MONITORUL OFICIAL AL ROMÂNIEI

Anul 190 (XXXIV) — Nr. 56

PARTEA I
LEGI, DECRETE, HOTĂRÂRI ȘI ALTE ACTE

Miercuri, 19 ianuarie 2022

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. 68
din 29 septembrie 2021

Dosar nr. 1.876/1/2021

Completul compus din:

Daniel Grădinaru	— președintele Secției penale a Înaltei Curți de Casație și Justiție — președintele completului
Săndel Lucian Macavei	— judecător la Secția penală
Simona Elena Cîrnaru	— judecător la Secția penală
Laura Mihaela Soane	— judecător la Secția penală
Ioana Alina Ilie	— judecător la Secția penală
Andrei Claudiu Rus	— judecător la Secția penală
Simona Daniela Encean	— judecător la Secția penală
Constantin Epure	— judecător la Secția penală
Dan Andrei Enescu	— judecător la Secția penală

S-a luat în examinare sesizarea formulată de către Curtea de Apel Ploiești, Secția penală și pentru cauze cu minori și de familie, prin care, în temeiul art. 476 alin. (1) raportat la art. 475 din Codul de procedură penală, s-a solicitat pronunțarea unei hotărâri prealabile pentru dezlegarea următoarei chestiuni de drept: *„În interpretarea dispozițiilor art. 360 alin. (1) din Codul penal privind accesul ilegal la un sistem informatic, în cazul persoanelor care pot interoga oricând o bază de date conținând informații nepublice, o asemenea interogare neurmată de efectuarea ulterioară a unor acte specifice exercitării atribuțiilor de serviciu în legătură cu interogarea efectuată poate reprezenta o depășire a limitelor pentru care a fost acordată autorizarea.”*

Completul pentru dezlegarea unor chestiuni de drept în materie penală a fost constituit conform prevederilor art. 476 alin. (6) raportat la art. 473 alin. (8) din Codul de procedură penală și art. 36 din Regulamentul privind organizarea și funcționarea administrativă a Înaltei Curți de Casație și Justiție, republicat, cu completările ulterioare.

Ședința este prezidată de către președintele Secției penale a Înaltei Curți de Casație și Justiție, domnul judecător Daniel Grădinaru.

La ședința de judecată participă domnul Florin Nicușor Mihalache, magistrat-asistent în cadrul Secțiilor Unite, desemnat în conformitate cu dispozițiile art. 38 din Regulamentul privind organizarea și funcționarea administrativă a Înaltei Curți de Casație și Justiție, republicat, cu completările ulterioare.

Judecător-raportor a fost desemnat, conform prevederilor art. 476 alin. (7) din Codul de procedură penală, doamna Ioana Alina Ilie, judecător în cadrul Secției penale a Înaltei Curți de Casație și Justiție.

Procurorul general al Parchetului de pe lângă Înalta Curte de Casație și Justiție este reprezentat de doamna Ecaterina Nicoleta Eucarie, procuror în cadrul Secției Judiciare a Parchetului de pe lângă Înalta Curte de Casație și Justiție.

Magistratul-asistent a prezentat referatul cauzei, arătând că la dosar a fost depus raportul întocmit în cauză de către judecătorul-raportor, acesta fiind comunicat părților potrivit dispozițiilor art. 476 alin. (9) din Codul de procedură penală.

Totodată, a învederat că, drept urmare a solicitărilor formulate în temeiul art. 476 alin. (10) raportat la art. 473 alin. (5) din Codul de procedură penală, la dosarul cauzei au fost depuse puncte de vedere asupra problemei de drept supuse dezlegării.

Președintele Completului pentru dezlegarea unor chestiuni de drept în materie penală, domnul judecător Daniel Grădinaru, a acordat cuvântul în dezbateri.

Reprezentantul Parchetului de pe lângă Înalta Curte de Casație și Justiție, doamna procuror Ecaterina Nicoleta Eucarie, a susținut că în cauză nu sunt îndeplinite cumulativ condițiile de admisibilitate prevăzute de dispozițiile art. 475 din Codul de procedură penală. Astfel, a arătat că, deși sesizarea a fost formulată de una dintre instanțele la care face referire textul de lege menționat, respectiv de Curtea de Apel Ploiești, cauza aflându-se în ultimul grad de jurisdicție pe rolul acesteia, iar asupra chestiunii de drept ce se solicită a fi dezlegată instanța supremă nu a statuat încă printr-o hotărâre prealabilă sau printr-un recurs în interesul legii, nefăcând nici obiectul unui asemenea recurs aflat în curs de soluționare, celelalte cerințe impuse de art. 475 din Codul de procedură penală nu sunt întrunite, întrucât nu există o veritabilă problemă de drept care să necesite o rezolvare cu valoare de principiu din partea Înaltei Curți de Casație și Justiție, iar soluționarea pe fond a apelului cu care a fost învestită Curtea de Apel Ploiești nu depinde de lămurirea chestiunii ce face obiectul prezentei sesizări.

