinovăției acestora.

Cuvinte cheie: infracțiuni, drepturi de proprietate intelectuală, proba, date informatice, sistem informatic, percheziție informatică, carențe legislative, valoare probatorie

Abstract. The role of the computer search warrant in proving copyright infringements
As is the case with other fields of human rights, intellectual property rights are also exposed to infringement. While in the past these infringements occurred by conventional methods and means of proving a case comprised solid evidence like taking depositions from people, in the present, taking into consideration the massive development of technology and its use both to the advantage, as well as to the disadvantage to humankind, that is, infringement of human rights, in general and infringement of intellectual property rights, in particular, there's a growing need for efficient methods in proving copyright violation. Like any human activity, which leaves a trace, no matter where it takes place, the use of IT methods like computer systems, as well as using individual components of advanced technology also leaves traces. IT/C specialists have shown though that by using technological procedures, these traces can be detected and identified, and they can also be transformed into easily recognizable evidence – all this concluding to the adoption of legislative procedures known today under the term computer search warrant. Given the fact that this type of evidence is a newly emerging one, incorporating adjoining measures into the criminal trial can present both positive, as well as negative aspects where the latter could exert a negative effect on the outcome of the criminal trial, such as: establishing the presence of copyright violation, identifying the perpetrators and establishing their responsibility.

Keywords: infringement, intellectual property rights, evidence, computer data, computer system, computer evidence search warrant, deficiencies in legislation, probative value.

Aşa cum se arăta în partea introductivă a unei lucrări recente elaborate în acest domeniu[1], infracționalitatea la regimul drepturilor de autor şi drepturilor conexe este un domeniu de maximă actualitate în materie penală datorită dinamicii tehnologiei şi diversificării activităților antisociale în mediul virtual, ca urmare a faptului că sistemele informatice (PC-urile – personal computer) oferă, în prezent, oportunități noi, unele chiar sofisticate, de încălcare a legilor şi creează un potențial ridicat de comitere a unor tipuri de infracțiuni realizate altfel decât în modurile cunoscute, tradiționale. Altfel spus, odată cu evoluția tehnologică, cu nivelul înalt la care au ajuns operațiunile pe care un sistem informatic le poate executa, nu există valoare socială conținută de drepturile de autor şi cele conexe acestora[2] care să nu poată fi lezată prin utilizarea unui sistem informatic. Mai mult, atingerea adusă acestora este mult mai facilă şi mai greu de depistat dacă are loc pe o astfel de cale.

Cum prin sistem informatic se înțelege „*orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relație funcțională, dintre care unul sau mai*

1 Lăncrănjan-Litvin-Pop 2015, 5.
2 A se vedea art. 7, art. 140 din Legea nr. 8/1996, publicată în Monitorul Oficial nr. 60 din 26 martie 1996.

multe asigură prelucrarea automată a datelor, cu ajutorul unui program informatic"[3], apare legitima apărare privind existența şi eficiența probelor în cazul comiterii unor asemenea infracțiuni.

În conformitate cu art. 97 alin. 1 Cod de procedură penală (în continuare CPP) proba este orice element de fapt care serveşte la constatarea existenței sau inexistenței unei infracțiuni, la identificarea persoanei care a săvârşit-o şi la cunoaşterea împrejurărilor necesare pentru justa soluționare a cauzei şi care contribuie la aflarea adevărului în procesul penal, iar datele informatice prelucrate prin sistemele informatice nu sunt altceva decât o reprezentare a unor fapte, informații sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic[4], ceea ce înseamnă că sistemele informatice prin intermediul cărora se comit infracțiuni în dauna drepturilor de autor şi drepturilor conexe, conțin înăuntrul lor probe cu un caracter informatic sau digital.

Specialiştii în domeniu au preferat să utilizeze noțiunea de probă digitală[5], deoarece are acoperirea cea mai largă, din moment ce datele digitale (bazate pe prelucrarea lor discretă ca amplitudine şi timp) stau la baza funcționării aparatelor electronice moderne, cu toate că în legislația europeană se utilizează noțiunea de probă electronică[6]. Definindu-se proba digitală s-a arătat că aceasta este orice informație cu valoare probantă care este fie stocată, prelucrată sau transmisă într-un format digital, ale cărei particularități constau în aceea că aparent nu este evidentă, fiind conținută în echipamentele informatice ce o stochează şi este foarte sensibilă, în sensul că poate fi modificată sau poate dispărea foarte uşor, prin metode care de multe ori sunt la îndemâna făptuitorilor.

