MONITORUL OFICIAL AL ROMÂNIEI

Anul 191 (XXXV) — Nr. 910

PARTEA I
LEGI, DECRETE, HOTĂRÂRI ȘI ALTE ACTE

Marți, 10 octombrie 2023

SUMAR

ACTE ALE ÎNALTEI CURȚI DE CASAȚIE ȘI JUSTIȚIE

ÎNALTA CURTE DE CASAȚIE ȘI JUSTIȚIE
COMPLETUL PENTRU DEZLEGAREA UNOR CHESTIUNI DE DREPT ÎN MATERIE PENALĂ

DECIZIA Nr. 56
din 18 septembrie 2023

Dosar nr. 1.235/1/2023

Completul compus din:

Eleni Cristina Marcu	— președintele Secției penale a Înaltei Curți de Casație și Justiție, președintele completului
Cristina Rotaru-Radu	— judecător la Secția penală
Rodica Aida Popa	— judecător la Secția penală
Dan-Andrei Enescu	— judecător la Secția penală
Lavinia-Valeria Lefterache	— judecător la Secția penală
Ioana Bogdan	— judecător la Secția penală
Alin Sorin Nicolescu	— judecător la Secția penală
Luminița Crișțiu-Ninu	— judecător la Secția penală
Valerica Voica	— judecător la Secția penală

1. Pe rol se află soluționarea cauzei având ca obiect sesizarea formulată de Curtea de Apel Pitești — Secția penală și pentru cauze cu minori și de familie în Dosarul nr. 2.485/90/2022/a1, în vederea pronunțării unei hotărâri prealabile pentru dezlegarea următoarelor *chestiuni de drept*:

„1. Dacă procedeul probator al accesului la un sistem informatic poate fi utilizat atunci când (i) suportul informatic se află în detenția fizică a organului de urmărire penală sau dacă acest procedeu probator permite doar (ii) pătrunderea de la distanță într-un astfel de sistem în vederea monitorizării/supravegherii activității derulate?

2. Dacă opțiunea asupra emiterii, obținerii și/sau utilizării unui mandat de acces la un sistem informatic sau a unui mandat de percheziție informatică în vederea copierii integrale a datelor aflate într-un sistem informatic aflat în posesia organului de urmărire penală reprezintă o chestiune de oportunitate, aflată în sfera de apreciere a organului de urmărire penală, sau o chestiune de legalitate, supusă cenzurii judecătorului de cameră preliminară?”

2. Completul pentru dezlegarea unor chestiuni de drept în materie penală a fost legal constituit, conform dispozițiilor art. 476 alin. (6) din Codul de procedură penală și ale art. 34 alin. (1) din Regulamentul privind organizarea și funcționarea administrativă a Înaltei Curți de Casație și Justiție, aprobat prin Hotărârea Colegiului de conducere al Înaltei Curți de Casație și Justiție nr. 20/2023 (*Regulament*).

3. Ședința a fost prezidată de președintele Secției penale a Înaltei Curți de Casație și Justiție, *doamna judecător Eleni Cristina Marcu*.

4. La ședința de judecată a participat *doamna Elena-Mihaela Mustață*, magistrat-asistent în cadrul Secțiilor Unite, desemnată în conformitate cu dispozițiile art. 36 din Regulament.

5. Procurorul general al Parchetului de pe lângă Înalta Curte de Casație și Justiție a fost reprezentat de *doamna procuror Nicoleta Eucarie*, procuror în cadrul Secției judiciare — Serviciul judiciar penal.

6. Judecător-raportor a fost desemnat, conform art. 476 alin. (7) din Codul de procedură penală, *doamna judecător Luminița Crișțiu-Ninu*, judecător în cadrul Secției penale a Înaltei Curți de Casație și Justiție.

7. Magistratul-asistent a prezentat referatul cauzei, arătând că au fost transmise *hotărâri relevante pronunțate în materie* și *opiniile magistraților* din cadrul următoarelor instanțe: Curtea de Apel Alba Iulia, Curtea de Apel Bacău, Curtea de Apel București, Curtea de Apel Constanța, Curtea de Apel Craiova, Curtea de Apel Galați, Curtea de Apel Iași, Curtea de Apel Pitești, Curtea de Apel Ploiești, Curtea de Apel Suceava, Curtea de Apel Timișoara, Tribunalul Alba, Tribunalul Argeș, Tribunalul Bistrița-Năsăud, Tribunalul Brașov, Tribunalul pentru Minori și Familie Brașov, Tribunalul București, Tribunalul Brăila, Tribunalul Buzău, Tribunalul Constanța, Tribunalul Covasna, Tribunalul Dolj, Tribunalul Galați, Tribunalul Giurgiu, Tribunalul Gorj, Tribunalul Hunedoara, Tribunalul Ialomița, Tribunalul Iași, Tribunalul Ilfov, Tribunalul Mehedinți, Tribunalul Neamț, Tribunalul Olt, Tribunalul Prahova, Tribunalul Sibiu, Tribunalul Sălaj, Tribunalul Teleorman, Tribunalul Vaslui, Judecătoria Agnita, Judecătoria Alba Iulia, Judecătoria Alexandria, Judecătoria Avrig, Judecătoria Baia Mare, Judecătoria Bacău, Judecătoria Bârlad, Judecătoria Bicaz, Judecătoria Bolintin-Vale, Judecătoria Buzău, Judecătoria Câmpina, Judecătoria Cornetu, Judecătoria Deva, Judecătoria Drobeta-Turnu Severin, Judecătoria Hațeg, Judecătoria Hunedoara, Judecătoria Huși, Judecătoria Iași, Judecătoria Luduș, Judecătoria Lugoj, Judecătoria Mizil, Judecătoria Onești, Judecătoria Orșova, Judecătoria Petroșani, Judecătoria Piatra-Neamț, Judecătoria Ploiești, Judecătoria Pogoanele, Judecătoria Răducăneni, Judecătoria Râmnicu Sărat, Judecătoria Reghin, Judecătoria Roman, Judecătoria Roșiori de Vede, Judecătoria Rupea, Judecătoria Sibiu, Judecătoria Sighișoara, Judecătoria Slobozia, Judecătoria Șimleu Silvaniei, Judecătoria Târgu-Neamț, Judecătoria Târnăveni, Judecătoria Timișoara, Judecătoria Turnu Măgurele, Judecătoria Urziceni, Judecătoria Vaslui, Judecătoria Vălenii de Munte, Judecătoria Vânju Mare, Judecătoria Videle, Judecătoria Zalău și Judecătoria Zimnicea.

8. *Reprezentantul Ministerului Public* a susținut că *prezenta sesizare este inadmisibilă*, nefiind îndeplinite cumulativ condițiile prevăzute de art. 475 din Codul de procedură penală.

9. Astfel, a arătat că nu este îndeplinită condiția de admisibilitate a sesizării privind existența unei chestiuni de drept de care să depindă soluționarea pe fond a cauzei în care a fost invocată, problemele de drept a căror dezlegare a solicitat-o Curtea de Apel Pitești fiind invocate în cadrul procedurii de cameră preliminară.

10. De asemenea, a susținut că este necesar ca sesizarea, în procedura întrebării prealabile, să fie efectuată doar în situația în care, în cursul soluționării unei cauze penale, se pune problema interpretării și aplicării unor dispoziții legale neclare, evazive, care ar putea da naștere unor situații diferite, generând astfel practică judiciară neunitară, or, în cauză, instanța de trimitere trebuie să analizeze legalitatea și temeinicia autorizării, de către procuror, a măsurii accesului la un sistem informatic, precum și legalitatea și temeinicia încheierii prin care a fost confirmată măsura de către judecătorul de drepturi și libertăți, iar prevederile art. 141 raportat la art. 138 alin. (1) lit. b) și art. 168 din Codul de procedură penală sunt clare, neechivoce.

11. *Președintele Completului pentru dezlegarea unor chestiuni de drept în materie penală, doamna judecător Eleni Cristina Marcu*, constatând că nu sunt întrebări de formulat din partea membrilor completului, a declarat dezbaterile închise, reținându-se dosarul în pronunțare privind sesizarea formulată.

ÎNALTA CURTE DE CASAȚIE ȘI JUSTIȚIE — COMPLETUL PENTRU DEZLEGAREA UNOR CHESTIUNI DE DREPT ÎN MATERIE PENALĂ,

deliberând asupra chestiunilor de drept cu care a fost sesizată, constată următoarele:

I. **Titularul și obiectul sesizării**

12. Prin Încheierea din data de 4 aprilie 2023, pronunțată în Dosarul nr. 2.485/90/2022/a1, **Curtea de Apel Pitești — Secția penală și pentru cauze cu minori și de familie**, în baza art. 475

alin. (1) din Codul de procedură penală, a sesizat Înalta Curte de Casație și Justiție în vederea pronunțării unei hotărâri prealabile pentru dezlegarea următoarelor chestiuni de drept:

„1. *Dacă procedeul probator al accesului la un sistem informatic poate fi utilizat atunci când (i) suportul informatic se află în detenția fizică a organului de urmărire penală sau dacă acest procedeu probator permite doar (ii) pătrunderea de la distanță într-un astfel de sistem în vederea monitorizării/ supravegherii activității derulate?*

2. *Dacă opțiunea asupra emiterii, obținerii și/sau utilizării unui mandat de acces la un sistem informatic sau a unui mandat de percheziție informatică în vederea copierii integrale a datelor aflate într-un sistem informatic aflat în posesia organului de urmărire penală reprezintă o chestiune de oportunitate, aflată în sfera de apreciere a organului de urmărire penală, sau o chestiune de legalitate, supusă cenzurii judecătorului de cameră preliminară?*"

II. **Expunerea succintă a cauzei**

13. Curtea de Apel Pitești — Secția penală și pentru cauze cu minori și de familie (completul de doi judecători de cameră preliminară) este învestită în ultim grad de jurisdicție, în etapa camerei preliminare, cu soluționarea contestațiilor declarate de inculpații H.B., M.Gh.C., R.U.-C., S.C.-M. și B.A.-M. împotriva Încheierii nr. 237 din data de 21.12.2022, pronunțată de judecătorul de cameră preliminară din cadrul Tribunalului Vâlcea în Dosarul nr. 2.485/90/2022/a1.

14. Prin Încheierea nr. 237 din data de 21.12.2022, pronunțată de judecătorul de cameră preliminară din cadrul Tribunalului Vâlcea în Dosarul nr. 2.485/90/2022/a1, în temeiul art. 345 alin. (1) și (2) din Codul de procedură penală au fost respinse, ca nefondate, cererile și excepțiile formulate de inculpații R.U.-C., S.C.-M., M.Gh.C, R.L.-Gh. și B.A.-M., prin care au contestat legalitatea sesizării instanței, legalitatea administrării probelor din cursul urmăririi penale și legalitatea actelor de urmărire penală.

15. În baza art. 346 alin. (2) din Codul de procedură penală, s-au constatat *legalitatea sesizării instanței* cu rechizitoriul emis la data de 25.08.2022, în Dosarul de urmărire penală nr. 1.055/D/P/2022 al Parchetului de pe lângă Înalta Curte de Casație și Justiție — Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism — Structura centrală, Secția de combatere a traficului de droguri, prin care s-a dispus trimiterea în judecată a **inculpaților: R.U.-C.**, pentru infracțiunea de trafic de droguri de mare risc (3 acte materiale), prevăzută de art. 2 alin. (1) și (2) din Legea nr. 143/2000 (acte materiale din datele de 30.03.2022, 4.04.2022 și 7.04.2022), cu aplicarea art. 35 alin. (1) și art. 41 alin. (1) din Codul penal, **S.C.M.**, pentru infracțiunea de trafic de droguri de mare risc (fapta din 4.04.2022), prevăzută de art. 2 alin. (1) și (2) din Legea nr. 143/2000, cu aplicarea art. 41 alin. (1) din Codul penal, și infracțiunea de deținere ilegală de droguri de risc, în vederea consumului propriu (fapta din 5.05.2022), prevăzută de art. 4 alin. (1) din Legea nr. 143/2000, cu aplicarea art. 41 alin. (1) din Codul penal, toate cu aplicarea art. 38 alin. (1) din Codul penal, **H.B.**, pentru infracțiunea de trafic de droguri de risc, prevăzută de art. 2 alin. (1) din Legea nr. 143/2000 (fapta din data de 5.05.2022), cu aplicarea art. 41 alin. (1) din Codul penal, **M.Gh.C.,** pentru infracțiunea de trafic de droguri de risc și mare risc, prevăzută de art. 2 alin. (1) și (2) din Legea nr. 143/2000, cu aplicarea art. 35 alin. (1) din Codul penal, **R.L-Gh.**, pentru infracțiunea de trafic de droguri de mare risc (fapta din 30.03.2022), prevăzută de art. 2 alin. (1) și (2) din Legea nr. 143/2000, și **B.A.-M.,** pentru infracțiunea de trafic de droguri de mare risc (fapta din 7.04.2022), prevăzută de art. 2 alin. (1) și (2) din Legea nr. 143/2000, *legalitatea administrării probelor, precum și legalitatea efectuării actelor de urmărire penală*.

16. S-a dispus începerea judecății cauzei privind pe inculpații mai sus menționați.

17. Astfel cum rezultă din încheierea pronunțată, inculpații trimiși în judecată au formulat o serie de cereri și excepții prin care au invocat nelegalitatea sesizării instanței, nelegalitatea administrării probelor și a efectuării unor acte de urmărire penală. Dintre aceștia, inculpații **R.U.C. și B.A.-M. au formulat cereri prin care au solicitat să se constate nelegalitatea percheziției informatice efectuate asupra telefoanelor mobile ridicate de la aceștia cu ocazia percheziției domiciliare și excluderea tuturor probelor obținute în urma percheziției informatice.**

18. În susținerea cererii formulate, inculpatul R.U.C. a arătat că hardurile celor trei telefoane mobile ce îi aparțineau au fost clonate în baza ordonanței emise la data de 5.05.2022 de Parchetul de pe lângă Înalta Curte de Casație și Justiție — D.I.I.C.O.T., prin care s-a autorizat provizoriu, pe o durată de 24 de ore, măsura de supraveghere tehnică mai sus menționată, iar inculpatul și apărătorul său nu au participat la această activitate, așa cum rezultă din procesul-verbal întocmit.

19. În raport cu aspectele învederate, a susținut că au fost nesocotite dispozițiile art. 168 alin. (2)—(5) din Codul de procedură penală, conform cărora percheziția informatică este efectuată în baza mandatului de percheziție emis de către judecătorul de drepturi și libertăți și nu poate fi autorizată provizoriu de către procuror pentru o perioadă de 24 de ore. În același timp, a mai menționat că dispozițiile art. 138 alin. (1) din Codul de procedură penală, care definesc măsurile de supraveghere tehnică, nu fac referire și la clonarea hardului unui sistem informatic ori la efectuarea unei percheziții informatice, astfel încât procurorul nu avea nici competența funcțională de a autoriza un astfel de procedeu probator și, prin urmare, toate actele efectuate în baza ordonanței de supraveghere tehnică sunt lovite de nulitate absolută.