Astfel, potrivit jurisprudenței Completului pentru dezlegarea unor chestiuni de drept în materie penală, admisibilitatea sesizării în vederea pronunțării unei hotărâri prealabile este condiționată, atât în cazul în care vizează o normă de drept material, cât și atunci când privește o dispoziție de drept procesual, de împrejurarea ca interpretarea dată de către instanța supremă să aibă consecințe juridice asupra modului de rezolvare a fondului cauzei.

Or, prin întrebarea ce face obiectul prezentei sesizări, instanța de trimitere solicită ca Înalta Curte de Casație și Justiție să stabilească în ce măsură constituie infracțiune de acces fără drept la un sistem informatic, prin depășirea limitelor autorizării, fapta persoanei care, fiind autorizată să acceseze o bază de date conținând informații nepublice, accesează această bază de date, dar ulterior nu efectuează acte specifice exercitării atribuțiilor de serviciu în legătură cu informațiile pe care le-a accesat. Așadar, *instanța de trimitere a pus accent pe o împrejurare exterioară și ulterioară accesului propriu-zis, constând în nevalorificarea datelor accesate în cadrul activităților de serviciu*.

În acest context s-a susținut de către procuror că, în realitate, din perspectiva tipicității obiective a infracțiunii prevăzute de art. 360 din Codul penal, nu interesează conduita ulterioară a autorului accesului cu privire la datele informatice accesate, ci

doar conduita sa pe durata accesului și măsura în care prin această conduită respectă sau nu autorizarea acordată, în condițiile în care de esența respectivei infracțiuni este ca accesul la sistemul informatic să se realizeze fără drept.

Făcând în continuare referire la înțelesul sintagmei „fără drept", reprezentantul Parchetului de pe lângă Înalta Curte de Casație și Justiție a arătat că aceasta nu este definită în Codul penal, însă, așa cum rezultă din considerentele Deciziei Curții Constituționale nr. 183 din 29 martie 2018, publicată în Monitorul Oficial al României, Partea I, nr. 486 din 13 iunie 2018, precum și din cele ale Deciziei nr. 4 din 25 ianuarie 2021, pronunțată de Completul pentru dezlegarea unor chestiuni de drept în materie penală, publicată în Monitorul Oficial al României, Partea I, nr. 171 din 19 februarie 2021, cerința ca acțiunea de accesare a unui sistem informatic să se realizeze fără drept are semnificația atribuită prin dispozițiile art. 35 alin. (2) din Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției, publicată în Monitorul Oficial al României, Partea I, nr. 279 din 21 aprilie 2003, din care rezultă că acționează fără drept persoana care se află în una dintre următoarele situații: a) nu este autorizată în temeiul legii sau al vreunui contract; b) depășește limitele autorizării; c) nu are permisiunea, din partea persoanei fizice sau juridice competente, potrivit legii, să o acorde, de a folosi, administra sau controla un sistem informatic ori de a desfășura cercetări științifice sau de a efectua orice altă operațiune într-un sistem informatic.

Așadar, din conținutul art. 35 alin. (2) din Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției rezultă că ipoteza depășirii limitelor autorizării presupune, prin definiție, preexistența unei autorizări legale sau contractuale care stabilește și limitele impuse cu privire la interacțiunea autorului cu sistemul informatic. Astfel, autorul este autorizat să interacționeze la nivel logic cu sistemul informatic, însă conținutul acestei interacțiuni depășește cadrul stabilit prin legea sau convenția care a permis-o.

Ca atare, s-a menționat de către procuror că analiza depășirii limitelor autorizării presupune o dublă evaluare atât a existenței autorizării, cât și a conținutului acesteia, conținut care furnizează criteriile obiective în raport cu care se stabilește caracterul legitim sau nelegitim al accesului la sistemul informatic. Or, o asemenea analiză este întotdeauna de natură factuală, deoarece presupune o evaluare în concret a datelor ce particularizează accesul și trebuie realizată de instanța învestită cu soluționarea fondului cauzei, în contextul verificării tipicității obiective a faptei, din perspectiva elementului material al laturii obiective.

Având în vedere că infracțiunea prevăzută de art. 360 din Codul penal este una de pericol, ce se consumă în momentul în care autorul, interacționând cu sistemul informatic, are posibilitatea de a beneficia de resursele sale, s-a apreciat de către procuror că atitudinea ulterioară a acestuia în raport cu datele informatice accesate, în sensul de a le folosi sau nu în cadrul activității de serviciu, nu face obiectul unei atari analize, deoarece intervine după momentul consumării infracțiunii.