Având în vedere particularitățile probei digitale materializarea ei se va putea face prin intermediul mijlocului de probă denumit percheziție[7] şi pentru că aceasta se realizează într-un sistem informatic, în legislația procesual penală română a căpătat denumirea de percheziție informatică[8].

Procedând la definirea percheziției informatice, legiuitorul român a stabilit în cuprinsul art. 168 alin. 1 CPP că „*Prin percheziție în sistem informatic sau a unui suport de stocare a datelor informatice se înțelege procedeul de cercetare, descoperire, identificare şi strângere a probelor stocate într-un sistem informatic sau suport de stocare a datelor informatice, realizat prin intermediul unor*

3 Art. 35 alin. 1 lit. a din Legea nr. 161/2003, publicată în Monitorul Oficial nr. 279 din 21 aprilie 2003.
4 Art. 35 alin. 1 lit. d din Legea nr. 161/2003.
5 Ghid introductiv pentru aplicarea dispozițiilor legale referitoare la criminalitatea informatică, http://www.riti-internews.ro, pag. 74.
6 A se vedea pct. 13 din Anexa la Recomandarea nr. R (95) 13 a Comitetului de Miniştri către statele membre cu privire la problemele de procedură penală legate de tehnologiile informaționale.
7 Art. 19 pct. 1 şi 2 din Convenția Consiliului Europei privind criminalitatea informatică, adoptată la Budapesta la 23 noiembrie 2001, ratificată prin Legea nr. 64 din 24 martie 2004 publicată în Monitorul Oficial nr. 343 din 20 aprilie 2004.
8 A se vedea art. 156 alin 1 şi denumirea marginală a art. 168 CPP.

mijloace tehnice şi proceduri adecvate, de natură să asigure integritatea informațiilor conținute de acestea."

Din definirea dată de către legiuitor percheziției informatice rezultă necesitatea clarificării semnificației a încă trei noțiuni: sistem informatic, suport de stocare şi date informatice.

În cuprinsul art. 35 alin. 1 Legea nr. 161/2003[9] legiuitorul a dat o definire pentru două din cele trei noțiuni, dar şi a altora care ne sunt necesare a le înțelege deplin. Astfel, noțiunea de sistem informatic are înțelesul arătat mai sus; prin prelucrarea automată a datelor se înțelege „*procesul prin care datele dintr-un sistem informatic sunt prelucrate prin intermediul unui program informatic*"; prin program informatic se înțelege „*un ansamblu de instrucțiuni care pot fi executate de un sistem informatic în vederea obținerii unui rezultat determinat*"; prin date informatice se înțelege „*orice reprezentare a unor fapte, informații sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic; în această categorie se include şi orice program informatic care poate determina realizarea unei funcții de către un sistem informatic;*" în ceea ce priveşte definirea noțiunii de suport de stocare, prin raportare la explicațiile etimologice[10], arătăm că acesta înseamnă o piesă sau un dispozitiv de adunare, de depozitare a datelor informatice.

Spre deosebire de percheziția domiciliară unde legiuitorul odată cu explicarea semnificației acesteia a stabilit anumite cazuri şi condiții în care se poate dispune, în cazul percheziției informatice astfel de cazuri şi condiții nu există, ceea ce înseamnă că sunt necesare a fi îndeplinite cerințele generale stabilite în art. 97 şi urm. CPP, cele ce se pot desprinde din definirea procedurii şi cele inserate în art. 168 alin. 2 ultima teză CPP, potrivit cărora percheziția informatică se poate dispune „*când pentru descoperirea şi strângerea probelor este necesară cercetarea unui sistem informatic sau a unui suport de stocare a datelor informatice.*"

Percheziția informatică poate avea loc doar în baza emiterii unui mandat de percheziție informatică, a cărui procedură de obținere comportă diferite particularități, după cum acesta este solicitat în cursul urmăririi penale sau în cel al judecății.

