CONSIDERAȚII ASUPRA PERCHEZIȚIEI INFORMATICE

SEARCH AND SEIZURE OF DIGITAL EVIDENCE

Paula CIOREA[1]
Masterand – Facultatea de Drept, UBB

Abstract

The jurisprudence of the European Court of Human Rights and the jurisprudence of United States's courts pay particular attention to individual privacy. The search and seizure of digital evidence is a very invasive procedure that should be permitted only in extreme situations. In present, the procedure can be disposed whenever appears the need to gather digital evidence. There are examples of safeguards that are not enough respected, like the situation when the presence of the accused is not required because the search and seizure is disposed when the prosecution is in rem. It is essential to protect the right of the accused to be present at the search and seizure because the absence of the accused involve the imposibility to check if the other safeguards are respected and to make observations. Also, if the subject of the search and seizure is a lawyer, the procedure should be realised with the respect of the professional secrecy. The law can be improved by providing more safeguards in order to protect the humans rights and if the law is inspired by jurisprudence, then the solutions provided are already tested in time.

Keywords: *safeguards, professional secrecy, specialist, computer search warrant, digital evidence, jurisprudence.*

Rezumat

Jurisprudența Curții Europene a Drepturilor Omului și jurisprudența instanțelor din Statele Unite ale Americii acordă o atenție deosebită dreptului persoanei la viață privată. Percheziția informatică este un procedeu probatoriu care prezintă un grad mare de ingerință, astfel încât trebuie să fie dispusă numai în mod excepțional. În prezent, percheziția informatică se poate dispune în toate cazurile când, „pentru descoperirea și strângerea probelor este necesară cercetarea unui sistem informatic sau a unui suport de stocare a datelor informatice" (art. 168 alin. (2), teza finală C.proc.pen.). Există situații în care garanțiile prevăzute pot fi eludate, precum este cazul percheziției informatice dispuse în timpul urmăririi penale in rem. Astfel, nefiind încă atribuită calitatea de suspect sau inculpat, nu este incidentă prevedere legală care impune prezența acestuia la efectuarea percheziției informatice. Este esențial ca utilizatorul sistemului informatic ori a mijlocului de stocare a datelor informatice să fie prezent la efectuarea procedeului probatoriu pentru a supraveghea respectarea dispozițiilor legale și pentru a formula obiecții, în cazul încălcării acestora. De asemenea, în cazul în care subiectul percheziției informatice este un avocat, procedeul probatoriu trebuie efectuat cu respectarea secretului profesional. Dispozițiile privitoare la percheziția informatică pot fi îmbunătățite prin reglementarea mai multor garanții, iar dacă regulile sunt inspirate din jurisprudență, avantajul este că ele sunt testate de timp.

Cuvinte-cheie: *garanții, secret profesional, specialist, mandat de percheziție informatică, probe digitale, jurisprudență.*

[1] E-mail: paula_ciorea@yahoo.com.

CUPRINS

I. ASPECTE INTRODUCTIVE

Percheziția informatică reprezintă un procedeu probatoriu din ce în ce mai utilizat în scopul obținerii de probe digitale, majoritatea infracțiunilor fiind susceptibile să genereze astfel de urme. Simpla infracțiune de amenințare poate fi probată, în anumite circumstanțe, cu ajutorul E-mailurilor care, de cele mai multe ori, în secţiunea *header*, conțin informații referitoare la adresa IP (*Internet Protocol address*) a sistemului informatic prin intermediul căruia e-mailurile au fost expediate. De asemenea, date informatice prezentând o listă a datornicilor pot dovedi comiterea infracțiunii de proxenetism, în forma obținerii de foloase patrimoniale de pe urma practicării prostituției.

Probele digitale reprezintă informații stocate, prelucrate sau transmise prin intermediul unui sistem informatic, care au putere doveditoare pentru organele de urmărire penală și pentru instanțele judecătorești.[2]

Printre mediile informatice relevante în materia percheziției informatice pot fi enumerate computerele, tabletele, telefoanele, dar și smart TV-urile ori computerele de la bordul autoturismelor. Recent a apărut conceptul de smart light bulb, bec care poate fi conectat la telefon prin intermediul unor aplicații special create în acest sens. Furnizorii acestor produse pot să le îmbunătățească prin atașarea unor camere de filmat, a unor microfoane sau a senzorilor, astfel încât mișcările, respectiv vocea utilizatorului să fie recunoscute ca elemente care determină punerea în funcțiune a becului inteligent. Există inclusiv becuri inteligente care detectează momentul în care utilizatorul se află în apropiere și se deschid automat. De asemenea, becul poate fi configurat astfel încât să se închidă în momentul în care utilizatoul părăsește locuința.[3] Prin urmare, becurile inteligente pot fi supuse atacurilor informatice, la fel ca toate produsele IoT (Internet of Things). Acest lucru a fost demonstrat când cercetători în materie de securitate au reușit să obțină parola conexiunii la internet, la o distanță de 30 de metri față de becul inteligent vizat. Cercetătorii au explicat că, în acest context, pot fi introduse apoi pachete în

[2] *Ghid introductiv pentru aplicarea dispozițiilor legale referitoare la criminalitatea informatică,* București, 2004, p. 70, disponibil online (*www.riti-internews.ro*).

[3] G. O'Driscoll, *10 Things You Need to Know About Smart Light Bulbs*, disponibil online la adresa *http://homementors.com/10-things-need-know-smart-light-bulbs/*.

rețeaua mesh[4], se pot captura detaliile Wi-Fi și decripta acreditările, toate fără autentificare prealabilă și fără atenționarea existenței unei prezențe străine.[5] Prin urmare, luând în considerare rapiditatea cu care tehnologia evoluează, se poate considera că inclusiv becul inteligent va putea fi supus percheziției informatice.

Internet of things, se referă în mod general la obiectele de zi cu zi care pot fi interconectate la o rețea.[6] Se pot imagina mai multe exemple de corupere a dispozitivului. Un hacker poate să unească mai multe dispozitive IoT, deja corupte, astfel încât să formeze o rețea de tip botnet[7] care să fie apoi folosită pentru a trimite spamuri. În același timp, hacker-ul poate încerca să acceseze rețeaua de acasă a victimei așa încât să infecteze sistemul informatic (de exemplu, computerul) și să exploateze existența unui dispozitiv IoT în rețea, fie el doar o mașină de spălat care poate comanda detergent suplimentar. În fapt, este de așteptat ca în viitor dispozitivele IoT să fie cele mai predispuse atacurilor venite din partea hackerilor, din moment ce vor exista diverse produse slabe calitativ, cu un nivel de securitate extrem de scăzut, care cel mai probabil vor fi imposibil de upgradat sau în privința cărora nu vor putea fi eliminate vulnerabilitățile descoperite.[8] În mod particular, hackerul poate să blocheze temporar accesul la un dispozitiv scump, și să ceară o sumă mare de bani pentru restabilirea funcționării. De exemplu, majoritatea tv-urilor vândute azi sunt îmbunătățite cu funcții smart care le fac apte să se conecteze la internet, dar fără a avea un sistem de protecție (firewall sau antivirus), astfel încât este suficient de facilă coruperea TV-ul prin intermediul unui virus ca pe ecran să apară un mesaj, care nu poate fi îndepărtat și prin care să se solicite remiterea unei anumite sume de bani pentru ca TV-ul să poată fi din nou folosit. Un atac asupra televizorului este mult mai eficient decât asupra computerului, de exemplu, pentru că nu există posibilitatea instalării unei versiuni noi a sistemului de operare a dispozitivului.[9]

Printre sistemele informatice poate fi enumerat și faxul. Conform art. 181 alin. (1) C.pen., faxul este un sistem informatic, având capacitatea de a stoca în memoria internă date informatice precum faxurile trimise și recepționate. De asemenea, și instumentul de plată electronică este un mijloc de stocare a datelor informatice.[10] Percheziția acestor instrumente precum sunt cardurile bancare, pot oferi probe digitale organului de urmărire penală. Cardurile bancare variază de la cele mai simple, care prezintă informații precum numărul de cont, numele utilizatorului ori data expirării, la cele mai complexe care pot oferi date precum istoricul plăților ori a retragerilor de numerar. Un asemenea istoric poate conduce organul de urmărire penală la identificarea locului de unde utilizatorul a interacționat cu un anumit bancomat și a orei când a fost îndeplinită activitatea de plată sau de retragere de numerar.[11] Aceste date pot fi extrem de valoroase în situația în care suspectul sau inculpatul invocă posesia unui card clonat, card care nu a fost folosit pentru retragerea de numerar, respectiva persoană nefiind singura care deține o clonă a cardului. O asemenea apărare este posibilă în contextul în care un instrument de plată electronică a fost clonat, în mod repetat, pentru a fi utilizatat de persoane diferite, care se află în zone georgrafice diferite.[12] Prin urmare, instrumentul de plată electronică, reprezentând un mijloc de stocare a datelor informatice care pot prezenta valență probantă pentru organele judiciare, poate fi supus

[4] Topologia mesh reprezintă o rețea care este destinată transportării datelor, instrucțiunilor și serviciilor de transport voce prin nodurile de rețea. Conexiunile vor fi continue chiar dacă există legături deteriorate sau blocate. Rețeaua *mesh* fără fir (*wireless*) este cea mai frecventă topologie folosită în prezent. A se vedea site-ul *http://igordoctor1.blogspot.ro/p/topologia-retelelor-de-calculatoare.html.*

[5] M. Rouse, *Smart Bulb (smart light bulb)*, disponibil online la adresa *http://internetofthingsagenda.techtarget.com/definition/smart-bulb-smart-light-bulb.*

[6] F. Xia, L. T. Yang, L. Wang, A. Vinel, *Internet of Things,* „International Journal of Communication Systems", în „International Journal of Communication", vol. 25, 2012, p. 1, disponibil online la adresa https://pdfs.semanticscholar.org/930c/4981e87584afa7e6f1f4977323e365aae097.pdf.

[7] O rețea de calculatoare infectate cu *software de tip bot* permite infractorilor numiți *boți* să preia, în mod ilegal, controlul acestora prin atacuri informatice sau trimiterea de mesaje *spam*. A se vedea A. Leția, *Metode de investigare a criminalității informatice*, „Dreptul", nr. 12/2013, p. 254, nota 10.

[8] E. Ronen, A. Shamir, *Extended Functionality Attacks on IoT Devices: The Case of Smart Lights*, Weizmann Institute of Science, Rehovot, Israel, p. 1, disponibil online la adresa (*http://www.wisdom.weizmann.ac.il/~eyalro/EyalShamirLed.pdf).*

[9] E. Ronen, A. Shamir, op. cit., p.2.

[10] S. Bogdan, D.A. Șerban, G. Zlati, *Noul Cod penal. Partea specială*, Universul Juridic, București, 2014, p. 697. A se vedea și M. Dobrinoiu, Comentariu, în V. Dobrinoiu și colab., *Noul Cod penal comentat. Partea specială*, vol. II, Universul Juridic, București, 2012, p. 911 și 912.

[11] G. Zlati, *Percheziția sistemelor informatice și a mijloacelor de stocare a datelor informatice (II),* în „Caiete de drept penal", nr. 4/2014, p. 77

[12] Ibidem.

percheziției informatice doar în baza unui mandat de percheziție valabil emis.

Dacă în cazul cardurilor bancare complexe nu apare nicio îndoială cu privire la capacitatea acestora de a reprezenta mijloace de stocare ce pot fi percheziționate informatic, cazul cardurilor bancare standard a făcut obiectul unor controverse legate de natura acestora.[13] Astfel, în cauza US v. Eric-Arnaud De L'Isle[14], Curtea a hotărât că citirea benzii magnetice a cardului bancar nu reprezintă o percheziție informatică.[15] Hotărârea a rămas definitivă prin respingerea căii de atac. Cauza este interesantă deoarece cunoaște și argumente în sens contrar, dezvoltate de către judecătorul Kelly. Acesta își pune întrebarea în ce măsură așteptarea la intimitate cu privire la informațiile stocate pe banda magnetică este sau nu rezonabilă. Potrivit judecătorului, răspunsul trebuie circumscris în funcție de existența unor bariere tehnice care să împiedice persoana să își rescrie informațiile pe banda magnetică a cardului. Astfel, dacă informațiile pot fi modificate fără prea mare dificultate, atunci există o așteptare rezonabilă la intimitate în privința conținutului benzii, în baza jurisprudenței conform căreia ori de câte ori se procedează la citirea conținutului unui suport rescriptibil de stocare a informației digitale, devin aplicabile garanțiile prevăzute în cazul unei percheziții informatice. Prin urmare, dacă banda magnetică a cardului este un dispozitiv de stocare digitală, chiar dacă are o capacitate de stocare limitată, citirea datelor informatice intră sub incidența prevederilor percheziției informatice. Contrar opiniei majoritare a curții, judecătorul consideră că este posibilă verificarea identității dintre datele stocate și informațiile existente pe partea din față a cardului doar în urma scanării cardului, iar rezultatul pozitiv al căutării nu poate justifica legalitatea ori nelegalitatea acțiunii. O percheziție nu poate să devină legală în urma a ceea ce s-a găsit prin efectuarea percheziției. În drept, verificarea se face de la începutul acțiunii, iar caracterul legal sau ilegal nu e schimbat în funcție de succesul acțiunii.

Prin urmare, dacă informația stocată poate să fie modificată în mod legal de către utilizator, prin operațiunea de rescriere, nu ar fi ilegal ca utilizatorul să rescrie pe banda magnetică a cardului pe care intenționează să nu îl mai folosească o lungă perioadă de timp, informația "parolacontuluimeubancareste78911Y783", pentru ca apoi să o recupereze în cazul în care o va uita. Judecătorul mai arată că viitoarele hotărâri ale instanțelor trebuie să aibă în vedere și evoluția tehnică și sistemele mai complexe care sunt deja în folosință sau în dezvoltare. Recent, multe dintre cardurile de credit din SUA conțin cipuri, astfel încât au o capacitate de stocare mult mai mare decât vechile carduri cu bandă magnetică.[16]

Percheziția informatică este o activitate care prezintă numeroase dificultăți cu atât mai mult cu cât acest procedeu probatoriu presupune un grad mare de ingerință în viața privată a utilizatorului sistemului informatic ori a mijlocului de stocare a datelor informatice. Situația din prezent a normelor specifice acestei activități este una defavorabilă, garanțiile reglementate sunt prea puține iar dintre cele prevăzute, multe pot fi cu ușurință eludate, astfel încât o viitoare condamnare a României la Ct.E.D.O. este probabilă.

Dificultățile se amplifică atunci când speța cuprinde elemente precum virtualizarea ori atunci când în

---

[13] **Nota redacției:** apreciem că nu există vreo diferență la nivelul cardurilor bancare ori a instrumentelor de plată electronice în general, atâta vreme cât acestea au natura unui mijloc de stocare a datelor informatice. Iar pentru aceasta este necesar să discutăm despre un suport fizic susceptibil să stocheze date informatice.

[14] *Hotărârea în Cauza 15-1316*, 8 iunie 2016, p. 2, disponibilă online (*http://media.ca8.uscourts.gov/opndir/16/06/151316P.pdf).*

[15] Stare de fapt: Eric-Arnaud De L'Isle este oprit în trafic și din cauza mirosului de marijuana, a fost percheziționată mașina conducătorului auto. În urma percheziției au fost găsite, nu droguri, ci numeroase carduri bancare. Acestea au fost scanate, activitate în urma căreia s-a descoperit că unele carduri nu conțineau nicio informație, iar altele conțineau informații neconforme cu realitatea. Judecat pentru deținerea de dispozitive de acces neautorizate sau contrafăcute, De L'Isle a cerut excluderea probelor obținute prin scanarea cardurilor întrucât reprezintă o percheziție informatică, efectuată în lipsa unui manadat de percheziție. În replică s-a arătat că majoritatea cardurilor de plastic conțin 3 linii cu informații stocate pe banda magnetică (număr de cont, nume utilizator și cod de identificare). Potrivit unui expert în investigarea fraudelor, banda magnetică conține în general și data de expirare a cardului. Informația regăsită pe banda magnetică ar trebui să fie aceeași cu cea găsită pe partea din față a cardului, așa încât nu există o așteptare rezonabilă la intimitate pentru informații aflate la vedere. Un card este re-codificat atunci când banda magentică este rescrisă. Cu privire la cardurile în cazul cărora nu s-au găsit informații în momentul scanării, expertul a arătat că lipsa datelor indică faptul că acestea sunt contrafăcute. În cauză, s-a considerat că scanarea cardului poate fi asemănată cu folosirea luminii ultraviolete pentru a identifica dacă un ordin de plată este autentic. Curtea a considerat că, în mod normal, informația stocată este identică informației scrise pe partea din față a cardului și că banda magnetică a cardurilor, în speță, nu conținea informații, ori conținea informații corespunzătoare unor carduri de credit furate, așa încât nu exista o așteptare rezonabilă la intimitate din moment ce informația nu exista ori aceasta era falsă.

[16] *Hotărârea în Cauza 15-1316*, *cit. supra,* 8 iunie 2016, p. 11 și urm.

cauză sunt incidente bazele de date. Virtualizarea crează inconveniente în efectuarea percheziției informatice deoarece presupune utilizarea unui singur computer pentru a fi rulate mai multe sisteme de operare. Inconvenientul cu care se confruntă specialistul ori lucrătorul de poliție specializat, în punerea în aplicare a mandatului de percheziție informatică constă în faptul că datele din mașina virtuală (virtual machine) sunt stocate fizic într-un mod în care devin vizibile doar atunci când mașina virtuală operează.

Pentru conectarea la mașina virtuală sau pentru decriptarea fișierelor, astfel încât informațiile să fie vizibile, este adesea necesară utilizarea cheilor de acces. Astfel, organele judiciare vor fi apte să localizeze fizic server-ul (sistemul informatic) care găzduiește datele informatice, dar fără a le fi accesibilă informația deoarece aceasta este stocată într-o mașină virtuală pentru rularea căreia este necesară o cheie de acces. Bazele de date relaționale reprezintă o altă variantă de stocare a informațiilor în fișiere, care se bazează pe legătura care intervine între părțile care formează informația. Câmpurile care conțin informații nu este necesar a fi stocate într-un singur sistem informatic ori mijloc de stocare a datelor informatice, dar software-ul care prelucrează bazele de date permite utilizatorului să introducă date și să realizeze operații din fața unui singur astfel de sistem. Fără software-ul potrivit, informațiile vor apărea ca o serie dintr-un câmp de informații, lipsit de sens.[17]

II. MEDIUL CLOUD

Mediul cloud poate fi catalogat drept unul dintre cele mai problematice elemente cu care se confruntă organul judiciar în dispunerea și efectuarea percheziției informatice. Acest mediu permite utilizatorilor acces la datele digitale prin intermediul internetului, indiferent care este sistemul informatic folosit.[18] Inconvenientul în realizarea percheziției informatice este cauzat de locația geografică în care datele informatice, aparținând utilizatorului sistemului informatic, se găsesc, pentru că, de cele mai multe ori, apar implicații de natură transfrontalieră.[19]

În multe cazuri, mandatele de percheziție informatică fac referire la o locație specifică, fără a se ține cont de natura probelor digitale, ajungându-se la compararea mijlocului de stocare a sistemului informatic cu un dulap cu sertare. Dezavantajul acestei abordări este acela potrivit căruia procurorul, înainte de începerea efectuării percheziției sau în momentul redactării referatului de încuviințare a efectuării percheziției informatice, este posibil să nu aibă cunoștință despre locația exactă a datelor. Utilizatorii pot fi conectați la o rețea printr-un sistem informatic care funcționează precum un simplu terminal. Majoritatea fișierelor se păstrează într-un alt sistem informatic, aflat într-o altă locație. E-mailurile, documentele, pozele, aplicațiile sau alte astfel de date informatice sunt fiecare stocate în cadrul unor servere (sisteme infomatice) diferite. Astfel, dacă specialistul ori lucrătorul de poliție specializat care efectuează percheziția, în prezența procurorului sau a organului de cercetare penală, va căuta probe digitale doar în sistemul informatic al utilizatorului, foarte puține informații vor fi găsite deoarece, în realitate, toate informațiile importante sunt stocate în alte sisteme informatice din cadrul rețelei.[20] Discuția este asemănătoare și cu privire la mediul cloud. Devine extrem de dificilă localizarea unui server pe care sunt stocate date informatice din moment ce infractorii se bazează pe accesul de la distanță pentru salvarea și procesarea informațiilor, folosind dispozitive îndepărtate. Popularitatea de care beneficiază mediul cloud a transformat urmărirea penală a infracțiunilor într-o operațiune dificilă. Mediul cloud poate fi folosit de infractori pentru stocarea datelor digitale pe un server care se află în afara jurisdicției instanțelor din țara de rezidență.

De-a lungul timpului au fost dezvoltate mai multe teorii pentru combaterea pierderii datelor digitale în lumea cloud. Abordarea tradițională a fost aceea a principiului teritorialității, în virtutea căruia este competentă instanța în circumscripția căreia sunt localizate datele. În principiu, această abordare împiedică investigațiile din cauza faptului că, de multe ori, nici furnizorul serviciului cloud nu știe unde sunt localizate exact datele digitale. O altă teorie este aceea a principiului naționalității, în virtutea căruia naționalitatea infractorului determină competența instanței. Principiul impune anumite restricții din moment ce infractorii pot, cu ușurință, să

[17] J. M. Cauthen, Executing Search Warrants in the Cloud, disponibil online la adresa *https://leb.fbi.gov/2014/october/executing-search-warrants-in-the-cloud.*

[18] S.M. Corradi, *Be Reasonable! Limit Warrantless Smart Phone Searches to Gant's Justification for Searches Incident to Arrest*, în „Case Western Reserve Law Review", vol 63, nr. 3, 2013, p. 959.