Așadar, chestiunea depășirii limitelor autorizării nu poate fi stabilită *in abstracto*, întrucât concluzia existenței sau inexistentei unei astfel de ipoteze este diferită, în funcție de circumstanțele particulare ale fiecărei cauze.

În aceste condiții, reprezentantul Parchetului de pe lângă Înalta Curte de Casație și Justiție a apreciat că ceea ce se solicită de către instanța de trimitere nu este interpretarea de principiu a unei dispoziții legale, ci lămurirea unei situații concrete, ce face obiectul cauzei pendinte. Astfel, problema pusă în discuție constituie obiectul căii de atac asupra căreia trebuie să se pronunțe Curtea de Apel Ploiești, Secția penală și pentru cauze cu minori și de familie, astfel încât prin soluționarea sesizării s-ar ajunge ca Înalta Curte de Casație și Justiție să soluționeze, în realitate, fondul cauzei, statuând dacă fapta ce formează obiectul acuzației penale este sau nu prevăzută de legea penală.

În consecință, în raport cu aspectele expuse, reprezentantul Parchetului de pe lângă Înalta Curte de Casație și Justiție a solicitat respingerea, ca inadmisibilă, a sesizării formulate de Curtea de Apel Ploiești, Secția penală și pentru cauze cu minori și de familie.

Constatând că nu sunt întrebări de formulat din partea membrilor completului, președintele Completului pentru dezlegarea unor chestiuni de drept în materie penală a declarat dezbaterile închise, iar Completul pentru dezlegarea unor chestiuni de drept în materie penală a reținut dosarul în pronunțare.

ÎNALTA CURTE DE CASAȚIE ȘI JUSTIȚIE,

I. **Titularul și obiectul sesizării**

Prin Încheierea de ședință din 14 iunie 2021, pronunțată în Dosarul nr. 4.710/105/2018, ce are ca obiect apelul declarat de inculpatul I.L. împotriva Sentinței penale nr. 247 din 28 septembrie 2020 a Tribunalului Prahova, Secția penală, Curtea de Apel Ploiești — Secția penală și pentru cauze cu minori și de familie a sesizat, în temeiul art. 475 din Codul de procedură penală, Înalta Curte de Casație și Justiție în vederea pronunțării unei hotărâri prealabile pentru dezlegarea următoarei chestiuni de drept: *„În interpretarea dispozițiilor art. 360 alin. (1) din Codul penal privind accesul ilegal la un sistem informatic, în cazul persoanelor care pot interoga oricând o bază de date conținând informații nepublice, o asemenea interogare neurmată de efectuarea ulterioară a unor acte specifice exercitării atribuțiilor de serviciu în legătură cu interogarea efectuată poate reprezenta o depășire a limitelor pentru care a fost acordată autorizarea."*

II. **Expunerea succintă a cauzei**

Prin Rechizitoriul nr. 247/P/2017 din 8 octombrie 2018 al Parchetului de pe lângă Curtea de Apel Ploiești s-a dispus trimiterea în judecată a inculpatului I.L. pentru săvârșirea a 12 infracțiuni de acces ilegal la un sistem informatic, prevăzute de art. 360 alin. (1), (2) și (3) din Codul penal, din care o parte cu aplicarea art. 35 alin. (1) din Codul penal, reținându-se, în esență, în fapt, că, în calitate de agent-șef adjunct de poliție în cadrul I.P.J. Prahova, Poliția Municipiului Ploiești:

— la data de 25 decembrie 2013, orele 02,45:53 și 02,47:17, a accesat fără drept (cu depășirea împuternicirii primite) bazele de date administrate de *D.R.P.C.I.V.* și, respectiv, de *D.E.B.A.P.D.* (sisteme informatice la care accesul este permis numai prin introducerea unui username și a unei parole, deci prin intermediul unor proceduri), folosind username-ul și parola pe care le putea utiliza pentru a accesa aceste sisteme informatice numai în exercitarea atribuțiilor de serviciu ca polițist, în scopul obținerii de date informatice, și anume a datelor de identificare ale autoturismului deținut de șeful Poliției Ploiești și

a datelor de stare civilă ale acestuia, acționând în interes personal, și nu în exercitarea atribuțiilor de serviciu;

— la aceeași dată, ora 02,46:44, a accesat fără drept (cu depășirea împuternicirii primite) baza de date administrată de D.R.P.C.I.V. (sistem informatic la care accesul este permis numai prin introducerea unui username și a unei parole, deci prin intermediul unor proceduri), folosind username-ul și parola pe care le putea utiliza pentru a accesa acest sistem informatic numai în exercitarea atribuțiilor de serviciu ca polițist, în scopul obținerii de date informatice, și anume a datelor de identificare ale autoturismelor deținute de S.C. VP — S.R.L., acționând în interes personal, și nu în exercitarea atribuțiilor de serviciu;

