

Incidența drepturilor fundamentale în procedura percheziției informatice

The prevalence of basic rights during the computer forensics procedure

Ioan Dumitru APACHIȚEI¹

Rezumat: Atât evoluția tehnologică, cât și diversificarea mijloacelor de utilizare a acestora creează atât oportunități cât și noi modalități de dovedire a infracțiunilor. Unul dintre cele mai utilizate mijloace de stabilire a vinovăției făptuitorului este reprezentat de percheziția informatică a unui sistem informatic ori a suportului de stocare a datelor informatice.

Având în vedere faptul că de regulă persoanele stochează pe dispozitivele mobile informații personale ori date confidențiale, aceasta determină necesitatea de a stabili care sunt drepturile fundamentale de care se poate prevala o persoană și limitele de ingerință în sfera de protecție. Verificarea acestor elemente a fost lăsată în sarcina judecătorului, motiv pentru care prin prezenta lucrare urmărim să propunem o serie de indicii pe care instanța să le aibă în vedere la soluționarea propunerii de încuviințare a efectuării percheziției informatice, în acord cu dispozițiile constituționale și procesual penale aplicabile.

Cuvinte-cheie: drepturi constituționale, percheziție informatică, sistem informatic, date confidențiale.

Abstract: The development of technology and the variety of ways it is applied provide up novel possibilities for criminal investigation and prosecutions. The computer search of an IT system or IT data storage environment is one of the most popular methods for proving the offender's guilt.

Given that most people keep private or sensitive information on their mobile devices, it is necessary to define the fundamental rights that are assertible as well as the boundaries of interference in the realm of protection. Since the judge was left to verify these elements, our goal in this paper is to present a set of indicators that the court should consider in order to decide whether to approve the computer search proposal in compliance with the relevant criminal procedural and constitutional provisions.

Keywords: constitutional rights, computer forensics procedure, IT system, sensitive information.

¹ Avocat în Baroul Iași, asist. univ. dr., Facultatea de Drept, Universitatea „Alexandru Ioan Cuza” din Iași, e-mail: ioan.apachitei@uaic.ro.

1. Incidența art. 23 alin. (2), 26 alin. (1), 27 alin. (3) și (4) și 72 alin. (2) din Constituția României

1.1. Aspecte generale

Trebuie specificat încă de la început faptul că în ansamblul dispozițiilor din Constituția României² nu se face referire în mod specific la noțiunea de percheziție informatică, ci doar la aceea de percheziție, fiind, astfel, incidente prevederile de la art. 23 alin. (2), art. 27 alin. (3) și (4), respectiv art. 72. Totodată, sunt avute în vedere și dispozițiile art. 8 din Convenția Europeană a Drepturilor Omului³ (în continuare C.E.D.O.) care reglementează dreptul la respectarea vieții private și de familie.

Privitor la corespondența dintre art. 23 și art. 27 din Constituție, s-a afirmat la nivelul doctrinei că „spre deosebire de art. 27 alin. (3) și (4), care se referă la percheziția domiciliară, art. 23 alin. (2) se referă la percheziția corporală”⁴. Pentru a stabili normele constituționale și convenționale incidente în materia percheziției informatice se impune mai întâi identificarea unor repere avute în vedere de legiuitorul fundamental, interpretate evolutiv.

Libertatea individuală (art. 23) implică atât obligația statului de a se abține de la orice acțiune prin care s-ar aduce atingere acestui drept, cât și obligația de a lua măsurile necesare pentru protejarea efectivă a dreptului persoanelor aflate sub jurisdicția sa. Libertatea individuală a mai fost înțeleasă atât prin raportare la libertatea fizică și de mișcare, cât și prin raportare la condițiile legale în care acest drept poate fi restrâns. Acest din urmă aspect conduce la cea de-a doua componentă prevăzută de alin. (1) al art. 23, reprezentată de siguranța persoanei, noțiune care presupune că atunci când statul reglementează măsuri de restrângere a libertății individuale, acestea să fie însoțite și de garanțiile necesare⁵.

În ceea ce privește percheziționarea, legiuitorul constituant s-a limitat doar la a preciza că este permisă „numai în cazurile și cu procedura prevăzută de lege” (art. 23 alin. (2)), lăsând, astfel, în sarcina legiuitorului ordinar obligația de a stabili cazurile, limitele și garanțiile în raport de care poate fi dispusă această măsură. Într-o opinie mult mai categorică și elocventă s-a reținut că „în privința percheziției, legea noastră fundamentală este destul de îngăduitoare: singura garanție pe care o instituie în favoarea libertății individuale constă în reglementarea prin lege a condițiilor și procedurilor de desfășurare a acesteia”⁶.

² Modificată și completată prin Legea nr. 429/2003 de revizuire a Constituției României, publicată în M. Of. nr. 758 din 29 octombrie 2003.

³ Consiliul Europei, semnată la data de 4 noiembrie 1950 la Roma, intrată la data de 3 septembrie 1953.