20. Inculpatul a invocat și nesocotirea dispozițiilor art. 168 alin. (11) din Codul de procedură penală, care, coroborate cu dispozițiile art. 159 alin. (10) și (11) din Codul de procedură penală, stabilesc într-o manieră imperativă că percheziția informatică este realizată în prezența suspectului sau inculpatului. În acest sens, s-a susținut că inculpatul și apărătorii aleși ai acestuia nu au fost înștiințați cu privire la derularea percheziției informatice, inculpatul fiind în timpul percheziției sub puterea unui mandat de aducere, ulterior fiind reținut și arestat preventiv, despre existența percheziției informatice aflând la momentul studierii dosarului de urmărire penală.

21. Pentru toate aceste considerente, a solicitat, în temeiul art. 345 din Codul de procedură penală, excluderea tuturor mijloacelor de probă obținute ca urmare a percheziției informatice derulate în mod nelegal, precum și a tuturor precizărilor privind rezultatul percheziției informatice din cuprinsul actelor de la dosar.

22. Inculpatul B.A.-M. a susținut că i-a fost ridicat un telefon mobil cu ocazia percheziției efectuate la sediul S.C. A.B. & C. — S.R.L., societate pe care o administra, iar în urma percheziției domiciliare efectuate și la locuința sa, la solicitarea organelor judiciare, a predat un al doilea telefon mobil, pe care îl folosea. Telefoanele mobile au fost accesate în baza ordonanței procurorului prin care s-a autorizat provizoriu supravegherea tehnică pentru o durată de 48 de ore, supraveghere constând în accesul la un sistem informatic, în urma căreia a fost copiat integral conținutul sistemelor informatice, fiind identificate probe (convorbiri purtate prin intermediul aplicațiilor Signal și Telegram) și copiate pe un hard extern.

23. Astfel, a arătat că identificarea, extragerea datelor și filmarea unor conversații purtate prin intermediul unor aplicații au fost efectuate fără a exista un mandat de percheziție informatică, în opinia inculpatului, în cauză nefiind aplicabile dispozițiile art. 138 alin. (3) și, implicit, cele ale art. 138 alin. (13) din Codul de procedură penală, vizând supravegherea tehnică, ci, în raport cu activitățile efectuate de specialist, era necesară efectuarea unei percheziții informatice, cu participarea inculpatului și a apărătorului acestuia.

24. În situația expusă, respectiv existența unui telefon mobil aflat deja în posesia organelor judiciare, bunul fiind ridicat anterior cu ocazia percheziției domiciliare, iar inculpatul, privat de libertate, apărarea a subliniat că procedeul probatoriu de urmat pentru identificare și strângerea probelor este percheziția informatică reglementată de art. 168 din Codul de procedură

penală, singura care permite în condițiile descrise cercetarea, descoperirea, identificarea și strângerea probelor stocate într-un sistem informatic sau mijloc de stocare a datelor informatice.

25. Accesul la un sistem informatic, ca metodă de supraveghere tehnică, în opinia apărării, se referă strict la pătrunderea într-un astfel de sistem, fie direct, fie de la distanță, prin programe specializate, fără însă să fie necesară ridicarea efectivă a bunului și permițând în continuare utilizarea acestuia de către posesor. Practic, există o monitorizare a activității derulate printr-un sistem informatic, în timp real, ceea ce explică apartenența la metodele de supraveghere tehnică, în timp ce percheziția informatică vizează operațiuni încheiate, urmărindu-se recuperarea datelor stocate în memorie.

26. S-a concluzionat că, raportat la regimul distinct al celor două procedee probatorii, probele au fost obținute în mod nelegal. Astfel, s-a precizat că, deși a existat o autorizare a judecătorului, aceasta a vizat doar accesul la un sistem informatic, respectiv pătrunderea în sistem, în fapt realizându-se și o strângere a probelor stocate în acest sistem, iar, în aceste condiții, judecătorul de drepturi și libertăți ar fi trebuit să lămurească obiectul cererii.

27. Prin urmare, în opinia apărării inculpatului, lipsa mandatului de percheziție și neparticiparea inculpatului și a procurorului la realizarea procedeului probator sunt de natură a atrage nulitatea absolută, cu consecința excluderii probelor nelegale.

28. Același inculpat a susținut că accesul la un sistem informatic oferea doar posibilitatea pătrunderii într-un astfel de sistem și a monitorizării/supravegherii activității derulate și nu permitea copierea integrală a datelor conținute de suportul informatic, astfel încât au fost încălcate grav limitele autorizării.

29. Suplimentar, au fost invocate și alte neregularități ale administrării acestei probe, apărarea inculpatului arătând că nu rezultă: când și în ce împrejurare a fost desigilat plicul în care se afla telefonul; cum a ajuns acesta din posesia organului de urmărire penală în posesia specialistului; când și în ce împrejurări a fost delegat specialistul să efectueze acte de urmărire penală, constând în identificarea, culegerea, fixarea de probe; de ce organele de urmărire penală nu au participat la activitate; de ce inculpatul și apărătorul său nu au fost citați la efectuarea operațiunii de copiere integrală a conținutului sistemului informatic reprezentat de telefonul mobil.

30. Prin încheierea din data de 6.05.2022, ora 16.00, a fost confirmată de către judecătorul de drepturi și libertăți din cadrul Tribunalului București măsura provizorie mai sus menționată.

31. *Cererile și excepțiile formulate de inculpați au fost apreciate ca nefondate de judecătorul de cameră preliminară.*

32. În esență, s-a reținut că accesul la un sistem informatic este, în fapt, o măsură de supraveghere tehnică, ce poate fi dispusă de procuror, pe o durată de 48 de ore.

33. Potrivit dispozițiilor art. 142 coroborate cu art. 92 din Codul procedură penală, în cursul urmăririi penale avocatul suspectului sau inculpatului are dreptul să asiste la efectuarea oricărui act de urmărire penală, cu excepția situației în care se utilizează măsuri speciale de supraveghere ori cercetare prevăzute în capitolul IV din titlul IV.

34. Din compararea dispozițiilor legale incidente rezultă că deosebirea esențială dintre accesul la un sistem informatic și percheziția informatică este dată, implicit, de scopul utilizării acestora. În acest sens, s-a reținut că accesul la un sistem informatic constituie o metodă de supraveghere, pe când percheziția informatică este o metodă de cercetare. Conform dispozițiilor art. 138 alin. (3) din Codul de procedură penală, accesul la un sistem informatic constă în pătrunderea într-un sistem informatic sau mijloc de stocare a datelor informatice, fie direct, fie de la distanță, prin intermediul unor programe specializate ori prin intermediul unei rețele, în scopul de a identifica probe. Potrivit art. 168 alin. (1) din Codul de procedură penală, percheziția informatică este un procedeu probatoriu care constă în activitățile de cercetare, descoperire, identificare și strângere a probelor stocate într-un sistem informatic sau suport de stocare a datelor informatice, realizate prin intermediul unor mijloace tehnice și proceduri adecvate, de natură să asigure integritatea informațiilor conținute de acesta.

35. În acest sens s-a reținut că accesul la un sistem informatic oferă acces la resursele sistemului informatic la un anumit moment, dar permite și supravegherea acestuia pe viitor, în timp ce percheziția informatică permite doar cercetarea resurselor sistemului informatic la momentul efectuării sale. Accesul la un sistem informatic permite monitorizarea pasivă a sistemului, în condiții de confidențialitate, fără știrea titularului sau utilizatorului, pe când percheziția informatică poate fi efectuată potrivit dispozițiilor art. 168 alin. (11) din Codul de procedură penală numai în prezența suspectului sau inculpatului.

36. De asemenea, din analiza comparativă a celor două instituții mai reiese că accesul la un sistem informatic se dispune pentru a identifica probe, în timp ce percheziția informatică este dispusă pentru descoperirea, identificarea și strângerea probelor.

37. În consecință, judecătorul de cameră preliminară a constatat că actul procedural la care se face referire este de fapt o măsură de supraveghere tehnică, dispusă de procuror, confirmată ulterior de judecătorul de drepturi și libertăți din cadrul Tribunalului București, iar nu o percheziție informatică, așa cum a susținut apărarea inculpatului, fiind respectate dispozițiile legale incidente în cauză.

38. În fine, neîntemeiată a fost apreciată și cererea inculpatului B.A.-M., prin care a solicitat excluderea probelor obținute, ca urmare a faptului că accesul la un sistem informatic nu permitea și copierea datelor obținute în urma accesului.

39. Judecătorul de cameră preliminară a reținut că, potrivit dispozițiilor art. 141 alin. (5) din Codul de procedură penală, procurorul poate dispune prin ordonanță efectuarea de copii ale datelor obținute ca urmare a accesului la un sistem informatic.

40. *Împotriva acestei încheieri au declarat contestații, potrivit art. 347 din Codul de procedură penală, inculpații H.B., M.Gh.C., R.U.C., S.C.M. și B.A.-M.,* prin care au criticat modul în care au fost soluționate cererile și excepțiile invocate în fața primului judecător de cameră preliminară, contestații înregistrate la Curtea de Apel Pitești, în Dosarul nr. 2.485/90/2022/a1 și repartizate spre soluționare unui complet de doi judecători de cameră preliminară.

41. La termenul acordat în vederea dezbaterilor asupra cererilor și excepțiilor formulate, 4 aprilie 2022, inculpatul B.A.-M., prin apărător, a formulat, în temeiul art. 475 alin. (1) din Codul de procedură penală, cerere de sesizare a Înaltei Curți de Casație și Justiție — Completul pentru dezlegarea unor chestiuni de drept în materie penală, în vederea dezlegării de principiu a problemelor de drept anterior menționate.

III. **Dispoziții legale relevante**

42. ***Legea nr. 135/2010 privind Codul de procedură penală***

Art. 138 — Dispoziții generale

„(1) Constituie metode speciale de supraveghere sau cercetare următoarele:

(…);

b) accesul la un sistem informatic;

(...).

(3) Prin *acces la un sistem informatic* se înțelege pătrunderea într-un sistem informatic sau mijloc de stocare a datelor informatice fie direct, fie de la distanță, prin intermediul unor programe specializate ori prin intermediul unei rețele, în scopul de a identifica probe.

(4) Prin *sistem informatic* se înțelege orice dispozitiv sau ansamblu de dispozitive interconectate ori aflate în relație funcțională, dintre care unul sau mai multe asigură prelucrarea automată a datelor, cu ajutorul unui program informatic.

(5) Prin *date informatice* se înțelege orice reprezentare de fapte, informații sau concepte sub o formă adecvată prelucrării într-un sistem informatic, inclusiv un program capabil să determine executarea unei funcții de către un sistem informatic.

(...)

(13) Prin *supraveghere tehnică* se înțelege utilizarea uneia dintre metodele prevăzute la alin. (1) lit. a)—d).”

Art. 139 — Supravegherea tehnică

„(1) Supravegherea tehnică se dispune de judecătorul de drepturi și libertăți atunci când sunt îndeplinite cumulativ următoarele condiții:

(...)."

Art. 141 — Autorizarea unor măsuri de supraveghere tehnică de către procuror

(1) Procurorul poate autoriza, pe o durată de maximum 48 de ore, măsurile de supraveghere tehnică atunci când:

a) există urgență, iar obținerea mandatului de supraveghere tehnică în condițiile art. 140 ar conduce la o întârziere substanțială a cercetărilor, la pierderea, alterarea sau distrugerea probelor ori ar pune în pericol siguranța persoanei vătămate, a martorului sau membrilor familiilor acestora; și

b) sunt îndeplinite condițiile prevăzute la art. 139 alin. (1) și (2).

(2) Ordonanța procurorului prin care se autorizează măsura de supraveghere tehnică trebuie să cuprindă mențiunile prevăzute la art. 140 alin. (5).

(3) Procurorul are obligația de a sesiza, în termen de cel mult 24 de ore de la expirarea măsurii, judecătorul de drepturi și libertăți 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 a emis ordonanța, în vederea confirmării măsurii, înaintând totodată un proces-verbal de redare rezumativă a activităților de supraveghere tehnică efectuate și dosarul cauzei.

(4) În cazul în care judecătorul de drepturi și libertăți apreciază că au fost îndeplinite condițiile prevăzute la alin. (1), confirmă în termen de 24 de ore măsura dispusă de procuror, prin încheiere, pronunțată în camera de consiliu, fără citarea părților.

(5) Cu privire la datele informatice identificate prin accesul la un sistem informatic, procurorul poate dispune, prin ordonanță:

a) realizarea și conservarea unei copii a acestor date informatice;

b) suprimarea accesării sau îndepărtarea acestor date informatice din sistemul informatic.

Copiile se realizează cu mijloace tehnice și proceduri adecvate, de natură să asigure integritatea informațiilor conținute de acestea.

(6) În cazul în care judecătorul de drepturi și libertăți apreciază că nu au fost respectate condițiile prevăzute la alin. (1), infirmă măsura luată de către procuror și dispune distrugerea probelor obținute în temeiul acesteia. Procurorul distruge probele astfel obținute și întocmește un proces-verbal în acest sens.

(7) Odată cu cererea de confirmare a măsurii sau separat, procurorul poate solicita judecătorului de drepturi și libertăți luarea măsurii supravegherii tehnice în condițiile art. 140.

(8) Încheierea prin care judecătorul de drepturi și libertăți se pronunță asupra măsurilor dispuse de procuror nu este supusă căilor de atac."

Art. 168 — Percheziția informatică

„(1) Prin *percheziție în sistem informatic sau a unui suport de stocare a datelor informatice* se înțelege procedeul de cercetare, descoperire, identificare și strângere a probelor stocate într-un sistem informatic sau suport de stocare a datelor informatice, realizat prin intermediul unor mijloace tehnice și proceduri adecvate, de natură să asigure integritatea informațiilor conținute de acestea.

(2) În cursul urmăririi penale, judecătorul de drepturi și libertăți 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 poate dispune efectuarea unei percheziții informatice, la cererea procurorului, atunci când pentru descoperirea și strângerea probelor este necesară cercetarea unui sistem informatic sau a unui suport de stocare a datelor informatice.

(3) Procurorul înaintează cererea prin care se solicită încuviințarea efectuării percheziției informatice împreună cu dosarul cauzei judecătorului de drepturi și libertăți.

(4) Cererea se soluționează în camera de consiliu, fără citarea părților. Participarea procurorului este obligatorie.

(5) Judecătorul dispune prin încheiere admiterea cererii, atunci când aceasta este întemeiată, încuviințarea efectuării percheziției informatice și emite de îndată mandatul de percheziție.

(...)

(8) 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 într-un alt sistem informatic ori 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, dispozițiile alin. (1)—(7) aplicându-se în mod corespunzător.

(9) În vederea executării percheziției dispuse, pentru asigurarea integrității datelor informatice stocate pe obiectele ridicate, procurorul dispune efectuarea de copii.