[19] J. M. Cauthen, *op. cit.*

[20] *Ibidem.*

fie cetățeni străini, având în vedere că infracționalitatea cibernetică este transfrontalieră și nu este nevoie de existența unei apropieri fizice în realizarea atacurilor. Mai mult, datele digitale nu au o naționalitate pentru că naționalitatea este un atribut al individului. A treia abordare este cea a principiului steagului, conform căruia infracțiunile comise pe nave, aeronave se supun jurisdicției statului în care navele sau aeronavele au fost înmatriculate, indiferent de locația lor la momentul comiterii infracțiunii (art. 22 Convenția cu privire la infracționalitatea cibernetică). Dezavantajul teoriei steagului este acela că infractorii ar putea fi determinați să aleagă un furnizor al serviciului cloud care să nu se supună niciunei jurisdicții (pirate flag).[21]

Microsoft a câștigat o luptă importantă pentru utilizatorii Europeni ai produselor companiei, într-un proces deschis împotriva Departamentului de Justiție din SUA. Reprezentanții Microsoft au arătat că au adus în fața instanței cazul deoarece consideră că cetățenii europeni și organizațiile își doresc ca datele să fie protejate de normele europene, nedorind ca e-mailurile și documentele lor să fie supuse riscului de a fi accesate de către guvernul SUA potrivit regulilor din SUA. Dacă inițial curtea a obligat compania Microsoft să furnizeze anumite E-mailuri localizate geografic în afara jurisdicției SUA, în calea de atac, s-a decis că mandatul de percheziție emis din interioriul SUA nu poate afecta datele clienților Microsoft stocate în străinătate. Curtea confirmă, prin urmare, că mandatul de percheziție informatică emis nu se aplică extrateritorial, cu privire la consumatori ale căror date sunt stocate în afara Statelor Unite, și arată că protecția legală din lumea fizică se aplică, în aceeași măsură, și domeniului digital.[22] Prin urmare, curtea de apel, în baza jurisprudenței Morrison v. National Australia Bank, a considerat că legislația americană este menită să se aplice doar în jurisdicția SUA.[23]

Amplasarea datelor provoacă numeroase dezbateri, în special în legătură cu riscurile la adresa confidențialității pe care le presupune transferul datelor în alte jurisdicții. Definitoriu, în cazul mediului cloud, este faptul că deservirea clienților se realizează din centre de date dispersate geografic. Chiar și în situația în care centrul de date și clientul se află în aceeași jurisdicție, datele utilizatorului sunt transferate în alte amplasamente, în vederea realizării clonelor (copii) de rezervă pentru recuperarea datelor în situația dezastrelor. Astfel, este mai importantă transparența cu privire la locul de stocare al principalelor seturi de date și a fluxurilor de date aferente, decât negocierea unui anumit amplasament al centrului de date.[24] Prin urmare, stocarea poate să se realizeze într-un centru de date din apropiere, sau informația poate să fie împărțită între mai multe centre de date ori stocată în străinătate. În anumite împrejurări, dacă utilizatorul este conectat prin intermediul unui sistem informatic care permite doar un control limitat, precum este tableta sau telefonul mobil, este probabil ca nici utilizatorul să nu poată identifica locul unde datele sunt, din punct de vedere fizic, localizate.

De asemenea, este posibil în vederea unor acorduri, ca furnizorul serviciilor să aibă acces fizic la informații dar fără posibilitatea de a căuta sau de a recupera date, deoarece acestea sunt deseori criptate printr-o cheie digitală privată. Astfel, cel responsabil cu efectuarea percheziției, va descoperi că a existat în trecut o conexiune la date, dar fără a obține informațiile căutate. În situația datelor criptate, chiar dacă specialistul ori lucrătorul de poliție specializat determină localizarea fizică a acestora, operațiunea este insuficientă deoarece informația criptată nu va putea fi folosită.[25]

Produsele companiei Apple au reprezentat, adesea, adevărate provocări pentru organele judiciare. Au existat numeroase hotărâri prin care compania a fost obligată să producă un software care să permită autorităților deblocarea telefoanelor create de companie. Între FBI și Apple au apărut conflicte declanșate de

[21] G. Vaciago, *Remote forensics and cloud computing: an italian and european legal overview*, în „Digital Evidence and Electronic Signature Law Review", vol. 8, 2011, p. 124.

[22] J. Frank , *Our search warrant case: Microsoft's commitment to protecting your privacy*, disponibil online la adresa https://blogs.microsoft.com/eupolicy/2016/09/05/our-search-warrant-case-microsofts-commitment-to-protecting-your-privacy/. Cazul a început în anul 2013 când o instanță din New York a emis un mandat prin care se solicita companiei Microsoft să identifice toate e-mailurile și informațiile private asociate unui anumit cont găzduit de aceasta. E-mailurile contului au fost localizate în Dublin, Irlanda, unul dintre centrele de date deținute de companie. Microsoft a furnizat informațiile cu privire la cont, care au fost localizate pe *serverele* (sistemele informatice) din SUA, dar a refuzat să predea și *e-mailurile*, invocând necompetența teritorială în emiterea unui mandat de percheziție informatică pentru informațiile stocate în străinătate.

[23] A. Orlowski, *Microsoft wins landmark Irish data slurp warrant case against the US*, disponibil online la adresa http://www.theregister.co.uk/2016/07/14/microsoft_wins_landmark_irish_warrant_case_against_usa/.

[24] S. Ahmed, *Cloud Computing: Aspecte legate de contractare și comformitate pentru departamentele juridice interne*, în „Revista română de drept al afacerilor", nr. 2/2014, p. 105-106.

[25] *Ibidem*.

faptul dacă și în ce măsură instanța poate să oblige producătorii să asiste la deblocarea telefoanelor mobile ale căror date sunt protejate prin criptare. În 2015 și 2016, Apple a atacat cel puțin 11 hotărâri provenite de la instanțe din SUA prin care compania era obligată să producă un astfel de software. În una dintre situații, FBI dorea deblocarea Iphon-ului recuperat de la unul dintre participanții la un atac terorist din decembrie 2015 din San Bernardino, California, în care au fost omorâte 14 persoane iar 22 de persoane au fost rănite. Cei doi atacatori au fost uciși de către polițiști, dar nu înainte ca infractorii să își distrugă telefoanele personale. Un telefon de serviciu a fost recuperat dar era blocat cu o cheie de acces, iar la introducerea unui număr de 10 parole greșite, telefonul era programat să șteargă toate informațiile. Apple a refuzat să creeze software-ul. Cu toate acestea, FBI au anunțat găsirea unei terțe părți aptă să asiste la deblocarea Iphon-ului. Prin urmare, FBI au renunțat la dreptul de a obliga compania Apple la crearea software-ului și au anunțat că au deblocat telefonul mobil. Au existat și hotărâri ale instanței în sens contrar, de exemplu, într-o speță, în Brooklyn, un judecător a decis că Apple nu poate fi obligat să deblocheze Iphon-ul. Hotărârea a fost atacată, dar apoi s-a renunțat la calea de atac în considerarea faptului că, în cele din urmă, a fost obținută cheia de acces corectă.

Criptarea datelor informatice poate fi considerată echivalentă lipsei acelor date informatice atât timp cât nu a fost utilizată cheia pentru decriptarea datelor, de aici rezultând miza uriașă a obținerii unei hotărâri care să oblige compania Apple la crearea unui software special în vederea deblocării telefonului și a decriptării datelor. În general, alternativă obligării utilizatorului să furnizeze o cheie de decriptare se anunță a fi mult mai problematică. Obligarea la decriptare a datelor informatice trebuie văzută ca un proces de creare a datelor incriminatorii, deoarece informațiile criptate nu pot folosi ca probe în acuzare din moment ce acestea nu pot fi supuse procesului de interpretare. Singura care conduce la dobândirea valențelor probatorii a datelor informatice este decriptarea acestora (transformarea conținutului ilizibil într-un conținut lizibil). Remiterea de către utilizator a conținutului necriptat presupune două constante: o declarație a apartenenței conținutului și o recunoaștere a faptului că acesta este criptat, confirmând astfel controlul, posesia și autenticitatea.

Prin urmare, valoarea actului de remitere este una testimonială. Un alt inconvenient rezultat din solicitarea decriptării de către utilizator a datelor informatice este acela potrivit căruia informațiile criptate pot prezenta un conținut care să nu fie relevant în cauză, situație în care utilizatorul este pus să selecteze informațiile relevante. Acțiunea de selectare va avea o valoare testimonială prin faptul că se recunoaște astfel puterea probantă a anumitor informații stocate în sistemul informatic.[26]

Utilizarea criptografiei nu poate fi percepută ca o acțiune care dovedește existența unei activități infracționale. Criptarea trebuie văzută ca o formă de protecție a datelor informatice. Faptul că aceasta poate fi utilizată și cu intenția de a ascunde probe digitale ale săvârșirii unei infracțiuni nu este decât o excepție, care nu poate suprima prezumția de nevinovăție de care trebuie să beneficieze suspectul sau inculpatul.[27] Procesul de criptate sau decriptare se realizează prin intermediul unei chei (key), precum este parola, memory stick-ul, urma papilară ori vocea utilizatorului. Este necesar a se face distincția între noțiunea de parolă, reprezentată de un șir de caractere și cea de cheie pentru decriptare, aceasta din urmă fiind o noțiune mai complexă care include chiar și vocea utilizatorului ori elemente tangibile precum este urma papilară.[28] Cheia de criptare are inclusiv rolul de a modifica, prin utilizarea ei, conținutul datelor informatice, iar nu doar de a permite accesul la acestea, așa cum se întâmplă în cazul parolei. În cazul transmiterii cheii, indiferent de modul în care se realizează, pe cale orală sau în scris, fiecare dintre aceste ipoteze poate determina activarea privilegiul contra autoincriminării.[29]

Dezvoltarea tehnologiei aduce cu sine necesitatea adaptării metodelor de combatere a fenomenului infracțional. Apariția telefoanelor mobile pentru deblocarea cărora se solicită amprenta utilizatorului constituie o nouă provocare cu care se confruntă organele judiciare. Lansarea de către compania Apple a telefonului care permite recunoașterea amprentei a fost considerat un salt în materie de securitate. Sistemul s-a dovedit sigur, amprentele scanate erau stocate, criptate și procesate local, fără a fi trimise companiei Apple pentru verificări, dar cu toate acestea, sistemul a creat motiv de îngrijorare pentru anumiți experți. Se punea problema modului

[26] G. Zlati, *Privilegiul contra autoincriminării și criptografia*, „Penalmente Relevant", nr. 1/2006, disponibil online (*http://www.revista.penalmente.ro/nr1-2016/autoincriminare-criptografie*), p. 46-47.

[27] *Idem*, p. 22.

[28] *Idem*, p. 24.

[29] *Idem,* p. 42-43.

în care telefonul securizat cu amprentă urma să fie manipulat în instanță. Confruntat cu o astfel de problemă, în 2014, un judecător din Virginia a hotărât că poliția poate să folosească forța pentru a debloca smartphonul cu ajutorul amprentei. De asemenea, un judecător din Los Angeles a emis un mandat de percheziție informatică, impunând posesoarei telefonului mobil folosirea amprentei pentru deblocarea telefonului, deși nu era clar scopul căutării. Telefonul aparținea unei femei de 29 de ani, prietena unui bărbat acuzat de apartenența la un grup infracțional. Autoritățile competente din Los Angeles au fost nevoite să acționeze de urgență în emiterea și executarea mandatului deoarece nedeblocarea dispozitivului într-un interval mai mare de 48 de ore conducea la imposibilitatea folosirii amprentei, solicitându-se codul de acces. Hotărârea instanței a fost fundamentată pe rațiunea că amprentele, precum și ADN-ul sau scrisul, sunt acceptate, nedezvăluind ceva ce se află în mintea suspectului ori a inculpatului.

Metoda prin care utilizatorul telefonului ar fi putut să evite această situație ar fi fost închiderea dispozitivului, astfel încât la deschiderea telefonului să fie necesară introducerea codului PIN sau a unei chei de acces.[30] Astfel cum se consideră în literatura de specialitate, există situații în care folosirea urmei papilare drept cheie în vederea decriptării datelor informatice determină aplicabilitatea privilegiului contra autoincriminării. În situația în care organele de urmărire penală nu cunosc modalitatea decriptării datelor, utilizatorul nu poate fi constrâns să coopereze.

Consimțământul utilizatorului nu va fi însă necesar în măsura în care organele de urmărire penală cunosc faptul că datele informatice pot fi decriptate prin folosirea urmei papilare. În cel din urmă caz, cooperarea este considerată a fi pasivă și nu va face obiectul privilegiului contra autoincriminării. Soluția este identică și cu privire la utilizarea ADN-ului ori a scanării retinei ori a irisului în scopul decriptării datelor informatice.[31] Decriptarea prin intermediul vocii utilizatorului implică rostirea unui anumit cuvânt sau fraze, fiind importantă nu doar identificarea caracteristicilor vocii utilizatorului ci și a conținutului care urmează a fi folosit.

Rezultă astfel existența unei componente testimoniale care va fi acoperită de privilegiul contra autoincriminării.[32] În situația în care prezintă relevanță numai caracteristicile vocii, atunci privilegiului contra autoincriminării nu poate fi invocat. Prin urmare, decriptarea datelor informatice incriminatorii prin folosirea vocii utilizatorului implică, de principiu, o recunoaștere a criptării datelor și a apartenenței acestora.[33]

III. DISPUNEREA PERCHEZIȚIEI INFORMATICE

Conform prevederilor art. 168 alin. (2) C.proc.pen., coroborate cu cele ale alin. (16) din același articol, percheziția informatică se dispune, la cererea procurorului, de către judecătorul de drepturi și libertăți, în cursul urmăririi penale sau de către instanță, la cererea procurorului, a părților, a persoanei vătămate sau din oficiu, în cursul judecății. Percheziția informatică se dispune atunci când „pentru descoperirea și strângerea probelor este necesară cercetarea unui sistem informatic sau a unui suport de stocare a datelor informatice", așa cum rezultă din teza finală a alin. (2), precum și din prevederile alin. (16). O asemenea cerință este insuficientă luând în considerare caracterul percheziției de a restrânge drepturi și libertăți fundamentale, dintre care dreptul la viața privată garantat de art. 8 din Convenția Europeană a Drepturilor Omului.

Convenția prevede în art. 8 parag. (1) faptul că „orice persoană are dreptul la respectarea vieții sale private și de familie, a domiciliului său și a corespondenței sale", în parag. 2 dispunându-se că „nu este admis amestecul autorității publice decât în măsura în care acest amestec este prevăzut de lege și dacă constituie o măsură care, într-o societate democratică, este necesară securității naționale, siguranței publice, bunăstării economice a țării, apărării ordinii și prevenirii faptelor penale, protecției sănătății sau a moralei, ori protecției drepturilor și libertăților altuia". Din cuprinsul acestor reglementări rezultă că inviolabilitatea domiciliului și a corespondenței sunt concepte în strânsă legătură cu respectul vieții intime și de familie.[34]

În literatura de specialitate s-a considerat că măsura percheziției domiciliare trebuie aplicată restrictiv, în cazuri excepționale, cu respectarea condițiilor de a fi vorba despre comiterea unei infracțiuni; de a fi începută

[30] K. Waddell, *Police Can Force You to Use Your Fingerprint to Unlock Your PhoneBut they can't make you cough up your passcode*, disponibil online la adresa http://www.theatlantic.com/technology/archive/2016/05/iphone-fingerprint-search-warrant/480861/.

[31] G. Zlati, *Privilegiul contra autoincriminării și criptografia*, *cit. supra.*, p.45.

[32] *Idem*, p. 36.

[33] *Idem,* p. 47.

[34] G. Mateuț, *Tratat de procedură penală, Partea generală*, vol. I, C.H. Beck, București, 2007, p. 244.

urmărirea penală pentru acea infracțiune; de a exista, cu privire la persoanele învinuite, elemente serioase de vinovăție, iar nu numai simple bănuieli; iar efectuarea percheziției să fie dictată de puternice prezumții că pe această cale se vor descoperi probe în sarcina învinuitului.[35] Având în vedere gradul ridicat de ingerință în viața privată a utilizatorului sistemului informatic ori a posesorului mijlocului de stocare, ar fi oportun ca și în dispunerea percheziției informatice să fie verificată îndeplinirea acestor condiții.

Percheziția informatică se va dispune doar atunci când măsura este necesară și proporțională cu scopul urmărit.[36] Totodată, nu este suficient ca legea să prevadă o ingerință în exercițiul unui drept, ci ea trebuie fie accesibilă tuturor, adică să fie publică, și să fie previzibilă, suficient de precisă pentru a permite individului să acționeze în conformitate cu prevederile ei. Prin urmare, legea trebuie să definească întinderea și modalitățile de exercitare a funcțiilor autorităților publice competente în materie cu suficientă claritate pentru a proteja individul împotriva arbitrariului[37] (cauza Rotaru c. României).

IV. CARACTERUL URGENT ȘI RESPECTAREA GARANȚIILOR

1. Constatarea tehnico-științifică

Percheziția sistemului informatic sau a suportului de stocare a datelor informatice reprezintă, astfel cum se prevede în art. 168 alin. (1) C.proc.pen., procedeul de cercetare, descoperire, identificare și strângere a probelor stocate într-un sistem informatic sau suport de stocare a datelor informatice. Percheziția se realizează prin intermediul unor mijloace tehnice și proceduri adecvate care să asigure integritatea informațiilor conținute.

În doctrină a fost evidențiat faptul că referirea în cadrul normelor de incriminare atât la sistemul informatic cât și la mijlocul de stocare a datelor informatice este lipsită de utilitate practică din moment ce datele informatice pot fi stocate doar pe un mijloc (suport) de stocare a datelor informatice. Mijlocul de stocare poate avea o existență autonomă față de orice alt sistem informatic, exemple în acest sens pot fi memory stick-ul ori hard drive-ul extern, sau poate reprezenta o parte integrantă a sistemului informatic, precum este hard drive-ul unui laptop. Esențial este faptul că percheziția informatică nu se poate efectua asupra unui sistem informatic căruia îi lipsește suportul de stocare. Prin urmare, s-a concluzionat că percheziția informatică se realizează asupra mijloacelor de stocare a datelor informatice, ca parte intergrantă ori independentă de un sistem informatic.[38]

Percheziția informatică diferă de o constatare tehnico-științifică, acesta din urmă reprezentând mijlocul prin care se folosesc, în faza de urmărire a procesului penal, cunoștințele unui specialist sau tehnician, pentru lămurirea urgentă a unor fapte sau împrejurări care necesită cunoștințe de specialitate. Prin urmare, privind aspecte diferite, obiectul percheziției informatice nu poate face obiectul unei constatări tehnico-științifice.

Dacă percheziția informatică vizează cercetarea, identificarea și strângerea de probe, constatarea tehnico-științifică are ca obiect lămurirea unor fapte sau împrejurări care necesită cunoștințe de specialitate. Astfel, redactarea unui raport de constatare tehnico-științifică în care să se consemneze realizarea unor activități specifice percheziției informatice trebuie să ducă la recalificarea acestuia ca fiind un veritabil proces-verbal de percheziție informatică și întreaga activitate trebuie să respecte prevederile art. 168 C.proc.pen. Caracterul urgent al activităților preconizate nu poate justifica efectuarea unei constatări tehnico-științifice, deoarece percheziția informatică propriu-zisă poate fi efectuată imediat după finalizarea copiei, fiind întocmit în acest sens un singur proces-verbal. Se poate imagina, prin excepție, situația în care activitățile componente ale percheziției informatice au loc în zile diferite, caz în care se vor încheia procese-verbale diferite, atunci când sunt percheziționate mai multe mijloace de stocare și se decide să se efectueze mai întâi copiile după fiecare mijloc de stocare în parte, după care, la o dată ulterioară, să fie efectuată percheziția în legătură cu fiecare copie în parte. În practica judiciară se întâlnește și ipoteza în care percheziția informatică propriu-zisă asupra copiei efectuate devine obiect al unei constatări tehnico-științifice. O asemenea abordare poate permite eludarea prevederilor legale ce instituie anumite garanții procedurale în contextul efectuării unei percheziții

[35] A se vedea I. Tanoviceanu, V. Dongoroz, *Tratat de drept și procedură penală*, vol. IV, ediținea a doua, Ed. Curierul Judiciar, București, 1927, p. 618.

[36] A. C. Moise, *Metodologia investigării criminalistice a infracțiunilor informatice*, Ed. Universul Juridic, București, 2011, p. 205.

[37] G. Mateuț, *Tratat de procedură penală, Partea generală, cit. supra.*, p. 245.

[38] M. Udroiu, G. Zlati, Comentariu în M. Udroiu (coord.), *Codul de procedură penală. Comentariu pe articole,* ediția a II-a, C.H.Beck, București, 2017, p. 831.

informatice, fiind nelegală.[39] Prin urmare, activitățile specifice unei percheziții informatice nu pot fi efectuate cu ajutorul constatărilor tehnico-științifice, dar, cu toate acestea, constatările tehnico-științifice pot fi utilizate pentru analiza datelor obținute în urma unei percheziții informatice. Cu ajutorul constatării tehnico-științifice se poate, de exemplu, stabili în ce măsură datele informatice au fost criptate, având în vedere faptul că prin operațiunea de criptare se obține nu doar securizare datelor digitale, ci se poate ajunge chiar la ipoteza în care procesul de criptare nu poate fi observat de către organele de urmărire penală deoarece datele vor lua forma unor secvențe aleatorii de biți.[40]

Prin invocarea unui caracter urgent al lucrării, procurorul va avea întotdeauna posibilitatea de a solicita specialistului sau lucrătorului de poliție specializat, realizarea unei constatări tehnico-științifice. În consecință, garanțiile regăsite în cadrul art. 168 C.proc.pen. ar cădea în desuetudine din moment ce este de necontestat faptul că la efectuarea constatării tehnico-științifice este exclusă prezența părților. Acestă abordare nu poate fi conformă cu prevederile art. 8 din Convenție. Ingerința în viața privată este posibilă doar în măsura în care există cadru normativ clar și care să ofere suficiente garanții procesuale pentru prevenirea unor abuzuri, de aceea percheziția informatică nu poate fi efectuată în lipsa unui mandat de percheziție informatică în cuprinsul căruia să se statueze în mod expres limitele ce se impun a fi respectate. În România, aceste garanții sunt cele prevăzute de art. 168 CPP.[41]

În acest sens este și hotărârea Ct.E.D.O. în cauza Smirnov c. Rusia[42]. Starea de fapt este plasată în anul 1999, când, deschisă fiind urmărirea penală împotriva domnului Sh, domnului G și împotriva a 15 alte persoane care erau suspectate de organizarea și participarea la un grup infracțional și de săvârșirea altor infracțiuni grave, a fost emis un mandat de percheziție informatică. În fața instanței naționale, Smirnov, avocat în cauză, supus fiind percheziției informatice, a arătat că datele digitale cu privire la clienți, în mod special, cele stocate în unitatea centrală a computerului și în notebook, nu conțineau informații relevante în cauză, astfel încât nu puteau fi folosite ca probe digitale. Mai mult căutările interferează și cu drepturile altor clienți pe care acesta îi apără. Instanța a obligat în cele din urmă înapoierea documentelor reclamantului, a unității centrale și a notebook-ului. Computerul nu a fost însă înapoiat. Cu toate acestea, calea de atac declanșată de avocat a fost respinsă, considerându-se că percheziția a fost efectuată în mod legal și că absența unui mandat anterior emis de un judecător este suplinită de posibilitatea efectuării unui control post factum.

Curtea observă că reclamantul nu era suspectat de nicio infracțiune, și se arată îngrijorată de faptul că la dispunerea percheziției apartamentului nu au existat garanții privind respectarea secretului profesional. Mandatul de efectuare a percheziției a fost exprimat în termeni foarte largi: orice documente sau obiecte care prezintă relevanță în cauză. Controlul post factum nu a suplinit aceste lacune. Curtea a concluzionat că efectuarea percheziției fără a exista suficiente motive și fără a exista garanții cu privire la protejarea secretului profesional poate avea consecințe negative în privința înfăptuirii justiției și, prin urmare, încalcă dreptul garantat de art. 6 din Convenție. De asemenea, s-a constatat încălcarea art. 8 din Convenție întrucât măsura nu era necesară într-o societate democratică cu atât mai mult cu cât reclamantul nu era suspectat de comiterea niciunei infracțiuni, ci reprezenta inculpații în același caz în care s-a dispus percheziția.