⁴ V. Cioclei în I. Muraru, E.S. Tănăsescu (coord.), *Constituția României. Comentariu pe articole*, ed. 2, Editura C.H. Beck, București, 2019, p. 236.

⁵ M. Safta, *Drept constituțional și instituții politice. Vol. I. Teoria generală a dreptului constituțional. Drepturi și libertăți*, ed. a VIII-a, Editura Hamangiu, București, 2023, p. 311.

⁶ M. Balan, *Drept constituțional și instituții politice. Vol. 1. Teoria generală a statului și a constituției. Constituția română în context european*, Editura Hamangiu, București, 2015, p. 373.

Art. 27 din Constituție are ca denumire marginală „inviolabilitatea domiciliului”, ceea ce particularizează conținutul reglementării la conceptele de „domiciliu” și „reședință”, excluzând parțial⁷ incidența instituției percheziției informatice. Cu toate acestea, alin. (3) al art. 27 impune condiția ca percheziția (domiciliară) să fie dispusă doar de către un judecător⁸, întrucât luarea măsurii presupune, în primul rând, o ingerință în dreptul la viață privată (art. 26). Astfel, este firesc ca și încuviințarea percheziției informatice să fie dispusă tot de către un judecător, având în vedere imperativul ocrotirii aceluiași drepturi fundamentale. În mod similar, la nivelul doctrinei s-a apreciat că prin conținutul art. 27 din Constituție „s-a dorit ca și celelalte cazuri cuprinse în art. 23, ca măsurile grave ce vizează persoana și drepturile sale să fie dispuse de judecător, perceput ca o autoritate independentă și imparțială în înfăptuirea justiției”⁹.

Din interpretarea sistematică a normelor constituționale amintite se remarcă o diferență între art. 23 alin. (2) și art. 27 alin. (3) sub aspectul organului competent să dispună percheziția. Astfel, textul revizuit al Constituției impune competența exclusivă a judecătorului de a dispune doar în privința percheziției domiciliare (art. 27 alin. (3)), în timp ce în ipoteza celorlalte forme de percheziție este lăsat la latitudinea legiuitorului ordinar să stabilească situațiile și procedura în care măsura poate fi dispusă. Dispozițiile art. 23 alin. (2) prevăd trei modalități de restrângere a libertății individuale, prin percheziționare, reținere și arestare (preventivă/la domiciliu), dintre acestea doar în cazul acesteia din urmă avem instituită la nivel constituțional condiția dispunerii de către judecător, conform alin. (4) al art. 23. Din ansamblul dispozițiilor enunțate rezultă că este de competența legiuitorului ordinar să stabilească competența funcțională a organului judiciar chemat să decidă cu privire la percheziția corporală, a unui vehicul și informatică. Aceste trei modalități de percheziție sunt reglementare în cuprinsul art. 165-168 C. proc. pen.¹⁰, dispoziții din care rezultă că doar în cazul percheziției informatice s-a impus obligativitatea dispunerii de către judecător.

1.2. Încuviințarea percheziției informatice în cazul deputaților și senatorilor

Art. 72 alin. (2) din Constituția României reglementează imunitatea parlamentară (imunitatea materială/inviolabilitatea)¹¹ conform căreia parlamentarul

⁷ *Idem.*, p. 372.

⁸ *Idem.*, p. 386. Autorul citat (nota 2) remarcă faptul că anteriori revizuirii Legii fundamentale percheziția trebuia încuviințată de către un „magistrat”, ceea ce presupunea și competența funcțională a procurorului.

⁹ A. Crișu în I. Muraru, E.S. Tănăsescu (coord.), *op. cit.*, p. 186.

¹⁰ Legea nr. 135/2010 privind Codul de procedură penală, publicată în M. Of. nr. 486 din 15 iulie 2010.

¹¹ În cuprinsul art. 20 alin. (1) din Legea nr. 96/2006 legiuitorul a definit imunitatea parlamentară ca reprezentând „ansamblul de dispoziții legale care asigură deputaților și senatorilor un regim juridic derogatoriu de la dreptul comun în raporturile lor cu justiția și în scopul de a le garanta independența”.

poate fi supus percheziției doar cu încuviințarea Camerei din care face parte¹². Imunitatea parlamentară având un regim de ordine publică nu poate fi suspendată/întreruptă, cum nici nu se poate renunța la aceasta¹³.

Privitor la procedura de încuviințare a percheziției, în doctrină s-a făcut trimitere doar la percheziția corporală și la cea domiciliară¹⁴, însă, norma constituțională poate și trebuie să fie interpretată în sensul în care este necesară încuviințarea și pentru efectuarea percheziției informatice, raționament confirmat și de practica parlamentară¹⁵.