(10) Dacă ridicarea obiectelor care conțin datele informatice prevăzute la alin. (1) ar afecta grav desfășurarea activității persoanelor care dețin aceste obiecte, procurorul poate dispune efectuarea de copii, care servesc ca mijloc de probă. Copiile se realizează cu mijloace tehnice și proceduri adecvate, de natură să asigure integritatea informațiilor conținute de acestea.

(11) Percheziția în sistem informatic sau a unui suport de stocare a datelor informatice se efectuează în prezența suspectului ori a inculpatului, dispozițiile art. 159 alin. (10) și (11) aplicându-se în mod corespunzător.

(12) Percheziția în sistem informatic ori a unui suport de stocare a datelor informatice se efectuează de un specialist care funcționează în cadrul organelor judiciare sau din afara acestora, în prezența procurorului sau a organului de cercetare penală.

(...)

(14) Organele de urmărire penală trebuie să ia măsuri ca percheziția informatică să fie efectuată fără ca faptele și împrejurările din viața personală a celui la care se efectuează percheziția să devină, în mod nejustificat, publice.

(...)."

Art. 168[1] — Efectuarea percheziției informatice de lucrători de poliție

„Efectuarea percheziției informatice prevăzută la art. 168 alin. (12) se poate realiza și de către lucrători de poliție specializați, în prezența procurorului sau a organului de cercetare penală."

IV. **Punctul de vedere al completului care a dispus sesizarea Înaltei Curți de Casație și Justiție**

43. Completul de doi judecători de cameră preliminară nu a expus un punct de vedere asupra chestiunilor de drept invocate, cu argumentul că, în acest fel, ar antama soluția asupra fondului cauzei.

V. **Punctele de vedere exprimate de către curțile de apel și instanțele judecătorești arondate**

44. Au fost solicitate punctele de vedere ale instanțelor judecătorești asupra chestiunilor de drept supuse dezlegării, iar în urma consultării acestora, s-a constatat că opiniile conturate nu sunt unitare, fiind identificate în răspunsurile transmise ***câte două opinii, asupra fiecăreia dintre cele două probleme de drept.***

45. ***În afara celor două opinii formulate asupra fondului problemelor a căror dezlegare se solicită, s-a exprimat și opinia inadmisibilității prezentei sesizări.***

46. V.1.a) ***Cu referire la prima chestiune de drept invocată, în opinie majoritară,*** s-a apreciat că procedeul probator al accesului la un sistem informatic poate fi utilizat atât în situația în care suportul informatic se află în detenția fizică a organului de urmărire penală, cât și în situația în care se pătrunde de la distanță într-un astfel de sistem, în acest sens fiind punctele de vedere exprimate de majoritatea judecătorilor de la Curtea de Apel Alba Iulia, Curtea de Apel Bacău, Curtea de

Apel București, Curtea de Apel Constanța, Curtea de Apel Craiova, Curtea de Apel Galați, Curtea de Apel Iași, Curtea de Apel Pitești, Curtea de Apel Ploiești, Tribunalul Alba, Tribunalul Argeș, Tribunalul Bistrița-Năsăud, Tribunalul Brașov, Tribunalul București, Tribunalul Brăila, Tribunalul Buzău, Tribunalul Constanța, Tribunalul Covasna, Tribunalul Dolj, Tribunalul Hunedoara, Tribunalul Ialomița, Tribunalul Iași, Tribunalul Ilfov, Tribunalul Neamț, Tribunalul Olt, Tribunalul Prahova, Tribunalul Sibiu, Tribunalul Sălaj, Tribunalul Teleorman, Tribunalul Vaslui, Judecătoria Agnita, Judecătoria Alba Iulia, Judecătoria Alexandria, Judecătoria Avrig, Judecătoria Baia Mare, Judecătoria Bacău, Judecătoria Bârlad, Judecătoria Bicaz, Judecătoria Buzău, Judecătoria Cornetu, Judecătoria Deva, Judecătoria Drobeta-Turnu Severin, Judecătoria Hațeg, Judecătoria Hunedoara, Judecătoria Huși, Judecătoria Iași, Judecătoria Lugoj, Judecătoria Onești, Judecătoria Orșova, Judecătoria Petroșani, Judecătoria Piatra-Neamț, Judecătoria Pogoanele, Judecătoria Răducăneni, Judecătoria Râmnicu Sărat, Judecătoria Reghin, Judecătoria Roman, Judecătoria Roșiori de Vede, Judecătoria Rupea, Judecătoria Sibiu, Judecătoria Sighișoara, Judecătoria Slobozia, Judecătoria Șimleu Silvaniei, Judecătoria Turnu Măgurele, Judecătoria Urziceni, Judecătoria Vânju Mare, Judecătoria Videle, Judecătoria Zalău și Judecătoria Zimnicea.

47. Punctul de vedere al Tribunalului Covasna a fost în sensul că procedeul probator al accesului la un sistem informatic poate fi utilizat și atunci când suportul informatic se află în detenția fizică a organului de urmărire penală, prin pătrunderea directă, în condițiile art. 138 alin. (3) din Codul de procedură penală, în scopul de a identifica probe, însă numai pentru datele informatice create în timpul monitorizării, pentru datele informatice anterioare fiind necesară autorizarea unei percheziții informatice, cu respectarea garanțiilor prevăzute de lege.

În sprijinul opiniei majoritare, s-au arătat următoarele:

48. Accesul la un sistem informatic este o metodă specială de supraveghere reglementată de art. 138 alin. (1) lit. b) din Codul de procedură penală, care permite atât realizarea accesului de la distanță, cât și a accesului direct și nemijlocit la sistemul informatic. În acest sens au fost avute în vedere dispozițiile legale mai sus menționate, care definesc accesul la un sistem informatic ca fiind pătrunderea într-un sistem informatic (orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate într-o relație funcțională, dintre care unul sau mai multe asigură prelucrarea automată a datelor) sau un mijloc de stocare a datelor informatice, fie direct, fie de la distanță, prin intermediul unor programe specializate ori prin intermediul unei rețele, în scopul de a identifica probe. Este o metodă specială de supraveghere, fiind necesară emiterea unui mandat de supraveghere tehnică de către judecător sau confirmarea acesteia de către judecător în cazul în care a fost autorizată de către procuror, în condițiile prevăzute de art. 141 din Codul de procedură penală.

49. S-a arătat că pătrunderea presupune cercetarea resurselor sistemului informatic în scopul descoperirii de informații existente în acesta sau a celor generate pe parcursul supravegherii tehnice sau pentru a obține reprezentarea sistemului. Pătrunderea se efectuează fie direct — contact fizic nemijlocit cu sistemul informatic ori mijlocul de stocare a datelor informatice, fie de la distanță (prin intermediul conexiunii la internet ori prin accesarea unei rețele wireless, în condiții de confidențialitate). Accesul fizic se desfășoară în locul în care se află sistemul informatic sau mijlocul de stocare a datelor informatice.

50. Prin urmare, în condițiile în care, chiar prin lege, se face trimitere, pe de o parte, la accesul de la distanță, iar, pe de altă parte, la accesul direct, nemijlocit, o restrângere a sferei de aplicare a acestei măsuri de supraveghere nu este posibilă. În acest sens, s-a arătat că legiuitorul nu distinge în cuprinsul dispozițiilor art. 138 alin. (3) din Codul de procedură penală, după cum suportul informatic se află în detenția organului de urmărire penală sau la distanță, iar o altă interpretare înseamnă adăugare la lege. În plus, dispozițiile care reglementează procedeul probator al percheziției informatice nu impun utilizarea acestuia în cazul în care sistemul informatic se află în detenția fizică a organului de urmărire penală.

51. S-a mai arătat că pentru ipoteza autorizării unor măsuri de supraveghere tehnică de către procuror, în cazuri urgente, dispozițiile art. 141 alin. (5) din Codul de procedură penală prevăd că procurorul poate dispune prin ordonanță cu privire la datele informatice identificate prin accesul la un sistem informatic: a) realizarea și conservarea unei copii a acestora; b) suprimarea accesării sau îndepărtarea acestor date din sistemul informatic. Copiile se realizează cu mijloace tehnice și proceduri adecvate, de natură să asigure integritatea informațiilor conținute de acestea. Potrivit art. 141 alin. (6) din Codul de procedură penală, în cazul în care judecătorul de drepturi și libertăți apreciază că nu au fost respectate condițiile prevăzute la alin. (1), infirmă măsura luată de către procuror și dispune distrugerea probelor obținute în temeiul acesteia.

52. Potrivit art. 168 alin. (1) din Codul de procedură penală, percheziția informatică reprezintă procedeul de cercetare, descoperire, identificare și strângere a probelor stocate într-un sistem informatic sau suport de stocare a datelor informatice, realizat prin intermediul unor mijloace tehnice și proceduri adecvate, de natură să asigure integritatea informațiilor conținute de acestea. Potrivit art. 168 alin. (2) din Codul de procedură penală, percheziția informatică se dispune în toate cazurile în care pentru descoperirea și strângerea probelor este necesară cercetarea unui sistem informatic sau a unui suport de stocare a datelor informatice.

53. În acest context, s-a arătat că, în timp ce percheziția informatică este folosită pentru obținerea de date informatice deja existente, localizate într-un sistem informatic aflat deja în custodia și sub controlul organului judiciar, în cazul datelor informatice reprezentate de conținutul mesajelor de tip e-mail sau VoIP stocate pe sistemele informatice ce nu se află în posesia organelor judiciare, procedeul probator prin care se pot obține aceste date este reprezentat de accesul la un sistem informatic. Și în această situație este necesară emiterea unui mandat de către judecătorul de drepturi și libertăți, datele fiind obținute cu ajutorul unor mijloace tehnice specifice, cu sau fără sprijinul furnizorilor de servicii de internet sau comunicații. Ceea ce diferențiază accesul la un sistem informatic de percheziția informatică este faptul că, pe când în cazul percheziției informatice datele informatice sunt deja existente în sistemul informatic percheziționat, fiind vorba despre date din trecut prin raportare la data emiterii mandatului de percheziție informatică, prin accesul la un sistem informatic se pot obține atât date cu privire la comunicații purtate anterior datei emiterii mandatului de supraveghere tehnică, cât și date despre comunicații ulterioare, efectuate între momentul emiterii mandatului de supraveghere tehnică și data-limită până la care acesta este valabil.

54. S-a mai arătat și că se impune efectuarea unei delimitări clare între cele două procedee probatorii, percheziția informatică și accesul la un sistem informatic, acestea fiind supuse unor reguli diferite care determină modalități diferite de a acționa din partea organelor judiciare, în sensul că, în timp ce percheziția informatică impune contactul fizic cu sistemul informatic supus percheziției, accesul la un sistem informatic se poate realiza atât în prezența sistemului informatic, cât și în lipsa acestuia.

55. În aceeași ordine de idei, s-a menționat și faptul că supravegherea tehnică sub forma accesului la un sistem informatic și percheziția informatică nu sunt instrumente de cercetare penală alternative, pe care procurorul să le poată accesa prin amalgamarea terminologiei procedurale, pentru că un atare mod de aplicare a legii desconsideră principiul legalității prevăzut de art. 2 din Codul de procedură penală și tinde la încălcarea garanțiilor procesuale prevăzute de lege. Supravegherea tehnică sub forma accesului la un sistem informatic și percheziția informatică sunt instituții distincte cu funcționalități precis determinate, prima fiind o metodă de cercetare secretă, iar a doua având caracter participativ.

56. S-a susținut că accesul la un sistem informatic presupune investigarea dinamică a setului de date aflate pe sistemul informatic în care se pătrunde, iar atunci când datele sunt înregistrate în sistemul informatic și nu există posibilitatea de modificare de la distanță a acestora, singurul procedeu permis de lege este percheziția informatică. Lipsa unui mandat de percheziție informatică nu poate fi suplinită prin măsura tehnică a accesului la un sistem informatic.

57. V.1.b) ***În opinie minoritară, cu privire la prima chestiune de drept invocată***, s-a apreciat că procedeul probator al accesului la un sistem informatic poate fi utilizat numai pentru a pătrunde de la distanță într-un astfel de sistem, în vederea monitorizării/supravegherii activității derulate, nu și atunci când suportul informatic se află în detenția fizică a organului de urmărire penală, în acest din urmă caz fiind necesară obținerea unui mandat de percheziție informatică. În acest sens au fost exprimate puncte de vedere de judecătorii de la Curtea de Apel Suceava, Curtea de Apel Timișoara, Tribunalul pentru Minori și Familie Brașov, Tribunalul Galați, Tribunalul Giurgiu, Judecătoria Bolintin-Vale, Judecătoria Câmpina, Judecătoria Luduș, Judecătoria Mizil, Judecătoria Ploiești, Judecătoria Vălenii de Munte, Judecătoria Târnăveni și Judecătoria Târgu-Neamț.

În sprijinul celei de-a doua opinii, s-au adus următoarele argumente:

58. Procedeul probator al accesului la un sistem informatic (metodă de supraveghere tehnică) poate fi utilizat în urma obținerii unui mandat sau a autorizării procurorului, doar în situația în care un astfel de sistem se află la distanță, în vederea monitorizării/supravegherii activității derulate. Procedeul probator al accesului la un sistem informatic poate fi utilizat în condițiile în care inculpatul nu este înștiințat despre folosirea acestuia, fiind diferit de procedeul probator al percheziției în sistem informatic, în acest din urmă caz suportul informatic trebuind să se afle efectiv în detenția organului de urmărire penală și nefiind necesară obținerea unui mandat de acces la sistemul informatic, ci doar a unui mandat de percheziție informatică, procedeu la care inculpatul poate participa, personal sau prin reprezentant legal.

59. S-a menționat că pentru obținerea de date informatice deja existente, localizate într-un sistem informatic aflat în custodia și sub controlul organului judiciar, este folosită percheziția informatică, iar, în cazul în care datele informatice sunt reprezentate de conținutul unor mesaje de tip e-mail sau VoIP stocate pe sisteme informatice ce nu se află în posesia organelor judiciare, procedeul probatoriu prin care pot fi obținute este reprezentat de accesul la un sistem informatic.

60. Din analiza comparativă a dispozițiilor art. 138 alin. (3) și ale art. 168 alin. (1) din Codul de procedură penală reiese că accesul la un sistem informatic permite organelor judiciare doar pătrunderea în sistemul respectiv, pentru a identifica probe, față de percheziția informatică, prin intermediul căreia datele stocate pe respectivul sistem informatic pot fi cercetate în conținutul lor pentru a obține probe care pot conduce, sau nu, la soluționarea cauzei. Accesul la un sistem informatic nu permite cercetarea conținutului probelor aflate în sistemul informatic, astfel că, în ipoteza identificării unor date ce ar putea prezenta relevanță sau utilitate pentru soluționarea cauzei, organele de urmărire penală trebuie să solicite emiterea unui mandat de percheziție informatică de la judecătorul de drepturi și libertăți.

61. În continuare, s-a arătat că, deși nu ar fi exclusă recurgerea la procedeul accesului la un sistem informatic atunci când sistemul se află în posesia organelor de urmărire penală, pentru identificarea unor eventuale date informatice care ar putea servi la aflarea adevărului, cu toate acestea, analiza conținutului acestor date se va putea realiza numai prin intermediul percheziției informatice.