În practică, ignorându-se gradul mare de ingerință a activităților specifice percheziției informatice, au existat și soluții în care s-a arătat că nu este necesară existența unui mandat pentru efectuarea percheziței informatice întrucât utilizatorul nu poate avea o așteptare rezonabilă la intimitate în situația folosirii sistemului informatic. Una dintre aceste hotărâri este pronunțată în cauza SUA v. Edward Joseph Matish III[43], de către judecătorul Henry Coke Morgan, care consideră că FBI poate să acceseze sistemul informatic în lipsa unui mandat de percheziție informatică și chiar fără să existe suspiciuni rezonabile cu privire la săvârșirea unei infracțiuni. Hotărârea privește Operațiunea Pacifier – vizând site-urile de pornografia infantilă în cadrul rețelelor anonime precum Tor[44]. FBI a implementat instrumente de hacking în computere din SUA, Chile,

[39] G. Zlati, *Percheziția sistemelor informatice și a mijloacelor de stocare a datelor informatice (II), cit. supra.*, p. 88.

[40] M. Udroiu, G. Zlati, Comentariu în M. Udroiu (coord.), *op. cit.,* p. 832.

[41] G. Zlati, *Percheziția sistemelor informatice și a mijloacelor de stocare a datelor informatice (II), cit. supra.*, p. 89.

[42] *Hotărârea din 12.11. 2007 (cerearea nr 71362/01).*

[43] *Hotărârea din 7.1.2016 (cauza nr. 4:16cr16*), hotărâre disponibilă online *(https://www.documentcloud.org/documents/2896909-Opinion-and-Order-in-Matish.html*).

[44] Tor (acronim de la The Onion Router) este un software liber ce permite păstrarea anonimității pe internet printr-un algoritm

Danemarca și Grecia și a identificat 1500 de pedofili în cadrul Dark Net. Judecătorul Morgan consideră că acțiunile FBI nu au încălcat drepturile cetățenilor SUA care îi protejează pe aceștia împotriva căutărilor nelegale, întrucât nu era nevoie de un mandat de percheziție pentru a se obține adresa IP a suspectului ori a inculpatului sau alte date stocate în sistemul informatic al acestuia. Judecătorul consideră că, în general, nu se poate vorbi despre o așteptare rezonabilă de a avea intimitate în momentul folosirii internetului. Chiar și un utilizator al rețelei Tor, care încercă mascarea adresei IP nu se poate aștepta în mod rezonabil la intimitate în privința adresei IP.

În principiu, judecătorul apreciază că sistemele sunt supuse acțiunii hackerilor în fiecare zi, astfel încât nimeni nu ar trebui să spere la intimitate în timpul operării online. În concluzie, judecătorul reține că numărul în creștere a sistemelor informatice accesate de către hackeri, prin intermediul internetului, a schimbat opinia societății cu privire la așteptarea rezonabilă la intimitate a utilizatorului, în prezent fiind nerezonabil a se considera că un computer conectat la internet este imun atacurilor.[45]

2. Utilizatorul sistemului informatic reținut ori arestat

Pretextul urgenței a fost invocat de organele de urmărire penală și în contextul realizării căutărilor în telefonul mobil cu prilejul arestării ori a reținerii utilizatorului. Susținerea organelor judiciare potrivit căreia, în cazul telefonului mobil, utilizatorul are opțiunea de a reveni la setările din fabrică și că astfel se vor pierde toate probele digitale anterior obținerii unui mandat de percheziție informatică, este lipsită de acuratețe întrucât niciun procedeu de ștergere a datelor nu lasă telefonul mobil liber de orice informații reziduale, ca și când ar fi fost nou. Recuperarea datelor digitale rămâne posibilă, dar operațiunea presupune folosirea de instrumente mai complexe pentru realizarea percheziției. Mai mult, organele de urmărire penală pot preveni ștergerea datelor, de exemplu, prin îndepărtarea bateriei, întrucât, pentru ștergerea datelor, este necesar ca telefonul sa fie pornit. De asemenea, dispozitivele Faraday împiedică ajungerea semnalului la telefon, astfel încât o ștergere de la distanță a datelor nu este posibilă.[46] În prezent, în multe cazuri, datele digitale sunt stocate în mai multe locații, iar ștergerea acestora din telefonul mobil nu echivalează cu distrugerea probelor digitale.

Problema obținerii unui mandat de percheziție informatică se pune nu numai în privința telefoanelor inteligente. Astfel cum a fost evidențiat în doctrină, inclusiv analiza unei cartele SIM prin utilizarea unui dispozitiv de citire specific reprezintă o activitate de percheziție informatică asupra unui mijloc de stocare a datelor informatice.[47]

În cauza Chimel v. California[48] s-a arătat că, pentru a fi permisă căutarea în telefonul mobil în momentul arestării ori reținerii, organul de urmărire penală trebuie să verifice dacă este rezonabilă bănuiala că vor fi găsite probe digitale în legătură cu infracțiunea pentru care utilizatorul este arestat ori reținut. De exemplu, în situația în care există suspiciunea rezonabilă că în agenda telefonului vor fi găsite date de contact ale participanților la săvârșirea infracțiunii, căutările se vor limita la verificarea jurnalului de apeluri și a listei de contact. O eventuală căutare a fotografiilor stocate este, însă, inacceptabilă.[49]

În cauza US v. Robinson[50], organul de urmărire penală, realizând percheziția corporală a arestatului a simțit în buzunarul acestuia un obiect, despre care nu se putea spune cu exactitate ce reprezintă. Organul de urmărire penală a identificat obiectul ca fiind un pachet de țigări, dar care nu conținea țigări ci heroină. Curtea a reținut că proba cu heroină este admisibilă pentru că organul judiciar avea puterea de a investiga obiectele

---

de rutare din aproape-în-aproape. În rețeaua Tor, traficul online generat este anonim, fără a se înregistra lista de termeni căutați și fără a ține o evidență a IP-urilor de unde au fost inițializate respectivele căutări. Activitatea utilizatorilor Tor nu poate fi depistată din cauza unui sistem special care ricoșează semnalele între diferite adrese ip. De asemenea, Tor permite prin acest mecanism accesul la site-uri ce sunt filtrate de serverele proxy instalate în rețea. Tor este și un browser (The Tor browser), o poartă de acces spre *darknet* (internetul întunecat)..

[45] J. Conditt, *Judge says the FBI can hack your computer without a warrant*, disponibil online la adresa (*https://www.engadget.com/2016/06/24/fbi-no-warrant-hack-computer/).*

[46] S.M. Corradi, *Be Reasonable! Limit Warrantless Smart Phone Searches to Gant's Justification for Searches Incident to Arrest, cit. supra.,* p.960.

[47] M. Udroiu, G. Zlati, Comentariu în M. Udroiu (coord.), *op. cit.,* p. 834.

[48] Hotărârea din 23.06.1969 (nr. 770).

[49] S.M. Corradi*, Be Reasonable! Limit Warrantless Smart Phone Searches to Gant's Justification for Searches Incident to Arrest, cit. supra.,* p. 962-963.

[50] Hotărârea 11.12.1973 (nr. 72-936).

activității de contrabandă. Astfel, sub jurisprudența Robinson, organul de urmărire penală nu mai trebuie să dovedească existența unei suspiciuni rezonabile de a nu fi ascunsă o armă sau de a nu fi distruse probe pentru realizarea unei căutări.[51] Prin urmare, în cauza US v. Robinson, Curtea a extins regula din cauza Chimel, reținând că organele de urmărire penală pot să efectueze căutări în cutiile închise deținute de o persoană sau în cutiile care se află în sfera controlului acesteia, ca și căutări valabile incidente arestului.[52] Prinde astfel formă teoria containerelor și a minicontainerelor, în considerarea căreia datele informatice sunt văzute ca și containere, iar fiecare minicontainer corespunde unui folder, fișier etc.[53] Teoria nu este unanim acceptată, astfel că în cauza US v. Chadwick[54], căutările cu privire la o cutie închisă cu cheia s-au constatat a fi nelegale, întrucât cutia nu reprezenta un pericol pentru organele de urmărire penală, iar faptul că aceasta era încuiată demonstra intenția posesorului de a păstra conținutul privat.[55]

Cauza Riley v. California, este o speță ulterioară în care judecătorii de la instanțele inferioare au ales să ia în considerare probele obținute în urma unei căutări în telefonul mobil al inculpatului, arestat în cauză, fără a exista un mandat de percheziție informatică. Spre deosebire de judecătorii de la instanțele inferioare, în unanimitate, Curtea Supremă a ajuns la concluzia conform căreia organul de urmărire penală trebuie să dețină un mandat de percheziție informatică pentru a realiza căutări în telefoanele mobile ale persoanele pe care le arestează. Prin urmare, Curtea Supremă înțelege că tehnologia și intimitatea sunt două fațete ale aceleași monede.[56] În speță, David Leon Riley aparținea unei grupări din San Diego, California. În 2 august 2009, el împreună cu alte persoane, au deschis focul împotriva membrilor unei grupări rivale, după care au fugit de la locul faptei. În 22 august 2009, Riley a fost oprit de poliție în timp ce conducea un automobil, având permisul de conducere suspendat, ocazie cu care poliția a găsit două arme aflate în posesia acestuia. În urma arestării lui Riley pentru posesie de arme de foc, telefonul mobil a fost accesat de către organul de urmărire penală, iar din fotografiile și videoclipurile descoperite, s-a constatat legătura acestuia cu gruparea din San Diego. Apare astfel întrebarea dacă descoperirea acestor probe apare ca urmare a unei percheziții informatice efectuate în afara legii. Curtea a reținut că se pot efectua căutări fără a exista un mandat de percheziție numai în acele cazuri urgente în care interesele statului sunt atât de mari încât percheziția ar fi rezonabilă.[57] Prin urmare, informația stocată în telefonul mobil este protejată de dreptul la viață privată, astfel încât organul de urmărire penală nu poate efectua căutări în telefonul arestatului, în lipsa unor circumstanțe deosebite.[58] În cauza Smallwood, Curtea Supremă din Florida[59] a avut, de asemenea, în vedere faptul că dispozitivele electronice au o capacitate imensă de stocare. S-a considerat, astfel, că în contextul dezvoltării tehnologice din prezent, protejarea datelor stocate în sistemele informatice este la fel de importantă ca și protejarea domiciliului.[60] New York v. Belton[61] este o altă cauză în care Curtea a arătat că, prin natura sa, telefonul necesită un nivel crescut de protecție. Căutarea în telefon, în lipsa unui mandat de percheziție informatică, nu asigură protecția datelor informatice împotriva unei distrugeri și nici nu contribuie la siguranța organului de urmărire penală.[62] Astfel cum au concluzionat Curtea Supremă din Ohio sau Curtea Supremă din Statele Unite, percheziția informatică a telefoanelor inteligente trebuie efectuată cu respectarea vieții private a utilizatorului și, prin urmare, cu respectarea anumitor garanții, printre care și existența unui mandat de percheziție informatică. În concluzie, a fost avut în vedere faptul că datele informatice nu pot fi distruse dacă sunt luate anumite măsuri

[51] L. Aaronson, *Constitutional Restraints on Warrantless Cell Phone Searches,* în „University of Miami Law Review", vol. 69, 2014, p. 903.

[52] S.M. Corradi, *Be Reasonable! Limit Warrantless Smart Phone Searches to Gant's Justification for Searches Incident to Arrest, cit. supra.,* p. 946.

[53] J. Goldfoot, *The Physical Computer and the Fourth Amendment*, „Berkeley Journal of Criminal Law", vol. 16, nr. 1, 2011, p. 112-123.

[54] Hotărârea din 21.06.1977 (nr. 75-1721).

[55] L. Aasronson, *Constitutional Restraints on Warrantless Cell Phone Searches*, *cit. supra.,* p. 905.

[56] B. Clausen, *Home computers aren't private: Virginia judge rules against Fourth Amendament,* disponibil online la adresa *http://www.dopplr.com/home-computers-arent-private/*.

[57] *Hotărârea din 25.06.2014, Riley v. California*, disponibilă online la adresa https://www.oyez.org/cases/2013/13-132.

[58] L. Aaronson, *Constitutional Restraints on Warrantless Cell Phone Searches*, *cit. supra.,* p. 900.

[59] Hotărârea din 2.05.2013 (SC11–1130).

[60] L. Aaronson, *Constitutional Restraints on Warrantless Cell Phone Searches*, *cit. supra.,* p. 913.

[61] Hotărârea din 1.07.1981 (nr. 80-328).

[62] L. Aaronson, *Constitutional Restraints on Warrantless Cell Phone Searches*, *cit. supra.,* p. 915.

de siguranță precum introducerea telefonului într-o pungă Faraday, până în momentul obținerii mandatului, și că este imposibil de comparat un telefon mobil, care are o capacitate imensă de stocare, cu o cutie de țigări, spre exemplu. Astfel, percheziția informatică a telefonului mobil nu poate fi justificată nici măcar de urgența incidentă în contextul unei arestări.[63] În cauza US v. Park[64], de asemenea, curtea a arătat că un telefon este asemănător unui laptop, mai degrabă decât unei agende, datorită capacității telefonului de a stoca o cantitate imensă de informații. Prin urmare, percheziția informatică poate fi efectuată doar în considerarea unui mandat de percheziție informatică anterior emis, având în vedere calitatea și cantitatea informațiilor care pot fi stocate pe un sistem informatic ori pe mijlocul de stocare a datelor informatice.[65]

3. Verificări la frontiere

Efortul de a stabili garanții prin care să fie protejată viața privată a utilizatorilor sistemelor informatice ori a posesorilor mijloacelor de stocare a datelor digitale și a conținutului informatic este minimalizat prin existența anumitor reglementări care conferă agenților de la frontieră puteri mult mai largi decât cele recunoscute, în mod obișnuit, organelor de urmărire penală care funcționează pe teritoriul statului. Astfel, o simplă deplasare în străinătate, activitate comună în prezent, poate să anuleze majoritatea acestor garanții. Obligația de a transmite cheia de acces, lipsa prezenței utilizatorului la efectuarea căutărilor, lipsa obligației de a fi încheiat un proces-verbal cu privire la activitățile efectuate asupra sistemului informatic sau a mijlocului de stocare ori realizarea percheziției informatice în lipsa unor suspiciuni rezonabile, sunt doar câteva exemple care transformă aceast procedeu probatoriu, într-o activitate care nu va fi îngrădită de respectarea garanțiilor, nici măcar a secretului profesional, atunci când aceasta se desfășoară la granița dintre state.[66] Un exemplu în acest sens este cazul unui inginer NASA, Bikkannavar, născut în SUA, care a fost reținut pe aeroportul din Huston, fiind obligat să transmită agenților statului cheia de acces a sistemul informatic destinat serviciului, aflat în posesia sa. Percheziția informatică a dispozitivului a fost efectuată în lipsa utilizatorului, și în lipsa unor suspiciuni rezonabile cu privire la săvârșirea unei infracțiuni. Sistemul informatic era în proprietatea laboratorului unde inginerul își defășura activitatea profesională, codul întipărit pe spatele telefonului atestând acest fapt. Prin urmare, obligația lui Bikkannavar era de a proteja conținutul sensibil al dispozitivului, fiind interzisă orice transmitere a cheii de acces. Agentul a înmânat inginerului un document intitulat „Inspecția dispozitivelor electronice", document în care erau prevăzute și sancțiunile la care se expune cel care refuză să coopereze. Astfel, furnizarea informațiilor este obligatorie, iar necooperarea conduce la detenție și/sau la percheziția dispozitivului electronic în discuție. Inginerul a luat în considerarea posiblitatea ca în urma căutărilor să fi fost realizată o copie a datelor informatice stocate, astfel a considerat că are obligația de a merge direct la locul de muncă, spre a raporta cele întâmplate. Percheziția sistemului informatic a constituit o încălcare a secretului profesional. Preluarea controlului mediului informatic a permis accesul agenților atât la informații de natură profesională cât și de natură personală, utilizatorul fiind conectat la ambele conturi. Prin urmare, este incert ce s-a întâmplat cu telefonul inginerului cât timp el s-a aflat în camera de așteptare. Nu este sigur nici dacă informațiile existente în sistemul informatic au fost păstrate sau șterse, în ipoteza în care a fost realizată o copie după aceste date digitale. Cert este că agenții aveau obligația ca, după verificarea informațiilor digitale stocate pe sistemul informatic, să nu păstreze nicio copie a datelor informatice în cazul în care nu există o suspiciune rezonabilă a săvârșirii unei infracțiuni.[67]

În lipsa protecției legale, utilizatorul sistemului informatic trebuie să fie extrem de precaut atunci când călătorește într-un alt stat. Una dintre măsurile de precauție poate fi achiziționarea unui nou dispozitiv care să fie folosit doar cu ocazia călătoriilor în străinătate și lăsarea tuturor celorlalte dispozitive la domiciliu. Noul sistem informatic nu va conține, prin urmare, niciun fel de informații personale cu privire la care agenții să efectueze căutări. O altă măsură este utilizarea unei chei de acces. Este exclusă însă blocare dispozitivului prin

[63] *Idem,* p. 923-924.

[64] Hotărârea din 9.06.1975 (nr. 74-215).

[65] S.M. Corradi, *Be Reasonable! Limit Warrantless Smart Phone Searches to Gant's Justification for Searches Incident to Arrest, cit. supra.*, p. 949-950.

[66] P. G. Lee, *Can US Customs and Border officials search your phone?*, TED-Ed Blog, disponibil online la adresa *http://blog.ed.ted.com/2017/03/14/can-us-customs-and-border-officials-search-your-phone-these-are-your-rights/*.

[67] K. Waddell, *A NASA Engineer Was Required to Unlock His Phone at the Border,* disponibil online la adresa *https://www.theatlantic.com/technology/archive/2017/02/a-nasa-engineer-is-required-to-unlock-his-phone-at-the-border/516489/*.

folosirea amprentei, din moment ce există deja practica obligării utilizatorului la cooperare în scopul deblocării sistemului informatic în acest caz. Rămâne însă întrebarea ce se va întâmpla în situația în care cheia de acces este o parolă despre care utilizatorul dispozitivului afirmă că nu își amintește conținutul.[68]

Concluziile la care s-a ajuns pe care jurisprudențială, determinate în special de împrejurarea percheziţiilor informatice în momentul arestării ori a reținerii utilizatorului sistemului informatic ar trebui să își păstreze valabilitatea și în situația percheziţiilor informatice efectuate la frontieră, cu atât mai mult cu cât este nefiresc să fie tolerată percheziția în lipsa unor suspiciuni rezonabile de a fi stocate date care pot constitui probe ale săvârșirii unei infracțiuni. Prin urmare, căutările în lipsa existenței unui mandat de percheziție informatică trebuie să fie permise numai în situații excepționale, în acele cazuri urgente în care interesele statului sunt atât de mari încât percheziția informatică ar deveni rezonabilă (cauza Riley v. California).

V. CRITERII APLICABILE PERCHEZIŢIILOR INFORMATICE

În materia percheziție informatice, flexibitatea regulilor este extrem de importantă pentru ca acestea să corespundă progresului tehnologic. Este necesar ca instanța să țină cont de faptul că fiecare caz are particularitățile sale, iar o regulă general valabilă în acest domeniu nu poate funcționa.[69]

Percheziția informatică este o activitate diferită de oricare alt procedeu probatoriu, fiind nevoie de reguli specifice prin care să se țină cont de natura acesteia. Făcând o paralelă, se poate avea în vedere exemplul unui laborator în care se consemnează rezultatele testelor de droguri într-o carte tipărită. Pe o coloană este trecut numele persoanei, iar pe altă coloană se notează rezultatul testului, astfel încât cartea va cuprinde rezultatele a peste 100 de persoane. În cazul în care organul de urmărire penală obține mandatul de percheziție pentru investigarea a zece dintre aceste persoane suspectate de posesie de droguri, cartea reprezintă un mijloc de probă. Cartea se găsește păstrată într-un birou, astfel că organul de urmărire penală trebuie să obțină mandatul de percheziție domiciliară cu privire la respectivul spațiu. Cartea poate să conțină probe și cu privire la alte stări de fapt, dar care nu prezintă legătură cu mandatul de percheziție. Cu toate acestea, nu vor putea fi cercetate decât acele pagini care conțin probe ale săvârșirii infracțiunii cu privire la care a fost emis mandatul. În schimb, dacă presupunem că această carte ar fi de fapt un document Excel, organul de urmărire penală poate ori să copieze datele informatice, ori să cerceteze hard drive-ul sistemului informatic.[70]

Conform unei opinii separate în cauza US v. Comprehensive Drug Testing[71], care prezintă, într-o oarecare măsură situația descrisă mai sus, este esențial ca organul de urmărire penală să identifice doar acele zece coloane corespunzătoare persoanelor despre care se face mențiune în mandatul de percheziție informatică. Fiind date digitale, acestea pot fi supuse realizării unei copii (clone) informatice, în urma procesului de selecție a datelor conform criteriilor din mandat. Astfel, vor fi cercetate doar informațiile relevante în speță.[72]

Se recurge, prin urmare, la teoria containerelor și a minicontainerelor, caz în care conceptual se divide conținutul hard drive-ului, al telefonului ori al altui sistem informatic în mai multe minicontainere, iar pentru fiecare dintre acestea trebuie să existe o justificare indivuală pentru a fi examinate.

Dificultatea primară a conceptului containerelor și a minicontainerelor este aceea că nu toate probele digitale sunt găsite sub formă de fișiere. Așa cum, de exemplu, computerul sau laptopul conține câte un hard drive, el conţine și o memorie tip Random Access Memory (RAM) care stochează temporar date informatice. Astfel, la fel ca și hard drive-ul,și memoria RAM poate să fie supusă percheziției infromatice. Mai mult, adesea, memoria RAM stochează informații care nu sunt găsite și pe hard drive, dar aceasta nu este organizată în fișiere. Memoria RAM se șterge odată ce computerul sau laptopul a fost închis.[73]

Importanța fișierelor temporare este aceea că ele pot să arate dacă un anumit fișier a fost creat, deschis, modificat. De asemenea, în Windows, se regăsește o vastă configurație de date informatice, denumită „registru”,

---

[68] B. X. Chen, *Crossing the border? Here's how to safeguard your data from searches*, disponibil online la adresa *https://www.nytimes.com/2017/03/21/technology/personaltech/crossing-the-border-heres-how-to-safeguard-your-data-from-searches.html?smid=fb-nytimes&smtyp=cur&_r=0.*

[69] S. Trepel, *Digital searches, general warrants, and the case for the courts*, în „Yale Journal of Law & Technology”, vol. 10, 2007-2008, p. 143.

[70] J. Goldfoot, *op. cit.,* p. 114.

[71] Hotărârea din 24.01.2008 (nr. 05-55354, 05-10067, 05-15006).

[72] J. Goldfoot, *op. cit.,* p.116.

[73] *Idem*, p. 126.

extrem de valoroasă pentru organul de urmărire penală pentru că arată comenzile recente ale utilizatorului, fișierele recent deschise, site-urile web recent vizitate, utilizarea memoriilor USB, sau punctele de access Wi-Fi folosite.[74] Prin urmare, utilizatorul sistemului informatic poate fi identificat și localizat pe baza analizării fișierelor jurnal (log files) care conțin înregistrările unor acțiuni și evenimente, cum ar fi conectarea sau deconectarea de la rețeaua de internet. Analiza fișierelor jurnal va furniza date referitoare la cine s-a conectat de la un anumit computer, unde este localizat acesta, când s-a stabilit conexiunea și cât a durat.[75] În concluzie, percheziția informatică a unor astfel de date informatice iese de sub incidența conceptului containerelor și a minicontainerelor.