Astfel, pentru prima etapă a procesului penal legiuitorul utilizează noțiunea în cursul urmăririi penale, ceea ce înseamnă că este suficient ca în cauză să fie începută urmărirea penală față de faptă conform art. 305 alin. 1, 2 CPP, că nu este necesară dispunerea continuării urmăririi penale față de o persoană anume şi nici punerea în mişcare a acțiunii penale în baza art. 305 alin. 3 CPP, respectiv, art. 309 CPP. Ea poate fi solicitată de către procuror, legiuitorul excluzând organul de cercetare penală şi poate fi dispusă de către judecătorul de drepturi şi libertăți (în continuare JDL) de la instanța căreia i-ar reveni competența să judece cauza în primă instanță sau de la instanța corespunzătoare în grad acesteia în a

9 Publicată în Monitorul Oficial nr. 279 din 21.04.2003.

10 https://dexonline.ro/definitie/suport şi a stoca.

cărei circumscripție se află sediul parchetului din care face parte procurorul care efectuează sau supraveghează urmărirea penală, ceea ce înseamnă că legiuitorul a stabilit o competență alternativă, alegerea uneia dintre cele două instanțe fiind lăsată la aprecierea procurorului, desigur că aceasta trebuie fundamentată pe criterii de celeritate şi oportunitate.

Percheziția informatică se solicită printr-o cerere, în legătură cu care legiuitorul nu menționează ce ar trebui să cuprindă, situație în care suntem de părere că ea trebuie să aibă un conținut corespunzător cererii de percheziție domiciliară cu modificările aferente, cerere care împreună cu dosarul cauzei se înaintează judecătorului de drepturi şi libertăți, conform competenței mai sus menționate.

Sub aspectul condițiilor formale, legiuitorul stabileşte că soluționarea cererii are loc în camera de consiliu, deoarece are regim de confidențialitate (ceea ce impune şi un regim aparte de păstrare a cauzei având un asemenea obiect, ea neavând un caracter public), fără citarea părților, pentru că dacă părțile ar fi citate şi ar cunoaşte date despre efectuarea ei, rezultatul scontat ar fi unul negativ, cu participarea obligatorie a procurorului, lipsa procurorului fiind un caz de nulitate absolută în condițiile art. 281 alin. 1 lit. d CPP şi ar conduce la anularea actelor procesuale şi procedurale dispuse şi efectuate în baza lor conform art. 280, 102 CPP.

Este de observat că în cazul acesteia legiuitorul nu mai impune un termen de soluționare a cererii, ca şi în cazul percheziției domiciliare, unde termenul este de 24 de ore de la înregistrarea cererii la instanța competentă, conform art. 158 alin. 5 CPP, ceea ce nu înseamnă că asupra cererii se poate dispune oricând, fiind de părere că ea trebuie soluționată de urgență, adică în ziua înregistrării sau cel mult a doua zi.

În ceea ce priveşte modalitățile de soluționare a cererii, există două posibilități şi anume atunci când cererea este întemeiată, JDL va dispune admiterea cererii şi încuviințarea efectuării percheziției. Cu acest prilej JDL va emite în mod obligatoriu doar două acte procesuale, acestea fiind în ordine cronologică următoarele: încheierea şi mandatul de percheziție, cu precizarea că legiuitorul nu mai face referire la necesitatea întocmirii minutei.

Totuşi, prin raportare la dispozițiile art. 400 CPP, care ar constitui un drept comun în materie, având în vedere faptul că JDL realizează o deliberare atunci când admite cererea, dar şi din rațiuni practice şi anume durata scurtă de timp necesară pentru redactarea minutei, raportat la durata mai lungă necesară redactării încheierii, considerăm că şi în acest caz este necesar a fi redactată minuta.

Legiuitorul prevede că încheierea trebuie să cuprindă denumirea instanței; data, ora şi locul emiterii; numele, prenumele şi calitatea persoanei care a emis mandatul de percheziție; perioada pentru care s-a emis mandatul şi în cadrul căreia trebuie efectuată activitatea dispusă; scopul pentru care a fost emis; sistemul informatic sau suportul de stocare a datelor informatice care urmează a fi percheziționat, precum şi numele suspectului sau inculpatului, dacă este cunoscut;

semnătura judecătorului şi ştampila instanței, fără ca acesta să mai facă referire la cuprinsul mandatului, raportat la care, pentru identitate de rațiune suntem de părere că mandatul trebuie să aibă acelaşi conținut ca şi încheierea, la fel ca în cazul percheziției domiciliare, potrivit art. 158 alin. 7 CPP.

Atunci când JDL apreciază că nu sunt îndeplinite condițiile prevăzute de lege va dispune respingerea cererii de efectuare a percheziției domiciliare (aspect care nu este reglementat de legiuitor, dar dedus din ansamblul normelor procesuale în materie), prilej cu care apreciem că este necesar a întocmi minuta şi încheierea cu un conținut asemănător încheierii de admitere, modificat corespunzător soluției date (nici acest aspect nu este reglementat de legiuitor, dar se poate deduce din ansamblul normelor procesuale în materie).