62. V.2. Cu referire la cea ***de-a doua chestiune de drept invocată, au fost exprimate două opinii.***

63. V.2.a) ***Într-o opinie*** s-a apreciat că opțiunea asupra emiterii, obținerii și/sau utilizării unui mandat de acces la un sistem informatic sau a unui mandat de percheziție informatică în vederea copierii integrale a datelor dintr-un sistem informatic aflat în posesia organului de urmărire penală reprezintă ***o chestiune de legalitate***, supusă cenzurii judecătorului de cameră preliminară.

64. În acest sens au fost exprimate puncte de vedere de către judecătorii de la Curtea de Apel Alba Iulia, Curtea de Apel Bacău, Curtea de Apel București — Secția a II-a penală, Curtea de Apel Constanța, Curtea de Apel Galați, Curtea de Apel Ploiești, Curtea de Apel Suceava, Curtea de Apel Timișoara, Tribunalul pentru Minori și Familie Brașov, Tribunalul Brăila, Tribunalul București, Tribunalul Constanța, Tribunalul Covasna, Tribunalul Dolj, Tribunalul Ialomița, Tribunalul Neamț, Tribunalul Prahova, Tribunalul Sălaj, Tribunalul Sibiu, Tribunalul Vaslui, Judecătoria Alba Iulia, Judecătoria Avrig, Judecătoria Bacău, Judecătoria Bicaz, Judecătoria Buzău, Judecătoria Câmpina, Judecătoria Huși, Judecătoria Ploiești, Judecătoria Pogoanele, Judecătoria Vălenii de Munte, Judecătoria Răducăneni, Judecătoria Râmnicu Sărat, Judecătoria Rupea, Judecătoria Slobozia, Judecătoria Șimleu Silvaniei, Judecătoria Târnăveni și Judecătoria Urziceni.

În susținerea primei opinii, s-au arătat următoarele:

65. În situația în care se urmăresc accesarea și copierea datelor dintr-un sistem informatic aflat în posesia organelor judiciare, se recurge, exclusiv, la percheziția informatică, utilizarea accesului la un sistem informatic, într-o atare situație, fiind o modalitate de eludare a garanțiilor specifice percheziției informatice. Prin urmare, fiind vorba despre efectuarea unei percheziții informatice în lipsa titularului sistemului, ea constituie o chestiune de legalitate, organele de urmărire penală neputând, după bunul plac, să efectueze o cercetare a sistemului informatic. În această ipoteză, opțiunea asupra utilizării unui mandat de acces la un sistem informatic sau a unui mandat de percheziție informatică va fi cenzurată de judecătorul de cameră preliminară, sub aspectul legalității administrării probelor de către organele de urmărire penală, conform art. 342 din Codul de procedură penală.

66. Atât accesul la un sistem informatic, cât și percheziția informatică sunt supuse testului de proporționalitate cu scopul urmărit, precum și celui de subsidiaritate, astfel încât intră în competența judecătorului de cameră preliminară analiza legalității încheierilor prin care judecătorul de drepturi și libertăți a încuviințat metoda specială de supraveghere, a legalității utilizării unui mandat de acces la un sistem informatic, respectiv a unui mandat de percheziție informatică în vederea copierii integrale a datelor dintr-un sistem informatic aflat în posesia organului de urmărire penală.

67. S-a arătat că, potrivit considerentelor Deciziei Curții Constituționale nr. 244/2017 (paragraful 63), în materia măsurilor de supraveghere tehnică, ce constituie o ingerință în viața privată a persoanelor supuse acestor măsuri, trebuie să existe un control *a posteriori* încuviințării și punerii în executare a supravegherii tehnice.

68. Spre deosebire de art. 138 alin. (3) din Codul de procedură penală, care prevede faptul că scopul metodei speciale de supraveghere a accesului la un sistem informatic este acela de a identifica probe, art. 168 alin. (1) din Codul de procedură penală prevede că scopul percheziției informatice este acela de a cerceta, identifica și strânge probe.

69. Astfel, plecând chiar de la scopul distinct precizat de legiuitor, se observă că doar în cazul percheziției informatice este permisă operațiunea de strângere a probelor. În măsura în care legiuitorul ar fi dorit să fie posibilă operațiunea de strângere a probelor și în cazul accesului la un sistem informatic, aceasta ar fi fost menționată în mod expres. Cu toate că termenii folosiți nu sunt suficient de clari pentru a elimina posibilitatea interpretărilor, este evident că prin sintagma ,,strânge probe” s-a făcut referire la culegerea probelor prin copierea datelor informatice, iar nu la operațiunea de strângere de probe în general. Scopul metodei de supraveghere a accesului la un sistem informatic este acela de a contribui la identificarea unor informații esențiale pentru desfășurarea anchetei în situațiile în care trecerea timpului ar afecta buna soluționare a cauzei,

iar nu de a permite copierea datelor, în acest scop existând posibilitatea efectuării unei percheziții informatice.

70. Mai mult decât atât, art. 138 alin. (13) din Codul de procedură penală prevede în mod explicit faptul că prin termenul de *supraveghere tehnică* se înțelege utilizarea uneia dintre metodele prevăzute la art. 138 alin. (1) lit. a)—d) din Codul de procedură penală, accesul la un sistem informatic fiind prevăzut la lit. b), aspect ce întărește opinia că accesul la sistem nu permite și copierea datelor, ci doar pătrunderea în sistemul informatic ori în mijlocul de stocare a datelor cu scopul de a cunoaște conținutul datelor și a analiza necesitatea solicitării emiterii unui mandat de percheziție informatică. Prin urmare, aspectul supus discuției este unul de legalitate.

71. Potrivit dispozițiilor art. 168 alin. (9) din Codul de procedură penală, procurorul poate efectua copii ale datelor informatice stocate pe sistemul ridicat în contextul încuviințării prealabile a percheziției informatice, copierea datelor realizându-se sub forma unei etape necesare pentru efectuarea în concret a percheziției informatice, iar, potrivit alin. (8) al aceluiași articol, organul de urmărire penală are posibilitatea de a dispune conservarea și copierea datelor informatice identificate în conținutul unui sistem informatic, în privința căruia se efectuează percheziția informatică, cercetarea acestor date presupunând mai departe obținerea unui mandat de percheziție informatică.

72. Față de aceste prevederi legale rezultă că procurorul este abilitat de legiuitor să realizeze conservarea și copierea datelor informatice aflate pe un suport informatic la care accesul a fost mediat de încuviințarea prealabilă a percheziției informatice, chiar asupra unui alt suport informatic, și nu printr-un alt procedeu, precum accesul la un sistem informatic. Prin urmare, ipotezele reglementate de legiuitor, în care procurorul poate realiza copia datelor informatice, sunt strâns legate de încuviințarea prealabilă a percheziției informatice, copierea realizându-se sub forma unei operațiuni necesare efectuării percheziției.

73. Or, având în vedere că procedeul probator al accesului la un sistem informatic presupune exclusiv identificarea datelor informatice stocate pe un suport informatic, ce ar putea fi relevante ori utile soluționării cauzei, fără a permite efectuarea unor alte operațiuni asupra respectivelor date, iar copierea datelor este reglementată de legiuitor drept o măsură intrinsecă efectuării percheziției informatice, s-a apreciat că operațiunea de copiere a datelor informatice nu poate fi realizată decât în baza unui mandat de percheziție informatică, apt a permite și cercetarea efectivă a conținutului acelor date, împrejurare ce implică, în mod necesar, respectarea cerințelor de legalitate reglementate de legiuitor, iar subsecvent, posibilitatea cenzurării acesteia de către judecătorul de cameră preliminară.

74. Informația stocată în sistemul informatic este protejată de dreptul la viața privată, astfel încât organul de urmărire penală nu poate efectua căutări în sistemul informatic în lipsa unor circumstanțe deosebite.

75. Deși, în raport cu caracterul urgent al activităților preconizate, pentru combaterea pierderii datelor digitale, procurorul poate opta pentru obținerea și/sau utilizarea unui mandat de acces la un sistem informatic în vederea copierii integrale a datelor aflate într-un sistem informatic pe care îl are în posesie (de exemplu, procurorul poate efectua o clonă a sistemului informatic sau a mijlocului de stocare atunci când observă că utilizatorul șterge documente din sistemul informatic), dată fiind ingerința în viața privată pe care o implică, conformitatea acestei abordări cu prevederile art. 8 din Convenția europeană a drepturilor omului este supusă controlului de legalitate în faza de cameră preliminară. Astfel, este de competența judecătorului de cameră preliminară analiza legalității încheierilor prin care judecătorul de drepturi și libertăți a încuviințat măsura de supraveghere tehnică sau percheziția informatică, precum și mijloacele de probă obținute în urma procedeului probatoriu încuviințat.

76. V.2.b) ***Într-o altă opinie*** s-a apreciat că opțiunea asupra emiterii, obținerii și/sau utilizării unui mandat de acces la un sistem informatic sau a unui mandat de percheziție informatică în vederea copierii integrale a datelor aflate într-un sistem informatic aflat în posesia organului de urmărire penală reprezintă ***o chestiune de oportunitate***, aflată la latitudinea organului de urmărire penală.

77. În acest sens au fost exprimate puncte de vedere de judecătorii de la Curtea de Apel București — Secția I penală, Curtea de Apel Iași, Curtea de Apel Pitești, Tribunalul Argeș, Tribunalul Bistrița-Năsăud, Tribunalul Brașov, Tribunalul Constanța, Tribunalul Galați, Tribunalul Giurgiu, Tribunalul Hunedoara, Tribunalul Iași, Tribunalul Ilfov, Tribunalul Mehedinți, Tribunalul Teleorman, Judecătoria Agnita, Judecătoria Alexandria, Judecătoria Baia Mare, Judecătoria Bârlad, Judecătoria Bolintin-Vale, Judecătoria Cornetu, Judecătoria Deva, Judecătoria Drobeta-Turnu Severin, Judecătoria Hațeg, Judecătoria Iași, Judecătoria Lugoj, Judecătoria Piatra-Neamț, Judecătoria Petroșani, Judecătoria Roman, Judecătoria Reghin, Judecătoria Roșiori de Vede, Judecătoria Sighișoara, Judecătoria Onești, Judecătoria Orșova, Judecătoria Târgu-Neamț, Judecătoria Turnu Măgurele, Judecătoria Videle, Judecătoria Zalău și Judecătoria Zimnicea.

78. Curtea de Apel Craiova și Tribunalul Olt au exprimat punctul de vedere potrivit căruia utilizarea unui mandat de acces la un sistem informatic sau a unui mandat de percheziție informatică reprezintă atât o chestiune de oportunitate aflată în sfera de apreciere a organului de urmărire penală, cât și o chestiune de legalitate supusă cenzurii judecătorului de cameră preliminară.

79. Judecătoria Luduș a nuanțat punctul de vedere în sensul că judecătorul de cameră preliminară este în drept să se pronunțe atât asupra legalității măsurii, cât și asupra oportunității, oportunitatea ținând în acest caz de legalitatea procedeului probator.

În susținerea celei de-a doua opinii, s-au adus următoarele argumente:

80. Obținerea unui mandat de acces la un sistem informatic sau a unui mandat de percheziție informatică în vederea copierii integrale a datelor dintr-un sistem informatic aflat în posesia organului de urmărire penală reprezintă o chestiune de oportunitate, putând exista necesitatea obținerii rapide a acestor date prin intermediul metodei de supraveghere tehnică a accesului la un sistem informatic, iar îndeplinirea condițiilor legale pentru încuviințarea măsurii supravegherii tehnice este verificată de judecătorul de drepturi și libertăți la momentul emiterii mandatului de supraveghere tehnică sau la momentul confirmării măsurii dispuse de procuror, conform art. 141 din Codul de procedură penală.

81. Judecătorul de cameră preliminară, raportat la obiectul procedurii prevăzute de art. 342 din Codul de procedură penală, nu are posibilitatea de a limita ori suplimenta probatoriul administrat în cursul urmăririi penale, în măsura în care au fost respectate condițiile de legalitate prevăzute de lege.

82. Odată autorizat mandatul de acces la un sistem informatic, copierea integrală a datelor aflate pe respectivul sistem rămâne o chestiune de oportunitate în sfera de apreciere a procurorului.

83. Opțiunea asupra emiterii, obținerii și/sau utilizării unui mandat de acces la un sistem informatic sau a unui mandat de percheziție informatică în vederea copierii integrale a datelor dintr-un sistem informatic aflat în posesia organului de urmărire penală reprezintă o chestiune de oportunitate aflată strict în sfera de apreciere a organului de urmărire penală, aspect relevat de însuși termenul „opțiune” cuprins în întrebarea adresată, fiind așadar o chestiune de temeinicie, și nu de legalitate, care să determine controlul din partea judecătorului de cameră preliminară.

84. Alegerea unui instrument probator sau a altuia reprezintă un aspect de oportunitate ce nu poate fi cenzurat de judecătorul de cameră preliminară, iar Codul de procedură penală nu impune o obligație în alegerea unui procedeu probator, cu prioritate față de altul. Organul de urmărire penală competent este cel care, în scopul obținerii de probe, apreciază, de la caz

la caz, asupra metodei de supraveghere tehnică ce ar putea conduce la realizarea acestui scop.

85. Revine organelor de urmărire penală ca, în funcție de împrejurările concrete ale fiecărei anchete, să aprecieze dacă se impune măsura de supraveghere tehnică a accesului la un sistem informatic sau procedeul probatoriu al percheziției informatice.

86. S-a mai susținut că este necesar a fi făcută diferența între metoda specială de supraveghere a accesului la un sistem informatic și procedeul probator al percheziției informatice, din punctul de vedere al realizării unor copii ale sistemului informatic. Potrivit art. 168 alin. (9) din Codul de procedură penală, în vederea executării percheziției, pentru asigurarea integrității datelor informatice stocate pe obiectele ridicate, procurorul dispune efectuarea de copii. După obținerea mandatului de percheziție informatică, procurorul este obligat să dispună efectuarea de copii (clone) ale dispozitivelor percheziționate în vederea asigurării integrității datelor acestora, în condițiile în care percheziția informatică se efectuează ulterior asupra clonei. În cazul metodei de supraveghere a accesului la un sistem informatic legea nu impune o astfel de obligație, accesul fiind efectuat în mod direct la sistemul informatic, iar nu la clona acestuia, de cele mai multe ori, această copie nefiind nici posibilă (de pildă, în cazul accesării e-mailurilor). Cu toate acestea, organele de urmărire penală pot realiza copii ale sistemului informatic identificat, de aceea opțiunea reprezintă o chestiune de oportunitate, aflată în sfera de apreciere a organului de urmărire penală, și nu o chestiune de legalitate.

87. V.3. S-a exprimat și ***opinia*** potrivit căreia ***prezenta sesizare*** a Înaltei Curți de Casație și Justiție în vederea dezlegării chestiunilor de drept menționate ***este inadmisibilă,*** fie în întregul ei, fie din perspectiva uneia sau alteia dintre cele două întrebări.