Acest concept prezintă și mai multe probleme în cazul în care lipsa existenței unor date informatice prezintă valoare probantă. Spre exemplu, inculpatul poate să afirme că este inocent pentru că infracțiunea a fost comisă de o altă persoană cu ajutorul unui virus. Astfel, absența virusului din sistemul informatic (hard drive) este acea probă negativă care infirmă povestea. La fel se întâmplă și atunci când E-mailul despre care infractorul vorbește, nu a fost găsit în sistem sau în mijlocul de stocare utilizat. Cu toate aceasta, pentru a dovedi că datele informatice nu se găsesc, este necesar a fi verificate datele informatice printre care s-ar putea regăsi și astfel să fie confirmată absența.[76] Prin urmare, și în această situație conceptul este lipsit de eficacitate.

Jurisprudența, în demersul său, a recurs și la o altă abordare, aceea a datelor aflate la vedere. Conform acesteia, un element se află la vedere dacă este observabil de către investigator, fără manipularea mediului din care provine informația (cauza Horton v. California, 1990). Astfel, conform acestei abordări, dacă urmare a unei percheziții informatice legale a unui sistem informatic ori a unui mijloc de stocare a datelor informatice, se descoperă probe ale săvârșirii unei alte infracțiuni, probele suplimentare sunt considerate a fi la vedere și obținute în mod legal. În schimb, dacă investigatorul este autorizat să percheziționeze numai anumite foldere, iar acesta depășește limitele conferite de mandat și accesează și alte date informatice, informațiile descoperite excedente mandatului nu sunt considerate a se afla la vedere, neputând fi folosite drept probe în procesul penal (cauza US v. Maxwell, 1996).[77]

În cauza SUA v. Tamura[78], Curtea a dezvoltat o procedură prin care să fie limitată intruziunea în viața privată a utilizatorului sistemului informatic în privința datelor care se află deja la dispoziția organelor de urmărie penală și care sunt sigilate. S-a arătat că încălcarea garanțiilor poate să fie evitată prin punerea la dispoziția judecătorului a datelor sigilate pentru a-și exprima acordul ori dezacordul cu privire la cercetarea acestora. Prin urmare, judecătorul decide dacă datele copiate au sau nu legătură cu scopul mandatului de percheziție informatică. Cu toate acestea, creșterea capacității sistemelor informatice de stocare a datelor și utilizarea frecventă a sistemelor informatice, ridică dificultăți în punerea în aplicare a acestei abordări.[79]

În cauza Carey v. US[80], organele de urmărire penală au început percheziția informatică efectuând căutări în fișierele text stocate în sistemul informatic, după anumite cuvinte cheie relevante pentru îndeplinirea scopului mandatului. Constatând că activitatea este lipsită de rezultate, s-a decis efectuarea căutărilor în afara limitelor mandatului, împrejurare în care a fost identificată o fotografie care conținea pornografie infantilă. Astfel, proba digitală dovedea săvârșirea unei alte infracțini decât cea în legătura cu care a fost emis mandatul. Prin urmare, în speță au fost copiate peste 200 de astfel de imagini, multe dintre ele fiind deschise pentru a se verifica dacă au același gen de conținut. Inculpatul a solicitat excluderea acestor probe susținând că au fost obținute prin depășirea limitelor mandatului. Acesta a susținut, de asemenea, că mandatul a fost emis numai în legătură cu obținerea de probe digitale prin care să se dovedească vânzarea sau distribuirea de substanțe interzise, astfel încât o căutare în sistemul informatic a probelor digitale în legătură cu infracțiunea de pornografie infantilă, a transformat acest mandat într-un mandat general, iar activitatea de percheziție a devenit nelegală. Curtea a respins acest argument, considerând că toate imginile vor fi înlăturate, cu excepția celei dintâi. Hotărârea s-a

[74] *Idem,* p. 127-128.

[75] I. Lucaci, R. Marin, Investigarea fraudelor informatice, Ed. Ministerului de Interne, București, 2002, p. 42.

[76] J. Goldfoot, *op. cit.,* p.141.

[77] M. E. Whitman, *Computer forensics search and seizure: challenges in the academe,* în „Proceedings of the 2005 Southern Association for Information Systems Conference", 2005, p. 64, disponibil online la adresa (*http://aisel.aisnet.org/sais2005/11).*

[78] Hotărârea din10.12.1982 (nr. 80-1838).

[79] S. Trepel, *op. cit.,* p. 128.

[80] Hotărârea din 14.04.1999 (nr. 98-3077).

întemeiat se faptul că prima imagine a fost descoperită întâmplător, dar celelalte imagini sunt rezultatul unor căutări care nu au fost încuviințate în prealabil. Era astfel necesar ca organul de urmărire penală să obțină un al doilea mandat de percheziție informatică privitor la săvârșirea infracțiunii de pornografie infrantilă.

Curtea a considerat că analogia cu o cutie (container) a sistemului informatic conduce la o simplificare exagerată a cauzei și la ignorarea realității în care sistemele informatice actuale au o capacitate de stocare a informației imensă.[81] Neajunsul perspectivei Carey – Tamura este acela potrivit căruia, de cele mai multe ori, infractorul nu va denumi documentul despre care știe că poate conține probe digitale în așa fel încât să conducă organul de urmărire penală exact la identificarea lui. Nu numai că denumirile pot să nu aibă nicio legătură cu conținutul, dar mai mult decât atât, extensia sub care datele sunt salvate poate să fie modificată cu ușurință. Astfel, un document text poate să fie salvat sub extensia .jpg, indicând faptul că aceea ar fi o imagine. În caz contrar, utilizatorul care dorește ascunderea unei imagini cu pornografie infantilă va salva imaginea sub extensia .doc, creând aparența că fotografia este un fișier word.[82]

Prin urmare, jurisprudența, în special cea din SUA, a creat în decursul timpului numeroase reguli, dar care nu pot fi de aplicabilitate generală, ci trebuie verificată incidența lor de la caz la caz. Este important a se găsi un echilibru între dreptul la viață privată al utilizatorului sistemelor informatice ori a mijloacelor de stocare a datelor informatice și dreptul statului de a obține probe cu privire la săvârșirea unei infracțiuni.[83]

Cu privire la încheierea prin care judecătorul de drepturi și libertăți se pronunță asupra cererii de încuviințare a efectuării percheziției informatice, aceasta nu este supusă căilor de atac, nici ordinare, dar nici celor extraordinare. Cu toate acestea, este de competența judecătorului de cameră preliminară analiza legalității încheierilor prin care judecătorul de drepturi și libertăți a încuviințat percheziția informatică, dar și a mijloacelor de probă obținute în urma procedeului probatoriu încuviințat. De exemplu, în cazul încălcării normelor de competență materială sau personală a judecătorului de drepturi și libertăți care a încuviințat efectuarea percheziției informatice, se poate constata nulitatea procedeului probatoriu. În doctrină s-a considerat, de asemenea, că pot fi analizate, de către judecătorul de drepturi și libertăți, de principiu, și generalitatea mandatului de percheziție informatică ori modalitatea în care mandatul de percheziție informatică este pus în executare, fiind depășite limitele impuse de mandat. Legalitatea mandatului de percheziție informatică se va aprecia de la caz la caz.[84]

VI. PROTEJAREA SECRETULUI PROFESIONAL

Există anumite categorii profesionale în cazul cărora este necesară reglementarea mai strictă a garanțiilor, comparativ cu procedura comună, astfel încât secretul profesional să fie realmente protejat. Prezentând un grad mare de ingerință în viața privată a utilizatorului, percheziția informatică poate avea repercusiuni și asupra înfăptuirii justiției, atunci când supus procedeului probatoriu este sistemul informatic ori mijlocul de stocare al avocatului, astfel cum se poate observa din jurisprudența Curții Europene a Drepturilor Omului. De asemenea, insuficienta reglementare a garanțiilor determină frecvent și încălcarea libertății de exprimare, în special în situația în care percheziția informatică privește un utilizator care activează în domeniul jurnalismului. Este de dorit ca percheziția informatică să fie reglementată mai restrictiv, prin norme care să țină cont de nevoile societății în care intervine. Spre exemplu, supravegherea tehnică, asemănătoare prin gradul de ingerință pe care îl presupune, beneficiază de o mai mare atenție înspre protejarea secretului profesional. Astfel, art. 139 alin. (4) C.proc.pen. prevede expres că „raportul dintre avocat și persoana pe care o asistă sau o reprezintă nu poate forma obiectul supravegherii tehnice decât dacă există date că avocatul săvârșește ori pregătește săvârșirea unei infracțiuni dintre cele prevăzute la alin. (2)", considerate ca fiind infracțiuni grave. Mai mult, „dacă pe parcursul sau după executarea măsurii rezultă că activitățile de supraveghere tehnică au vizat și raporturile dintre avocat și suspectul sau inculpatul pe care acesta îl apără, probele obținute nu pot fi folosite în cadrul niciunui proces penal, urmând a fi distruse, de îndată, de către procuror. Judecătorul care a dispus măsura este informat de îndată de către procuror".

Prin urmare, în principiu, raportul dintre avocat și persoana pe care o asistă sau o reprezintă nu poate

[81] S. Trepel, *op. cit., p.* 130-131.
[82] *Idem, p.* 135.
[83] *Idem,* p. 122.
[84] M. Udroiu, G. Zlati, Comentariu în M. Udroiu (coord.), *op. cit.,* p. 846-847.

reprezenta obiectul supravegherii tehnice. Apar astfel întrebări cu privire la raţiunea pentru care percheziţia informatică nu conţine reglementări asemănătoare supravegherii tehnice, cu privire la legătura dintre avocat şi persoana asistată sau reprezentată, deşi codul de procedură penală face adesea referire la importanţa secretului profesional. De exemplu, art. 306 alin. (6) C.proc.pen., reglementând obligaţiile organelor de urmărire penală, prevede că „secretul bancar şi cel profesional, cu excepţia secretului profesional al avocatului, nu sunt opozabile procurorului, după începerea urmăririi penale".

De asemenea, conform art. 79 C.proc.pen., „persoana obligată a păstra secretul profesional nu poate fi ascultată ca martor cu privire la faptele şi împrejurările de care a luat cunoştinţă în exerciţiul profesiei, fără încuviinţarea persoanei sau a unităţii faţă de care este obligată a păstra secretul".

Fundamentul prevederii anterior menționate cu privire la supravegherea tehnică îl reprezintă necesitatea protejării secretului profesional de către avocat, sub aspectul raporturilor strict profesionale dintre avocat și persoana asistată sau reprezentată în proces. Astfel, orice element care depășește acest cadru poate fi supus supravegherii tehnice.[85] Pentru identitate de raţiune, aceeași regulă trebuie să devină aplicabilă și percheziției informatice, astfel încât acest procedeu probatoriu să nu poată viza raportul profesional dintre avocat și client.

În literatura de specialitate, se arată că nu există în Codul de procedură penală nicio procedură specială care să reglementeze percheziționarea unui cabinet de avocat. Se impune astfel reglementarea expresă a caracterului excepțional al procedeului probatoriu în acest caz, numai pentru motive foarte grave și numai în legătură strânsă cu obiectul precis al procedeului. Astfel, excepția ar opera strict în cazul în care este imputată o infracțiune avocatului însuși, iar documentele ridicate sunt susceptibile să probeze participarea avocatului la săvârșirea unei infracțiuni.[86]

Observațiile au fost aduse privitor la percheziția domiciliară, dar cu atât mai îngrijorătoare este situația percheziției informatice, atât timp cât capacitatea de stocare a unui sistem informatic ori a unui mijloc de stocare este extrem de vastă, astfel încât o circumscriere inexactă a scopului mandatului de percheziție poate produce consecințe grave în privința clienților avocatului pe care acesta îi asistă ori îi reprezintă în alte cauze. Prin urmare, lipsa reglementării unei proceduri speciale a percheziției informatice în privința efectuării acesteia atunci când utilizatorul este avocat, pune grav în pericol dreptul protejat prin art. 6 din Convenție.

Jurisprudența Ct.E.D.O. oferă exemple de condamnări în privința aspectelor menționate mai sus, dintre care, relevantă este și cauza Vinci contra Franței.[87] Curtea a concluzionat că percheziţiile la sediile celor două societăți au fost disproporționate în raport cu obiectivul urmărit și a constatat încălcarea art. 6 parag. 1 – dreptul la un process echitabil și art. 8 – dreptul la respectarea vieţii private şi de familie, din Convenție.[88]

În același sens este și cauza Yuditskaya contra Rusia.[89] Ct.E.D.O. a considerat că mandatul de

[85] G. Mateuț, D. Nițu, L. Criste, *Aspecte actuale de drept și procedură penală*, Hamangiu, București, 2015, p. 55-56.

[86] *Idem,* p. 61-62.

[87] În fapt, prin cererea sa, Direcţia Generală de Concurenţă a cerut instanţei competente din Paris autorizarea efectuării unor percheziţii la sediile societăților reclamante, ca parte a unei anchete privind fapte ilicite. Judecătorul a admis această cerere, iar în urma percheziţiilor, mai multe documente şi fişiere din calculatoare au fost ridicate, inclusiv corespondenţa electronică a unor angajaţi. În căile de atac introduse împotriva hotărârii judecătoreşti privind aceste percheziţii, reclamanţii au afirmat că acestea au fost efectuate într-un mod masiv şi nediferenţiat, fiind ridicate mii de documente aflate în calculatoare, multe dintre ele neavând legătură cu ancheta, şi multe fiind protejate de confidenţialitatea comunicărilor avocat – client. Reclamanţilor le-au fost respinse căile de atac, considerându-se că percheziţiile au respectat dispoziţiile Codului Comercial şi ale Codului de procedură penală, precum şi drepturile garantate de Convenţia Europeană a Drepturilor Omului. Judecătorul a considerat că respectarea confidenţialităţii comunicărilor avocat – client nu interzice ridicarea comunicărilor acoperite de acest secret. Recursul în casaţie al reclamanţilor a fost, de asemenea, respins. În aceste condiţii, reclamanţii s-au adresat Ct.E.D.O., invocând art. 6, art. 8 şi art. 13 din Convenţie. Hotărârea curţii s-a axat pe punerea în balanţă a intereselor legate, pe de o parte, de interesul legitim al statului de a căuta dovezi privind infracţiuni prevăzute de dreptul concurenţei şi, pe de altă parte, de respectarea dreptului la viaţă privată şi corespondenţă, inclusiv confidenţialitatea între avocat şi client.

[88] UNBR, *Decizii CEDO privind percheziții la sediul firmelor de avocați*, disponibil online la adresa https://www.juridice.ro/382694/unbr-decizii-cedo-privind-perchezitii-la-sediul-firmelor-de-avocati.html.

[89] Doamna Yuditskaya a fost prima reclamantă la Ct.E.D.O., dar plângerea sa a fost urmată de alte 4 plângeri ale colegilor săi din societatea de avocatură din care făcea parte. Acestora le-au fost ridicate calculatoarele în cadrul unei proceduri penale, în care era implicat un alt coleg al lor avocat. Cel din urmă era suspectat că a încheiat un contract fictiv de asistență juridică, în numele societății de avocatură, cu o compania de stat, pentru a acoperi o dare de mită. În condițiile în care numai unul dintre avocați era suspect de complicitate la infracțiunea respectivă și chiar dacă fiecare avocat avea calculatorul său, au fost confiscate toate calculatoarele societății. Instanța națională a autorizat percheziția la sediul societății și, de asemenea, percheziția informatică a tuturor calculatoarelor găsite.

percheziție a fost formulat în termeni foarte generali, oferind anchetatorilor un drept de apreciere discreționară în efectuarea percheziției. Curtea a criticat faptul că instanța națională nu a explicat de ce nu ar fi suficientă o percheziție doar la calculatorul utilizat de avocatul implicat. Mai mult, în mandatul emis de judecător nu a fost atinsă problema datelor acoperite de secretul profesional, deși era evident faptul că reclamanții sunt membrii unui Barou și dețin documente confidențiale. Potrivit jurisprudenței curții, mandatele de percheziție trebuie să fie elaborate, pe cât posibil, într-un asemenea mod încât impactul lor să se situeze în limite rezonabile. Având în vedere materialele care au fost inspectate, curtea a constatat că perchezițiile aduc atingere secretului profesional într-o măsură disproporționată în raport cu scopul legitim urmărit. Curtea a reamintit, în acest sens, că, în cazul în care este implicat un avocat, o violare a secretului profesional ar putea avea repercusiuni asupra dreptului la un proces echitabil, garantat de articolul 6 din Convenție.

În concluzie, Curtea a considerat că cercetarea efectuată în absența unei suspiciuni rezonabile sau a oricăror măsuri de protecție împotriva violării secretului profesional la birourile de avocatură ale reclamanților și ridicarea computerelor a mers dincolo de ceea ce a fost „necesar într-o societate democratică" pentru atingerea scopului legitim urmărit. Prin urmare, a existat o încălcare a articolului 8 din Convenție.[90]

În privința protejării surselor jurnalistice, reprezentativă este cauza Saint-Paul Luxembourg S.A. v. Luxembourg[91]. Ct.E.D.O. a constatat încălcarea art. 8 din Convenție, observând că, din elementele speței, aspectele cercetate puteau fi lămurite cu ușurință fără a fi necesară efectuarea unei percheziții în acest sens. Mai mult, judecătorul național ar fi putut să dispună o măsură mai puțin gravă pentru a afla numele real al jurnalistului care a semnat articolul. Prin urmare, în acea etapă a investigației, o asemenea măsură nu era necesară, astfel că în speță a existat o încălcare a dreptului la viață privată. De asemenea, Curtea a arătat că organele de urmărire penală au avut posibilitatea să acceseze informații care nu ar fi trebuit să devină publice și care se aflau sub protecția surselor jurnalistice. În concluzie, s-a reținut că percheziția informatică efectuată a fost disproporționată cu scopul urmărit, constatându-se în unanimitate încălcarea art. 10 din CEDO.

VII. GARANȚII

1. Prezența avocatului la efectuarea percheziției informatice

Pentru a fi demonstrată necesitatea prezenței avocatului în cadrul efectuării percheziției informatice, apare ca necesară prezentarea cauzei Wieser și Bicos Beteiligungen GmbH v. Austria[92]. În speță, Ct.E.D.O a arătat că nu există nicio rațiune a se distinge între corespondența unei persoane private și corespondența unei persoane juridice. S-a observat că percheziția informatică a fost dispusă cu privire la o terță persoană suspectată de trafic de droguri, scopul legitim fiind prevenirea săvârșirii de infracțiuni. Percheziția a fost dispusă în considerarea unei suspiciuni rezonabile, dar fără a fi respectate garanțiile prevăzute de lege. Astfel, deși a fost prezent un reprezentant al Baroului pentru o scurtă perioadă de timp, acesta a fost obligat să supravegheze

[90] Ibidem. A se vedea Hotărârea din 12.02.2015 (cererea nr. 5678/06).

[91] Hotărârea din 18.07.2013 (cererea nr. 26419/10). În ziarul aparținând companei Saint-Paul Luxembourg S.A., a fost publicat un articol în care era descrisă situația familiilor care au pierdut custodia copiilor lor. A fost prezentat astfel și cazul a doi adolescenți și a asistentului social, fiind specificat numele acestora. Despre tânăra adolescentă s-a susținut că a suferit o tentativă de viol, iar despre tânărul băiat s-a afirmat că a ars cu țigara un prieten. Lista oficială a jurnaliștilor din Luxemburg nu conținea numele sub care a fost semnat articolul, „Domingos Martins", dar la litera „D" a fost identificat un jurnalist numit De Araujo Martins Domingos Alberto. În urma unei plângeri întocmite pentru defăimarea sistemului judiciar și social din Luxembourg și în mod special a asistentului social, a fost deschisă urmărirea penală. În cauză a fost emis și un mandat de percheziție informatică, privitor la sistemele informatice aparținând companiei. Calea de atac urmată de inculpat a fost respinsă ca neîntemeiată, percheziția fiind considerată legal efectuată.

[92] Hotărârea din 16.1.2008 (cererea nr. 74336/01). Primul aplicant este un avocat, deținătorul și managerul celui de al doilea aplicant, o companie. Cea din urmă este compania mamă a persoanei juridice Novamed. Ca stare de fapt, în cursul unei urmăriri penale pentru trafic de droguri, instanța a emis un mandat de percheziție cu privire la sediul companiei aplicante și la Novamed, ambele companii având sediul la biroul de avocatură al primului aplicant. La efectuarea percheziției informatice a participat și un specialist IT, dar care a plecat înainte de finalizarea procedurii. Organele de urmărire penală nu au întocmit niciun proces-verbal cu ocazia încheierii procedeului probatoriu, și nici nu au informat despre rezultatul percheziției. Procesul-verbal a fost întocmit mai târziu, în aceeași zi. Reclamantul a susținut că nu a avut ocazia să formuleze obiecții cu privire la efectuarea percheziției informatice și, de asemenea, nu a fost prezent la sigilarea suporturilor informatice pe care au fost stocate datele găsite în urma percheziței informatice. Aceste obiecții au fost însă respinse de către instanță. De regulă, în situația în care utilizatorul sistemului informatic contestă modul în care au fost efectuate căutările cu privire la anumite date digitale, este obligatorie realizarea unei copii (clone) a datelor informatice, sigilată, iar instanța va decide dacă este necesară sau nu examinarea acelor informații digitale. De asemenea, în principiu, informațiile protejate de secretul profesional nu pot fi supuse percheziției informatice.

și operațiuna de căutare a documentelor tipărite, nereușind să supravegheze în totalitatea desfășurarea percheziției informatice. Procesul-verbal nu a fost întocmit imediat după finalizarea procedeului probatoriu, iar reprezentantul Baroului nu a fost informat despre rezultatul căutărilor. Este adevărat că reclamantul ar fi putut să solicite, de o manieră generală, la începutul efectuării percheziției, ca fiecare suport informatic să fie, ulterior salvării datelor digitale, sigilat și supus instanței pentru verificarea relevanței. Cu toate acestea, din moment ce Codul de procedură penală prevede obligativitatea întocmirii unui proces-verbal la sfârșitul percheziției, ar fi fost de așteptat ca procedura reglementată să fie urmată.

Curtea a mai reținut că maniera în care au fost efectuate perchezițiile, cu privire la primul reclamant, crează un risc asupra păstrării secretului profesional. În concluzie, s-a constatat că nu au fost respectate toate garanțiile procedurale prevăzute de lege menite să protejeze împotriva abuzului, a arbitrariului și să protejeze secretul profesional, astfel încât art. 8 din CEDO este încălcat cu privire la ambii reclamanți. Prezența unui reprezentat al Baroului la efectuarea percheziției informatice a fost analizată de către Ct.E.D.O., în această speță, ca o condiție necesară pentru legalitatea procedeului probatoriu. Reglementarea expresă a participării unui avocat la realizarea percheziției informatice este necesară și în legislația din România. Prezența unui reprezentant al Baroului în cazul efectuării percheziției, atunci când utilizatorul este un avocat, ar fi de dorit cu atât mai mult cu cât raporturile dintre avocat – client trebuie să fie atent reglementate, în scopul protejării secretului profesional.