Important de precizat este faptul că încheierea prin care judecătorul de drepturi şi libertăți se pronunță asupra cererii de încuviințare a efectuării percheziției domiciliare, indiferent de soluția adoptată, nu este supusă căilor de atac, ceea ce înseamnă că nu poate fi supusă examinării instanței de control judiciar, ea fiind definitivă la data adoptării.

În ceea ce priveşte percheziția informatică nu există condiționarea unei noi cereri de percheziție pentru acelaşi sistem informatic sau mijloc de stocare, de apariția sau descoperirea de fapte sau împrejurări noi, necunoscute la momentul soluționării cererii anterioare de către judecător, fiind însă de părere că numai în atare situații s-ar justifica formularea unei noi cereri, considerentele inițiale ale judecătorului ce au fundamentat o primă soluție putând suferi modificări numai dacă apar elemente noi.

Percheziția informatică poate fi solicitată şi în cursul judecății, dar nu şi în etapa de cameră preliminară al cărei obiect reglementat în art. 342 CPP are în vedere verificarea legalității probelor, iar nu administrarea acestora. În ceea ce priveşte etapa executării hotărârii, regula este că nu se poate efectua percheziție domiciliară, excepția fiind că se poate, dar numai dacă face parte din procedura dării în urmărire legiferată în art. 521 şi urm. CPP, unde art. 523 alin. 1 lit. c CPP prevede printre activitățile ce pot fi efectuate şi percheziția, fără a identifica sub care formă, ca atare considerăm că şi cea informatică, dacă este utilă îndeplinirii scopului procedurii dării în urmărire.

În cursul judecății, instanța competentă potrivit regulilor generale de competență prevăzute în art. 35 şi urm. CPP (de astă dată legiuitorul nu mai are în vedere o competență alternativă, este drept că nici nu face vreo altă referire, însă apreciem că se aplică regulile generale de competență) poate decide din oficiu că percheziția informatică este necesară sau poate fi solicitată de către procuror, părți ori persoana vătămată, cu mențiunea că ultimele două categorii de participanți neavând posibilitatea a solicita efectuarea percheziției domiciliare, doar această formă de percheziție şi numai în cursul judecății, în cursul urmăririi penale titularul cererii putând fi doar procurorul. Percheziția va putea fi dispusă în această

etapă de către instanță, dar legiuitorul nu precizează nici aici care anume, însă prin raportare la prevederile art. 354 alin. 2 CPP cu referire la continuitatea completului de judecată, suntem de părere că o va putea dispune doar cea învestită cu judecarea cauzei, adică acea instanță căreia i s-a repartizat aleatoriu cauza spre soluționare şi care va trebui să adopte soluția pe fond în acea cauză.

Conform reglementărilor actuale percheziția în sistem informatic ori a unui suport de stocare a datelor informatice se efectuează de către un specialist care funcționează în cadrul organelor judiciare sau din afara acestora sau lucrători de poliție specializați.

Referitor la specialiştii care funcționează în cadrul organelor judiciare, considerăm că pe lângă studiile în domeniul informatic pe care aceştia trebuie să le aibă este necesar să fie specializați în astfel de activități, în sensul că trebuie să fie familiarizați cu procedura de urmat, programele informatice care trebuie utilizate, modalitățile de obținere şi valorificare a rezultatelor, specialişti asemenea inspectorilor antifraudă conform art. 3 alin. 3-4 OUG 74/2013[11]. În ceea ce priveşte specialistul din afara organelor judiciare, suntem de părere că acesta nu poate fi decât o persoană din categoria acelora autorizate de către Ministerul Justiției, pentru simplul motiv că aceştia trebuie să se supună anumitor rigori, însă în lipsa acestora pot fi şi altă categorie de specialişti, noțiunea utilizată de legiuitor şi lipsa îngrădirilor dând această posibilitate, criteriile principale de selecție fiind profesionalismul, probitatea morală şi imparțialitatea.

Percheziția în sistem informatic sau a unui suport de stocare a datelor informatice se efectuează în prezența suspectului ori a inculpatului, pe de o parte şi a procurorului sau a organului de cercetare penală, pe de altă parte.

Persoanei al cărei sistem informatic sau suport de stocare a datelor este percheziționat i se va permite să fie asistată ori reprezentată de o persoană de încredere. Când persoana al cărei sistem informatic sau suport de stocare a datelor este percheziționat este reținută ori arestată, va fi adusă la percheziție. În cazul în care nu poate fi adusă, percheziția se face în prezența unui reprezentant ori martor asistent.