88. În acest sens au fost formulate puncte de vedere de către Tribunalul Gorj, Judecătoria Mizil, Judecătoria Timișoara și Judecătoria Vaslui.

89. *Inadmisibilitatea sesizării* a fost argumentată diferit în punctele de vedere formulate.

90. Astfel, s-a arătat că nu sunt întrunite condițiile prevăzute cumulativ de dispozițiile art. 475 din Codul de procedură penală, deoarece chestiunea de drept a cărei dezlegare se solicită nu este ivită în cursul judecății, așa cum se menționează explicit în textul de lege mai sus menționat, ci în procedura de cameră preliminară, iar de lămurirea acestei probleme nu depinde soluționarea în fond a cauzei.

91. Într-un alt punct de vedere s-a arătat că sesizarea este inadmisibilă în raport cu ambele întrebări formulate, cu argumentul că nu este necesară pronunțarea unei hotărâri prealabile pentru dezlegarea unei chestiuni de drept, dispozițiile legale care reglementează pătrunderea în sistemul informatic [art. 138 alin. (3) din Codul de procedură penală] fiind clare, în sensul că se realizează fie direct, fie de la distanță. Tot astfel sunt și dispozițiile care reglementează emiterea mandatului de acces la un sistem informatic și a mandatului de percheziție informatică, în vederea copierii integrale a datelor dintr-un sistem informatic aflat în posesia organelor de urmărire penală. S-a apreciat că și în acest caz dispozițiile legale sunt clare și nu necesită pronunțarea unei hotărâri prealabile.

92. Într-o altă opinie, inadmisibilitatea vizează întrebarea nr. 2, cu referire la opțiunea asupra emiterii, obținerii și/sau utilizării unui mandat de acces la un sistem informatic sau a unui mandat de percheziție informatică, cu referire la aspectul dacă reprezintă o chestiune de oportunitate sau de legalitate, susținându-se în argumentarea inadmisibilității că textul de lege este suficient de clar, în sensul că judecătorul de drepturi și libertăți este cel care dispune accesul la un sistem informatic sau percheziția informatică.

93. Tot în ceea ce privește întrebarea nr. 2, s-a arătat că răspunsul reiese în mod direct din normele procedurale la care se face trimitere. Dat fiind faptul că mandatul de acces este un act procedural, emis ca urmare a actului procesual al încuviințării și al dispoziției de emitere, este lesne de stabilit că inclusiv acesta va intra în sfera de verificare a judecătorului de cameră preliminară.

VI. **Opinia specialiștilor consultați**

94. În conformitate cu dispozițiile art. 476 alin. (10) raportat la art. 473 alin. (5) din Codul de procedură penală, a fost solicitată specialiștilor în drept penal opinia asupra chestiunilor de drept supuse examinării, fiind transmise puncte de vedere de către *Facultatea de Drept a Universității Babeș-Bolyai din Cluj-Napoca* și *Facultatea de Drept a Universității de Vest din Timișoara.*

95. ***Facultatea de Drept a Universității Babeș-Bolyai din Cluj-Napoca*** *a opinat în sensul că sunt îndeplinite condițiile de admisibilitate a sesizării,* astfel cum acestea sunt reglementate de dispozițiile art. 475 alin. (1) din Codul de procedură penală, și că, în privința întrebării nr. 2, se impune reformularea.

96. În ceea ce privește prima întrebare s-a arătat faptul că, așa cum rezultă din dispozițiile art. 138 alin. (3) din Codul de procedură penală, accesul la un sistem informatic se poate realiza fie direct, fie de la distanță. În consecință, în baza interpretării textuale, se poate conchide că măsura de supraveghere tehnică constând în accesul la un sistem informatic poate fi realizată direct, ipoteză în care organul de urmărire penală are contact direct și nemijlocit cu sistemul informatic sau cu mijlocul de stocare a datelor informatice. Ca atare, accesul la un sistem informatic, așa cum este prevăzut de art. 138 alin. (1) lit. b), alin. (3) și (13) din Codul de procedură penală, poate fi utilizat și atunci când sistemul informatic se află în posesia organului de urmărire penală.

97. În ceea ce privește a doua întrebare, potrivit dispozițiilor art. 342 din Codul de procedură penală, judecătorul de cameră preliminară nu are competența funcțională de a verifica dreptul de apreciere al organului de urmărire penală în ceea ce privește utilizarea unui procedeu probatoriu sau a altuia; competența judecătorului de cameră preliminară privește doar legalitatea utilizării unui anumit procedeu probatoriu.

98. Având o natură esențialmente investigativă, desfășurarea urmăririi penale, inclusiv opțiunea pentru un anumit procedeu probatoriu sau opțiunea pentru o anumită cronologie a procedeelor probatorii, intră în dreptul de apreciere al organului de urmărire penală. Exercitarea acestui drept nu intră, în mod direct, în obiectul camerei preliminare.

99. Pe de altă parte, verificând legalitatea unui mijloc de probă, judecătorul de cameră preliminară analizează respectarea condițiilor prevăzute de lege pentru administrarea acestuia. Această analiză nu privește însă dreptul de apreciere al organului de urmărire penală în alegerea procedeelor probatorii, ci respectarea dispozițiilor legale în ceea ce privește procedeul probatoriu ales.

100. Având în vedere cele de mai sus, s-a menționat că judecătorul de cameră preliminară are competența de a verifica legalitatea utilizării accesului la un sistem informatic sau legalitatea percheziției informatice, având în vedere condițiile specifice prevăzute de lege pentru fiecare dintre ele. În această analiză, judecătorul de cameră preliminară poate concluziona în sensul că organul de urmărire penală nu a respectat dispozițiile legale pentru utilizarea măsurii de supraveghere tehnică a accesului la un sistem informatic, iar în funcție de elementele de fapt concrete ale cauzei judecătorul de cameră preliminară poate arăta că, în concret, organul de urmărire penală ar fi trebuit să utilizeze procedeul probatoriu al percheziției informatice.

101. În realitate, problema de drept supusă analizei judecătorilor de cameră preliminară în procedura de soluționare a contestației a fost aceea a distincției dintre accesul la un sistem informatic în mod direct și percheziția informatică, însă instanța de trimitere nu a formulat întrebări care să vizeze în mod direct această chestiune.

102. În măsura în care Înalta Curte de Casație și Justiție va aprecia că este necesară pronunțarea și asupra acestei chestiuni, s-au formulat anumite observații.

103. Potrivit Codului de procedură penală, accesarea datelor informatice poate fi realizată fie prin utilizarea măsurilor de

supraveghere tehnică, așa cum este și accesul la un sistem informatic, fie prin percheziție informatică. În analiza distincției între cele două procedee probatorii, accesul la un sistem informatic și percheziția informatică, s-a apreciat că este esențial să fie avută în vedere natura juridică distinctă a celui dintâi. Accesul la un sistem informatic, inclusiv atunci când este realizat în mod direct, este o măsură de supraveghere tehnică reglementată în capitolul IV „Metode speciale de supraveghere sau cercetare" al titlului IV, natură conferită în mod expres de art. 138 alin. (13) din Codul de procedură penală.

104. Accesul la un sistem informatic are drept caracteristici: (1) este o metodă de supraveghere tehnică ce poate fi dispusă doar atunci când sunt îndeplinite condițiile prevăzute de art. 139 din Codul de procedură penală; (2) este o metodă de supraveghere tehnică cu caracter secret, iar acest lucru este de esența utilizării sale; (3) este o metodă de supraveghere tehnică utilizată pe o perioadă de timp expres indicată în încheierea judecătorului de drepturi și libertăți, putând fi prelungită atunci când este necesar în vederea obținerii de probe; (4) este o metodă de supraveghere tehnică ce are drept scop accesul la date informatice stocate și la date produse în perioada supravegherii.

105. În schimb, percheziția informatică are următoarele caracteristici: (1) este un procedeu probatoriu ce poate fi dispus doar atunci când sunt îndeplinite condițiile prevăzute de art. 168 alin. (1) din Codul de procedură penală; (2) este un procedeu probatoriu ce nu are caracter secret, suspectul sau inculpatul având dreptul să participe la efectuarea acesteia; (3) este un procedeu probatoriu ce poate fi utilizat doar pe o perioadă expres indicată în încheierea judecătorului de drepturi și libertăți sau în încheierea instanței de judecată, iar această perioadă este necesară doar pentru punerea în aplicare a procedeului probatoriu (spre exemplu, efectuarea de copii pentru a păstra integritatea datelor) și nu pentru urmărirea în timp a unor activități ulterioare; (4) este un procedeu probatoriu ce are drept scop accesul la date informatice stocate.

106. În ceea ce privește cea de-a patra caracteristică este important de precizat faptul că dispozițiile art. 168 din Codul de procedură penală fac referire, în mod expres, doar la probe „stocate". Cu referire la acest aspect, în literatura de specialitate s-a arătat că, *spre deosebire de percheziția în sistem informatic, procedeul probator al accesului la un sistem informatic are caracter confidențial față de persoana vizată, care nu este încunoștințată și nu participă la activitatea organelor judiciare, și vizează atât datele informatice anterioare, cât și pe cele create în timpul monitorizării* [G. Zlati, R. Slăvoiu, *Metode speciale de supraveghere sau cercetare,* în M. Udroiu (coordonator), *Codul de procedură penală. Comentariu pe articole,* Ed. C.H. Beck, București, 2020, ediția a III-a, p. 921]; *spre deosebire de accesul informatic, percheziția informatică va avea un caracter static, deoarece va surprinde numai datele informatice existente la un moment dat, or, accesul la un sistem informatic permite monitorizarea tehnică a activităților pe care le desfășoară făptuitorul pe o perioadă mai întinsă de timp* (în acest sens, M. Suian, *Metode speciale de supraveghere sau cercetare,* Ed. Solomon, București, 2021, p. 265).

107. În ipoteza în care accesul la un sistem informatic este realizat la distanță, distincția între această măsură de supraveghere tehnică și percheziția informatică este ușor de realizat. Pe de altă parte, dificultăți pot să apară atunci când accesul la un sistem informatic este realizat în mod direct. În această ultimă ipoteză, criteriul care permite distincția între accesul la un sistem informatic și percheziția informatică este natura juridică diferită a acestora.

108. Chiar dacă este realizat în mod direct, accesul la un sistem informatic își păstrează natura juridică de metodă de supraveghere tehnică. Acest lucru înseamnă că, în raport cu elementele de fapt concrete ale cauzei, organul de urmărire penală apreciază că este necesar caracterul secret al acestei metode de supraveghere și desfășurarea ei continuă pe o perioadă de timp în scopul obținerii de date stocate și de date produse în perioada supravegherii.

109. Păstrarea caracterului secret, caracteristică esențială a metodelor tehnice de supraveghere, trebuie justificată de organul de urmărire penală prin trimitere la elementele de fapt concrete ale cauzei. Spre exemplu, un investigator sub acoperire, a cărui activitate este autorizată conform legii, a sustras un telefon al suspectului și l-a predat organului de urmărire penală; pentru a păstra caracterul secret al metodei de investigare tehnică și pentru a obține atât date stocate, cât și date produse în timp real, procurorul solicită judecătorului de drepturi și libertăți autorizarea accesului la un sistem informatic sau dispune, dacă sunt îndeplinite condițiile prevăzute de art. 141 din Codul de procedură penală, autorizarea de urgență pe o perioadă de maximum 48 de ore. Verificarea îndeplinirii condițiilor prevăzute de lege, în raport cu elementele de fapt concrete ale cauzei, aparține judecătorului de cameră preliminară.

110. ***Universitatea de Vest din Timișoara — Facultatea de Drept, Centrul de cercetări în științe penale*** *a opinat în sensul că nu sunt îndeplinite toate condițiile de admisibilitate prevăzute de art. 475 din Codul de procedură penală.*

111. În acest sens, s-a menționat că, deși sunt îndeplinite primele trei condiții de admisibilitate (cauza se află în fața unui complet de judecători de cameră preliminară care se va pronunța prin încheiere definitivă asupra contestațiilor formulate; chestiunea de drept *pendinte* nu a făcut obiectul altor sesizări pentru pronunțarea unei hotărâri prealabile sau a unui recurs în interesul legii și nici nu face obiectul unui recurs în interesul legii în curs de soluționare; chestiunea de drept este aptă să influențeze soluția pe fondul cauzei, întrucât în funcție de modul de soluționare a problemei se va putea decide soluția în privința contestației, respectiv dacă soluția judecătorului de cameră preliminară inițial învestit este legală sau nu, cu consecința admiterii sau respingerii căii de atac, legalitatea administrării probelor în faza de urmărire penală având aptitudinea de a influența nu doar soluția pronunțată în cameră preliminară, ci și soluționarea fondului cauzei), nu este îndeplinită și cea de-a patra condiție, dedusă din jurisprudența Înaltei Curți de Casație și Justiție — Completul pentru dezlegarea unor chestiuni de drept în materie penală, referitoare la împrejurarea ca problema ridicată să fie o veritabilă problemă de drept penal sau procesual penal, cu caracter dificil, să aibă caracter de noutate și să necesite o rezolvare de principiu, în raport cu potențialul acesteia de a genera interpretări diferite în practica judiciară.

112. În punctul de vedere formulat s-a apreciat că la ambele probleme de drept invocate se poate da un răspuns pe baza textelor de lege incidente din Codul de procedură penală.

113. Astfel, *cu referire la prima întrebare:* „Dacă procedeul probator al accesului la un sistem informatic poate fi utilizat atunci când (i) suportul informatic se află în detenția fizică a organului de urmărire penală sau dacă acest procedeu probator permite doar (ii) pătrunderea de la distanță într-un astfel de sistem în vederea monitorizării/supravegherii activității derulate?", s-a apreciat că răspunsul se găsește în însăși definiția legală a accesului la un sistem informatic, prevăzută în art. 138 alin. (3) din Codul de procedură penală. Potrivit normei menționate, prin *acces la un sistem informatic* se înțelege „pătrunderea într-un sistem informatic sau mijloc de stocare a datelor informatice, fie direct, fie de la distanță, prin intermediul unor programe specializate ori prin intermediul unei rețele, în scopul de a identifica probe". În consecință, acest procedeu probatoriu permite pătrunderea nu doar de la distanță, ci și direct, prin interacțiune directă, la locul unde este amplasat sau unde se găsește sistemul informatic, fără cunoștința persoanei supravegheate, prin infiltrarea, accesarea directă și copierea unor date informatice.