Dreptul avocatului suspectului sau a inculpatului de a asista la efectuarea oricărui act de urmărire penală suportă două excepții și presupune formularea din partea avocatului a unei solicitări exprese în acest sens. Data și ora efectuării actului de urmărire penală ori a audierii realizate de judecătorul de drepturi și libertăți se vor comunica prin notificare telefonică, fax, e-mail sau prin alte asemenea mijloace, încheindu-se în acest sens un proces-verbal. Lipsa avocatului nu împiedică efectuarea actului de urmărire penală sau a audierii, dacă există dovada că acesta a fost încunoștințat în mod legal. În literatura de specialitate se consideră că solicitarea avocatului este generală, atât timp cât înștiințarea provenită de la organul de urmărire penală ori de la judecătorul de drepturi și libertăți este condiționată de formularea prealabilă a solicitării. În consecință, pentru a fi eficientă, ea trebuie prezentată, în faza de urmărire penală, odată cu depunerea delegației, din chiar momentul încheierii contractului de asistență juridică sau, în cazul avocatului din oficiu, din momentul desemnării acestuia, în cazurile prevăzute de lege. Ea este valabilă și în fața judecătorului de drepturi și libertăți.[93]

Conform alin. (1) al art. 92 C.proc.pen., în cursul urmăririi penale, avocatul suspectului sau inculpatului are dreptul să asiste la efectuarea oricărui act de urmărire penală. Excepția de la această regulă este reprezentată de situația în care se utilizează metode speciale de supraveghere ori de cazul în care se efectuează cercetare și percheziția corporală sau a vehiculelor, în cazul infracțiunilor flagrante.[94] În faza de cameră preliminară și judecată, exercițiul drepturilor nu mai este condiționat de o solicitare expresă, precum se întâmplă în faza de urmărire penală, existând chiar obligația judecătorului de cameră preliminară și a instanței de judecată de a asigura o apărare efectivă și concretă. Reglementarea art. 92 alin. (7) C.proc.pen. este generală și ea se completează cu dispozițiile legale referitoare la procedura în camera preliminară și în fața instanței în cursul judecății.[95]

Pecheziția informatică nu este enumerată printre cazurile de excepție, dar nu există nici prevederi care să facă referire la prezența avocatului, astfel cum se întâmplă în situația percheziției domiciliare. Astfel, potrivit art. 159 alin. (9) C.proc.pen. este reglementat „dreptul ca la efectuarea percheziţiei să participe un avocat. Dacă se solicită prezenţa unui avocat, începerea percheziţiei este amânată până la sosirea acestuia, dar nu mai mult de două ore de la momentul la care acest drept este comunicat, luându-se măsuri de conservare a locului ce urmează a fi percheziţionat. În cazuri excepţionale, ce impun efectuarea percheziţiei de urgenţă, sau în cazul în care avocatul nu poate fi contactat, percheziţia poate începe și înainte de expirarea termenului de două ore". Se observă că prevederile art. 168 C.proc.pen., în cadrul cărora este reglementată pecheziția informatică nu fac trimitere la prevederile art. 159 alin. (9), ci doar la alin. (10) și (11) ale aceluiași articol, referitoare la reprezentant. Indiferent dacă lipsa reglementării este o omisiune a legiuitorului ori o eliminare voită a acestei garanții, este de dorit ca pe viitor să fie prevăzută expres facultatea participării avocatului utilizatorului sistemului informatic ori a mijlocului de stocare a datelor digitale la efectuarea percheziției informatice, și obligativitatea prezenței unui

[93] G. Mateuț, D. Nițu, L. Criste, *Aspecte actuale de drept și procedură penală, cit. supra.,* p. 42.
[94] *Idem,* p. 41.
[95] *Idem*, p. 43.

reprezentat al Baroului dacă percheziția se efectuează în legătură cu exercitarea profesiei de avocat.

În practică se regăsesc și exemple pozitive în care percheziția informatică este suficient reglementată astfel încât efectuarea procedeului probatoriu cu respectarea dreptului intern a fost în concordanță și cu prevederile Convenției. Un exemplu în acest sens este cauza Sérvulo & Associados - Sociedade de Advogados, Rl v. Portugalia[96]. Speța presupune un grad mai mare de dificultate, percheziția fiind efectuată în legătură cu sistemele informatice utilizate în cadrul unui birou de avocatură, caz în care datele informatice sunt protejate de secretul profesional. Reclamanții, o societate de avocatură, avocați și parteneri ai societății de avocatură Sérvulo & Associados – Sociedade de Advogados RL, invocă încălcarea art. 8 din Convenție. Sediul principal al societății se află în Lisabona. În contextul urmăririi penale cu privire la infracțiuni precum spălarea de bani și corupție, în legătură cu care era suspectat și un avocat din cadrul societății de avocatură reclamante, instanța a emis un mandat de percheziție informatică. În mandat erau precizate 35 de cuvinte-cheie în funcție de care să fie efectuată căutarea datelor informatice. Printe aceste cuvinte erau incluse nume ale companiilor și băncilor care aveau legătură cu investigațiile și termeni precum cel de contribuție financiară. Înainte ca percheziția informatică să înceapă, reclamantul a contestat măsura și a arătat că acele cuvinte-cheie erau frecvent folosite de către firmele de avocatură și, prin urmare, ar determina căutari cu privire la un număr disproporționat de documente care nu au legătură cu acea cauză și care erau protejate de secretul profesional. Instanța a avut în vedere argumentele utilizatorului și a dispus ca toate documentele rezultate din percheziția informatică efectuată în conformitate cu criteriile prevăzute în mandat să fie sigilate și puse la dispoziția judecătorului, fără a fi cercetate, pentru a hotărî dacă în cauză este valabilă ridicarea secretului profesional invocat. Ulterior verificării datelor informatice obținute de către organele de urmărire penală, ca și consecință a efectuării percheziției informatice, instanța a dispus ștergerea a 850 de date care conțineau informații personale sau date protejate de secretul profesional, în conformitate cu legea. În cele din urmă s-a renunțat la urmărirea penală.

Curtea a reținut că, în conformitate cu Legea pentru organizarea și exercitarea profesiei de avocat, documentele protejate de secretul profesional nu pot să facă obiectul percheziților, cu excepția situației în care a fost începută urmărirea penală cu privire la avocatul în discuție. Codul de procedură penală și Statutul Avocatului prevăd, de asemenea, o serie de garanții cu privire la efectuarea percheziției informatice în cazul unui birou de avocatură. Curtea observă că în prezenta speță toate garanțiile au fost respectate. Astfel, reclamantul a fost prezent în momentul efectuării percheziției informatice, alături de un reprezentant al Baroului. Un judecător, de asemenea, a verificat operațiunile efectuate. Un proces-verbal a fost întocmit la finalizarea procedeului probatoriu. Curtea observă că, sub legea portugheză, investigațiile au fost conduse de procuror, iar cu privire la percheziția informatică realizată la cabinetul de avocatură, judecătorul a exercitat un rol de supraveghere înainte, în timpul și după efectuarea operațiunilor. Ct.E.D.O. a obervat că datele informatice au fost sigilate. Posibilitatea contestării limitelor mandatului de percheziție informatică constituie un remediu efectiv și adecvat, iar activitatea judecătorului de supraveghere compensează scopul larg al mandatului de percheziție informatică. Curtea nu vede nicio rațiune pentru care să pună la îndoială raționamentul instanței care a verificat legalitatea operațiunii de percheziție și, în special, incidența secretului profesional. În legătură cu utilizarea datelor informatice cu privire la alți suspecți sau inculpați, curtea consideră că au existat suficiente garanții împotriva arbitrariului și abuzului. În concluzie, curtea constată că, în pofida scopului mandatului de percheziție informatică, garanțiile incidente împotriva abuzului și cu privire la ridicare secretului profesional au fost adecvate și suficiente. Prin urmare, percheziția informatică nu a presupus o ingerință disproporționată cu privire la dreptul reclamantului la viață privată și de familie. Astfel, Curtea reține că nu a existat o încălcare a art. 8 din Convenție.

2. Obligativitatea prezenței specialistului

Cerința conform căreia percheziția informatică se realizează de un specialist în domeniul informatic ori de un lucrător al poliției specializat este expresia realității că doar o persoană cu suficiente cunoștințe de specialitate poate realiza această activitate în condiții optime. Printre responsabilitățile specialistului în informatică judiciară se regăsesc activități precum protejarea datelor informatice împotriva modificărilor; asigurarea sistemului informatic astfel încât acesta să nu fie distrus ori deteriorat; identificarea fișierelor ascunse, șterse, criptate sau protejate cu o cheie de acces; recuperarea fișierelor șterse; accesarea fișierelor protejate sau

[96] *Hotărârea din 03.09.2015, (cerere nr. 27013/10).*

criptate; analiza datelor descoperite; depunerea mărturiei și oferirea consultanței de specialitate în legătură cu sistemul informatic ori mijlocul de stocare supus percheziției informatice.[97] Prezența specialistului la efectuarea percheziției informatice este impusă și prin jurisprudența Ct.E.D.O. Astfel, în cauza Wieser and Bicos Beteiligungen GmbH c. Austriei, s-a considerat că participarea specialistului la doar o parte din operațiunile pe care le-a presupus acest procedeu probatoriu, a contribuit la încălcarea art. 8 din Convenție.

Organul de urmărire penală, prin specialistul ori organul de poliție specializat desemnat să efectueze percheziția informatică are, de asemenea, obligația de a coroborara urmele digitale în scopul elucidării stării de fapt. Recent a apărut inclusiv o formă de șantaj ce constă în introducerea unor date informatice, conținând, de exemplu, pornografie infantilă, pe un sistem informatic vulnerabil ori mijloc de stocare și constrângerea ulterioară a utilizatorului respectivului sistem ori mijloc de stocare, în scopul transferării unei sume de bani într-un cont bancar, pentru a evita să fie denunțat cu privire la săvârșirii infracțiunii de pornografie infantilă.[98] În situația în care suspectul sau inculpatul invocă această apărare, rolul specialistului devenine și mai dificil. Dacă activitatea infracțională a fost realizată de o terță persoană prin intermediul unui program malițios, sistemul informatic al suspectului sau inculpatului este, de principiu, utilizat de la distanță de adevăratul făptuitor. Astfel, specialistul, pentru a strânge probele necesare în scopul stabilirii adevărului în cauză, pe lângă identificarea programului malițios, trebuie să arate și în ce măsură programul malițios a fost executat și care au fost urmările produse.[99]

Protejarea probelor de către specialist este extrem de importantă. Ținerea unei evidențe a persoanelor care au interacționat cu datele digitale pe parcursul căutărilor permite demonstrarea faptului că acestea nu au fost corupte. În caz contrar, suspiciunile care planează asupra integrității probelor digitale se va răsfrânge și asupra rezultatului examinărilor. Obligativitatea asigurării integrității informaţiilor conţinute într-un sistem informatic sau pe suportul de stocare a datelor informatice este prevăzută expres în cadrul art. 168 alin. (1) C.proc.pen.

3. Prezența suspectului sau a inculpatului la efectuarea percheziției informatice

Percheziția sistemului informatic sau a suportului de stocare a datelor informatice se efectuează în prezența suspectului ori a inculpatului, căruia i se va permite să fie asistat ori reprezentat de o persoană de încredere, conform art. 168 alin. (11), coroborat cu art. 159 alin. (10) C.proc.pen. În situația în care suspectul sau inculpatul este reținut ori arestat, va fi adus la percheziție, iar dacă nu poate fi adus, percheziția în sistem informatic sau a suportului de stocare a datelor informatice se efectuează în prezența unui reprezentant ori martor asistent, astfel cum rezultă din reglementarea art. 168 alin. (11) coroborat cu art. 159 alin. (11) C.proc. pen.

Garanțiile oferite suspectului sau inculpatului de a fi prezent la efectuarea percheziției mediului informatic pot fi cu ușurință eludate în măsura în care percheziția informatică este dispusă cât timp urmărirea penală se efectuează in rem, deși există o bănuială rezonabilă cu privire la identitatea suspectului ori a inculpatului. Efectuarea percheziției informatice cât timp urmărirea penală se efectuează in rem, este posibilă în virtutea prevederilor art. 168 alin. (2) C.proc.pen, potrivit cărora percheziția informatică poate fi dispusă în cursul urmăririi penale de către judecătorul de drepturi și libertăți, fără a se face în acest sens vreo distincție între urmărirea penală in rem ori cea in personam. De asemenea, art. 168 alin. (6) lit. f) C.proc.pen, care privește încheierea de încuviințare, prevede că aceasta trebuie să cuprindă, în mod obligatoriu, sistemul informatic sau mijlocul de stocare a datelor informatice ce urmează a fi percheziționat, numele suspectului ori inculpatului regăsindu-se în încheiere doar în măsura în care sunt cunoscute.

Sancționarea încălcării dispozițiilor legale privind prezența suspectului sau a inculpatului atunci când participarea sa este obligatorie, corespunzător situațiilor particulare prevăzute de art. 282 alin. (1) lit. e) și f) C.proc.pen, figurează formal printre cazurile de nulitate absolută. Nulitatea nu poate fi invocată în orice stare a procesului, ci, prin derogare de la regulă, numai până la încheierea procedurii în cameră preliminară „dacă încălcarea a intervenit în cursul urmăririi penale sau în procedura camerei preliminare". Această prevedere reduce cele două cazuri de nulitate absolută, privitoare la dreptul la apărare, la nivelul unor nulități relative, fiind diminuată importanța dreptului la apărare și a garantării acestuia în raport cu celelalte valori ocrotite prin

[97] A. C. Moise, *Invetigarea criminalistică a infracțiunilor informatice*, „Dreptul", nr. 4/2009, p. 236.
[98] D. Haagman, B. Ghavalas, *Trojan defense: A forensic view*, „Digital Investigation", nr. 2, 2005, p. 24.
[99] *Ibidem.*

reglementarea principiilor procesului penal. Acest mod de sancționare a nerespectării dreptului la prezența personală și la asistență juridică a suspectului sau a inculpatului demonstrează excluderea regulilor referitoare la dreptul la apărare din sfera dispozițiilor de ordin public.[100]

4. Prezența persoanei vătămate, a părții civile și a părții responsabile civilmente la efectuarea percheziției informatice

Reglementarea art. 168 alin. (11) C.proc.pen este deficitară din perspectiva garanțiilor pe care ar trebui să le stabilească privitor la persoana vătămată, partea civilă sau partea responsabilă civilmente. Prevederea menționată face trimitere doar la prezența obligatorie a suspectului sau a inculpatului la realizarea percheziției informatice, deși mediile informatice percheziționate pot fi ridicate nu doar de la aceștia. Atât timp cât un sistem informatic ori un mijloc de stocare a datelor informatice poate fi ridicat inclusiv de la persoana vătămată, partea responsabilă civilmente ori de la un terț, este necesar ca și acești utilizatori să poată invoca dreptul de a participa în proprie persoană ori prin reprezentant (în cazul entităților juridice) la efectuarea percheziției informatice. Prezența persoanei de la care s-a ridicat mediul percheziționat reprezintă o garanție procedurală a desfășurării actului de urmărire penală cu respectarea tuturor dispozițiilor legale.

În schimb, lipsa persoanelor menționate implică imposibilitatea obiectivă de a observa neregularitățile care afectează procedeul probatoriu și, în consecință, șansa de a formula obiecții. Activitatea specialistului ori a organului de poliție specializat este și ea îngreunată, în cazul în care acesta are nevoie de lămuriri de la utilizatorul mediului informatic.[101]

Este posibil ca utilizatorul mediului informatic să fie însuși făptuitorul, însă percheziția informatică să fie dispusă în cursul urmăririi penale in rem, astfel că nu este încă funcțională calitatea de suspect sau inculpat. Nefiind obligatorie prezența utilizatorului la efectuarea procedeului probatoriu în acest caz, ar fi injustă obligarea persoanei să coopereze în scopul decriptării conținutului informatic. Apare, din nou, ca necesară prevederea expresă a posibilității participării utilizatorului sistemului informatic ori a mijlocului de stocare a datelor informatice la efectuarea percheziției.[102]

Regretabil este faptul că în practică se întâlnesc situații în care utilizatorul sistemului informatic ori a mijocului de stocare a datelor informatice nu are cunoștință despre faptul că a fost supus acestui procedeu probatoriu. Compania Microsoft a intentat un proces împotriva Departamentului de Justiție din SUA, luând poziție împotriva modului în care se realizează în mod frecvent căutări secrete în datele informatice ale clienților. Compania a arătat că este adoptată o politică nelegală de către Guvern, prin realizarea de căutări în informațiile clienților Microsoft și forțarea companiei să păstreze tăcerea în această privință. În mod firesc, utilizatorul trebuie să fie informat cu privire la efectuarea unei percheziții, fie ea domiciliară sau informatică.[103]

5. Mandatul de percheziție informatică și scopul acestuia

Orice omisiune în detalierea mandatului de percheziție informatică este aptă să confere puteri discreționare organelor de urmărire penală, permițând verificarea arbitrară a datelor informatice, în scopul identificării probelor digitale. Este recomandat ca mandatul de percheziție informatică să includă, atunci când este posibil, orice referiri obiective pentru identificarea datelor digitale relevante. Un mandat care face referire la data creării, modificării, ștergerii datelor și la subiect (materie) sau la indivizii ori entitățile implicate în activitatea infracțională poate să limiteze suficient de mult puterea organului de urmărire penală.[104] În cadrul art. 168 alin. (6) lit. e) C.proc.pen este prevăzută necesitatea existenței unui scop în considerarea căruia să fie emis mandatul de perchezitie, însă apare întrebarea care va fi situația în cazul în care scopul percheziției informatice se modifică pe parcurs. Firesc este ca activitatea de percheziție informatică să fie efectuată în continuare atunci când scopul inițial cuprinde și scopul actual al căutării. Această soluție apare în considerarea faptului că scopul căutării se referă, de cele mai multe ori, la locul căutării, la infracțiunea care se dorește a fi dovedită, la probele care se preconizează a fi obținute, și mai puțin la metodologia folosită în căutare.

În emiterea mandatului de percheziție informatică privitor la persoana juridică este necesar să fie luat în

[100] G. Mateuț, D. Nițu, L. Criste, Aspecte actuale de drept și procedură penală, cit. supra., p. 21-22.

[101] G. Mateuț, D. Nițu, L. Criste, *Aspecte actuale de drept și procedură penală, cit. supra.*, p. 21-22.

[102] G. Zlati, *Percheziția sistemelor informatice și a mijloacelor de stocare a datelor informatice (II), cit. supra.,* p. 87.

[103] G. Zlati, *Privilegiul contra autoincriminării și criptografia*, *cit. supra.*, p. 40.

[104] J. Pagliery, *Microsoft sues government for secret searches*, disponibil online la adrewsa *http://money.cnn.com/2016/04/14/technology/microsoft-secret-search-lawsuit/*.

considerare faptul că, de regulă, activitatea persoanei juridice nu este în totalitate de natură infracțională. Astfel, atunci când suspiciunea săvârșirii de infracțiuni nu planează asupra întregii activități, se impune ca mandatul să cuprindă criterii pentru identificarea datelor care vor fi supuse percheziției. Cu toate acestea, în cauza SUA v. Diaz, Curtea a constatat că scopul mandatului de percheziție informatică este dificil de detaliat în special în cazul în care fișierele conțin atât informații care nu sunt relevante din punct de vedere penal, cât și probe digitale. Într-un asemenea caz, în care este imposibilă delimitarea exactă a scopului mandatului de percheziție informatică, trebuie acceptate limitele mai largi ale mandatului, comparativ cu situațiile în care documentele pot fi subclasificate. De asemenea, în ipoteza în există suficiente motive a se crede că întreaga activitate a persoanei juridice are caracter infracțional, este permisă emiterea unui mandat de percheziție informatică ale cărui limite să fie mai largi decât în mod general. Asemănător cauzei SUA v. Diaz, în cauza SUA v. Kow Curtea a stabilit că un mandat general de percheziție informatică în cazul unei persoane juridice, poate să fie justificat dacă există suspiciunea rezonabilă că întreaga activitate a acesteia face parte dintr-un plan de fraudare sau că toate datele informatice privitoare la utilizatorul persoană juridică sunt susceptibile să contituie probe digitale.[105] Indiferent de forma legală de organizare, exercitarea profesiei de avocat precum și activitatea desfășurată în domeniul jurnalismului reprezintă excepții de la această regulă. Orice mandat de percheziție informatică la adresa acestor utilizatori trebuie atent detaliat, astfel încât să se asigure păstrarea secretului profesional, respectiv protejarea surselor jurnalistice.

În cauza SUA v. Kow, percheziția informatică a fost limitată la 14 categorii de date informatice, dar fără ca mandatul de percheziție să conțină limitări cu privire documentele care aparțineau fiecărei categorii și fără a se face referire la existența unei legături a documentelor cu o activitate infracțională specifică. Având în vedere că nu sunt precizate criterii mai exacte în funcție de care vor fi selectate datelor informatice supuse percheziției, mandatul este considerat a fi general. Clasificările generice într-un mandat sunt acceptate numai atunci când nu este posibilă o descriere mai precisă, dar în acest caz, mandatul putea fi particularizat. În mod evident, mandatul trebuia să prevadă activitatea infracțională în legătură cu care a fost emis. Era, de asemenea, posibilă o limitare a scopului percheziției la o anumită perioadă de timp în cadrul căreia infracțiunea a fost săvârșită. Ar fi fost astfel necesar ca mandatul să prevadă o limită de timp, locația și legătura datelor informatice cu infracțiunea în cauză.[106] Prin urmare, prevederile art. 168 alin. (5) lit. e) C.proc.pen, trebuie înțelese în sensul în care, în mandatul de percheziție informatică, scopul se referă atât la infracțiunea în legătură cu care se cercetează sistemul informatic pentru descoperirea probelor digitale, dar și la o detaliere a elementelor în funcție de care se va realiza selecția datelor ce urmează a fi cercetate. O astfel de detaliere privește precizarea unui interval de timp în cadrul căruia datele informatice au fost create, modificate sau șterse, a cuvintelor-cheie folosite în scopul căutării, care prezintă relevanță în cauză, raportul dintre datele digitale și infracțiunea în legătură cu care a fost emis mandatul și eventual specificarea locației datelor. În caz contrar, dacă mandatul de percheziție informatică nu este suficient de bine circumscris, este inevitabilă condamnarea României de către Ct.E.D.O., din cauza atribuirii de puteri discreționare organelor de urmărire penală în realizarea percheziției informatice, fapt care duce la încălcarea drepturilor protejate prin Convenție. În literatura de specialitate s-a arătat că este de dorit o reglementare expresă a obligației judecătorului de drepturi și libertăți de a stabili, prin intermediului mandatului de percheziței informatică, limitele în care procedeul probatoriu va fi efectuat. Lipsa criteriilor va permite specialistului ori lucrătorului de poliție specializat, de exemplu, identificarea de materiale cu conținut pornografic, deși cauza ar privi fapte de corupție, fără amenințarea unei sancțiuni prevăzute de C.proc.pen.[107]

Este de precizat faptul că referirea în cadrul mandatului la sistemul informatic asupra căruia se efectuează percheziția informatică poate include și mijlocul de stocare a datelor informatice în funcție de existența autonomă ori dependentă de sistemul informatic a mijlocului de stocare. Astfel, menționarea sistemului informatic în mandatul de percheziție informatică va permite și analiza mijlocului de stocare a datelor informatice, parte integrantă din sistem, precum este hard drive-ul intern. În schimb, mijloacele de

[105] Relevante în acest sens sunt *cauzele US v. Kow, David v. Gracey* şi *US v. Humphries*.