Pentru realizarea percheziției informatice în cazul parlamentarilor este necesar ca în prealabil să fie obținută încuviințarea Camerei din care deputatul sau senatorul face parte, fiind aplicabilă procedura prevăzută de art. 24 din Legea nr. 96/2006 privind statutul deputaților și al senatorilor¹⁶. Astfel, Parchetul de pe lângă Înalta Curte de Casație și Justiție formulează cererea de încuviințare a percheziției parlamentarului, pe care o înaintează ministrului justiției și pe care acesta o comunică președintelui Camerei din care face parte parlamentarul. Președintele Camerei înștiințează Biroul permanent și transmite cererea către Comisia juridică care, în termen de 3 zile, întocmește raportul. Cererea ministrului justiției și raportul Comisiei juridice se supun spre dezbateră și adoptare plenului Camerei, în termen de 5 zile de la depunerea raportului. Hotărârea Camerei, astfel adoptată, se publică în Monitorul Oficial al României, Partea I, și se comunică de îndată ministrului justiției.

Cererea de încuviințare a percheziției pe care procurorul general al Parchetului de pe lângă Înalta Curte de Casație și Justiție o transmite ministrului justiției nu trebuie să fie identică sub aspectul formei cu cererea prin care procurorul de caz solicită judecătorului încuviințarea efectuării percheziției. Această diferență decurge din însăși natura controlului, în timp ce Camera competentă realizează un control exclusiv politic¹⁷, judecătorul analizează doar din punct de vedere al legalității și temeiniciei. De aici decurge consecința că cererea adresată judecătorului trebuie să cuprindă unele elemente specifice cum ar fi determinarea exactă a sistemului informatic sau a suportului de stocare a datelor informatice care urmează să fie percheziționate.

¹² Se mai remarcă din ansamblul dispozițiilor constituționale faptul că Președintele României se bucură de imunitate procedurală în ceea ce privește instituția percheziției, în temeiul art. 84 alin. (2) raportat la art. 72 alin. (1) din Constituție, cu omiterea intenționată a dispozițiilor art. 72 alin. (2).

¹³ Art. 21 alin. (1) din Legea nr. 96/2006.

¹⁴ I. Muraru, R. Popescu în I. Muraru, E.S. Tănăsescu (coord.), *op. cit.*, p. 628.

¹⁵ A se vedea, spre exemplificare, hotărârile Camerei Deputaților nr. 81 din 06.12.2021 și nr. 78 din 21.11.2022 prin care au fost încuviințate cererile de efectuare a perchezițiilor informatice.

¹⁶ Publicată în M. Of. nr. 49 din 22 ianuarie 2016.

¹⁷ C. Ionescu, *Tratat de drept constituțional contemporan*, ed. 3, Editura C.H. Beck, București, 2019, p. 1182.

Ulterior obținerii încuviințării din partea Camerei, procurorul de caz va solicita instanței să dispună efectuarea percheziției informatice. În ceea ce ne privește, apreciem că instanța nu este ținută de încuviințarea Camerei, putând să admită sau să respingă cererea procurorului.

S-a reținut la nivelul doctrinei că ridicarea imunității parlamentare este doar parțială, aceasta vizând doar faptele și actele pentru care a fost solicitată¹⁸. Astfel, apreciem că odată încuviințată cererea de percheziție privind faptele sau actele pentru care deputatul ori senatorul este urmărit penal aceasta permite dispunerea percheziției domiciliare/informatică în raport de obiectul dosarului de urmărire penală ori de câte ori este necesar.

2. Garanții legale privind percheziția informatică

2.1. Satisfacerea condițiilor de necesitate și proporționalitate

Condiția ca percheziția informatică să fie una *necesară* vizează stabilirea unei limite superioare, astfel încât să nu depășească ceea ce ar fi suficient pentru realizarea scopului urmărit sau, dacă există alte metode/măsuri care ar respecta caracterul necesar, atunci organele judiciare sunt ținute de acestea. Prin prisma caracterului necesar trebuie analizată și proporționalitatea în materia stabilirii echilibrului între interesele organelor judiciare și drepturile fundamentale ale persoanelor vizate.

Apreciem că este satisfăcută condiția necesității atunci când niciun alt procedeu probatoriu mai puțin restrictiv nu ar putea oferi garanții suficiente pentru aflarea adevărului. Astfel, dacă un alt procedeu probatoriu satisface condiția *necesității*, organele de urmărire penală ar trebui să se orienteze către acesta (caracterul subsidiar)¹⁹.

Verificarea, în faza de urmărire penală, de către judecătorul de drepturi și libertăți a condițiilor privind proporționalitatea și subsidiaritatea percheziției informatice se realizează prin raportare la cererea prin care procurorul solicită încuviințarea acesteia și prin raportare la conținutul dosarului de urmărire penală.