— la data de 20 ianuarie 2014, ora 21,55:29, a accesat fără drept (cu depășirea împuternicirii primite) baza de date administrată de D.E.P.A.B.D. (sistem informatic la care accesul este permis numai prin introducerea unui username și a unei parole, deci prin intermediul unor proceduri), folosind username-ul și parola pe care le putea utiliza pentru a accesa acest sistem informatic numai în exercitarea atribuțiilor de serviciu ca polițist, în scopul obținerii de date informatice, și anume a datelor de stare civilă ale unui lucrător de poliție din cadrul B.C.C.O. Ploiești;

— la data de 14 februarie 2014, ora 00,42:05, a accesat fără drept (cu depășirea împuternicirii primite) baza de date administrată de D.R.P.C.I.V., folosind username-ul și parola pe care le putea utiliza pentru a accesa acest sistem informatic numai în exercitarea atribuțiilor de serviciu ca polițist, în scopul obținerii de date informatice, și anume a datelor de identificare ale autoturismului deținut de șeful Secției 3 Poliție Ploiești și a datelor de stare civilă ale acestuia, acționând în interes personal, și nu în exercitarea atribuțiilor de serviciu;

— la data de 5 noiembrie 2014, ora 15,54:39, a accesat fără drept (cu depășirea împuternicirii primite) baza de date administrată de D.E.P.A.B.D., folosind username-ul și parola pe care le putea utiliza pentru a accesa acest sistem informatic numai în exercitarea atribuțiilor de serviciu ca polițist, în scopul obținerii de date informatice, și anume a datelor de stare civilă ale unui lucrător de poliție din cadrul I.P.J. Prahova, acționând în interes personal, și nu în exercitarea atribuțiilor de serviciu;

— la data de 10 noiembrie 2014, în intervalul orar 09,18:33—15,15:48, a accesat fără drept (cu depășirea împuternicirii primite) baza de date administrată de D.E.P.A.B.D., folosind username-ul și parola pe care le putea utiliza pentru a accesa acest sistem informatic numai în exercitarea atribuțiilor de serviciu ca polițist, în scopul obținerii de date informatice, și anume a datelor de stare civilă ale unor lucrători din cadrul I.P.J. Prahova, al Brigăzii de Operațiuni Speciale Ploiești, al B.C.C.O. Ploiești, al I.G.S.U., Centrul de Pregătire Ciolpani, și al Secției 4 Poliție Ploiești (79), acționând în interes personal, și nu în exercitarea atribuțiilor de serviciu;

— la data de 10 noiembrie 2014, în intervalul orar 09,19:45—15,16:01, a accesat fără drept (cu depășirea împuternicirii primite) baza de date administrată de D.E.P.A.B.D., folosind username-ul și parola pe care le putea utiliza pentru a accesa acest sistem informatic numai în exercitarea atribuțiilor de serviciu ca polițist, în scopul obținerii de date informatice, și anume a datelor de stare civilă ale unor lucrători de poliție din cadrul I.P.J. Prahova (20) și ale soților/soțiilor/rudelor/afinilor acestora, acționând în interes personal, și nu în exercitarea atribuțiilor de serviciu;

— la data de 19 noiembrie 2014, în intervalul orar 11,06:40—11,11:04, a accesat fără drept (cu depășirea împuternicirii primite) baza de date administrată de D.E.P.A.B.D., folosind username-ul și parola pe care le putea utiliza pentru a accesa acest sistem informatic numai în exercitarea atribuțiilor de serviciu ca polițist, în scopul obținerii de date informatice, și anume a datelor de stare civilă ale unor lucrători din cadrul Instituției Prefectului și al I.P.J. Prahova (5) și, după caz, ale soților/soțiilor/rudelor/afinilor acestora, acționând în interes personal, și nu în exercitarea atribuțiilor de serviciu;

— la data de 5 decembrie 2014, orele 11,42:52 și 11,43:38, a accesat fără drept (cu depășirea împuternicirii primite) bazele de date administrate de D.E.B.A.P.D. și, respectiv, de D.R.P.C.I.V., folosind username-ul și parola pe care le putea utiliza pentru a accesa aceste sisteme informatice numai în exercitarea atribuțiilor de serviciu ca polițist, în scopul obținerii de date informatice, și anume a datelor de stare civilă ale șefului Poliției Municipiului Ploiești, ale soției și ale fiului acestuia, precum și a datelor de identificare ale autoturismelor deținute de cei trei, acționând în interes personal, și nu în exercitarea atribuțiilor de serviciu;