[106] Hotărârea din 21.06.1995 (nr. 94-10258), disponibil online (http://caselaw.findlaw.com/us-9th-circuit/1225333.html).

[107] G. Zlati, Privilegiul contra autoincriminării și criptografia, cit. supra., p. 40-41.

stocare autonome nu sunt incluse în noțiunea de sistem informatic, indiferent dacă în speță sunt atașate ori inserate în respectivul sistem informatic despre care mandatul de percheziție informatică face referire. Prin urmare, pentru realizarea unei percheziții informatice asupra unui CD, DVD ori memory stick, este necesară individualizarea unui astfel de mijloac de stocare autonom în cuprinsul mandatului de percheziție informatică. În ipoteza în care în momentul efectuării unei percheziții informatice asupra unui sistem informatic este identificat un memory stick în portul USB, mandatul nu este valabil și cu privire la mijlocul de stocare găsit, astfel încât este necesară obținerea unui nou mandat de percheziție informatică. Dispozițiile art. 168 alin. (8) C.proc.pen. nu sunt incidente în această situație.[108]

Scopul percheziției informatice constă în strângerea de probe digitale, operațiune ce presupune copierea acelor date digitale care prezintă relevanță, în limitele mandatului de percheziție informatică. Activitatea ulterioară strângerii de probe digitale, concretizată în analiza acestor date informatice stocate pe un mijloc de stocare aparținând organelor de urmărire penală iese de sub incidența prevederilor art. 168 C.proc.pen. Având în vedere aceste considerente, în literatura de specialitate s-a arătat că deși este posibilă, trierea, după efectuarea unei copii, a datelor digitale în funcție de relevanța lor în cauză, trebuie evitată. În momentul în care se recurge la copierea tuturor datelor informatice stocate pe copia realizată potrivit prevederilor art. 168 alin. (9) C.proc.pen., fără niciun proces de selecție a datelor în funcție de relevanța acestora și de limitele mandatului de percheziție informatică, se va ajunge la cercetare și identificarea efectivă a datelor informatice în afara operațiunii de percheziție informatică. În acest mod, vor fi realizate activități specifice unei percheziții informatice, cu nerespectarea garanțiilor procesuale prevăzute de art. 168 C.proc.pen.[109]

6. Intervalul de timp în care percheziția informatică se poate realiza

Percheziția sistemului informatic ori a suportului de stocare a datelor informatice se efectuează în intervalul de timp în considerarea căruia a fost emis mandatul, astfel cum prevede art. 168 alin. (5) lit. d) C.proc.pen. Cu privire la intervalul orar, în vechea reglementare (art. 103 C.proc.pen. din 1968 la care făcea trimitere art. 56 alin. 4 din Legea 161/2003) se preciza faptul că percheziția, cu două excepții, trebuia începută între orele 6-20, cu posibilitatea de a continua și în timpul nopții. În viziunea noului C.proc.pen. nu a mai fost considerată oportună stabilirea unui interval orar. Chiar și în lipsa unei prevederi exprese în cadrul art. 168 noul C.proc.pen., în situația în care, cu ocazia efectuării percheziției domiciliare, sistemul informatic nu este ridicat, de exemplu din cauza faptului că ar fi afectată grav desfășurarea activității utilizatorului, iar percheziția în sistemul informatic sau a suportului de stocare a datelor informatice se desfășoară „în timp real", la fața locului, vor fi avute în vedere dispozițiile art. 159 alin. (3) C.proc.pen.[110] Astfel, în ipoteza efectuării percheziției informatice „în timp real", la fața locului, procedeul probatoriu nu poate fi început înainte de ora 6,00 sau după ora 20,00, cu excepţia infracţiunilor flagrante sau atunci când percheziţia urmează să se realizeze într-un local deschis publicului la ora respectivă.

În literatura de specialitate s-a considerat că întreruperea activității de percheziție informatică și reluarea acesteia la un moment ulterior atrag nelegalitatea procedurii efectuate ulterior întreruperii. Conform art. 158 alin. (7) lit. j) C.proc.pen., mandatul de percheziție domiciliară poate fi folosit o singură dată, ceea ce implică desfășurarea acestei activități fără întreruperi. Cu toate acestea, s-a arătat că, în practică, apar situații în care ridicarea anumitor sisteme informatice precum serverele (sistemele informatice) unei persoane juridice, ar afecta în mod grav desfășurarea activității persoanei ce le deține, caz în care, în conformitate cu art. 168 alin. (10) C.proc.pen., procurorul poate dispune efectuarea de copii (clone). Problema care apare este dacă, în situațiile în care este imposibilă efectuarea clonelor într-un termen rezonabil, activitatea de percheziție domiciliară poate fi întreruptă. Un exemplu în acest sens este ipoteza în care efectuarea unei copii (clone) este estimată că va dura 48 de ore, iar organul de urmărire penală decide să inițieze procesul de copiere după care procedează la sigilarea încăperii, urmând a reveni la un alt moment în vederea reluării activității. Firesc este a se considera că mandatul de percheziție domiciliară încetează să mai producă efecte în momentul întreruperii activității.[111] Pentru a fi eliminate orice îndoieli cu privire la natura întreruperilor intervenite în cursul procedeului probatoriu, este utilă prevederea expresă a faptului că mandatul de percheziție informatică poate fi folosit o singură dată. Astfel,

[108] G. Zlati, *Privilegiul contra autoincriminării și criptografia, cit. supra.,* p. 40-41.
[109] M. Udroiu, G. Zlati, Comentariu în M. Udroiu (coord.), *op. cit.,* p. 834.
[110] *Idem,* p. 837.
[111] G.I. Ioniță, *Aspecte procesual penale și tehnice referitoare la percheziția informatică*, în „Dreptul", nr. 12/2014, p. 212.

orice întreruperi nefirești intervenite în cursul efectuării percheziției informatice marchează finalitatea acesteia. Prin urmare, pentru clarificarea situației pe cale normativă este de dorit ca legea să prevadă expres calitatea mandatului de percheziție informatică de a fi folosit o singură dată și a naturii activității de copiere ca parte integrantă din întregul procedeu probatoriu al percheziției informatice.

7. Conservarea datelor informatice

Conform art. 154 C.proc.pen., „dacă există o suspiciune rezonabilă cu privire la pregătirea sau săvârşirea unei infracţiuni, în scopul strângerii de probe ori identificării făptuitorului, suspectului sau a inculpatului, procurorul care supraveghează sau efectuează urmărirea penală poate dispune conservarea imediată a anumitor date informatice, inclusiv a datelor referitoare la traficul informaţional, care au fost stocate prin intermediul unui sistem informatic şi care se află în posesia sau sub controlul unui furnizor de reţele publice de comunicaţii electronice ori unui furnizor de servicii de comunicaţii electronice destinate publicului, în cazul în care există pericolul pierderii sau modificării acestora". Ce se întâmplă, însă, în situația în care există o suspiciune rezonabilă cu privire la pregătirea sau săvârșirea unei infracțiuni și este necesară conservarea unor date care nu se află în posesia sau sub controlul unui furnizor de rețele publice de comunicații electronice ori unui furnizor de servicii de comunicații electronice destinate publicului, precum sunt datele informatice stocate în memoria RAM, existând pericolul pierderii ori modificării acestor date? Art. 154 C.proc.pen. nu acoperă această ipoteză deoarece în cadrul lui se face referire expresă la datele care se află deja în posesia sau sub controlul unui furnizor de reţele publice de comunicaţii electronice ori unui furnizor de servicii de comunicaţii electronice destinate publicului. Soluția realizării unei copii (clone) a datelor este și ea exlusă, având în vedere faptul că activitatea de copiere este parte integrantă a percheziției informatice. Varianta ridicării sistemului informatic, în condițiile art. 169 C.proc.pen. nu este plauzibilă atât timp cât, așa cum s-a arătat anterior, datele informatice volatile se vor pierde în momentul scoaterii din funcțiune a sistemului informatic. De asemenea, art. 169 C.proc.pen. nu poate fi aplicat nici în situația în care activitatea persoanelor care dețin aceste obiecte ar fi grav afectată ca urmare a ridicării obiectelor care conțin date digitale.

Prin urmare, pentru situații cu totul excepționale, reglementarea ipotezei obținerii autorizării efectuării percheziției informatice subsecventă desfășurării acestei operațiuni ar fi utilă, cu atât mai mult cu cât o singură comandă lansată pe sistemul informatic, poate distruge probe într-o secundă. De exemplu, efectuarea unei copii (clone) a sistemului informatic sau a mijlocului de stocare, anterior emiterii unui mandat de percheziție informatică, poate să fie justificată în situația în care organul de cercetare penală ori procurorul observă că utilizatorul șterge documente din sistemul informatic. O circumstanță, de asemenea excepțională, este aceea în care bateria sistemului informatic este aproape epuizată, iar informațiile se vor pierde în momentul în care sistemul informatic încetează să mai funcționeze. De principiu, pentru a obține informații cu valoare doveditoare stocate, prelucrate sau transmise prin intermediul unui sistem informatic, de lege lata, organele de urmărire penală trebuie să obțină atât mandatul de percheziție domiciliară, dar și mandatul de percheziție informatică.[112]

Soluționarea acestor cazuri excepționale ar putea să își găsească fundamentul într-o viitoare reglementare a posibilității efectuării percheziției informatice, anterior obținerii încuviințării instanței. Cazurile excepționale sunt cele în care apare ca iminentă distrugerea datelor digitale și numai atunci când există suspiciunea rezonabilă că acestea constituie probe digitale ale săvârșirii unei infracțiuni. Efectuarea percheziției va fi încuviințată, în aceste ipoteze, de către procuror. Procurorul va înainta ulterior efectuării percheziției informatice, și fără întârziere, cererea prin care solicită încuviințarea judecătorului, în cazul căruia se prevede un termen pentru soluționarea cererii.

Luând în considerare art. 158 alin. (5) C.proc.pen., care reglementează termenul în care se soluționează cererea privind încuviințarea efectuării percheziției domiciliare, un termen de 24 de ore acordat pentru soluționare apare ca fiind optim și în aceste cazuri. Se impune, însă, ca judecătorul să procedeze la un control post factum, în cadrul căruia să fie verificată relevanța datelor informatice obținute ca urmare a percheziției informatice autorizate de procuror. Pentru conservarea datelor informatice va fi suficientă realizarea unei copii, în condițiile prevăzute de 168 alin. (9) sau (10) C.proc.pen., fără ca datele informatice copiate să fie supuse procesului de analiză de către organul de urmărire penală în scopul identificării probelor digitale. Copia

[112] N. Grofu, *Reflecții referitoare la percheziția informatică*, în „Dreptul", nr. 6/2010, p. 199.

realizată va fi însă sigilată și supusă verificărilor judecătorului. Acesta va decide dacă datele informatice prezintă importanță cauzei ori dacă, sau care dintre datele informatice copiate vor fi șterse sau distruse.

În cauza Sérvulo & Associados – Sociedade de Advogados, Rl v. Portugalia, chiar dacă mandatul de percheziției informatică a conferit limite prea largi organului de urmărire penală, existența unui control post factum a compensat acestă neregularitate, astfel încât Ct.E.D.O. a considerat că nu a existat o încălcare a drepturile protejate de Convenție. Astfel, un control post factum poate fi reglementat atât cu privire la efectuarea unei eventuale percheziții informatice încuviințate de procuror, cât și cu privire la ipoteza în care utilizatorul sistemului informatic contestă modul în care a fost efectuată percheziția informatică, invocând faptul că nu a fost respectat scopul mandatului și, în consecință, criteriile după care ar fi trebuit selectate datele informatice copiate. În concluzie, reglementarea posibilității dispunerii unei percheziții informatice de către procuror în situații excepționale, nu va pune probleme de compatibilitate cu Convenția, atât timp cât va fi însoțită de prevederea expresă a controlului post factum.

Este de precizat faptul că art. 168 alin. (8) C.proc.pen. este inaplicabil în cazurile excepționale precizate anterior, având în vedere faptul că textul face referire la „datele informatice căutate", date cu ajutorul cărora se dorește obținerea de probe în legătura cu infracțiunea în considerarea căreia a fost emis mandatul de percheziție informatică. Potrivit art. 168 alin. (6), lit. f) C.proc.pen. rezultă necesitatea precizării, în încheierea prin care se admite efectuarea percheziției informatice, a sistemului informatic sau a suportului de stocare a datelor informatice care urmează a fi percheziționat.

De principiu, este necesar ca fiecare entitate ce urmează a fi supusă percheziției informatice să fie atent individualizată. Este bine-venită însă alegerea legiuitorului de a atenua rigiditatea prevederii anterior menționate, prin intermediul dispozițiilor art. 168 alin. (8) C.proc.pen. Este astfel reglementată posibilitatea ca, „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 căutate sunt cuprinse în alt sistem informatic sau suport de stocare a datelor informatice și sunt accesibile din sistemul sau suportul inițial, procurorul dispune de îndată conservarea, copierea datelor informatice identificate și va solicita de urgență completarea mandatului". Este posibil însă ca organul de urmărire penală să constate existența unor date care să probeze săvârșirea unei alte infracțiuni și să fie obligat să rămână în pasivitate până în momentul emiterii unui mandant de percheziție informatică privitor la noua infracțiune, caz în care poate fi prea târziu.

Conform conceptului datelor la vedere, la care s-a apelat în jurisprudența din SUA, datele informatice descoperite întâmplător în cadrul efectuării percheziției informatice cu respectarea scopului mandatului, sunt considerate legal obținute și pot fi folosite în procesul penal.

8. Percheziţia informatică şi ridicarea datelor informatice

Percheziția domiciliară urmată de ridicarea de obiecte este considerată legitimă atunci când s-a realizat pentru a fi obținute probe materiale ale săvârșirii unor infracțiuni. Legea internă trebuie să ofere, însă, toate garanțiile împotriva unor eventuale abuzuri din partea autorităților competente (cauza Keslassy c. Franței)[113]. „Aceste garanții constau, în esență, în necesitatea autorizării judiciare prealabile efectuării ei, după verificarea de către un judecător, a elementelor de fapt pe care se întemeiază cererea organului judiciar competent să efectueze percheziția și plasarea întregii proceduri sub autoritatea unui judecător".[114] În procesul-verbal prin care se consemnează activitățile desfășurate în cadrul percheziției domiciliare (art. 161 C.proc.pen.) va fi menționată obligatoriu seria entității ridicate. Doar în măsura în care o astfel de serie nu este vizibilă se poate proceda la identificarea dispozitivului prin raportare la alte criterii: model, culoare etc. În măsura în care este vorba despre un mijloc de stocare extern, precum un harddisk ori un memory stick, în procesul-verbal se menționează seria acestuia, fiind insuficientă precizarea referitoare doar la seria sistemului informatic.[115]

Nelegalitatea percheziției domiciliare este susceptibilă să atragă nelegalitatea percheziției informatice ori a ridicării mediului informatic, astfel cum prevede art. 280 alin. (2) C.proc.pen. De exemplu, necompetența materială a judecătorului de drepturi și libertăți (în faza de urmărire penală) ori a instanței (în faza de judecată) determină nelegalitatea mandatului de percheziție domiciliară. Aceasta va atrage nelegalitatea percheziției domiciliare, care se răsfrânge totodată asupra actelor procedurale îndeplinite ulterior și cu care se află într-o

[113] G. Mateuț, *Tratat de procedură penală, Partea generală, cit. supra.,* p. 246.
[114] *Idem,* p. 248.
[115] G. Zlati, *Percheziția sistemelor informatice și a mijloacelor de stocare a datelor informatice (I), cit. supra.*, p. 25.

legătură directă, în speță, percheziția informatică ori ridicarea sistemelor informatice sau a mijloacelor de stocare a datelor informatice.[116]

Dispozițiile de drept comun care reglementează percheziția domiciliară, percheziția informatică și ridicarea de obiecte nu sunt suficiente pentru a asigura secretul profesional atunci când subiectul acestor proceduri este avocatul. Conform art. 35 alin. (1), teza I din Legea 51/1995, „pentru asigurarea secretului profesional, actele și lucrările cu caracter profesional aflate asupra avocatului sau în cabinetul său sunt inviolabile". Potrivit tezei a doua din același articol, „percheziționarea avocatului, a domicilului ori a cabinetului sau ridicarea de înscrisuri și bunuri nu poate fi făcută decât de procuror, în baza unui mandat emis în condițiile legii". Statulul profesiei de avocat, în temeiul art. 228, îl obligă pe avocat să se opună percheziționării domiciliului, a sediului profesional principal, secundar și a biroului de lucru, precum și percheziției corporale, cu privire la actele sau lucrările cu caracter profesional aflate în locurile sus-menționate ori asupra sa. Găsind fundament în cadrul aceluiași articol, avocatul are și obligația a se opune ridicării înscrisurilor și bunurilor constând în acte și lucrări cu caracter profesional, dacă nu sunt îndeplinite condițiile art. 35 din lege. În doctrină se arată, că prevederile cuprinse în legea specială nu pot suplini lacuna în reglementarea percheziției la domiciliul sau sediul avocatului. Prin urmare, chiar dacă în aceste situații ar fi necesară o procedură specială în temeiul căreia să se efectueze percheziția domiciliară, în lipsa reglementării, se va aplica procedura de drept comun. În toate cazurile, însă, avocatul este obligat să informeze asupra celor întâmplate pe decanul baroului. Singura derogare de la procedura comună constă în faptul că, în aceste situații, percheziția se efectuează doar de procuror, fără posibililtatea de a fi efectuată și de organul de cercetare penală. Ridicarea obiectelor sau a înscrisurilor, deci inclusiv a sistemelor informatice ori a mijloacelor de stocare a datelor electronice, atunci când posesorul este un avocat, se poate realiza doar de procuror, ca excepție de la regula comună.[117]

În cazul percheziției informatice legea prevede expres, în cadrul art. 168[1] C.proc.pen., faptul că percheziția informatică se efectuează în prezența procurorului sau a organului de cercetare penală. De asemenea, prezența organului de cercetare penală este suficientă, nefiind obligatorie prezența procurorului și potrivit prevederilor art. 168 alin. (12) C.proc.pen. Invocând raționamentul Ct.E.D.O. (cauza Robathin c. Austria)[118], conform căruia regulile percheziției documentelor se aplică și percheziției datelor electronice, apare firesc ca și percheziția informatică privitoare la utilizatorul avocat, iar nu doar percheziția domiciliară ori ridicarea de obiecte, să beneficieze de o reglementare derogatorie, cel puțin sub aspectul ca aceasta să fie efectuată doar în prezența procurorului, nefiind suficientă prezența organului de cercetare penală. De asemenea, pentru identitate de rațiune, avocatul ar trebui să informeze, asupra procedeului probatoriu la care a fost supus, pe decanul Baroului.[119]

---

[116] *Idem,* p. 24.

[117] G. Mateuț, D. Nițu, L. Criste, *Aspecte actuale de drept și procedură penală, cit. supra.,* 62-63.

[118] *Hotărârea din 3.10.2012 (cererea nr. 30457/06).*

[119] Ca stare de fapt, în *cauza Robathin c. Austria* reclamantul susține că percheziția informatică realizată asupra sistemelor informatice existente în biroul de avocatură a fost efectuată cu încălcarea dreptului la viață privată, protejat prin art. 8 din Convenție. În 2005 a început urmărirea penală împotriva lui Robathin și a altor persoane pentru fapte de furt calificat și delapidare. În 2006 în cauză a fost emis un mandat de percheziție a sediului reclamantului și de percheziție informatică a sistemelor informatice ori a mijloacelor de stocare găsite la sediul acestuia. Organele de urmărire penală au procedat în consecință și au copiat (clonat) datele informatice găsite. Reprezentantul Baroului s-a opus acestei operațiuni, susținând că procedeul probatoriu s-a efectuat în mod abuziv, disproporționat, atât timp cât tehnic există posibilitatea de a fi efectuate căutări după anumite criterii, astfel încât să fie copiate doar acele date care corespund mandatului de percheziție informatică. Organele de urmărire penală au copiat (clonat) toate datele care au corespuns criteriilor căutării după inițialele "R" și "G", iar separat au fost copiate toate celelalte date. După copierea informațiilor, suporturile de stocare au fost sigilate. Instanța de control nu a prezentat niciun motiv pentru care nu ar fi fost suficientă examinarea datelor digitale doar cu privire la R și G. Obligația avocatului de a proteja secretul profesional a fost ridicată numai în legătură suspiciunile împotriva lui raportat la cei doi clienți, dar nu și cu privire la celelalte relații avocat – client, care au rămas protejate de secretul profesional. Mai mult, asupra colaboratorului său, avocat al aceluiași cabinet de avocatură, nu plana nicio suspiciune în sensul implicării acestuia în activități infracționale. În 2009, reclamantul a fost condamnat pentru delapidare, și a fost achitat cu privire la celelalte infracțiuni. În 2010, Curtea de apel a menținut hotărârea inițială. Ulterior, inculpatul a obținut probe care au fost necunoscute la momentul judecării cauzei, iar ca urmare a redeschiderii procesului, acesta a fost achitat. În conformitate cu jurisprudența instanțelor, dispozițiile relevante percheziției și ridicării de documente se aplică, de asemenea, *mutatis mutandis* percheziției datelor electronice. În situația în care utilizatorul sistemului informatic ori a mijlocului de stocare, se opune percheziției, dispozitivele respective vor fi sigilate, iar instanța va decide cu privire la relevanța lor.