114. În continuare, s-a arătat că întrebarea referitoare la utilizarea acestui procedeu atunci când „suportul" se află în detenția fizică a organului de urmărire penală se referă la situația de fapt din speță, în care organul de urmărire penală procedase la ridicarea unor telefoane mobile cu ocazia percheziției domiciliare. Sistemul informatic sau mijlocul de stocare cu care organul de urmărire penală a intrat în contact

fizic se pretează fie la o interacțiune prin intermediul procedeului de acces la un sistem informatic, fie prin intermediul procedeului percheziției informatice. Diferența constă în faptul că primul procedeu are caracter confidențial, pe când cel de-al doilea se face în prezența obligatorie a suspectului sau inculpatului. În consecință, atunci când sistemul informatic sau mijlocul de stocare a datelor informatice a ajuns în detenția fizică a organului de urmărire penală, procedeul de aplicat este cel al percheziției informatice, întrucât, prin ipoteză, caracterul confidențial al accesului la un sistem informatic nu mai poate fi avut în vedere. Utilizarea într-o asemenea situație a procedeului de acces la un sistem informatic este nelegală, întrucât înfrânge drepturile apărării, prin absența suspectului sau a inculpatului. Tentația de a folosi acest procedeu numai pentru că accesul poate fi permis provizoriu prin autorizarea emisă de procuror eludează dispozițiile imperative ce impun emiterea unui mandat de judecătorul de drepturi și libertăți.

115. *Cu privire la cea de-a doua întrebare:* „Dacă opțiunea asupra emiterii, obținerii și/sau utilizării unui mandat de acces la un sistem informatic sau a unui mandat de percheziție informatică în vederea copierii integrale a datelor aflate într-un sistem informatic aflat în posesia organului de urmărire penală reprezintă o chestiune de oportunitate, aflată în sfera de apreciere a organului de urmărire penală, sau o chestiune de legalitate supusă cenzurii judecătorului de cameră preliminară?”, s-a apreciat că răspunsul se regăsește, de asemenea, în prevederile exprese ale Codului de procedură penală. Astfel, dispozițiile art. 141 alin. (5) din Codul de procedură penală prevăd: „Cu privire la datele informatice identificate prin accesul la un sistem informatic, procurorul poate dispune, prin ordonanță, realizarea și conservarea unei copii a acestor date informatice [...]. Copiile se realizează cu mijloace tehnice și proceduri adecvate, de natură să asigure integritatea informațiilor conținute de acestea.” În aceeași chestiune, art. 168 alin. (9) și (10) din Codul de procedură penală prevede că: „În vederea executării percheziției dispuse, pentru asigurarea integrității datelor informatice stocate pe obiectele ridicate, procurorul dispune efectuarea de copii. Dacă ridicarea obiectelor care conțin datele informatice prevăzute la alin. (1) ar afecta grav desfășurarea activității persoanelor care dețin aceste obiecte, procurorul poate dispune efectuarea de copii, care servesc ca mijloc de probă. Copiile se realizează cu mijloace tehnice și proceduri adecvate, de natură să asigure integritatea informațiilor conținute de acestea”. În consecință, ambele procedee informatice permit efectuarea unei copii integrale a datelor informatice.

116. Nuanța întrebării dacă ar exista o alegere între un procedeu și celălalt la discreția organului de urmărire penală, care are în posesie sistemul informatic sau mijlocul de stocare a datelor informatice, vizează, de asemenea, aplicarea literală a legii. Opțiunea nu există cât timp cele două procedee au regimuri diferite, motivate de apartenența accesului la un sistem informatic la categoria măsurilor de supraveghere tehnică (măsuri oculte) și a percheziției informatice la categoria procedurilor de investigare transparente. În toate cazurile, modul în care a ales un organ de urmărire penală să utilizeze un procedeu probator ce conduce la obținerea unor mijloace de probă apte să fie utilizate în procesul penal trebuie și poate fi supus cenzurii de legalitate din partea judecătorului de cameră preliminară, potrivit art. 342 din Codul de procedură penală.

117. În concluzie, fără a se impune interpretări sofisticate în materie, răspunsul la întrebările adresate se poate face în mod facil, situație ce nu deschide calea sesizării instanței supreme în procedura prevăzută de art. 475 din Codul de procedură penală.

VII. **Punctul de vedere exprimat de Ministerul Public — Parchetul de pe lângă Înalta Curte de Casație și Justiție — Secția judiciară** a fost *în sensul inadmisibilității sesizării* prin care s-a solicitat Înaltei Curți de Casație și Justiție să dea o dezlegare de principiu celor două chestiuni de drept anterior menționate.

118. Ministerul Public a susținut că nu sunt îndeplinite cumulativ toate cele trei condiții prevăzute de art. 475 din Codul de procedură penală, lipsind condiția ca de lămurirea chestiunii de drept să depindă soluționarea pe fond a cauzei în care a fost invocată.

119. S-a arătat că situația juridică premisă care a generat sesizarea Completului pentru dezlegarea unor chestiuni de drept în materie penală se regăsește în cauza în care a fost formulată sesizarea, respectiv, cu prilejul unei percheziții domiciliare, a fost ridicat un telefon mobil, aparținând unuia dintre inculpați, în aceeași zi, procurorul autorizând provizoriu accesul la telefonul mobil pe o perioadă de 48 de ore, în baza art. 141 alin. (1) din Codul de procedură penală. În baza ordonanței procurorului, un ofițer de poliție specialist din cadrul I.G.P.R. — D.C.C.O. — Serviciul de Combatere a Criminalității Informatice a accesat sistemul informatic și a procedat la copierea integrală și extragerea conținutului acestuia, inclusiv a unor convorbiri purtate prin intermediul aplicațiilor Signal și Telegram și a înregistrării video a unei discuții efectuate cu telefonul mobil, toate activitățile de supraveghere efectuate fiind consemnate într-un proces-verbal. Ulterior, măsura de supraveghere tehnică provizorie a fost confirmată de judecătorul de drepturi și libertăți.

120. În ceea ce privește condiția de admisibilitate a sesizării privind existența unei chestiuni de drept de care să depindă soluționarea pe fond a cauzei în care a fost invocată, s-a arătat că a fost consacrată jurisprudențial de Completul pentru dezlegarea unor chestiuni de drept în materie penală, între altele, prin deciziile nr. 11 din 2 iunie 2014, nr. 17 din 1 septembrie 2014, nr. 22 din 6 octombrie 2014, nr. 23 din 6 octombrie 2014, nr. 24 din 6 octombrie 2014, nr. 7 din 17 aprilie 2015, nr. 11 din 12 septembrie 2018 și nr. 21 din 29 octombrie 2019. În aceste decizii s-a reținut că, prin instituirea condiției anterior menționate, s-a urmărit excluderea de la procedura reglementată de art. 475 din Codul de procedură penală a problemelor de drept de care nu depinde soluționarea pe fond a cauzelor penale și care pot fi interpretate pe calea recursului în interesul legii; totodată, că nu este îndeplinită condiția privind legătura problemei de drept a cărei dezlegare se solicită cu soluționarea pe fond a cauzei, în ipoteza în care chestiunea de drept nu vizează soluționarea acțiunii penale sau civile a cauzei, astfel cum prevăd dispozițiile art. 349 și următoarele din Codul de procedură penală.

121. În plus, în jurisprudența recentă a Înaltei Curți de Casație și Justiție, reflectată în deciziile nr. 2 din 27 ianuarie 2022 și nr. 44 din 19 septembrie 2022, s-a statuat că nu este îndeplinită cerința de admisibilitate menționată, din perspectiva existenței unei chestiuni de drept care să vizeze o judecată propriu-zisă a acțiunii penale, în cauzele în care nu s-a dispus încă începerea judecății, ca fază distinctă a procesului penal, în care se dă o rezolvare raportului juridic penal de conflict, problema de drept cu a cărei dezlegare a fost sesizată instanța supremă fiind invocată în fața judecătorului de cameră preliminară, a cărui competență funcțională nu include și judecarea pe fond a litigiului, ci se limitează exclusiv la verificarea competenței și a legalității sesizării instanței, a legalității administrării probelor și a efectuării actelor de către organele de urmărire penală.

122. Din această perspectivă, s-a subliniat și o reconsiderare a practicii instanței supreme, exprimată în Decizia nr. 23 din 4 mai 2022 a Completului pentru dezlegarea unor chestiuni de drept în materie penală, în cuprinsul căreia s-a reținut că este îndeplinită condiția admisibilității sesizării, atunci când dezlegarea dată produce consecințe asupra soluției ce ar putea fi dată fondului problematicii specifice camerei preliminare.

123. În cauză, problemele de drept a căror dezlegare a solicitat-o Curtea de Apel Pitești nu au fost invocate cu prilejul judecării pe fond a cauzei, ci în cadrul procedurii de cameră preliminară, cu prilejul soluționării contestației formulate în temeiul art. 347 din Codul de procedură penală, împotriva încheierii prin care au fost soluționate cererile și excepțiile privind legalitatea administrării probelor și a efectuării actelor de urmărire penală.

124. În consecință, lămurirea chestiunilor ce formează obiectul întrebării prealabile nu se repercutează în niciun fel asupra modalității de soluționare a fondului cauzei, neexistând relația de dependență necesară între problemele de drept supuse interpretării și rezolvarea acțiunii penale și/sau civile, ceea ce determină inadmisibilitatea sesizării pentru neîndeplinirea uneia dintre condițiile prevăzute cumulativ de art. 475 din Codul de procedură penală.

125. S-a mai arătat că sesizarea este inadmisibilă și din alte considerente. Din analiza jurisprudenței Înaltei Curți de Casație și Justiție — Completul pentru dezlegarea unor chestiuni de drept în materie penală rezultă că sesizarea, în procedura întrebărilor prealabile, trebuie efectuată doar în situația în care, în cursul soluționării unei cauze penale, se pune problema interpretării și aplicării unor dispoziții legale neclare, evazive și care ar putea da naștere unor soluții diferite, generând astfel practică judiciară neunitară (în acest sens fiind deciziile nr. 2 din 8 februarie 2018, nr. 15 din 24 septembrie 2019, nr. 11 din 18 februarie 2021 și nr. 17 din 17 martie 2021 ale Completului pentru dezlegarea unor chestiuni de drept în materie penală).

126. Raportat la cele mai sus menționate, s-a arătat că instanța de trimitere avea de analizat legalitatea și temeinicia autorizării de către procuror a măsurii accesului la un sistem informatic, precum și legalitatea și temeinicia încheierii prin care a fost confirmată măsura de către judecătorul de drepturi și libertăți și, în acest sens, legiuitorul a prevăzut, în cuprinsul art. 141 raportat la art. 138 alin. (1) lit. b) din Codul de procedură penală, condițiile în care se poate dispune, în cursul urmăririi penale, accesul la un sistem informatic de către procuror, iar, în cuprinsul art. 168 din Codul de procedură penală, condițiile în care se poate efectua o percheziție în sistem informatic.

127. Astfel, din cuprinsul prevederilor art. 138 alin. (3) din Codul de procedură penală rezultă că pătrunderea într-un sistem informatic sau mijloc de stocare a datelor informatice se poate face fie direct, la locul unde se află sistemul informatic, fie de la distanță, prin intermediul unor programe specializate ori prin intermediul unei rețele de comunicații, utilizându-se softuri specializate, în scopul de a identifica probe.

128. Dispozițiile art. 141 alin. (1) din Codul de procedură penală stipulează condițiile în care procurorul poate autoriza provizoriu măsura de supraveghere tehnică, instituind o excepție de la regula competenței exclusive a judecătorului de drepturi și libertăți în ce privește dispunerea supravegherii tehnice, justificată de existența unei stări de urgență și de riscul producerii unor consecințe negative (pentru probatoriul cauzei sau pentru siguranța unei persoane), dacă s-ar urma procedura obișnuită de autorizare a măsurii. Prin urmare, autorizarea provizorie de către procuror a măsurii accesului la un sistem informatic este posibilă în măsura în care, în funcție de elementele de fapt specifice cauzei, parcurgerea procedurii de emitere a mandatului de supraveghere tehnică de către judecător ar duce la pierderea momentului operativ, a posibilității de a obține anumite probe sau la punerea în pericol a siguranței persoanei vătămate, a martorului sau a membrilor familiilor acestora.

129. Întrucât scopul accesului la un sistem informatic este identificarea de probe, iar potrivit art. 285 alin. (1) din Codul de procedură penală, urmărirea penală are ca obiect, între altele, strângerea probelor necesare cu privire la existența infracțiunilor, la identificarea persoanelor care au săvârșit o infracțiune și la stabilirea răspunderii penale a acestora, constatarea îndeplinirii condițiilor cumulative prevăzute de art. 141 alin. (1) lit. a) și b) din Codul de procedură penală intră în competența procurorului care efectuează sau supraveghează urmărirea penală. Art. 141 alin. (3) din Codul de procedură penală instituie, însă, obligația procurorului, ca, în termen de cel mult 24 de ore de la expirarea măsurii, să sesizeze judecătorul de drepturi și libertăți în vederea verificării legalității și temeiniciei autorizării accesului la un sistem informatic și confirmării măsurii.

130. În ceea ce privește datele informatice identificate prin pătrunderea în sistemul informatic, procurorul poate dispune, prin ordonanță, potrivit art. 141 alin. (5) lit. a) și b) din Codul de procedură penală, realizarea și conservarea unei copii a datelor cu mijloace tehnice și proceduri adecvate de natură să asigure integritatea informațiilor conținute de acestea sau suprimarea accesării sau îndepărtarea datelor din sistemul informatic.

131. În cauza de față, organele de urmărire penală s-au aflat în contact fizic cu sistemul informatic, iar accesarea acestuia s-a făcut în mod direct, în locul unde se afla telefonul mobil, potrivit art. 138 alin. (3) din Codul de procedură penală, care prevede această modalitate de pătrundere în sistemul informatic, fiind urmată de copierea integrală a sistemului informatic, inclusiv a unor convorbiri purtate prin intermediul aplicațiilor Signal și Telegram. Măsura de supraveghere provizorie a fost supusă controlului judiciar *a posteriori,* fiind confirmată de judecătorul de drepturi și libertăți.

132. În ceea ce privește identificarea și strângerea probelor aflate într-un sistem informatic prin intermediul percheziției informatice, potrivit dispozițiilor art. 168 din Codul de procedură penală, a căror dificultate de interpretare și aplicare a constatat-o instanța de trimitere, se stipulează în termeni clari și concișii care sunt condițiile în care poate fi dispusă percheziția informatică și scopul urmărit prin aceasta, împrejurare de natură să împiedice orice confuzie cu măsura de supraveghere tehnică constând în accesul la un sistem informatic.

133. Potrivit dispozițiilor mai sus menționate, percheziția informatică reprezintă un procedeu de cercetare, descoperire, identificare și strângere a probelor stocate într-un sistem informatic sau suport de stocare a datelor informatice, realizat prin intermediul unor mijloace tehnice și proceduri adecvate, de natură să asigure integritatea informațiilor conținute. În vederea executării percheziției informatice, pentru asigurarea integrității datelor informatice stocate pe obiectele ridicate, procurorul dispune efectuarea de copii.