— la data de 30 decembrie 2014, ora 00,11:07, a accesat fără drept (cu depășirea împuternicirii primite) baza de date administrată de D.E.P.A.B.D., folosind username-ul și parola pe care le putea utiliza pentru a accesa acest sistem informatic numai în exercitarea atribuțiilor de serviciu ca polițist, în scopul obținerii de date informatice, și anume a datelor de stare civilă ale numitului S.C., ziarist, acționând în interes personal, și nu în exercitarea atribuțiilor de serviciu;

— la data de 9 ianuarie 2015, în intervalul orar 09,25:29—09,28:50, a accesat fără drept (cu depășirea împuternicirii primite) baza de date administrată de D.E.P.A.B.D., folosind username-ul și parola pe care le putea utiliza pentru a accesa acest sistem informatic numai în exercitarea atribuțiilor de serviciu ca polițist, în scopul obținerii de date informatice, și anume a datelor de stare civilă ale unor lucrători de poliție din cadrul în cadrul I.P.J. Prahova (5), acționând în interes personal, și nu în exercitarea atribuțiilor de serviciu;

— la data de 19 ianuarie 2015, în intervalul orar 22,45:42—23,49:13, a accesat fără drept (cu depășirea împuternicirii primite) baza de date administrată de D.E.P.A.B.D., folosind username-ul și parola pe care le putea utiliza pentru a accesa acest sistem informatic numai în exercitarea atribuțiilor de serviciu ca polițist, în scopul obținerii de date informatice, și anume a datelor de stare civilă ale unor lucrători din cadrul I.P.J. Prahova (13), acționând în interes personal, și nu în exercitarea atribuțiilor de serviciu;

— la data de 20 aprilie 2015, ora 11,25:50, a accesat fără drept (cu depășirea împuternicirii primite) baza de date administrată de D.E.P.A.B.D., folosind username-ul și parola pe care le putea folosi pentru a accesa acest sistem informatic numai în exercitarea atribuțiilor de serviciu ca polițist, în scopul obținerii de date informatice, și anume datele de stare civilă ale unui lucrător din cadrul I.P.J. Prahova și ale fiicei acestuia, acționând în interes personal, și nu în exercitarea atribuțiilor de serviciu.

Prin Sentința penală nr. 247 din 28 septembrie 2020 a Tribunalului Prahova, Secția penală, pronunțată în Dosarul nr. 4.710/105/2018, inculpatul I.L. a fost condamnat, în temeiul art. 396 alin. (2) din Codul de procedură penală, pentru săvârșirea infracțiunii de acces ilegal la un sistem informatic, în

formă continuată, prevăzută de art. 360 alin. (1), (2) și (3) din Codul penal, cu aplicarea art. 35 alin. (1) din Codul penal — 177 acte materiale (ca urmare a schimbării încadrării juridice date faptelor prin rechizitoriu dintr-o pluralitate de infracțiuni într-o infracțiune unică, prin Încheierea de ședință din 15 iulie 2020), la pedeapsa de 2 ani închisoare, în condițiile art. 91 și următoarele din Codul penal, reținându-se, în esență, raportat la situația de fapt prezentată în actul de sesizare a instanței și dovedită de materialul probator administrat în cauză în ambele faze procesuale, că accesarea de către acuzat a sistemelor informatice care stochează datele personale și cele de identificare ale autoturismelor ce au fost consultate de către acesta s-a realizat fără drept, respectiv cu depășirea limitelor autorizării, întrucât username-ul și parola primite și pe care le-a folosit trebuiau utilizate numai în exercitarea atribuțiilor sale de serviciu ca lucrător de poliție, și nu în interes personal.

Împotriva acestei sentințe a declarat apel inculpatul I.L. pentru motive de nelegalitate și netemeinicie, criticând, printre altele, sub acest din urmă aspect, greșita sa condamnare pentru infracțiunea prevăzută de art. 360 alin. (1), (2) și (3) din Codul penal, context în care a apreciat că sunt incidente dispozițiile art. 421 pct. 2 lit. a) din Codul de procedură penală, cu consecința pronunțării unei soluții de achitare, conform art. 16 alin. (1) lit. b) sau art. 16 alin. (1) lit. d) din același cod, pe considerentul că faptele de care este acuzat nu sunt prevăzute de legea penală sau, după caz, au fost comise în condițiile necunoașterii unor prevederi legale extrapenale, fiind aplicabilă cauza de neimputabilitate reglementată de art. 30 alin. (4) din Codul penal.