Organele de urmărire penală trebuie să ia măsuri ca percheziția informatică să fie efectuată fără ca faptele şi împrejurările din viața personală a celui la care se efectuează percheziția să devină, în mod nejustificat, publice, principiu ce se desprinde şi din conținutul Convenției de la Budapesta.

Percheziția informatică dispusă în cursul judecății, se va efectua prin comunicarea mandatului de efectuare a percheziției informatice procurorului, care va proceda ca şi când ar efectua o percheziție dispusă în cursul urmăririi penale.

În acord cu reglementările legale suntem de părere că înainte de efectuarea percheziției propriu-zise, pot fi luate măsuri pregătitoare, legiuitorul având în vedere situația în care ridicarea obiectelor care conțin datele informatice ar afecta

11 Publicată în Monitorul Oficial nr. 389 din 29 iunie 2013.

grav desfăşurarea activității persoanelor care dețin aceste obiecte, când procurorul poate dispune efectuarea de copii, care servesc ca mijloc de probă, fiind necesar ca acele copii să se realizeze cu mijloace tehnice şi proceduri adecvate, de natură să asigure integritatea informațiilor conținute de acestea. A face o copie în sensul legii nu înseamnă a achiziționa, a reproduce ori a confecționa un obiect identic sau similar cu cel asupra căruia urmează a se efectua percheziția, ci a-i copia conținutul, ca atare copia poate fi realizată prin transferul întregului conținut dintr-un sistem informatic ori mijloc de stocare în altul, cu menținerea intactă a conținutului inițial. Cerințele ar fi ca mijlocul de stocare pe care se face copia să aibă dimensiunea suficientă pentru a prelua întreaga informație, să fie gol şi să asigure integritatea datelor ce i-au fost transferate prin copiere. În această situație, copia înlocuieşte originalul şi va constitui mijloc de probă. Deşi legea nu distinge, considerăm că actul procesual prin care procurorul dispune realizarea copiei este ordonanța conform art. 286 CPP.

O altă măsură pregătitoare, ce este obligatoriu a fi luată în vederea executării percheziției dispuse şi pentru asigurarea integrității datelor informatice stocate pe obiectele ridicate, constă în dispunerea de către procuror prin ordonanță la efectuarea de copii, ceea ce înseamnă că percheziția informatică nu se va efectua niciodată asupre originalului, ci asupra copiei acestuia. Raportat la cele expuse mai sus, vor putea exista situații în practica judiciară în care va exista o copie efectuată pentru a nu fi afectată activitatea şi o altă copie a celei dintâi asupra căreia se va efectua percheziția informatică.

În privința desfăşurării percheziției constatăm că legiuitorul nu a venit cu reglementări în pofida conținutului Convenției de la Budapesta şi Anexei la Recomandarea nr. R (95) 13 a Comitetului de Miniştri, motiv pentru care aceştia se vor ghida în activitatea lor după norme internaționale[12] care au un mare avantaj, deoarece sunt elaborate de către specialişti renumiți în domeniu, numai că prin nepreluarea lor în dreptul intern sunt facultative în aplicare, ceea ce poate duce la utilizarea de proceduri diferite în cauze cu obiecte similare.

Potrivit uzanțelor specialistul sau organul de poliție specializat va efectua percheziția utilizând echipamente care să împiedice transmiterea de date (de tip *blocker*) şi programe nevirusate cu ajutorul cărora să se efectueze căutarea (de exemplu EnCase Forensic Software[13]).

Preluând din reglementările Convenției de la Budapesta, legiuitorul a prevăzut că în cazul în care, cu ocazia efectuării percheziției unui sistem informatic sau a unui suport de stocare a datelor informatice, se constată că datele informatice

12 Standarde în domeniul probelor digitale, stabilite de Scientific Working Group on Digital Evidence, https://www.swgde.org; Principii în domeniul probelor digitale, emise de International Organization on Computer Evidence, http://www.uia.org; Proceduri model de examinare criminalistică a sistemelor informatice şi Codul etic al IACIS, elaborate de International Association of Computer Investigation Specialists, http://www.iacpcybercenter.org.