Reclamantul a argumentat că achitarea sa a arătat că nu a existat niciun temei rezonabil pentru a fi suspectat. În opinia

Curtea a constatat că percheziţia informatică a constituit o ingerinţă în dreptul reclamantului la respectarea vieții private și de familie, protejat de art. 8 din Convenţie. Astfel, Curtea a verificat în continuare dacă măsura care a făcut obiectul plângerii a fost „necesară într-o societate democratică", cu alte cuvinte, dacă relaţia dintre scopul urmărit și mijloacele folosite poate fi considerată proporţională. În cauze asemănătoare, Curtea a examinat dacă dreptul și practica interne ofereau garanţii adecvate și eficiente împotriva oricărui abuz (a se vedea, de exemplu, Société Colas Est și alţii). Pentru aceasta s-a considerat că prezintă importanţă următoarele elemente: dacă percheziţia s-a bazat pe un mandat emis de un judecător și pe o suspiciune rezonabilă; dacă domeniul de aplicare a mandatului era limitat în mod rezonabil; și – în ceea ce privea percheziţia unui birou de avocatură – dacă a fost realizată în prezenţa unui observator independent pentru a se asigura respectarea secretului profesional. În cazul de faţă percheziţia informatică a fost întemeiată pe un mandat emis de judecător în cursul unui proces penal cu privire la săvârșirea infracțiunilor de furt calificat, înșelăciune în formă calificată și delapidare. Robathin era inculpat în cauză, cercetat cu privire la săvârșira infracțiunii de furt. Mandatul oferea detalii privind pretinsele acte, momentul comiterii lor și daunele cauzate. Curtea a respins așadar argumentul reclamantului privind faptul că achitarea sa a indicat lipsa unei suspiciuni rezonabile încă de la început. Mai degrabă, existenţa suspiciunii rezonabile urmează să fie apreciată la momentul emiterii mandatului de percheziţie. În circumstanţele descrise anterior, Curtea a considerat că mandatul de percheziţie se baza, în mod corect, pe suspiciunea rezonabilă de la acea vreme. Faptul că reclamantul a fost în cele din urmă achitat, trei ani mai târziu, nu poate schimba această apreciere. Revenind la întrebarea dacă domeniul de aplicare a mandatului era limitat în mod rezonabil, Curtea a apreciat că mandatul de percheziţie era formulat în termeni foarte generali.

Curtea a constatat deja în cauza Wieser and Bicos Beteiligungen GmbH că legea în Austria prevede următoarele garanţii procedurale în privinţa percheziţiei informatice: (a) ocupantul biroului va fi prezent; (b) un raport va fi întocmit la sfârșitul percheziţiei; (c) dacă proprietarul se opune percheziției, datele digitale vor fi sigilate și trimise judecătorului pentru a hotărî dacă vor fi folosite sau nu în procesul penal; și (d) în cazul percheziţiei unui birou de avocatură, este necesară prezenţa unui reprezentant al Baroului. Curtea a reținut că, în cauză, scopul mandatului ar fi trebuit să se limiteze la relația dintre reclamant şi "R" şi "G". Astfel, Curtea a constatat că trebuia să existe motive întemeiate pentru a permite percheziţia tuturor celorlalte date, având în vedere circumstanța specială a realizării percheziției cu privire la un birou de avocatură. Totuși, în cazul de faţă, nu au existat asemenea motive nici în mandatul de percheziţie nici în orice alt document. În aceste împrejurări, examinarea tuturor datelor a depășit ce era necesar într-o societate democratică pentru îndeplinirea scopului legitim. Prin urmare, concluzia a fost aceea că art. 8 din Convenţie a fost încălcat.

În doctrină s-a mai arătat că subzistă, în toate cazurile, obligația respectării secretului profesional al avocatului, care poate fi opus în condițiile legii atât percheziționării, cât și ridicării de obiecte și înscrisuri cu caracter profesional, cu excepția cazurilor în care ar exista date privind pregătirea sau săvârșirea de către avocat a unor infracțiuni.[120] De asemenea, conform art. 35 alin. (1^1) introdus prin Legea nr. 25/2017 privind modificarea și completarea Legii nr. 51/1995 pentru organizarea și exercitarea profesiei de avocat, „sunt exceptate de la măsura ridicării de înscrisuri şi de la măsura confiscării: a) înscrisurile care conţin comunicări între avocat şi clientul său; b) înscrisurile care conţin consemnări efectuate de către avocat cu privire la aspecte referitoare la apărarea unui client".

Art. 169 C.proc.pen. permite ridicarea sistemului informatic, organul de urmărire penală sau instanța având obligația să procedeze în acest sens dacă obiectele și înscrisurile pot servi ca mijloc de probă în procesul penal. Astfel, ridicarea sistemului informatic se realizează independent de efectuarea percheziției informatice, deci fără a fi supusă regulilor acesteia din urmă. Cu toate acestea, ridicarea sistemului informatic sau a mijlocului de stocare este lipsită de rațiune în cazul în care nu este urmată de efectuarea percheziției informatice, astfel încât să fie identificate datele digitale care au valoare probantă.

Cu privire la copierea (clonarea) datelor informatice, operațiune necesară, care se interpune între ridicarea sistemului informatic ori a mijlocului de stocare și efectuarea percheziției informatice, este necesar a se identifica natura acestei operațiuni pentru a se stabili dacă se poate sau nu realiza în lipsa mandatului de

reclamantului, achitarea confirmă faptul că percheziția informatică a fost disproporționată, dacă nu chiar arbitrară.

[120] G. Mateuț, D. Nițu, L. Criste, *Aspecte actuale de drept și procedură penală, cit. supra.,* p. 63.

percheziție informatică. Apare astfel întrebarea dacă activitatea de copiere (clonare) a datelor informatice este parte integrantă din întregul procedeu probatoriu al percheziției informatice. Dacă răspunsul este negativ, atunci realizarea de copii (clone) iese de sub protecția garanțiilor acordate utilizatorului al cărui sistem informatic este supus percheziției.[121]

Jurisprudența a cunoscut ambele răspunsuri, astfel că în cauza Scarfo, s-a reținut copierea (clonarea) ca fiind o activitate de percheziție, pe când, în cauza Gorshkov concluzia a fost diferită. Din rațiuni de protecție a datelor informatice și a utilizatorului, dat fiind faptul că percheziția reprezintă un procedeu susceptibil să aducă atingeri grave dreptului la viață privată al utilizatorului, copierea (clonarea) datelor ar trebui considerată ca fiind o activitate corespunzătoare efectuării percheziției informatice.[122] Prin urmare, clonarea datelor informatice, în scopul obținerii de probe digitale, ar trebui să fie inclusă în procedeul probatoriu al percheziției informatice, fiind obligatorie prezența suspectului sau a inculpatului la realizarea acesteia. Astfel cum se arată în literatura de specialitate, percheziția informatică se finalizează în momentul în care datele informatice, considerate a fi relevante cauzei, au fost transferate într-o sursă externă, aflându-se la dispoziția organului de urmărire penală. Analiza ulterioară a probelor digitale excede cadrului percheziției informatice, cu posibilitatea ca operațiunea să se extindă și după expirarea termenului prevăzut în mandatul de percheziție informatică.[123] Așadar, după momentul identificării și strângerii probelor digitale, sfera activității la care suspectul ori inculpatul are dreptul să asiste este depășită. Astfel, deși prevederile art. 168 alin. (11) C.proc.pen. instituie obligativitatea și totodată dreptul suspectului ori inculpatului de a asista la percheziția informatică, după încheierea procesului-verbal și resigilarea mediilor percheziționate, în măsura în care acestea nu sunt restituite în baza art. 162 alin. (4) C.proc. pen., percheziția informatică s-a încheiat.[124]

Cu privire la restituirea mediilor informatice ridicate, este esențial ca acestea să fie înapoiate utilizatorului într-un termen rezonabil, astfel încât să nu fie încălcat dreptul la proprietate al utilizatorului. Un exemplu în acest sens este oferit de cauza Smirnov c. Rusia[125]. În speță, reclamantul a susținut, printre altele, și încălcarea dreptului la proprietate, protejat de art. 1 Protocol 1 din Convenție, întrucât unitatea centrală ridicată nu putea fi folosită, prin ea însăși, ca probă în procesul penal. Aceasta nu era obiect, produs sau instrument al infracțiunii și nici nu conținea urme ale infracțiunii.

Mai mult, datele digitale stocate erau lipsite de valoare probantă din cauza faptului că unitatea centrală, fiind în posesia organului de urmărire penală pentru o perioadă îndelungată, asupra datelor plana suspiciunea de a fi fost modificate sau șterse. Reclamantul a susținut că ridicarea sistemului informatic l-a împiedicat pe acesta să aibă acces la mai mult de 200 de date privitoare la clienți, aducând prejudicii cu privire la activitatea sa profesională, desfășurată în domeniul legal, privită în ansamblu. Este indiscutabil faptul că reclamantul era deținătorul legal al sistemului informatic, și se afla în posesia legitimă a acestuia, astfel încât situația nu poate fi încadrată în dreptul statului de a verifica dreptul de proprietate asupra sistemului informatic, în conformitate cu interesul general. Cea mai importantă cerință în respectarea art. 1 din Protocol 1 este ca orice ingerință a autorității publice cu privire la posesia liniștită să fie legitimă. Curtea admite că reținerea de probe fizice este necesară într-o societate democratică, dar acestă măsură trebuie să fie proporțională cu scopul urmărit. Se constată că sistemul informatic era utilizat în desfășurarea profesiei de avocat, fiind stocate date informatice cu privire la clienți. Ridicarea sistemului informatic nu doar că a cauzat reclamantului inconveniente de ordin personal, dar a împiedicat și realizarea activității lui profesionale, determinând consecințe negative asupra înfăptuirii justiției. Prin urmare, curtea constată încălcarea art. 1 protocol 1 din Convenție.

Raportul dintre art. 170 alin. (1) C.proc.pen. și percheziția informatică este și el problematic. Conform art. 170 alin. (1) C.proc.pen., „în cazul în care există o suspiciune rezonabilă cu privire la pregătirea sau săvârșirea unei infracțiuni și sunt temeiuri de a se crede că un obiect ori un înscris poate servi ca mijloc de probă în cauză, organul de urmărire penală sau instanța de judecată poate dispune persoanei fizice sau juridice în posesia căreia se află să le prezinte și să le predea, sub luare de dovadă". Astfel, este prevăzută în textul legal posibilitatea

[121] S. W. Brenner, B. A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, în „Michigan Telecommunications and Technology Law Review", vol. 8, nr. 1, 2002, p. 108, disponibil online la adresa *http://repository.law.umich.edu/mttlr/vol8/iss1/2.*

[122] *Idem*, p. 113.

[123] G. Zlati, *Percheziția sistemelor informatice și a mijloacelor de stocare a datelor informatice (I), cit. supra.,* p. 23.

[124] *Idem,* p. 23-24.

[125] *Hotărârea din 12.11. 2007 (cererea nr 71362/01).*

remiterii benevole de probe, prin conformarea persoanelor fizice sau juridice cu privire la dispozițiile organului judiciar.[126]

Având în vedere argumentele prezentate în literatura de specialitate, și expuse anterior, cu privire la privilegiul contra autoincriminării, textul nu își poate găsi aplicabilitatea în situația în care persoana fizică sau juridică are calitatea de suspect sau de inculpat în cauză. Astfel, prevederile art. 170 alin. (1) C.proc.pen. pot fi invocate cu succes numai în ipoteza în care probele digitale se află în posesia unui terț față de infracțiunea în legătură cu care există suspiciuni rezonabile că se pregătește săvârșirea ei ori că a fost săvârșită. În toate cazurile, avocatul ar trebui sa fie îndreptățit să refuze predarea obiectelor, înscrisurilor sau a datelor informatice. Având în vederea argumentele cu privire la percheziția domiciliară ori ridicarea de obiecte în cazul avocatului, și reamintind că ridicarea ori percheziția se pot dispune în cazul acestuia numai pentru probarea faptului că avocatul este implicat în săvârșirea faptei prevăzute de legea penală, în caz contrar fiind încălcat secretul profesional, și considerând că în situația suspectului ori a inculpatului nu poate fi incident art. 170 alin. (1) fără a se încălca privilegiul contra autoincriminării, rezultă faptul că avocatul trebuie să fie întotdeauna exclus de la aplicarea art. 170 alin. (1) C.proc.pen.

Extrem de problematică este situația desfășurării urmăririi penale in rem, caz în care calitatea de suspect sau inculpat nu este încă atribuită. La fel de multe semne de întrebarea apar și în cazul terțului care se află în posesia de date digitale care pot constitui probe informatice ale implicării acestuia în săvârșirea infracțiunii. Asemănător, este posibil ca datele digitale să conțină probe ale implicării terțului în alte activități infracționale, decât cele care fac obiectul cauzei, caz în care practic terțul trebuie să facă o selecție a datelor informatice pe care urmează să le prezinte organului de urmărire penală ori instanței. Obligarea terțului să selecteze datele informatice care pot dovedi implicarea acestuia în activități infracționale ar trebui să declanșeze, și în aceste cazuri, activarea privilegiului contra autoincriminării. Astfel, privilegiul contra autoincriminării apare ca un refugiu care îl îndreptățește pe posesorul datelor electronice să refuze predarea acestora organului de urmărire penală ori instanței. De principiu, aplicarea art. 170 alin. (1) C.proc.pen. înlocuiește practic prima etapă a percheziției informatice, efectuarea de copii (clone) a datelor informatice.

9. Efectuarea de copii (clone) pentru asigurarea integrității datelor informatice

O altă garanție, în vederea asigurării integrității datelor informatice stocate în mediul informatic ridicat ori pe mijlocul de stocare, o reprezintă efectuarea de copii (clone), obligație instituită în cadrul prevederilor art. 168 alin. (9) C.proc.pen. În literatura de specialitate, se arată că realizarea clonelor către specialist sau organul de poliție specializat, se fundamentează pe ordonanța emisă de către procuror, fiind deopotrivă necesară existența unui mandat de percheziție informatică. Prin urmare, reglementara obligației de efectuare a clonelor impune existența unui mandat de percheziție informatică anterior emis, astfel încât copierea devine parte integrantă a percheziției informatice, fiind aplicabile toate garanțiile corespunzătoare percheziției, dintre care cea mai importantă este prezența suspectului sau a inculpatului la efectuarea acestei activități.

De cele mai multe ori, procesul de obținere a clonei se realizează prin conectarea mijlocului de stocare ce urmează a fi supus copierii la un dispozitiv de tip write blocker. Cel din urmă dispozitiv este, la rândul său, conectat la sistemul informatic aparținând specialistului ori lucrătorului de poliție specializat. Pentru efectuarea propriu-zisă a clonei se recurge la rularea unor programe informatice specifice precum EnCase Forensic ori Forensic ToolKit.[127] Realizarea unei clone a mediului informatic se impune și atunci când ridicarea obiectelor care conțin date informatice este susceptibilă să afecteze grav activitatea utilizatorului, consecință care apare ca iminentă încă din momentul efectuării percheziției domiciliare. În astfel de situații nu se va proceda la ridicarea obiectelor care conțin datele informatice ci se vor aplica prevederile art. 168 alin. (10) C.proc.pen., procurorul având facultatea de a dispune efectuarea de copii (clone) care servesc ca mijloc de probă.

În pofida faptului că textul indică o opțiune a procurorului, îndeplinirea acesteia este condiționată fie de existența unui mandat de percheziție informatică, fie de consimțământul titularului sistemului informatic ori a mijlocului de stocare în cauză. În mod obișnuit, în momentul efectuării percheziției domiciliare nu există un mandat de percheziție informatică, astfel încât procurorul nu poate decide să aplice art. 168 alin. (10) C.PROC. PEN. decât cu acordul titularului sistemului informatic ori a mijlocului de stocare.[128]

[126] M. Udroiu (coordonator), *Codul de procedură penală. Comentariu pe articole,* C.H. Beck, București, 2015, p. 495.
[127] G. Zlati, *Percheziția sistemelor informatice și a mijloacelor de stocare a datelor informatice (I), cit. supra*., p. 22.
[128] *Idem*, p. 24, nota 5.

În practică pot să apară și situații în care, deși ridicarea mediilor informatice nu este susceptibilă să afecteze grav activitatea utilizatorului, nu se poate proceda în acest sens din cauza faptului că oprirea sistemului va determina pierderea unor probe digitale, precum sunt fișierele temporare sau memoria RAM (random access memory).[129] De asemenea, în anumite ipoteze, oprirea sistemului informatic poate determina inițierea funcţiei de criptate, astfel încât va fi generat un conţinut inaccesibil.[130] Criptarea datelor informatice transformă procedeul probatoriu al percheziției informatice într-o activitate lipsită de obiect. Efectuarea unei clone a mediului informatic ori a suportului de stocare al datelor informatice își pierde utilitatea, având în vedere faptul că și copia va cuprinde același conținut criptat, precum sursa datelor digitale. Rezultă, astfel, imposibilitatea finalizării procedeului probatoriu atât timp cât conținutul criptat nu poate fi supus analizei, deci nu pot fi identificate probele digitale cu relevanță în cauză.[131] Aceste inconveniente pot să își găsească rezolvarea în realizarea, de către organele de urmărire penală, a unei copii de la distanţă (remote imaging) sau în efectuarea percheziției informatice la distanță, pe sistemul informatic activ. Astfel, pe de o parte nu se vor pierde datele informatice volatile, iar pe de altă parte conţinutul obţinut nu va fi unul criptat. Această activitate nu este însă lipsită de dificultăți.

În primul rând, trebuie să existe un mandat de percheziţie informatică care să vizeze exact sistemul informatic ce urmează să fie supus acestei percheziţii „în timp real".

Îl al doilea rând, este necesar să se procedeze în așa fel încât să nu fie modificate date informatice stocate pe sistemul percheziţionat „în timp real". Se are în vedere faptul că nu pot fi utilizate dispozitive hardware de tip write blocker, astfel cum se procedează de regulă, fiind necesar să se utilizeze instrumente software.

Prin urmare, în literatura de specialitate a fost identificată soluția conectării în paralel a sistemului percheziţionat cu un sistem informatic de pe care se va realiza percheziţia informatică efectivă. Interacţiunea directă cu sistemul informatic vizat este strict interzisă, având în vedere faptul că o asemenea intervenţie produce modificări raportat la nivelul datelor informatice respective.[132] Este de precizat faptul că în literatura de specialitate s-a apreciat că art. 168 alin. (10) reprezintă o derogare de la prevederile art. 168 alin. (9), cu relevanță în contextul efectuării percheziției domiciliare.[133] După efectuarea de copii (clone), specialistul va interacționa doar cu acestea, în literatura de specialitate, considerându-se că întotdeauna activitățile specifice art. 168 alin. (1) C.proc.pen. vor fi efectuate asupra copiei (clonei) obținute în conformitate cu dispozițiile legale. Realizarea unei copii (clone) asupra căreia să fie ulterior efectuate activitățile de percheziție informatică propriu-zisă prezintă relevanță și în contextul apariției unor suspiciuni de alterare a datelor informatice, caz în care există posibilitatea verificării autenticității respectivei copii.[134]

În doctrină se consideră necesară sigilarea corespunzătoare a sistemelor informatice și a mijoacelor de stocare identificate. Existența unui contact extern ulterior cu acestea va conduce la apariția de suspiciuni care vor plana asupra autenticității probelor digitale identificate. Spre exemplu, ultima intervenție asupra sistemului informatic prin deschiderea acestuia generează probe digitale cu privire la ultima accesare a sistemului informatic (reprezentând o variabilă timestamp), care poate fi obținută prin intermediul unor programe informatice specifice, precum EnCase Forensic, în momentul analizării fişierelor de sistem ce stochează această informaţie. Cu toate acestea, în situația în care sistemul informatic este dezasamblat și conectat la un dispozitiv de tip write blocker, apar dificultăți în identificarea momentului în care datele informatice au fost accesate sau copiate în altă sursă, din moment ce accesarea și copierea în acest mod a datelor se realizează în condiții de siguranță.

Din această cauză, se poate realiza, în mod nelegal, o percheziție informatică în lipsa unui mandat. Situația este îngrijorătoare din perspectiva respectării drepturilor suspectului sau ale inculpatului de a fi prezenți la efectuarea percheziției. Astfel, deși eventualele probe digitale obținute prin efectuarea percheziției informatice în mod nelegal vor fi excluse conform art. 102 alin. (2) C.proc.pen., a existat posibilitatea de a fi

---

[129] *Idem*, p. 27.

[130] E. Casey, G. Fellowa și colab., *The growing impact of full disk encryption on digital forensics*, în „Digital Investigation", nr. 8, 2011, p. 129-134.

[131] G. Zlati, *Privilegiul contra autoincriminării și criptografia, cit. supra.,* p. 25.

[132] M. Udroiu, *Procedură penală. Partea generală – Noul Cod de procedură penală*, C.H. Beck, București, 2014, p. 299. A se vedea *Idem,* nota de subsol nr. 1, p.300.

[133] M. Udroiu, G. Zlati, Comentariu în M. Udroiu (coord.), *op. cit.,* p. 848.

[134] *Idem,* p. 849.

obținute date care nu ar fi fost obținute în alt mod.[135] Sigilarea se impune și cu privire la copia (clona) efectuată în baza art. 168 alin. (9) sau alin. (10) C. proc. pen., luând în considerare faptul că omisiunea sigilării poate permite specialistului ori lucrătorului de poliție specializat obţinerea de date informatice suplimentare, în afara procedurii percheziţiei informatice.[136] Prin urmare, este necesar să se prevadă expres obligativitatea sigilării, atât a mediilor informatice ori a mijloacelor de stocare a datelor informatice ce urmează a fi supuse percheziției informatice, cât și a copiei efectuate în considerarea art. 168 alin. (9) și (10) C. proc. pen. În cauza Robathin c. Austria, se observă că sigiliarea datelor informatice este tratată de către organele judiciare ca un lucru firesc și necesar.

10. Posibila neconstituționalitate a prevederilor art. 168 alin. (12) C.proc.pen.

Analizând art. 168 alin. (12) C.proc.pen. din perspectiva garanțiilor pe care textul legal trebuie să le confere celui care urmează a fi percheziționat, apare întrebarea dacă textul legal este constituțional sub aspectul previzibilității și al clarității normei în măsura în care percheziția informatică este efectuată de un specialist care funcționează în afara organelor judiciare. Percheziția informatică determină o ingerință semnificativă în viața privată, astfel încât această activitate trebuie să fie foarte bine circumscrisă pentru a garanta respectarea drepturilor fundamentale ale persoanei care urmează a fi percheziționată. Un text lipsit de previzibilitate este foarte probabil să încurajeze abuzul. În formularea unui răspuns la adresa constituționalității art. 168 alin. (12) C.proc.pen. este relevantă Decizia 51 din 16 februarie 2016 a Curții Constituționale cu privire la supravegherea tehnică. În motivarea excepţiei de neconstituţionalitate se susţine că sintagma „alte organe specializate ale statului" din cuprinsul art.142 alin. (1) din Codul de procedură penală este lipsită de claritate, precizie și previzibilitate, astfel încât textul criticat contravine prevederilor art.1 alin. (5) din Constituţie. Lipsa de claritate, previzibilitate și precizie provine din faptul că dispoziţiile Codului de procedură penală nu precizează exact care sunt organele care intră în categoria „altor organe specializate ale statului" și care pot efectua supravegherea tehnică, conform art.142 alin. (1) din Codul de procedură penală, alături de procuror, de organele de cercetare penală și de lucrătorii specializaţi din cadrul poliţiei.

Se susţine că formularea criticată creează posiblilitatea ca Serviciul Român de Informaţii să efectueze acte de procedură în cadrul procesului penal, prin interceptarea și înregistrarea de convorbiri în cauzele penale, fapt care este inacceptabil din moment ce aceste servicii secrete ale statului nu sunt organe de urmărire sau de cercetare penală, nefiind prevăzute, ca atare, în Codul de procedură penală. Din acest considerent, posibilitatea participării lor la realizarea actelor de urmărire sau de cercetare penală lipsește de claritate, precizie și previzibilitate dispoziţiile procesual penale care reglementează punerea în executare a mandatului de supraveghere tehnică, (aceeași suspiciune planând și asupra percheziției informatice). Pentru aceleași considerente, se susţine că textul criticat contravine prevederilor art.21 din Constituţie și art.6 din Convenţie.