În argumentarea acestui motiv de apel, inculpatul a susținut, în esență, că faptele reținute în sarcina sa nu întrunesc condițiile de tipicitate ale infracțiunii pentru care a fost condamnat, din moment ce accesul la sistemele informatice pe care sunt stocate bazele de date administrate de Direcția pentru Evidența Persoanelor și Administrarea Bazelor de Date și de Direcția Regim Permise de Conducere și Înmatriculare a Vehiculelor s-a făcut în mod legal, acționând în baza unui temei contractual (contractul de muncă și fișa postului), în virtutea căruia i-au fost atribuite username-ul și parola folosite, și în exercitarea strictă a atribuțiilor de serviciu, astfel cum atestă ansamblul probator al cauzei. Ca atare, apelantul a arătat că nu se poate reține comiterea faptei prevăzute de art. 360 din Codul penal cu depășirea limitelor autorizării, așa cum eronat a apreciat instanța de fond, cu atât mai mult cu cât dispozițiile art. 35 alin. (2) din Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției, care includ această ipoteză în conținutul noțiunii de acțiune „fără drept”, nefiind prevăzute de codificarea penală generală, nu pot completa norma de incriminare. Or, în atari condiții, în care această sintagmă („depășirea limitelor autorizării”) nu este clar reglementată decât printr-o normă extrapenală, respectiv prin Protocolul comun de colaborare între Inspectoratul General al Poliției Române și Direcția pentru Evidența Persoanelor și Administrarea Bazelor de Date nr. 59/2010 emis de Ministerul Afacerilor Interne, sunt aplicabile prevederile art. 30 alin. (4) din Codul penal referitoare la eroarea cu privire la o dispoziție legală extrapenală.

Calea de atac promovată de inculpat a fost înregistrată sub același număr de dosar *pe rolul Curții de Apel Ploiești, Secția penală și pentru cauze cu minori și de familie*, care, la termenul de judecată din data de 8 iunie 2021, a pus în discuția contradictorie a reprezentantului Ministerului Public și apelantului I.L. solicitarea scrisă a celui din urmă de sesizare a Înaltei Curți de Casație și Justiție în vederea „lămuririi sintagmei «depășirea limitelor autorizării» pentru a se putea înțelege clar când se comite infracțiunea, la accesarea bazei de date cu respectarea normelor la care s-a făcut referire (*n.n.* Instrucțiunile ministrului afacerilor interne nr. 27 din 3 februarie 2010; procedura internă PRO PG 21; procedura internă PRO PG 11; Protocolul comun de colaborare între Inspectoratul General al Poliției Române și Direcția pentru Evidența Persoanelor și Administrarea Bazelor de Date nr. 59 din 22 noiembrie 2010, emis de Ministerul Afacerilor Interne) sau la accesarea bazei de date fără respectarea acelor norme și măsuri de securitate.”

Cu acest prilej, instanța de apel, din oficiu, a pus în discuție împrejurarea că aspectele care trebuie lămurite de Înalta Curte de Casație și Justiție „ar trebui să aibă în vedere fișa postului pe care o avea inculpatul, faptul că se recunoaște un acces nerestricționat în baza de date, acces efectuat pe baza unei parole distribuite, precum și faptul că, în absența unor îndrumări specifice din fișa postului, verificarea periodică a acestei baze de date, neînsoțită de efectuarea altor lucrări ulterioare de specialitate, poate întruni condițiile de tipicitate a infracțiunii cu care instanța a fost sesizată”.

Prin Încheierea de ședință din 14 iunie 2021, Curtea de Apel Ploiești, Secția penală și pentru cauze cu minori și de familie, reformulând întrebarea adresată de apelantul inculpat I.L. în cuprinsul memoriului depus la dosar, prin raportare la aspectele puse în discuție din oficiu la termenul din 8 iunie 2021, a admis solicitarea acestuia și a dispus sesizarea Înaltei Curți de Casație și Justiție în vederea pronunțării unei hotărâri prealabile prin care să se statueze asupra următoarei chestiuni de drept: *„În interpretarea dispozițiilor art. 360 alin. (1) din Codul penal privind accesul ilegal la un sistem informatic, în cazul persoanelor care pot interoga oricând o bază de date conținând informații nepublice, o asemenea interogare neurmată de efectuarea ulterioară a unor acte specifice exercitării atribuțiilor de serviciu în legătură cu interogarea efectuată poate reprezenta o depășire a limitelor pentru care a fost acordată autorizarea.”*

III. **Opinia completului care a dispus sesizarea și punctele de vedere ale procurorului și inculpatului**

III.1. **Cu privire la admisibilitatea sesizării Înaltei Curți de Casație și Justiție**

Curtea de Apel Ploiești, Secția penală și pentru cauze cu minori și de familie a constatat îndeplinite toate cerințele de admisibilitate prevăzute de art. 475 din Codul de procedură penală, respectiv: instanța care sesizează Înalta Curte de Casație și Justiție este învestită cu soluționarea cauzei în apel, ca ultimă instanță din ciclul procesual ordinar; problema de drept în discuție nu a mai fost supusă examenului Înaltei Curți de Casație și Justiție și nu s-a mai statuat asupra ei printr-o altă hotărâre prealabilă sau de recurs în interesul legii și nici nu face obiectul unui recurs în interesul legii în curs de soluționare; de lămurirea chestiunii de drept în discuție depinde soluționarea pe fond a cauzei, respectiv reținerea unui acces ilegal la un sistem informatic, prin depășirea limitelor autorizării, sau lipsa acestei cerințe esențiale pentru infracțiunea prevăzută de art. 360 din Codul penal.