2.2. Autorizarea efectuării percheziției informatice doar de către un judecător

Dispozițiile art. 168 alin. (2) C. proc. pen. stabilesc că în cursul urmăririi penale percheziția informatică este autorizată la cererea procurorului de către judecătorul de drepturi și libertăți (competența funcțională) de la instanța căreia i-ar reveni competența să judece cauza în primă instanță sau de la instanța corespunzătoare în grad acesteia în a cărei circumscripție se află sediul parchetului din care face parte procurorul care efectuează sau supraveghează urmărirea penală (competența teritorială). Astfel, organele de urmărire penală nu au posibilitatea de

¹⁸ I. Muraru, R. Popescu în I. Muraru, E.S. Tănăsescu (coord.), *op. cit.*, p. 628.

¹⁹ Pentru precizări suplimentare, a se vedea I.D. Apachiței, *Principiul proporționalității reflectat în jurisprudența Curții Constituționale a României și a Consiliului Constituțional al Franței* în Revista de Drept Constituțional, nr. 2/2020, p. 160.

a dispune în mod provizoriu efectuarea percheziției informatice, fiind incidentă sancțiunea nulității absolute (art. 281 alin. (1) lit. b) C. proc. pen.)²⁰.

Cererea procurorului, conform alin. (4) al art. 168 C. proc. pen., se va soluționa în camera de consiliu, fără citarea părților și cu prezența obligatorie a procurorului. În ceea ce ne privește, dispozițiile amintite sunt inexacte prin raportare la art. 32 și 33 C. proc. pen., întrucât fac referire doar la „părți” (inculpatul, partea civilă și partea responsabilă civilmente), iar nu și la subiecții procesuali principali (suspectul și persoana vătămată). Totodată, trebuie precizat faptul că legiuitorul nu a stabilit un termen în care judecătorul de drepturi și libertăți trebuie să soluționeze cererea privind încuviințarea efectuării percheziției informatice²¹, astfel încât, apreciem că aceasta trebuie soluționată de îndată.

Judecătorul de drepturi și libertăți este ținut să se pronunțe asupra cererii procurorului de încuviințare a efectuării percheziției informatice în limitele în care aceasta a fost solicitată, cu alte cuvinte nu poate admite solicitarea cu privire la alte sisteme informatice decât cele indicate în cuprinsul cererii²².

Autorizarea efectuării percheziției informatice poate fi dispusă și în cursul fazei de cameră preliminară de către judecătorul de cameră preliminară²³ și în cursul judecății de către instanță²⁴.

2.3. Imposibilitatea organelor de urmărire penală de a extinde percheziția informatică

Alin. (8) al art. 168 C. proc. pen. stabilesc că dacă pe parcursul efectuării percheziției unui sistem informatic sau a unui suport de stocare a datelor informatice, se constată că datele informatice căutate sunt cuprinse într-un alt sistem informatic ori suport de stocare a datelor informatice și sunt accesibile din sistemul sau suportul inițial, procurorul va dispune de îndată conservarea, copierea datelor informatice identificate și *va solicita de urgență judecătorului de drepturi și libertăți să completeze mandatul*. Aceasta reprezintă o diferență față de dispozițiile art. 159 alin. (7) C. proc. pen. care prevăd posibilitatea/dreptul organelor de urmărire penală de a extinde percheziția domiciliară la locuințele învecinate.

²⁰ M. Udrioiu, *Sinteze de Procedură penală. Partea generală*, Vol. I, ed. 5, Editura C.H. Beck, București, 2024, p. 820.

²¹ Cum este prevăzut, spre exemplu, în ipoteza cererii de încuviințare a efectuării percheziției domiciliare – art. 158 alin. (5) C. proc. pen.

²² M. Udrioiu, *op. cit.*, pp. 820-821.

²³ Conform art. 345 alin. (1) C. proc. pen. (modificat prin Legea nr. 201/2023, publicată în M. Of. nr. 618 din 6 iulie 2023) judecătorul de cameră preliminară urmează să soluționeze cererile și excepțiile formulate, precum și excepțiile ridicate din oficiu, și în baza altor mijloace de probă decât cele administrate în faza de urmărire penală.

²⁴ În temeiul art. 374 alin. (9) și (10) C. proc. pen.

2.4. Durata și scopul pentru care se emite mandatul de percheziție informatică

Dispozițiile legale aplicabile percheziției informatice omit să indice perioada maximă de timp în care percheziția trebuie realizată, legiuitorul indicând doar obligația judecătorului de a menționa în încheierea de încuviințare perioada pentru care mandatul a fost emis și în interiorul căreia trebuie efectuată percheziția informatică. Astfel, este lăsată la latitudinea judecătorului aprecierea perioadei de timp rezonabile în interiorul căreia organele de urmărire penală trebuie să ducă la îndeplinire mandatul. Omisiunea judecătorului de a indica perioada de timp poate atrage sancțiunea nulității relative, în măsura în care este dovedită vătămarea drepturilor părților sau ale subiecților procesuali principali și care nu ar putea fi înlăturată altfel decât prin desființarea actului.