De asemenea, întrucât supravegherea tehnică (precum și percheziția informatică) este o măsură procesual penală ce are ca efect o restrângere a vieţii private și de familie, se susţine că lipsa de precizie și previzibilitate a normei referitoare la punerea în executare a mandatului este de natură a încălca dreptul fundamental prevăzut la art. 8 din Convenţie, precum și încălcarea prevederilor art. 20 și art. 53 din Constituţie. Curtea a aratat că actele îndeplinite de organele prevăzute la art.142 alin.(1) teza a doua din C.proc.pen. reprezintă procedee probatorii care stau la baza procesului-verbal de consemnare a activităţii de supraveghere tehnică, ce constituie un mijloc de probă. Pentru aceste motive, organele care pot participa la realizarea acestora sunt numai organele de urmărire penală. Curtea constată că legiuitorul a inclus, în cuprinsul art.142 alin.(1) C.proc.pen., pe lângă procuror, organul de cercetare penală și lucrătorii specializaţi din cadrul poliţiei și a altor organe specializate ale statului.

Aceste organe specializate ale statului nu sunt definite, nici în mod expres, nici în mod indirect în cuprinsul Codului de procedură penală. De asemenea, norma criticată nu prevede nici domeniul de activitate specific acestora. Având în vedere aceste argumente, Curtea reţine că sintagma „ori de alte organe specializate ale statului" apare ca fiind lipsită de claritate, precizie și previzibilitate, nepermiţând subiecţilor să înţeleagă care sunt aceste organe abilitate să realizeze măsuri cu un grad ridicat de ingerință în viaţa privată a persoanelor.

În concluzie, având în vedere aceste argumente și caracterul intruziv al măsurilor de supraveghere

[135] G. Zlati, *Percheziția sistemelor informatice și a mijloacelor de stocare a datelor informatice (I), cit. supra.,* p. 26.

[136] G. Zlati, *Privilegiul contra autoincriminării și criptografia, cit. supra.*, p. 40-41.

tehnică, Curtea a constatat că este obligatoriu ca aceasta să se realizeze într-un cadru normativ clar, precis și previzibil, atât pentru persoana supusă acestei măsuri, cât și pentru organele de urmărire penală și pentru instanţele de judecată. În caz contrar, s-ar ajunge la posibilitatea încălcării într-un mod abuziv a unora dintre drepturile fundamentale esenţiale într-un stat de drept: viaţa intimă, familială și privată și secretul corespondenţei. Drepturile prevăzute la art. 26 și art. 28 din Constituţie nu sunt absolute, însă limitarea lor trebuie să se facă cu respectarea dispoziţiilor art. 1 alin. (5) din Legea fundamentală, iar gradul de precizie a termenilor și noţiunilor folosite trebuie să fie unul ridicat, dată fiind natura drepturilor fundamentale limitate. Așadar, standardul constituţional de protecţie a vieţii intime, familiale și private și a secretului corespondenţei impune ca limitarea acestora să se realizeze într-un cadru normativ care să stabilească expres, într-un mod clar, precis și previzibil care sunt organele abilitate să efectueze operaţiunile care presupun un grad ridicat de ingerință.[137]

În literatura de specialitate s-a evidențiat, de asemenea, o problemă de compatibilitate a dispozițiilor art. 168 alin. (12) C.proc.pen. raportate la D.C.C. nr. 315/2016. Prin decizia menționată Curtea a arătat că funcționarea în cadrul instanțelor și a parchetelor a unor specialiști are scopul de a sprijini activitatea judecătorilor și a procurorilor prin clarificarea aspectelor tehnice. Efectuarea unei percheziții informatice presupune, însă, mai mult decât o simplă contribuție tehnică. În concret, nu se poate afirma că percheziția informatică se limitează la clarificarea de aspecte de natură tehnică. Astfel, activitatea specialiștilor la care face referire art. 168 alin. (12) C.proc.pen. implică efectuarea de acte de urmărire penală – cercetare, descoperire, identificare, strângere de probe digitale – sub supravegherea organelor de urmărire penală. În urma activităților întreprinse de specialist, se vor obține mijloace de probă – date informatice relevante. Urmând același raționament, este evidentă neconcordanța dintre art. 168 alin. (12) și D.C.C. nr. 51/2016 în ipoteza în care specialistul care efectuează percheziția informatică realizează un act de urmărire penală prin care aduce atingeri grave dreptului la viață privată. Este de precizat faptul că art. 55 C.proc.pen. nu menționează specialistul printre organele de urmărire penală. Mai mult, art. 168 alin. (12) permite participarea inclusiv a specialistului din afara organelor judiciare. Comparativ, în cazul supravegherii tehnice nu este permisă punerea în executarea a mandatului de supraveghere tehnică de către specialiști. Astfel, spre deosebire de percheziția informatică, conform art. 142 alin. (1) C.proc.pen., punerea în executarea a mandatului de supraveghere tehnică se realizează de către procuror, organul de cercetare penală ori lucrători specializați din cadrul poliției.[138]

Cu privire la raportul dintre dispozițiile art. 168 alin. (12) C.proc.pen. și prevederile art. 168[1] C.proc. pen., în doctrină s-a apreciat ca fiind discutabilă referirea din cadrul art. 168[1] la reglementarea prevăzută de art. 168 alin. (12), atât timp cât ambele fac referire strict la competența persoanelor care pot efectua percheziția informatică. S-a apreciat, astfel, ca fiind mai potrivit a se face referire în cadrul art. 168[1] C.proc.pen. la prevederile art. 168 alin. (1) C.proc.pen. și la dispozițiile art. 168 alin. (9) C.proc.pen. În privința complementarității dintre art. 168 alin. (12) și art. 168[1] C.proc.pen. s-a apreciat că art. 168[1] servește la o extindere a competenței de efectuare a percheziției informatice și cu privire la lucrătorii de poliție specializați. Concluzia extinderii competenței reiese din statutul diferit al organelor abilitate să efectueze percheziția informatică. Lucrătorii specializați la care face referire art. 168[1] C.proc.pen. sunt organe de cercetare penală ale poliției judiciare, iar specialiștii din cadrul organelor de urmărire penală sunt ingineri cu statut de funcționari publici.[139]

11. Efectuarea percheziției informatice în lipsa autorizării instanței

Problema care apare este aceea în ce măsură se poate proceda la efectuarea de activități corespunzătoare activităților pe care le presupune o percheziție informatică, în lipsa unei autorizări din partea judecătorului de drepturi și libertăți, respectiv din partea instanței, deci în lipsa unui mandat de percheziție informatică. O primă ipoteză este aceea în care operațiunile efectuate au ca obiect accesul la informații, iar nu conținutul propriu-zis al comunicațiilor. Astfel, informațiile sunt transmise de furnizori care au obligația de a coopera cu organele judiciare potrivit art. 170 alin. (2) C.proc.pen. De exemplu, furnizorul de servicii de telefonie mobilă, la cerere, este obligat să furnizeze organelor judiciare lista cu apelurile efectuate de către persoana vizată, fără însă ca organul judiciar să poată obține transcrierea unora dintre aceste conversații.[140]

[137] A se vedea site-ul *https://www.ccr.ro/files/products/Decizia_51_2016.pdf.*

[138] M. Udroiu, G. Zlati, Comentariu în M. Udroiu (coord.), *op. cit.,* p. 859.

[139] *Idem,* p. 860-861.

[140] A se vedea site-ul *http://www.juridice.ro/24841/cat-de-adanc-pot-intra-procurorii-diicot-in-computerele-private-precizarile-*

Prin urmare, procurorul poate solicita doar informații despre traficul comunicărilor electronice dintre două sau mai mult persoane, mai exact despre existența unei corespondențe electronice între persoane. Informațiile solicitate privesc existența si numărul e-mailurilor, iar nu conținutul acestora. În schimb, în cazul în care se confirmă existența unei corespondențe electronice între persoanele vizate, în contextul cercetării unor infracțiuni, procurorul dorind acces la conținutul acesteia, va solicita judecătorului emiterea autorizației pentru percheziționarea sistemului informatic ori a mijlocului de stocare, operațiune în cadrul căreia pot fi citite e-mailurile stocate. Această informație primară, dacă există corespondența electronică între două sau mai multe persoane, va fundamenta solicitarea încuviințării, procurorul dovedind în fața judecătorului de drepturi și libertăți ori a instanței că există corespondență electronică între respectivele persoane.

O altă situație de acces a procurorului, fără o autorizație din partea instanței ori a judecătorului de drepturi și libertăți, este solicitarea de identificare a IP-urilor (numărul de identificare a calculatorului dintr-o rețea). De exemplu, în cazul în care pe un site sunt postate imagini pornografice, procurorul poate autoriza accesul la sistemul informatic doar pentru a identifica IP-urile celor care postează astfel de imagini. După aflarea IP-urilor, procurorul poate solicita emiterea unui mandat de percheziție informatică, dar fără identificarea sistemului informatic (în speță, a calculatorului), a sursei, este imposibilă solicitarea mandatului de percheziție informatică. Un alt exemplu, se referă la situația în care procurorul are indicii temeinice că un site este utilizat pentru a se comercializa droguri și solicită identificarea IP-urilor celor care au comunicat prin intermediul site-ului. Pentru a afla care este conținutul concret al comunicațiilor purtate între calculatoarele-sursa, procurorul trebuie sa solicite emiterea mandatului de percheziție informatică ori a unui mandat pentru supraveghere, interceptare sau înregistrare a comunicațiilor.[141]

De asemenea, ridică probleme și ipoteza în care utilizatorul unui sistem informatic care prezintă defecțiuni solicită unei persoane fizice sau entități juridice, repararea acestuia. Ce se întamplă în situația în care tehnicianul descoperă, în activitatea depusă în scopul reparării, imagini cu pornografie infantilă? Cel mai des, dovezile furnizate organelor judiciare de către cel care repară computerul, în sensul săvârșirii unei infracțiuni, sunt folosite pentru a justifica emiterea unui mandat în vederea efectuării percheziției informatice a întregului sistem informatic. Cu toate acestea, dovezile pe care le obține tehnicianul trebuie să se rezume la fotografierea ecranului prin intermediul altui dispozitiv, furnizând o înregistrare a ceea ce era afișat.

Tehnicianul nu va putea proceda la o investigare privată a sistemului informatic care conține probe ale infracțiunii, în caz contrar probele obținute de acesta vor fi lipsite de legalitate, neputând fi folosite în procesul penal. Chiar dacă este vorba și în acest caz despre un specialist în informatică, o investigație privată este exclusă întrucât nu ar putea să ofere suficiente garanții cu privire la respectarea drepturilor și libertăților fundamentale ale utilizatorului sistemului informatic. Cea mai evidentă încălcare a garanțiilor oferite de Codul de procedură penală este, în acest caz, încălcarea art. 168 alin. (10), care impune ca percheziția informatică să se desfășoare în prezența suspectului sau a inculpatului. În același timp, nu se va putea dovedi cu certitudine integritatea informațiilor obținute, așa cum pretinde art. 168 alin. (1), teza finală din C.proc.pen., cu atât mai mult cu cât nu se ține cont nici de prevederile alin. (9) sau (10) ale aceluiași articol, care indică efectuarea de copii (clone) pentru asigurarea integrității informațiilor.

Prin urmare, persoana însărcinată cu depanarea sistemului informatic, în măsura în care surprinde, în urma îndeplinirii obligațiilor asumate corespunzătoare activității de reparare, date informatice suspecte, va înceta orice interacțiune cu sistemul informatic pentru a nu compromite probele digitale și va anunța de îndată organul de urmărire penală care va proceda în consecință, cu respectarea exigențelor legale.

Un sistem informatic poate fi percheziționat, fără un mandat de percheziție dacă există consimțământul persoanei care urmează a fi percheziționată. Cu toate acestea, refuzul suspectului sau a inculpatului de a permite percheziția, la fel ca si refuzul de a da declarații, nu trebuie interpretat în defavoarea persoanei. Relevant în acest sens este art. 83 alin. (1) lit. a) C.proc.pen.[142] Cu toate astea, în cazul în care se obține consimțământul utilizatorului sistemului informatic în vederea efectuării percheziției, organul de urmărire penală este obligat

ministerului-justitiei.html.

[141] *Ibidem.*

[142] Art. 83 C.proc.pen. Drepturile inculpatului. „În cursul procesului penal, inculpatul are următoarele drepturi: a) dreptul de a nu da nicio declarație pe parcursul procesului penal, atrăgându-i-se atenția că dacă refuză să dea declarații nu va suferi nicio consecință defavorabilă, iar dacă va da declarații acestea vor putea fi folosite ca mijloace de probă împotriva sa."

să respecte limitele impuse de utlizator, fără a extinde această activitate la aspecte nevizate de consimțământ. Pentru aceste din urmă aspecte este necesar mandatul de percheziție informatică, ori un nou consimțământ din partea utilizatorului. Dincolo de aceste aspecte, trebuie avut în vedere faptul că utilizatorul poate să își revoce consimțământul până în momentul efectuării propriu-zise a percheziției informatice.[143]

Consimțământul provenit doar din partea unuia dintre utilizatorii sistemului informatic este valabil cu privire la acea porțiune destinată utilizării comune, atunci când sistemul informatic este folosit de mai multe persoane, astfel încât consimțământul unuia dintre ei îl va înlocui pe al celorlalți, iar probele obținute în acest fel sunt legale. Totuși, dacă unul dintre indivizi protejează documentele din aria comună cu o cheie de acces, consimțământul celorlalți utilizatori nu este valabil cu privire la aceste fișiere.[144] De asemenea, în situația în care computerul este folosit de ambii soți sau parteneri, fără a fi utilizat în baza unor conturi diferite și fără a fi protejat cu o cheie de acces cunoscută numai de unul dintre soți sau parteneri, dacă oricare dintre ei anunță autoritățile cu privire la săvârșirea unei infracțiuni și solicită autorităților să efectueze căutările necesare în sistemul informatic, un mandat de percheziție informatică nu este necesar deoarece există deja consimțământul unuia dintre utilizatori.[145]

Valabilitatea consimțământului utilizatorului sistemului informatic ori a mijlocului de stocare a datelor informatice în vederea efectuării de activități specifice percheziției informatice, în lumina Codului de procedură penală, a fost analizată cu ocazia întâlnirii reprezentanților ICCJ cu președinții secțiilor penale ale curților de apel, la Brașov, în perioada 4-5 iunie 2015. Astfel, „într-o opinie, s-a arătat că atunci când persoana își dă acordul pentru efectuarea percheziţiei (domiciliare sau informatice) aceasta va fi efectuată fără a mai fi necesară vreo autorizaţie din partea judecătorului, cu argumentarea că o persoană poate renunţa la garanţiile oferite de lege în materia protecţiei dreptului la viaţă privată și domiciliu. Într-o altă opinie, s-a arătat că autorizarea din partea judecătorului este obligatorie și în situaţia în care persoana în cauză consimte la efectuarea percheziţiei (domiciliare sau informatice). Participanţii la întâlnire au fost de acord cu cea de a doua opinie, deoarece textele legale incidente (art. 154 și art. 168 alin. 2 Cod de procedură penală) instituie reguli imperative și nu sunt prevăzute excepţii de la acestea. În ceea ce privește intenţia persoanei de a renunţa la garanţiile oferite de lege în materia protecţiei sale private, acesta se poate valorifica prin intermediul instituţiei predării obiectelor, înscrisurilor și a datelor informatice."[146]

În literatura de specialitate a fost analizată sancțiunea procesuală care intervine în cazul efectuării activităților specifice percheziției informatice în lipsa unui mandat de percheziție informatică, dar cu încuviințarea utilizatorului sistemului informatic ori a mijlocului de stocare a datelor informatice. S-a arătat că o asemenea situație reprezintă, în fapt, o încălcare competenței funcționale, atât timp cât efectuarea percheziției informatice poate fi dispusă numai de judecătorul de drepturi și libertăți ori de către instanța de judecată. Astfel, în considerarea acestei teze, sancțiunea procesuală care intervine este nulitatea absolută.[147]

VIII. CONCLUZII

De lege ferenda, activitatea specifică percheziției informatice nu poate face obiectul constatării tehnico-științifice; efectuarea de copii (clone), în considerarea art. 168 alin. (9) și alin. (10) C.proc.pen., presupune și sigilarea acestora; se impune, de asemenea, sigilarea mediilor informatice ori a mijloacelor de stocare a datelor informatice, ridicate; restituirea sistemului informatic ori a mijlocului de stocarea a datelor informatice, ridicate în temeiul art. 168 alin. (9) C.proc.pen. se realizează într-un termen rezonabil; posibilitatea dispunerii, de către procuror în cazuri excepționale, a efectuarii de copii (clone), cu obligația obținerii încuviințării ulterioare a judecătorului de drepturi și libertăți ori a instanței, care va realiza un control post factum cu privire la copiile (clonele) obținute; posibilitatea contestării modului de efectuare a percheziției informatice,

[143] E. Hagen, N Judish, H. M. Jarrett, M. W. Bailie, *Searching and seizing computers and obtaining electronic evidence in criminal investigations*, Computer Crime and Intellectual Property Section Criminal Division, Office of Legal Education Executive Office for United States Attorneys, 2009, p.17-18, disponibil online (https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf).

[144] *Ibidem,* p. 20.

[145] *Ibidem,* p. 21.

[146] Minuta întâlnirii reprezentanților ICCJ cu președinții secțiilor penale ale curților de apel, la Brașov, în perioada 4-5 iunie 2015 este disponibilă online (http://www.inm-lex.ro/fisiere/d_1032/Minuta%20intalnire%20presedinti%20sectii%20penale.pdf).

[147] M. Udroiu, G. Zlati, Comentariu în M. Udroiu (coord.), *op. cit.,* p. 857-858.

caz în care se va realiza un control post factum de către judecătorul de drepturi și libertăți, respectiv de către instanță, asupra copiilor (clonelor), sigilate, obținute; percheziția informatică se efectuează de către un lucrător de poliție specializat ori de către un specialist din cadrul organelor judiciare; posibilitatea avocatului de a fi prezent la efectuarea percheziției informatice, respectiv obligația ca un reprezentant al Baroului să fie prezent atunci când percheziția se realizează în legătură cu exercitarea profesiei de avocat; obligația ca utilizatorul sistemului informatic ori a mijlocului de stocare a datelor informatice să fie prezent la efectuarea percheziției informatice; efectuarea percheziției informatice în legătură cu exercitarea profesiei de avocat se realizează numai în prezența procurorului; percheziția informatică se efectuează cu respectarea secretului profesional și cu respectarea privilegiului contra autoincriminării; realizarea copiei (clonei) este o activitate specifică percheziției informatice; percheziția informatică se va dispune numai în cazuri excepționale, dacă a fost începută urmărirea penală in personam și există elemente serioase de vinovăție cu privire la suspect ori inculpat, iar efectuarea percheziției este dictată de puternice prezumții că pe această cale se vor descoperi probe în sarcina suspectului ori a inculpatului; mandatul de percheziție informatică poate fi folosit o singură dată; în mandatul de percheziție informatică se precizează și numele suspectului sau a inculpatului din cauza cu privirea la care s-a emis mandatul de percheziție informatică; mandatul cuprinde criterii în funcție de care se realizează percheziția informatică.

References / Bibliografie

Aaronson, L., Constitutional Restraints on Warrantless Cell Phone Searches, în „University of Miami Law Review", vol. 69, 2014.

Ahmed, S., Cloud Computing: Aspecte legate de contractare și comformitate pentru departamentele juridice interne, în „Revista română de drept al afacerilor", nr. 2/2014.

Bogdan, S., Șerban, D.A., Zlati, G., Noul Cod penal. Partea specială, Ed. Universul Juridic, București, 2014.

Brenner, S. W., Frederiksen, B. A., Computer Searches and Seizures: Some Unresolved Issues, în „Michigan Telecommunications and Technology Law Review", vol. 8, nr. 1, 2002.

Casey, E., Fellowa, G. și colab., The growing impact of full disk encryption on digital forensics, în „Digital Investigation", nr. 8, 2011.

Dobrinoiu, M., Comentariu, în V. Dobrinoiu și colab., Noul Cod penal comentat. Partea specială, vol. II, Ed. Universul Juridic, București, 2012.

Ghid introductiv pentru aplicarea dispozițiilor legale referitoare la criminalitatea informatică, București, 2004.

Goldfoot, J., The Physical Computer and the Fourth Amendment, în „Berkeley Journal of Criminal Law", vol. 16, nr. 1, 2011.

Grofu, N., Reflecții referitoare la percheziția informatică, în „Dreptul", nr. 6/2010.

Haagman, D, , Ghavalas, B., Trojan defense: A forensic view, în „Digital Investigation", nr. 2, 2005.

Hagen, E., Judish, N, Jarrett, H. M., Bailie, M. W., Searching and seizing computers and obtaining electronic evidence in criminal investigations, Computer Crime and Intellectual Property Section Criminal Division, Office of Legal Education Executive Office for United States Attorneys, 2009.

Ioniță, G.-I., Aspecte procesual penale și tehnice referitoare la percheziția informatică, în „Dreptul", nr. 12/2014.

Ioniță, G.-I., Infracțiunile din sfera criminalității informatice, ediția a II-a, Ed. Pro Universitaria, București, 2013.

Leția, A., Metode de investigare a criminalității informatice, în „Dreptul", nr. 12/2013.

Lucaci, I., Marin, R., Investigarea fraudelor informatice, Editura Ministerului de Interne, București, 2002.

Mateuț, G., Nițu, D., Criste, L., Aspecte actuale de drept și procedură penală, Hamangiu, București, 2015.

Mateuț, G., Tratat de procedură penală, Partea generală, vol. I, București, 2007.

Moise, A. C., Invetigarea criminalistică a infracțiunilor informatice, în „Dreptul", nr. 4/2009.

Moise, A. C., Metodologia investigării criminalistice a infracțiunilor informatice, Universul Juridic, București, 2011.

Ronen, E., Shamir, A., Extended Functionality Attacks on IoT Devices: The Case of Smart Lights, Weizmann Institute of Science, Rehovot, Israel.

S.M. Corradi, Be Reasonable! Limit Warrantless Smart Phone Searches to Gant's Justification for Searches Incident to Arrest, în „Case Western Reserve Law Review", vol 63, nr. 3, 2013.

Souvignet, T., Hatin, J., ș.a., Payment card forensic analysis: From concepts to desktop and mobile analysis tools, în „Digital Forensics", vol. 11, 2014.

Stancu, E., Tratat de criminalistică, ediția a IV-a, Universul Juridic, București, 2007.

Tanoviceanu, I., Dongoroz, V., Tratat de drept și procedură penală, vol. IV, Ediținea a doua, Curierul Judiciar, București, 1927.

Udroiu, M. (coord.), , Codul de procedură penală. Comentariu pe articole, ediția a II-a, C.H. Beck, București, 2017.

Udroiu, M. (coord.), Codul de procedură penală. Comentariu pe articole, C.H. Beck, București, 2015.

Udroiu, M., Procedură penală. Partea generală – Noul Cod de procedură penală, C.H. Beck, București, 2014.