134. Distincția între cele două procedee probatorii a fost analizată în doctrină, constatându-se că accesul la un sistem informatic presupune pătrunderea într-un sistem informatic sau într-un mediu de stocare a datelor informatice, fie direct, fie de la distanță, prin intermediul unor programe specializate sau a unei rețele, în scopul de a identifica probele existente sau pe cele generate pe parcursul supravegherii tehnice, pe când percheziția informatică constă în cercetarea unui sistem informatic sau a unui mediu de stocare a datelor informatice, în vederea descoperirii și strângerii probelor existente pe acesta. În continuare, au fost menționate și diferențele în ceea ce privește organul competent să autorizeze măsurile (accesul la un sistem informatic poate fi autorizat provizoriu și de către procuror, pe când percheziția poate fi dispusă în cursul urmăririi penale numai de către judecătorul de drepturi și libertăți), precum și diferențele privind regimul de confidențialitate, respectiv participare la procedură (percheziția în sistem informatic se efectuează în prezența suspectului sau a inculpatului, pe când accesul la un sistem informatic are caracter confidențial, desfășurându-se în lipsa persoanei vizate de măsură sau a avocatului acesteia).

135. Prin urmare, în opinia Ministerului Public, în cursul urmăririi penale, alegerea uneia dintre cele două modalități legale de obținere a mijloacelor de probă este lăsată la aprecierea procurorului, fiind o chestiune de oportunitate legată de particularitățile cauzei, neputând astfel face obiectul verificării în camera preliminară. Legalitatea administrării probelor obținute prin aceste procedee probatorii urmează a fi supusă verificării judecătorului de cameră preliminară, potrivit art. 342 din Codul de procedură penală.

136. S-a apreciat astfel că prevederile art. 141 raportat la art. 138 alin. (1) lit. b) și art. 168 din Codul de procedură penală sunt clare, neechivoce, iar aplicarea corectă a dreptului se impune într-un mod evident, încât nu lasă loc de îndoială cu privire la modul de soluționare a întrebării adresate.

137. În fine, s-a arătat că inadmisibilitatea decurge și din aceea că problemele de drept invocate nu privesc interpretarea *in abstracto* a unor dispoziții legale determinate, adică nu au ca finalitate o dezlegare cu valoare de principiu, ci tind către rezolvarea unor chestiuni ce țin de particularitățile cauzei. Or, potrivit practicii constante a Completului pentru dezlegarea unor

chestiuni de drept în materie penală (de exemplu, Decizia nr. 14 din 12 mai 2015, Decizia nr. 21 din 4 iunie 2015, Decizia nr. 10 din 12 aprilie 2016, Decizia nr. 14 din 18 mai 2016, Decizia nr. 68 din 29 septembrie 2021 etc.), pentru a constitui o problemă de drept, premisa de la care se pornește trebuie să aibă izvorul în dispozițiile legale și nu într-o stare de fapt.

138. Pentru toate aceste considerente, în temeiul dispozițiilor art. 475—477 din Codul de procedură penală, s-a solicitat respingerea, ca inadmisibilă, a sesizării.

VIII. **Examenul jurisprudenței în materie**

1. ***Jurisprudența națională relevantă***

139. În materialul transmis de curțile de apel a fost identificată o singură hotărâre judecătorească, cu relevanță pentru problema de drept ridicată în speță.

140. Astfel, a fost comunicată încheierea din 16.10.2020 a judecătorului de drepturi și libertăți din cadrul Judecătoriei Sectorului 1 București, pronunțată în Dosarul nr. 32.521/299/2020, prin care, deși a fost respinsă cererea de acces la sisteme informatice ridicate de organele de urmărire penală cu ocazia percheziției domiciliare, ca neîntemeiată, prezintă relevanță din perspectiva clarificării conceptului de acces la un sistem informatic și a distincției în raport cu percheziția informatică.

141. S-a reținut că accesul la un sistem informatic presupune, în esență, identificarea probelor aflate într-un dispozitiv de prelucrare automată a datelor (calculator, tabletă, telefon mobil etc.) sau într-un mijloc de stocare (hard, drive, CD, memory stick etc.) prin folosirea unor procedee tehnice care să asigure confidențialitatea acestui demers. Scopul acestei măsuri de supraveghere tehnică este acela de a obține datele și probele necesare anchetei, fără ca inculpații să cunoască acest lucru.

142. Accesul la un sistem informatic prevăzut de art. 138 alin. (3) din Codul de procedură penală nu trebuie confundat cu percheziția informatică reglementată de art. 168 din Codul de procedură penală, între cele două existând diferențe esențiale, printre care și faptul că percheziția necesită prezența obligatorie a suspectului sau a inculpatului, pe când accesul la un sistem informatic are caracter confidențial față de persoana vizată și are în vedere atât datele informatice anterioare, cât și pe cele create în timpul monitorizării. Garanțiile existente în materia percheziției informatice prin raportare la măsura de supraveghere a accesului la un sistem informatic sunt net favorabile inculpaților, în condițiile în care, în cazul percheziției informatice, este necesar să se realizeze o copie de pe mijloacele de stocare a datelor informatice, ceea ce implică utilizarea unor mijloace tehnice adecvate, accesul la un sistem informatic fiind lipsit de astfel de garanții.

143. În fine, s-a mai reținut că, dacă în cazul efectuării percheziției informatice nu există riscuri de modificare a variabilelor atașate respectivelor date informatice, în ipoteza accesului, acest risc nu este înlăturat, modificările putând interveni și involuntar (de pildă, în ipoteza accesării unui fișier va putea fi schimbată data ultimei accesări), aspect ce poate conduce la alterarea probatoriului.

2. ***Jurisprudența Înaltei Curți de Casație și Justiție***

144. Cu referire la problemele de drept ce fac obiectul sesizării, nu au fost identificate decizii obligatorii, menite să asigure unificarea practicii judiciare.

145. În ceea ce privește deciziile de speță, la nivelul Completului de 5 Judecători nu au fost identificate hotărâri în care să fi fost analizată problema de drept supusă dezlegării.

3. ***Jurisprudența Curții Constituționale***

146. Nu au fost identificate decizii relevante în problema de drept supusă analizei.

IX. **Jurisprudența relevantă a Curții Europene a Drepturilor Omului**

147. În jurisprudența CEDO au fost identificate mai multe decizii referitoare la percheziția informatică, fără însă a fi analizate aspecte referitoare la problemele de drept ce fac obiectul sesizării, din perspectiva diferențierii celor două procedee probatorii, în jurisprudența identificată fiind relevate aspecte ce țin de asigurarea garanțiilor în vederea protejării drepturilor reglementate de Convenția Europeană a Drepturilor Omului.

148. Curtea Europeană a criticat de-a lungul jurisprudenței sale modalitatea de redactare a mandatelor de percheziție în termeni excesiv de largi, care a permis organelor judiciare o putere discreționară în efectuarea percheziției și în stabilirea documentelor ce prezintă importanță pentru ancheta penală (CEDO, hotărârea din 4 februarie 2020, Cauza *Kruglov ș.a. c. Rusiei*; CEDO, hotărârea din 22 decembrie 2008, Cauza *Aleksanyan c. Rusiei*; CEDO, hotărârea din 3 iulie 2012, Cauza *Robathin c. Austriei*). În același timp, a reiterat importanța proporționalității măsurii cu scopul urmărit și cu mijloacele folosite și a necesității măsurii într-o societate democratică. A statuat, în numeroase rânduri, asupra necesității emiterii mandatului de percheziție de către un judecător și a respectării dreptului la viață privată.

149. De pildă, în Cauza *Sérvulo & Associados — Sociedade de Advogados v. Portugalia* (Hotărârea din 3.09.2015 — Cererea nr. 27.013/10), Curtea, evaluând asigurarea garanțiilor necesare în vederea respectării art. 8 din Convenție, a apreciat că nu a existat o încălcare din acest punct de vedere. În esență, în cauză fuseseră percheziționate sisteme informatice folosite de un cabinet de avocatură, iar procurorul, în baza unui mandat de percheziție emis de judecător, a obținut și date informatice aflate sub secret profesional sau care conțineau și date personale. În urma contestării măsurii, judecătorul a dispus sigilarea documentelor obținute și, în urma verificărilor efectuate asupra acestora, a dispus ștergerea celor care erau protejate de secretul profesional și care conțineau date personale. Curtea a observat astfel că au fost respectate toate garanțiile, reclamantul fiind prezent personal la efectuarea percheziției, fiind, de asemenea, prezent, și un avocat desemnat de barou. Totodată, a observat că, deși investigația a fost condusă de un procuror, cu toate acestea, un judecător a exercitat controlul asupra percheziției informatice, anterior, în timpul derulării acesteia și ulterior finalizării sale, posibilitatea contestării limitelor mandatului de percheziție informatică fiind un remediu efectiv și adecvat, iar controlul judecătorului compensând limitele mai largi ale mandatului de percheziție informatică.

X. **Direcția Legislație, jurisprudență și contencios — Serviciul pentru studiul și unificarea jurisprudenței din cadrul Înaltei Curți de Casație și Justiție** a comunicat că au fost identificate încheierile nr. 137 din 4 martie 2019, nr. 787 din 13 decembrie 2022 și nr. 1/C din 31 ianuarie 2023, pronunțate de Înalta Curte de Casație și Justiție — Secția penală, care cuprind considerente relevante pentru soluționarea sesizării. Cu toate acestea, nu au fost identificate hotărâri judecătorești prin care să fie rezolvate în mod direct problemele de drept deduse interpretării.

XI. **Opinia judecătorului-raportor**

150. Soluția propusă de judecătorul-raportor a fost aceea de *respingere, ca inadmisibilă, a sesizării* formulate de Curtea de Apel Pitești — Secția penală și pentru cauze cu minori și de familie, în vederea pronunțării unei hotărâri prealabile pentru dezlegarea chestiunilor de drept invocate.

XII. **Înalta Curte de Casație și Justiție**

Admisibilitatea sesizării

151. Potrivit dispozițiilor art. 475 din Codul de procedură penală, dacă, în cursul judecății, un complet de judecată învestit cu soluționarea cauzei în ultimă instanță, constatând că există o chestiune de drept, de a cărei lămurire depinde soluționarea pe fond a cauzei respective și asupra căreia Înalta Curte de Casație și Justiție nu a statuat printr-o hotărâre prealabilă sau printr-un recurs în interesul legii și nici nu face obiectul unui recurs în interesul legii în curs de soluționare, va putea solicita Înaltei Curți de Casație și Justiție să pronunțe o hotărâre prin care să se dea rezolvare de principiu chestiunii de drept cu care a fost sesizată.

152. În raport cu textul legal evocat se constată că admisibilitatea unei sesizări formulate în procedura pronunțării unei hotărâri prealabile este condiționată de *îndeplinirea, în mod cumulativ, a următoarelor cerințe*: întrebarea să fie formulată de un complet al Înaltei Curți de Casație și Justiție, al unei curți de apel sau al unui tribunal învestit cu soluționarea cauzei în ultimă

instanță; soluționarea pe fond a acelei cauze să depindă de lămurirea chestiunii de drept ce formează obiectul sesizării; problema de drept să nu fi fost încă dezlegată de Înalta Curte de Casație și Justiție prin mecanismele legale ce asigură interpretarea și aplicarea unitară a legii de către instanțele judecătorești sau să nu facă în prezent obiectul unui recurs în interesul legii.

153. Totodată, din economia dispozițiilor legale invocate, precum și din jurisprudența Completului pentru dezlegarea unor chestiuni de drept în materie penală reiese că admisibilitatea sesizării este condiționată, în mod esențial, de existența unei veritabile probleme de drept, care să facă necesară o rezolvare de principiu prin pronunțarea unei hotărâri prealabile de către Înalta Curte de Casație și Justiție, aceasta constituind, de fapt, premisa fundamentală ce justifică intervenția instanței supreme prin mecanismul de unificare a practicii judiciare instituit de art. 475 și următoarele din Codul de procedură penală.

154. Astfel, cu privire la *prima condiție*, se constată că *este îndeplinită*, în cauză, solicitarea de lămurire a problemei de drept invocate aparținând unei instanțe învestite cu soluționarea cauzei în ultim grad de jurisdicție, respectiv Curtea de Apel Pitești, pe rolul căreia se află înregistrat dosarul nr. 2.485/90/2022/a1, ce are ca obiect contestațiile formulate de inculpații H.B., M.Gh.C., R.U.-C., S.C.-M. și B.A.-M. împotriva Încheierii nr. 237 din data de 21.12.2022, pronunțată de judecătorul de cameră preliminară din cadrul Tribunalului Vâlcea.

155. De asemenea, se constată *îndeplinită și condiția ce vizează caracterul de actualitate a problemei de drept invocate în cauză*, din relațiile comunicate de Parchetul de pe lângă Înalta Curte de Casație și Justiție și din verificările efectuate la nivelul instanței supreme rezultând că nu au fost pronunțate hotărâri prealabile sau în recurs în interesul legii de către Înalta Curte de Casație și Justiție cu privire la chestiunea de drept supusă analizei și aceasta nici nu face obiectul unui recurs în interesul legii în curs de soluționare.

156. **Cu privire la condiția existenței unei legături între chestiunea de drept supusă interpretării și soluționarea pe fond a cauzei**, în doctrină s-a evidențiat că aceasta este îndeplinită ori de câte ori interdependența procedurilor specifice cauzei influențează într-o măsură soluționarea fondului, soluția dată acțiunii penale sau civile în procesul penal.

157. În jurisprudența Completului pentru dezlegarea unor chestiuni de drept în materie penală s-a statuat asupra înțelesului ce trebuie atribuit sintagmei „chestiune de drept de a cărei lămurire depinde soluționarea pe fond a cauzei”, regăsită în cuprinsul art. 475 din Codul de procedură penală.

158. S-a subliniat, sub un prim aspect, că între problema de drept a cărei lămurire se solicită — indiferent dacă ea vizează o normă de drept material sau o dispoziție de drept procesual — și soluția ce urmează a fi dată de către instanța de trimitere trebuie să existe o relație de dependență, în sensul în care decizia instanței supreme să fie de natură a produce un efect concret asupra conținutului hotărârii din procesul principal (Decizia nr. 11 din 2 iunie 2014, publicată în Monitorul Oficial al României, Partea I, nr. 503 din 7 iulie 2014, și Decizia nr. 19 din 15 septembrie 2014, publicată în Monitorul Oficial al României, Partea I, nr. 769 din 23 octombrie 2014).

159. În al doilea rând, s-a evidențiat necesitatea ca dezlegarea chestiunii de drept care formează obiectul sesizării să fie determinantă pentru rezolvarea acțiunii penale sau a acțiunii civile în procesul penal, ceea ce presupune ca respectiva chestiune de drept să vizeze, ca regulă, o problemă de drept material de care depinde soluționarea pe fond a cauzei și doar ca excepție o problemă de drept procesual, aceasta din urmă în măsura în care soluția dată respectivei probleme de drept s-ar repercuta semnificativ asupra rezolvării fondului cauzei (Decizia nr. 11 din 12 septembrie 2018, publicată în Monitorul Oficial al României, Partea I, nr. 907 din 29 octombrie 2018).

160. În fine, s-a apreciat că hotărârile prealabile pronunțate de instanța supremă nu pot conduce la rezolvarea directă a unor chestiuni ce țin de particularitățile factuale ale cauzei și nici la dezlegarea unor probleme pur teoretice, deoarece s-ar crea astfel riscul transformării acestui mecanism de unificare a practicii judiciare fie într-o procedură dilatorie pentru litigii caracterizate, prin natura lor, ca fiind urgente, fie într-o procedură care se va substitui mecanismului recursului în interesul legii (Decizia nr. 17 din 17 martie 2021, publicată în Monitorul Oficial al României, Partea I, nr. 514 din 18 mai 2021).