Reprezentantul Ministerului Public a opinat că nu sunt întrunite toate condițiile de admisibilitate reglementate de art. 475 din Codul de procedură penală pentru sesizarea Înaltei

Curți de Casație și Justiție, în condițiile în care textul de lege este clar și acoperă situația din speța dedusă judecății, respectiv accesul la sistemul informatic prin depășirea limitelor autorizării, iar solicitarea inculpatului se referă, în realitate, la modul de interpretare a probatoriului în vederea stabilirii unei anumite stări de fapt.

Inculpatul apelant I.L. a solicitat sesizarea Înaltei Curți de Casație și Justiție pentru pronunțarea unei hotărâri prealabile, lăsând însă la aprecierea instanței modul de formulare a întrebării adresate în procedura prevăzută de art. 475 și următoarele din Codul de procedură penală.

III.2. **Cu privire la chestiunea de drept ce formează obiectul sesizării**

Pornind de la împrejurarea că în calea de atac a apelului a fost criticată soluția primei instanțe de condamnare a inculpatului pentru infracțiunea de acces ilegal la un sistem informatic, prin reținerea depășirii limitelor autorizării, Curtea de Apel Ploiești, Secția penală și pentru cauze cu minori și de familie a apreciat că exprimarea unui punct de vedere ar putea fi considerată o antepronunțare cu privire la condițiile de tipicitate obiectivă ale infracțiunii deduse judecății, motiv pentru care nu a expus într-o manieră explicită o opinie referitoare la chestiunea a cărei dezlegare se solicită.

Cu toate acestea, făcând o prezentare a „problemelor de drept" care, în opinia sa, se ridică în legătură cu textul art. 360 din Codul penal, instanța de trimitere a realizat o analiză a elementelor constitutive ale infracțiunii pentru care inculpatul I.L. a fost deferit judecății și a textelor de lege aplicabile [menționând că prevederile art. 35 alin. (2) din Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției nu pot completa norma de incriminare întrucât nu sunt cuprinse în Codul penal, astfel încât noțiunea de „acces fără drept" trebuie raportată la fiecare categorie de persoane cărora prin lege li se conferă un asemenea acces], cu referire concretă la faptele ce formează obiectul trimiterii în judecată a acestuia, concluzionând că, spre deosebire de situația în care „accesul în sine a fost autorizat de către utilizatorul legitim al sistemului informatic vizat (sau de către proprietarul ori deținătorul legal) și acest acces este o formă de exercitare a atribuțiilor de serviciu", caz în care „nu se va reține existența unei infracțiuni de acces ilegal" la sistemul informatic, în ipoteza în care acuzațiile au fost formulate împotriva unor „persoane care au dreptul de interogare a bazelor de date în virtutea exercitării atribuțiilor de serviciu", cum este și situația din speță, depășirea limitelor autorizării nu poate fi stabilită decât „prin raportare la acțiunile subsecvente interogării bazei de date în baza parolei și username-ului oferit de angajator".

Sub acest aspect s-a apreciat că, în lipsa unor asemenea acțiuni ulterioare ale persoanei împuternicite cu interogarea bazei de date tocmai pentru exercitarea atribuțiilor de serviciu, „va interveni o problemă de aplicare a normei de incriminare, în sensul dacă lipsa de relevanță și lipsa valorificării ulterioare în exercițiul funcțiunii a informațiilor obținute (…) pot constitui un acces ilegal la sistemul informatic".

Ca atare, s-a menționat că se impune a se stabili, prin intermediul întrebării prealabile, dacă, în cazul persoanelor care pot interoga oricând o bază de date conținând informații nepublice, „va fi reținută o depășire a limitelor legale ale autorizării în cazul unei situații de fapt în care interogarea bazei de date să fie considerată necesară, însă informațiile obținute în urma interogării să nu prezinte relevanță pentru exercitarea ulterioară a atribuțiilor de serviciu și nici să nu fie valorificate în scop extraprofesional de titularul parolei de acces la baza de date".

Având în vedere poziția exprimată în sensul inadmisibilității sesizării Înaltei Curți de Casație și Justiție, procurorul nu și-a mai exprimat opinia cu referire la fondul chestiunii ce formează obiectul întrebării prealabile, cu atât mai mult cu cât reformularea acesteia s-a realizat cu ocazia deliberării.