Stabilirea duratei exacte în care trebuie dus la îndeplinire mandatul de percheziție informatică are rolul de a indica limitele temporale în care exercițiul dreptului la viață privată al persoanei urmează să fie restrâns.

Totodată, prin încheierea instanței trebuie să se indice și scopul pentru care este încuviințată percheziția informatică, astfel încât să fie evitată pe de o parte restrângerea arbitrară a exercițiului dreptului fundamental la viață privată, iar pe de altă parte pentru a nu permite organelor de urmărire penală să efectueze percheziția informatică cu încălcarea acestor limite stricte. În situația în care procurorul ar dispune prin ordonanță efectuarea percheziției informatice cu depășirea limitelor stabilite prin încheierea instanței ar fi incidentă nulitatea absolută a mijlocului de probă, fiind încălcată competența funcțională a instanței²⁵.

Privitor la scopul mandatului și obligativitatea indicării sistemului informatic sau a suportului de stocare a datelor informatice care urmează să fie percheziționat s-a arătat în doctrină că acestea trebuie să fie clar delimitate, fiind exclusă ipoteza unui mandat general. În acest sens, s-a mai susținut faptul că „standardele de protecție a vieții private aplicabile în materia percheziției domiciliare cu privire la conținutul mandatului de percheziție trebuie aplicate în mod corespunzător și în materia percheziției informatice; astfel, existența unui mandat redactat în termeni generali în care nu se precizează nimic despre fapta anchetată sau datele informatice care trebuiau ridicate constituie o încălcare a dispozițiilor art. 8 din Convenția europeană (...) în plus, este de remarcat că în unele situații mandatele generale de percheziție informatică pot intra în conflict și cu dreptul la liberă exprimare și la protecția surselor jurnaliștilor garantate de art. 10 din Convenția europeană, astfel cum a statuat Curtea de la Strasbourg în cauza *Nagla c. Letoniei* sau în cauza *Saint Paul Luxembourg c. Luxemburgului*”²⁶.

²⁵ M. Udrioiu, G. Zlati în M. Udrioiu (coord.), *Codul de procedură penală. Comentariu pe articole. Art. 1-603*, ed. 4, Editura C.H. Beck, București, 2023, p. 1460.

²⁶ M. Udrioiu, *op. cit.*, p. 822.

2.5. Asigurarea prezenței suspectului sau inculpatului și/sau a apărătorului la efectuarea percheziției informatice

Cadrul de reglementare este reprezentat de dispozițiile art. 168 alin. (11) C. proc. pen. care stabilesc obligația în sarcina organelor judiciare ca la percheziția în sistem informatic sau a unui suport de stocare a datelor informatice să participe și suspectul ori inculpatul, asistat sau reprezentat de o persoană de încredere. De asemenea, atunci când persoana este reținută ori arestată aducerea sa la percheziția informatică este obligatorie, iar dacă nu poate fi adusă, percheziția se realizează în prezența unui reprezentant ori martor asistent.

Trebuie remarcat faptul că dispozițiile art. 168 alin. (11) C. proc. pen. prevăd că percheziția „se efectuează în prezența” suspectului ori a inculpatului, cu alte cuvinte organele judiciare au obligația de a depune toate diligențele pentru ca suspectului sau inculpatul să participe *efectiv* la percheziția informatică. Obligația incumbă în sarcina organelor judiciare cu atât mai mult cu cât suspectul ori inculpatul este reținut sau arestat. În raport de ipotezele amintite este incident și art. 281 alin. (1) lit. e) C. proc. pen. care determină incidența nulității absolute a actului întocmit fără prezența suspectului sau a inculpatului, atunci când participarea acestora este impusă de lege.

Dacă sistemul informatic sau suportul de stocare a datelor informatice aparține unei alte persoane, care nu are calitatea de suspect sau de inculpat în cauză, organele judiciare păstrează obligația de a asigura prezența acesteia. În această ipoteză, apare ca fiind evidentă lipsa de incidență a prevederilor art. 281 alin. (1) lit. e) C. proc. pen., motiv pentru care putem avea în vedere doar sancțiunea nulității relative a actului întocmit cu încălcarea acestei obligații legale.

Prevederile art. 168 alin. (11) C. proc. pen. mai fac trimitere la art. 159 alin. (10) și (11) C. proc. pen. care prevăd dreptul la asistență ori reprezentare, inclusiv prin intermediul unui avocat. Astfel, sunt incidente prevederile art. 92 și 93 C. proc. pen. care stabilesc o serie de drepturi în materia asistenței juridice: dreptul avocatului de a fi încunoștințat în prealabil cu privire la data și ora efectuării actului de urmărire penală și de a asista la acesta, dreptul de a formula plângeri, cereri și obiecțiuni, dreptul de a lua legătura în mod confidențial cu persoana pe care o asistă ori o reprezintă.