13 https://www.guidancesoftware.com/encase-forensic.

căutate sunt cuprinse într-un alt sistem informatic ori suport de stocare a datelor informatice şi sunt accesibile din sistemul sau suportul inițial, procurorul dispune de îndată conservarea, copierea datelor informatice identificate şi va solicita de urgență completarea mandatului, fără a mai face alte precizări. În această situație, cu privire la modalitatea de conservare a datelor informatice considerăm că procedura de urmat nu este alta decât cea reglementată în art. 154 CPP, care se aplică în mod corespunzător, iar copierea datelor se face potrivit procedurii mai sus menționate, procurorul putând da o singură ordonanță prin care să dispună asupra ambelor proceduri de urmat.

Datele informatice descoperite vor fi evidențiate cu ajutorul programului informatic utilizat care are abilitatea de a emite un raport asupra activității de căutare desfăşurate, legiuitorul menționând că acestea au un caracter secret şi se păstrează în condițiile legii, ceea ne duce cu gândul la limitele reale ale utilizării acestora, având în vedere că secretele sunt considerate a fi informațiile a căror divulgare neautorizată este de natură să producă daune securității naționale[14], ceea ce ne face să credem că este o utilizare nepotrivită a noțiunii, impunându-se înlocuirea sa cu noțiunile „caracter confidențial" ori „caracter nepublic".

Rezultatele percheziției informatice vor fi valorificate prin consemnarea lor într-un proces-verbal, care trebuie să cuprindă, aşa cum rezultă din conținutul art. 168 alin. 13 CPP: numele persoanei de la care a fost ridicat sistemul informatic sau suporturile de stocare a datelor informatice ori numele persoanei al cărei sistem informatic este cercetat; numele persoanei care a efectuat percheziția; numele persoanelor prezente la efectuarea percheziției; descrierea şi enumerarea sistemelor informatice ori a suporturilor de stocare a datelor informatice față de care s-a dispus percheziția; descrierea şi enumerarea activităților desfăşurate; descrierea şi enumerarea datelor informatice descoperite cu ocazia percheziției; semnătura sau ştampila persoanei care a efectuat percheziția; semnătura persoanelor prezente la efectuarea percheziției; care reprezintă o probă de sine stătătoare, ce nu trebuie confundată cu procesul-verbal prevăzut de art. 198 alin. 2, art. 199 CPP care cuprinde constatările personale ale organelor judiciare, care nu există în cazul percheziției informatice, constatările fiind aici ale specialistului ce o efectuează.

Deşi reglementările nu fac referire, suntem de părere că la procesul verbal se anexează şi raportul generat de programul de căutare, care vine să susțină veridicitatea celor consemnate în cuprinsul procesului-verbal.

Făcând trimitere la dispozițiile art. 103 CPP se impune să arătăm că, deşi are un caracter predominant tehnic, care teoretic nu ar avea voie să conțină erori, nici percheziția informatică nu are o valoare dinainte stabilită prin lege, fiind supusă liberei aprecieri a organelor judiciare în urma evaluării tuturor probelor

14 A se vedea art. 15 alin. 1 lit. f din Legea nr. 182 din 12 aprilie 2002, publicată în Monitorul Oficial nr. 248 din 12 aprilie 2002.

administrate în cauză, mai ales că este de notorietate prezența viruşilor informatici şi a uşurinței cu care un sistem informatic sau un mijloc de stocare a datelor poate fi contaminat, motiv pentru care susținem ideea că atunci când se contestă prezența unor probe digitale nu trebuie să existe rezerve în a se dispune efectuarea unei expertize informatice în baza art. 172 şi urm. CPP care are posibilitatea de a stabili şi certifica existența acestora, precum şi modalitatea în care a ajuns acolo cu trimitere la coordonate temporale.

Referințe

Anexa la Recomandarea nr. R (95) 13 a Comitetului de Miniştri către statele membre cu privire la problemele de procedură penală legate de tehnologiile informaționale

Codul etic al IACIS, elaborat de International Association of Computer Investigation Specialists, http://www.iacpcybercenter.org

Ghid introductiv pentru aplicarea dispozițiilor legale referitoare la criminalitatea informatică, http://www.riti-internews.ro

Lăncrăjan, A., Litvin, M., Pop, M. 2015. *Ghid de investigarea infracțiunilor de proprietate intelectuală săvârşite în mediul digital*, Bucureşti, Patru Ace

Principii în domeniul probelor digitale, emise de International Organization on Computer Evidence, http://www.uia.org;

Proceduri model de examinare criminalistică a sistemelor informatice

Standarde în domeniul probelor digitale, stabilite de Scientific Working Group on Digital Evidence, https://www.swgde.org