161. A). Din perspectiva acestor argumente teoretice se constată că **prima întrebare** menționată în sesizarea de față, respectiv *„Dacă procedeul probator al accesului la un sistem informatic poate fi utilizat atunci când (i) suportul informatic se află în detenția fizică a organului de urmărire penală sau dacă acest procedeu probator permite doar (ii) pătrunderea de la distanță într-un astfel de sistem în vederea monitorizării/supravegherii activității derulate?”, are legătură cu soluționarea cauzei*, respectiv cu *soluția* pe care completul de doi judecători de cameră preliminară este chemat să o pronunțe asupra cererilor și excepțiilor formulate de inculpați, în calea de atac a contestației.

162. În același timp, *întrebarea menționată are legătură și cu soluționarea pe fond a cauzei.* Din această perspectivă, se reține că legalitatea administrării probelor în faza de urmărire penală influențează soluționarea fondului, întrucât vizează chiar stabilirea mijloacelor de probă care pot fi luate în considerare pentru a pronunța o soluție cu privire la acțiunea penală și la acțiunea civilă.

163. În acest sens, se constată că, în esență, inculpații au solicitat excluderea probelor obținute ca urmare a procedeului probator utilizat de procuror în cursul urmăririi penale, acela al accesului la un sistem informatic, susținând că în măsura în care sistemul informatic se afla deja în posesia organului de urmărire penală, singurul procedeu probator ce putea fi folosit pentru identificarea și strângerea probelor era percheziția informatică, iar în acest scop era necesară emiterea unui mandat de către judecătorul de drepturi și libertăți. În același timp, s-a susținut și că autorizarea pătrunderii în sistemul informatic nu permitea și copierea integrală a datelor conținute de acesta, fiind încălcate limitele autorizării.

164. Ca urmare, dezlegarea prealabilă a acestei probleme de drept ar putea avea, în principiu, o înrâurire decisivă nu doar asupra hotărârii finale în camera preliminară, ci, implicit, și asupra evoluției ulterioare a procesului penal. Prin urmare, chiar dacă efectele dezlegării obligatorii date acestei probleme de drept se repercutează într-un mod indirect asupra rezolvării fondului cauzei, legătura dintre hotărârea preliminară și soluționarea cauzei este suficient de însemnată pentru a se considera îndeplinită condiția de admisibilitate analizată.

165. În același timp, însă, *cu referire la problema de drept menționată*, deși, așa cum s-a arătat mai sus, are legătură cu soluționarea cauzei, cu toate acestea, se constată că **nu este îndeplinită o altă condiție de admisibilitate, aceea ca problema de drept să fie una veritabilă, care să facă necesară o rezolvare de principiu prin pronunțarea unei hotărâri prealabile de către Înalta Curte de Casație și Justiție, aceasta constituind, de fapt, premisa fundamentală ce justifică intervenția instanței supreme prin mecanismul de unificare a practicii judiciare instituit de art. 475 și următoarele din Codul de procedură penală.**

166. Chiar dacă punctele de vedere transmise de către instanțe reflectă opinii divergente asupra primei probleme de drept ce face obiectul sesizării, totuși, **norma procesual penală a cărei interpretare se solicită nu este una ambiguă** și permite instanței de trimitere să stabilească cu suficientă certitudine conținutul și sensul textului legal ce face obiectul întrebării prealabile. În același timp, se reține că nu au fost

identificate hotărâri judecătorești prin care să se fi aplicat neunitar norma de drept în discuție.

167. Prin chiar dispozițiile art. 138 alin. (3) din Codul de procedură penală se arată că „prin *acces la un sistem informatic* se înțelege pătrunderea într-un sistem informatic sau mijloc de stocare a datelor informatice, fie direct, fie de la distanță, prin intermediul unor programe specializate ori prin intermediul unei rețele, în scopul de a identifica probe". Totodată, potrivit dispozițiilor art. 141 alin. (5) din Codul de procedură penală, „cu privire la datele informatice identificate prin accesul la un sistem informatic, procurorul poate dispune, prin ordonanță: a) realizarea și conservarea unei copii a acestor date informatice; (…). Copiile se realizează cu mijloace tehnice și proceduri adecvate, de natură să asigure integritatea informațiilor conținute de acestea".

168. În această privință, se constată că, prin Decizia nr. 5 din 10 februarie 2016, publicată în Monitorul Oficial al României, Partea I, nr. 183 din 11 martie 2016 (ale cărei considerente au fost reluate apoi în Decizia nr. 6 din 2 martie 2016, publicată în Monitorul Oficial al României, Partea I, nr. 287 din 15 aprilie 2016; Decizia nr. 19 din 27 septembrie 2016, publicată în Monitorul Oficial al României, Partea I, nr. 874 din 1 noiembrie 2016; Decizia nr. 20 din 14 iunie 2017, publicată în Monitorul Oficial al României, Partea I, nr. 542 din 10 iulie 2017; Decizia nr. 27 din 12 decembrie 2017, publicată în Monitorul Oficial al României, Partea I, nr. 65 din 22 ianuarie 2018; Decizia nr. 5 din 21 martie 2019, publicată în Monitorul Oficial al României, Partea I, nr. 381 din 15 mai 2019; Decizia nr. 19 din 29 octombrie 2019, publicată în Monitorul Oficial al României, Partea I, nr. 108 din 12 februarie 2020; Decizia nr. 6 din 17 februarie 2020, publicată în Monitorul Oficial al României, Partea I, nr. 518 din 17 iunie 2020; Decizia nr. 65 din 29 septembrie 2021, publicată în Monitorul Oficial al României, Partea I, nr. 81 din 27 ianuarie 2022; Decizia nr. 67 din 29 septembrie 2021, publicată în Monitorul Oficial al României, Partea I, nr. 86 din 28 ianuarie 2022), Completul pentru dezlegarea unor chestiuni de drept în materie penală a stabilit că „scopul unei asemenea proceduri este de a da dezlegări asupra unor probleme veritabile și dificile de drept. Sesizarea Înaltei Curți de Casație și Justiție conform art. 475 din Codul de procedură penală trebuie efectuată doar în situația în care, în cursul soluționării unei cauze penale, se pune problema interpretării și aplicării unor dispoziții legale neclare, echivoce, care ar putea da naștere mai multor soluții. Interpretarea urmărește cunoașterea înțelesului exact al normei, clarificarea sensului și scopului acesteia, așa încât procedura prealabilă nu poate fi folosită în cazul în care aplicarea corectă a dreptului se impune într-un mod atât de evident, încât nu lasă loc de îndoială cu privire la modul de soluționare a întrebării adresate".

169. Instanța supremă este chemată să dea o rezolvare de principiu unei chestiuni de drept cu care a fost sesizată, în interpretarea unei norme care ar fi afectată de o asemenea ambiguitate, încât nu ar permite instanței de trimitere ca, prin intermediul unor metode de interpretare a normelor juridice recunoscute în dreptul intern, să stabilească cu suficientă certitudine conținutul și sensul textelor legale ce fac obiectul întrebării prealabile (Decizia Înaltei Curți de Casație și Justiție — Completul pentru dezlegarea unor chestiuni de drept nr. 6 din 17 februarie 2020, publicată în Monitorul Oficial al României, Partea I, nr. 518 din 17 iunie 2020).

170. În acest context, se apreciază că, **în ceea ce privește prima problemă de drept, nu este îndeplinită condiția rezultată din chiar practica Completului pentru dezlegarea unor chestiuni de drept în materie penală, referitoare la caracterul neechivoc al normei legale și la dificultatea problemei de drept ce face obiectul întrebării.**

171. Ca atare, *nu se poate folosi procedura hotărârii prealabile dacă aplicarea corectă a dreptului se impune într-un mod atât de evident, încât să nu lase loc niciunei îndoieli rezonabile cu privire la modul de soluționare a întrebării adresate în cauză*, context în care **prima întrebare urmează a fi respinsă, ca inadmisibilă**. Simpla lectură a dispozițiilor mai sus menționate este lămuritoare și nu este necesară intervenția instanței supreme prin mecanismul întrebării prealabile.

172. B). În ceea ce privește **cea de-a doua întrebare adresată**, aceea *„Dacă opțiunea asupra emiterii, obținerii și/sau utilizării unui mandat de acces la un sistem informatic sau a unui mandat de percheziție informatică în vederea copierii integrale a datelor aflate într-un sistem informatic aflat în posesia organului de urmărire penală reprezintă o chestiune de oportunitate, aflată în sfera de apreciere a organului de urmărire penală, sau o chestiune de legalitate, supusă cenzurii judecătorului de cameră preliminară?"*, se apreciază că aceasta **nu are legătură cu soluționarea cererilor și excepțiilor formulate în faza camerei preliminare și, cu atât mai puțin, cu soluția ce ar putea fi pronunțată asupra raportului juridic de conflict.**

173. În fapt, se constată că, *deși problema de drept enunțată are caracter abstract, ea nu influențează, în sine, soluția asupra fondului cauzei, deoarece, pe calea acestei întrebări, se tinde la obținerea, de către instanța de trimitere, a clarificării competenței funcționale a judecătorului de cameră preliminară în procedura filtru de verificare a legalității trimiterii în judecată, a legalității administrării probelor și a actelor de urmărire penală, în condițiile în care această competență nu a fost contestată de inculpați, și care, de altfel, au învestit judecătorul de cameră preliminară cu cenzurarea alegerii procedeului probator de către procuror, în vederea clonării datelor din sistemul informatic aflat la dispoziția acestuia.*

174. Este de subliniat, în acest context, că organul de urmărire penală poate dovedi acuzațiile formulate în cursul urmăririi penale cu probe rezultate din mijloacele de probă prevăzute de lege și obținute prin procedee probatorii legale, între acestea, și metode speciale de supraveghere și cercetare, iar legalitatea administrării probelor la care se referă art. 342 din Codul de procedură penală vizează legalitatea actelor prin care probele și mijloacele de probă au fost dispuse, autorizate sau confirmate, legalitatea mijloacelor de probă și a procedeelor probatorii prin care acestea au fost obținute. Se reține, în acest sens, că, indiferent care sunt mijloacele de probă administrate și procedeele probatorii prin care au fost obținute și pe care procurorul a înțeles să le utilizeze în faza de urmărire penală, legalitatea acestora face obiectul verificării din partea judecătorului de cameră preliminară.

175. **Întrebarea adresată instanței supreme — și anume cenzurarea ori nu de către judecătorul de cameră preliminară a alegerii de către organul de urmărire penală a procedeelor probatorii — reflectă o abordare teoretică a unei chestiuni care, examinată în contextul particularităților cauzei, nu are, în realitate, o înrâurire propriu-zisă asupra modului de rezolvare a chestiunilor invocate în etapa filtru a procesului penal.**

176. În același timp, în cadrul examenului de admisibilitate a sesizării, trebuie avute în vedere și elementele de diferențiere dintre acest mecanism de unificare a practicii judiciare și cel al recursului în interesul legii. Finalitatea hotărârii preliminare este aceea de a asigura predictibilitate jurisprudenței anterior apariției unei practici neunitare consistente în rândul instanțelor judecătorești, pe când recursul în interesul legii are menirea de a înlătura o practică neunitară deja intervenită. Așa cum s-a statuat anterior în jurisprudența Completului pentru dezlegarea unor chestiuni de drept în materie penală, din modul de reglementare a celui dintâi mecanism de unificare a practicii judiciare rezultă că *legiuitorul a înțeles să excludă din sfera acestui demers unificator chestiunile de drept care nu se repercutează semnificativ asupra fondului cauzei*, acestea din urmă fiind susceptibile de o interpretare obligatorie numai pe calea recursului în interesul legii (Decizia nr. 11/2018).

177. Pentru aceste considerente, **și cea de-a doua întrebare prealabilă urmează a fi respinsă, ca inadmisibilă.**

178. Pentru considerentele expuse, constatând că nu sunt îndeplinite, cumulativ, condițiile de admisibilitate prevăzute de art. 475 și 476 din Codul de procedură penală, *sesizarea formulată de Curtea de Apel Pitești este apreciată ca inadmisibilă*, în temeiul dispozițiilor art. 477 din Codul de procedură penală.

P E N T R U A C E S T E M O T I V E

În numele legii

D E C I D E:

Respinge, ca inadmisibilă, sesizarea formulată de Curtea de Apel Pitești — Secția penală și pentru cauze cu minori și de familie, în Dosarul nr. 2.485/90/2022/a1, în vederea pronunțării unei hotărâri prealabile pentru dezlegarea următoarelor chestiuni de drept:

„1. Dacă procedeul probator al accesului la un sistem informatic poate fi utilizat atunci când (i) suportul informatic se află în detenția fizică a organului de urmărire penală sau dacă acest procedeu probator permite doar (ii) pătrunderea de la distanță într-un astfel de sistem în vederea monitorizării/supravegherii activității derulate?

2. Dacă opțiunea asupra emiterii, obținerii și/sau utilizării unui mandat de acces la un sistem informatic sau a unui mandat de percheziție informatică în vederea copierii integrale a datelor aflate într-un sistem informatic aflat în posesia organului de urmărire penală reprezintă o chestiune de oportunitate, aflată în sfera de apreciere a organului de urmărire penală, sau o chestiune de legalitate, supusă cenzurii judecătorului de cameră preliminară?”

Obligatorie de la data publicării în Monitorul Oficial al României, Partea I, potrivit art. 477 alin. (3) din Codul de procedură penală.

Pronunțată în ședință publică, astăzi, 18 septembrie 2023.

PREȘEDINTELE SECȚIEI PENALE A ÎNALTEI CURȚI
DE CASAȚIE ȘI JUSTIȚIE
judecător **ELENI CRISTINA MARCU**

Magistrat-asistent,
Elena-Mihaela Mustață

EDITOR: PARLAMENTUL ROMÂNIEI — CAMERA DEPUTAȚILOR

MONITORUL OFICIAL

„Monitorul Oficial” R.A., Str. Parcului nr. 65, sectorul 1, București; 012329
C.I.F. RO427282, IBAN: RO55RNCB0082006711100001 BCR
și IBAN: RO12TREZ7005069XXX000531 DTCPMB (alocat numai persoanelor juridice bugetare)
Tel. 021.318.51.29/150, fax 021.318.51.15, e-mail: marketing@ramo.ro, www.monitoruloficial.ro

Adresa Centrului pentru relații cu publicul este: șos. Panduri nr. 1, bloc P33, sectorul 5, București; 050651.
Tel. 021.401.00.73, 021.401.00.78, e-mail: concursurifp@ramo.ro, convocariaga@ramo.ro
Pentru publicări, încărcați actele pe site, la: https://www.monitoruloficial.ro, secțiunea Publicări.

5 948493 476030

Monitorul Oficial al României, Partea I, nr. 910/10.X.2023 conține 16 pagini. Prețul: 8 lei **ISSN** 1453—4495