Din ansamblul dispozițiilor menționate decurg o serie de consecințe: organele judiciare au obligația de a lua măsuri efective pentru a asigura prezența persoanei/persoanelor vizate de percheziția informatică, respectiv de a încunoștința avocatul ori de a informa persoana vizată că are dreptul de a fi asistată ori reprezentată de o altă persoană de încredere. Astfel, obligația organelor judiciare este îndeplinită și atunci când suspectul sau inculpatul ori avocatul refuză în mod expres să participe la efectuarea percheziției informatice.

Având în vedere faptul că efectuarea percheziției informatice poate fi dispusă oricând pe parcursul fazei de urmărire penală, cameră preliminară sau judecată, cu privire la un sistem informatic sau suport de stocare a datelor informatice aparținând oricărei persoane, apreciem că dispozițiile art. 168 alin. (11) C. proc. pen. trebuie modificate astfel încât să impună în sarcina organelor judiciare

obligația de a asigura prezența persoanei/persoanelor care deține/dețin sistemul informatic ori suportul de stocare a datelor informatice, indiferent dacă are calitatea de parte sau de subiect procesual.

În raport de cadrul de reglementare amintit sunt incidente două drepturi de rang constituțional: dreptul la apărare (art. 24) și dreptul la viață privată (art. 26). Primul dintre acestea se reflectă în drepturile și obligațiile pe care le au participanții la procesul penal în raport de asigurarea unei apărări efective și de drepturile de care trebuie să beneficieze avocatul pentru a-și îndeplini mandatul primit. Dreptul la viață privată este incident în raport de ingerința pe care o presupune procedeu probatoriu al percheziției informatice. Având în vedere că sistemul informatic sau suportul de stocare al datelor informatice pot conține și date informatice care vizează viața privată a persoanei, care pot să nu aibă legătură cu obiectul cauzei, apare ca evident dreptul (și interesul) acesteia de a asista la efectuarea percheziției informatice.

2.6. Existența unui control *a posteriori*

Prin parag. 63-67 din Decizia nr. 244/2017²⁷ instanța de contencios constituțional s-a pronunțat privitor la necesitatea existenței unui control *a posteriori* în cazul măsurilor de supraveghere tehnică, considerente pe care le apreciem aplicabile *mutatis mutandis* și în privința controlului de legalitate privind percheziția informatică.

În materia percheziției informatice, ce se constituie ca o ingerință în viața privată a suspectului sau inculpatului, este necesar să existe un control *a posteriori* momentului la care a fost autorizată și a fost executat mandatul de percheziție informatică. Persoana care este supusă mandatului de percheziție informatică trebuie să aibă accesibilă o cale efectivă de atac în vederea verificării îndeplinirii condițiilor stabilite de lege pentru emiterea mandatului de percheziție informatică și efectuarea percheziției informatice. Sub acest aspect, în cadrul controlului *a posteriori* trebuie să se aibă în vedere analiza condițiilor de legalitate a procedurii percheziției informatice. Un astfel de control constituie o veritabilă garanție pentru respectarea dreptului la viață privată și, în consecință, mijlocul procesual prin care se stabilește existența proporționalității dintre ingerința adusă de procedura percheziției informatice și scopul anchetei penale, de aflare a adevărului.

Cererile și excepțiile formulate în procedura de cameră preliminară și care vizează (ne)legalitatea probelor care au fost obținute prin intermediul percheziției informatice permit judecătorului să verifice îndeplinirea tuturor condițiilor legale privitoare la această procedură. Sub acest aspect, s-a concluzionat că prin percheziția informatică se aduce atingere vieții private a persoanelor care sunt vizate de această măsură și, prin urmare, trebuie să fie reglementat un control *a posteriori* încuviințării și punerii în executare a mandatului de percheziție informatică²⁸.

²⁷ Publicată în M. Of. nr. 529 din 6 iulie 2017.

²⁸ M. Udriou, *op. cit.*, p. 824.

Astfel, judecătorul de cameră preliminară este competent să verifice legalitatea încheierii judecătorului de drepturi și libertăți prin care a fost încuviințată efectuarea percheziției informatice, legalitatea administrării mijlocului de probă obținut în urma percheziției informatice, respectiv să analizeze legalitatea îndeplinirii condițiilor de necesitate și proporționalitate a măsurii în raport de scopul urmărit²⁹. În măsura în care judecătorul de cameră preliminară admite cererile și excepțiile formulate ori ridicate din oficiu și, în consecință, dispune excluderea probelor și a mijloacelor de probă ce au fost obținute cu încălcarea prevederilor ce reglementează percheziția informatică acesta va putea dispune, cu îndeplinirea celorlalte condiții, restituirea cauzei la parchet, conform art. 346 alin. (3) lit. c) C. proc. pen., urmând ca procurorul să poată readministra procedeul probatoriu al percheziției informatice cu îndeplinirea condițiilor de legalitate³⁰.

3. Dispunerea confiscării speciale asupra sistemului informatic. Studiu de caz

În practica judiciară, cel mai frecvent, sistemele informatice sunt ridicate în urma perchezițiilor domiciliare și, ulterior, fac obiectul confiscării speciale. În continuare vom reda un extras din jurisprudență pentru a indica modalitatea în care sistemul informatic (telefonul inteligent) a fost întrebuințat de către inculpați și raționamentul avut în vedere de către instanță pentru a dispune confiscarea specială.

*„Inculpatul A.A. a mai rămas în România cca. o săptămână după terminarea sesiunii din vară și i-a dat prietenului său B.B. acces la contul lui de Instagram „*****”, după ce i-a luat telefonul și s-a logat direct pe acest cont de pe mobilul său.*

*La rândul său, inculpatul B.B. deținea un cont de Instagram „*****”, însă a declarat că nu a folosit niciodată acest cont pentru a comunica cu clienții cumpărători de droguri, aspect confirmat de rezultatul percheziției informatice.*

*Din coroborarea datelor informatice rezultate în urma punerii în executare a mandatului de supraveghere tehnică și a mandatului de percheziție informatică, a reieșit că inculpatul B.B. a fost conectat pe aplicația de socializare Instagram cu două conturi, respectiv un cont cu numele de utilizator „*****” cu ID-ul numeric asociat ***** cont personal folosit pentru conversații cu familia, prieteni, colegi de facultate), iar al doilea cont cu numele de utilizator „*****” cu ID-ul numeric asociat ***** (cont personal folosit pentru „bussines” cu droguri – cannabis și rezină de cannabis).*

*Istoricul conversațiilor purtate prin intermediul aplicației Instagram de pe contul cu numele de utilizator „*****” relevă un număr de 70 de discuții purtate cu persoane care doreau să se aprovizioneze cu droguri de risc – cannabis și/sau hașiș, în cele mai multe cazuri, „clienții” întrebând, prin mesaje scrise, „dacă îi pot ajuta cu ceva”, „dacă pot trece (pe la el)”, „în cât timp să vină” sau la ce locație, fiind îndrumați la „et. *, ușa * sau la etaj *, ușa *”.*

²⁹ Idem., p. 823.

³⁰ Al. Boroi, G. Negruț, *Drept procesual penal*, ed. a III-a, Editura Hamangiu, București, 2022, p. 307.

*În baza art.112 alin.1 lit. „b” Cod penal, confiscarea specială a telefonului mobil a telefonului mobil marca Iphone 13, de culoare albastru ce prezintă o fisură în partea mediană a ecranului extinsă către capete, în formă de X, cu codul IMEI 1: ***** și IMEI 2: ***** , cu cartela SIM SFR, cu seria ***** , aparținând inculpatului B.B., utilizat în activitatea infracțională de acesta (respectiv pentru comunicarea cu „clienții”, așa cum a rezultat din supravegherea tehnică și/sau din perchezițiile informatice), depus Camera de Corpuri Delicte-I.P.Ț. *** conform dovezii seria ***** din data de *****; În ceea ce privește acest telefon mobil, instanța apreciază că se impune confiscarea sa în temeiul dispozițiilor art.112 alin.1 lit. „b” Cod penal, considerând – pe baza probelor administrate în cauză (procesele-verbale de percheziție informatică, declarațiile martorilor și ale inculpatului, rezultatul accesului autorizat la acest sistem informatic) că acest bun a fost folosit pentru comiterea infracțiunii deduse judecății, respectiv pentru a asigura comunicarea cu clienții interesați să achiziționeze produsele cu efect psihotrop comercializate”³¹.*

În cauza amintită cei doi inculpați utilizau dispozitivele mobile pentru ca prin intermediul unei rețele de socializare să comunice cu persoanele cărora le vindeau substanțele psihoactive. În cauză, telefoanele au fost ridicate în urma percheziției domiciliare.

Este necesar de avut în vedere două mențiuni: a) ridicarea telefonului mobil presupune privarea de acces a inculpatului la toate datele informatice care se aflau stocate pe acesta, chiar și în situația în care doar unele dintre acestea au constituit probe; b) măsura confiscării speciale reprezintă, așa cum se admite în doctrină și în jurisprudență, o veritabilă pedeapsă care vizează înlăturarea unei stări de pericol și preîntâmpinarea săvârșirii altor fapte relevante penal, astfel încât măsura confiscării speciale să fie necesară și proporțională cu ingerința în dreptul de proprietate.

Cele mai multe sisteme informatice sunt reprezentate de laptopuri, telefoane inteligente și tablete, acestea fiind apte de a stoca o cantitate mare de date informatice care pot să nu facă obiectul cauzei penale (rezultatele unor analize medicale, lucrări de specialitate, documente private) ori care, spre exemplu, au rol de portofel digital, în toate cazurile vizând viața privată a inculpatului, și asupra cărora persoana pierde dreptul de proprietate ca urmare a dispunerii măsurii confiscării speciale.

În cauza penală indicată anterior este evident faptul că inculpații utilizau telefoanele inteligente pentru comunicarea cu persoanele cărora urmau să le vândă drogurile, ipoteză în care nu apreciem cum confiscarea specială a unui telefon poate să înlăture starea de pericol și să preîntâmpine săvârșirea altor fapte relevante penal. În egală măsură, apreciem că instanțele trebuie să manifeste prudență în dispunerea confiscării speciale a sistemelor informatice care au suport de stocare a datelor integrate și care conțin date informatice privind viața privată a persoanei, de cele mai multe ori acestea putând să aibă o valoare (financiară/științifică/sentimentală) mult superioară față de valoarea economică a bunului ce face

³¹ Tribunalul Iași, secția penală, Sentința penală nr. 351/2024, www.rejust.ro, ultima accesare la data de 14 iulie 2024.

obiectul confiscării speciale și care, cu atât mai mult, pot să nu aibă legătură cu infracțiunea de care inculpatul este acuzat.

4. Concluzii

Procedeu probatoriu reprezentat de percheziția informatică reprezintă un mijloc legal de obținere a mijloacelor de probă, dar care constituie o ingerință în drepturile și libertățile fundamentale ale persoanei. Pornind de la această teză am dezvoltat prezenta lucrare pe trei coordonate, astfel, într-o primă etapă am identificat dispozițiile de rang constituțional care sunt incidente în raport de percheziția informatică, o atenție sporită a presupus analiza modalității de realizare a percheziției informatice în cazul deputaților și senatorilor, dat fiind implicațiile procedurilor parlamentare de ridicare a imunității.

În urma acestei prime etape am concluzionat că percheziția informatică este în conformitate cu prevederile constituționale, chiar dacă legiuitorul constituant nu a făcut referire în mod expres la acest procedeu probatoriu. Acest aspect îl apreciem ca fiind în acord cu caracteristicile normei constituționale, nefiind obligația constituantului de a indica tipurile de percheziții sau competența organelor judiciare. Cu toate acestea, am apreciat ca fiind necesară remarca privitoare la similitudinile dintre percheziția domiciliară și cea informatică, prin prisma legislației infraconstituționale, raportat la norma constituțională; astfel, dacă legiuitorul constituant a impus obligativitatea dispunerii percheziției domiciliare de către judecător, apare ca fiind firească instituirea acestei obligații și în privința organului judiciar chemat să dispună efectuarea percheziției informatice. Cu toate acestea, o astfel de prevedere a fost avută în vedere de legiuitorul ordinar.

În cea de-a doua etapă a lucrării au fost evidențiate garanțiile prevăzute de Codul de procedură penală pentru protejarea drepturilor fundamentale în raport de încuviințarea și efectuarea percheziției informatice.

Ultima parte a lucrării a presupus corelarea aspectelor indicate anterior cu instituția confiscării speciale, în cazul particular în care obiectul supus confiscării este reprezentat de un sistem informatic cu suport de stocare a datelor integrate (telefon inteligent/laptop/tabletă). Studiul de caz analizat ne-a indicat existența unei posibile lacune legislative care poate determina deficiențe la nivelul practicii judiciare. În concret, am vizat ipoteza în care bunul care a făcut obiectul percheziției informatice ajunge să fie supus măsurii confiscării speciale, cu toate că acesta poate conține date informatice care privesc viața privată a persoanei și care pot să nu aibă relevanță pentru judecarea cauzei. În această ipoteză, inculpatul/condamnatul este privat de dreptul de a-și recupera datele personale, aspect pe care îl apreciem ca fiind în contradicție cu dreptul fundamental la viață privată.

Referințe

- Apachiței I. D., *Principiul proporționalității reflectat în jurisprudența Curții Constituționale a României și a Consiliului Constituțional al Franței* în Revista de Drept Constituțional, nr. 2/2020.
- Balan M., *Drept constituțional și instituții politice. Vol. 1. Teoria generală a statului și a constituției. Constituția română în context european*, Editura Hamangiu, București, 2015.

- Boroi Al., Negruț G., *Drept procesual penal*, ed. a III-a, Editura Hamangiu, București, 2022
- Ionescu C., *Tratat de drept constituțional contemporan*, ed. a III-a, Editura C.H. Beck, București, 2019.
- Muraru I., Tănăsescu E.S. (coord.), *Constituția României. Comentariu pe articole*, ed. a II-a, Editura C.H. Beck, București, 2019.
- Safta M., *Drept constituțional și instituții politice. Vol. I. Teoria generală a dreptului constituțional. Drepturi și libertăți*, ed. a VIII-a, Editura Hamangiu, București, 2023
- Udroiu M. (coord.), *Codul de procedură penală. Comentariu pe articole. Art. 1-603*, ed. a IV-a, Editura C.H. Beck, București, 2023.
- Udroiu M., *Sinteze de Procedură penală. Partea generală*, Vol. I, ed. a V-a, Editura C.H. Beck, București, 2024.