Un punct de vedere clar și coerent nu a formulat nici apelantul inculpat I.L., aserțiunile sale orale de la termenul din 8 iunie 2021 și cele din cuprinsul notelor scrise referindu-se, în principal, la aspecte privind interpretarea probatoriului administrat și a dispozițiilor din legislația primară și secundară considerate a fi incidente în speță.

IV. **Punctele de vedere exprimate de către curțile de apel și instanțele judecătorești arondate cu privire la chestiunea de drept ce formează obiectul sesizării**

În urma consultării instanțelor de judecată, în conformitate cu dispozițiile art. 476 alin. (10) din Codul de procedură penală cu referire la art. 473 alin. (5) din Codul de procedură penală, s-a evidențiat *opinia majoritară* potrivit căreia, în cazul persoanelor care pot interoga oricând o bază de date conținând informații nepublice, o asemenea interogare neurmată de realizarea ulterioară a unor acte specifice exercitării atribuțiilor de serviciu în legătură cu interogarea efectuată poate reprezenta o depășire a limitelor pentru care a fost acordată autorizarea, indiferent dacă persoana respectivă folosește (în interes personal sau în interesul altor persoane) sau nu datele astfel obținute.

În argumentare s-a arătat, în esență, că accesul fără drept la un sistem informatic presupune fie inexistența unui temei legal sau contractual, fie depășirea limitelor pentru care s-a dat autorizarea, situație care se regăsește și în ipoteza în care accesul nu s-a făcut în interes de serviciu, ci în interes personal, neavând relevanță sub aspectul calificării faptei ca infracțiune (art. 360 din Codul penal) faptul că parola de acces și contul folosite pentru autentificare au fost reale, din moment ce autorul nu a acționat în exercitarea atribuțiilor de serviciu.

Astfel, s-a apreciat că, întrucât autorizarea a fost acordată cu un anumit scop, și anume efectuarea de acte ulterioare proprii îndeplinirii sarcinilor specifice funcției deținute și în legătură cu care trebuia realizată interogarea, deturnarea acesteia de la finalitatea inițială depășește limitele autorizării, constituind infracțiunea de acces ilegal la un sistem informatic, prevăzută de art. 360 din Codul penal.

Totodată, s-a mai menționat că, pentru stabilirea în concret a limitelor autorizării, nu este necesar a fi avută în vedere conduita ulterioară a făptuitorului, fiind suficientă examinarea contextului în care s-a realizat accesarea sistemului informatic (în exercitarea atribuțiilor de serviciu), fără a prezenta importanță pentru încadrarea faptei în norma de incriminare modul în care funcționarul folosește datele accesate, utilizare care, de regulă, îmbracă forma unor infracțiuni distincte (divulgarea informațiilor secrete de serviciu sau nepublice; abuz în serviciu; folosirea, în orice mod, direct sau indirect, de informații ce nu sunt destinate publicității ori permiterea accesului unor persoane neautorizate la aceste informații).

Acest punct de vedere a fost exprimat de curțile de apel București, Secția a II-a penală, Galați și Iași, de tribunalele Ialomița și instanțele arondate, Giurgiu, Vaslui, Caraș-Severin

și Bacău, precum și de judecătoriile Iași, Huși, Bârlad, Videle, Reșița, Caransebeș și Onești.

În sens contrar, curțile de apel București, Secția I penală, Pitești și Constanța, tribunalele Teleorman și Timiș și judecătoriile Roșiori de Vede, Turnu Măgurele, Alexandria și Timișoara au apreciat că, în cazul persoanelor care pot interoga oricând o bază de date conținând informații nepublice, o asemenea interogare neurmată de efectuarea ulterioară a unor acte specifice exercitării atribuțiilor de serviciu în legătură cu interogarea realizată nu întrunește condițiile de tipicitate ale infracțiunii prevăzute de art. 360 din Codul penal, nefiind îndeplinită cerința esențială ca sistemul informatic să fie accesat fără drept, din moment ce respectivele persoane au dreptul de a interoga oricând o asemenea bază de date.

Deopotrivă, în legătură cu acest aspect, s-a mai arătat de către o parte din instanțele indicate anterior (Curtea de Apel Pitești, Tribunalul Teleorman și judecătoriile Roșiori de Vede, Turnu Măgurele, Alexandria, Timișoara) că, atât timp cât sistemele informatice ce stochează bazele de date în discuție sunt folosite în mod uzual de anumite categorii de funcționari, în virtutea atribuțiilor de serviciu, „depășirea limitelor autorizării” se poate stabili doar ulterior, în funcție de modul în care informațiile obținute în urma interogării au fost valorificate.

Într-o opinie izolată, Curtea de Apel Timișoara a apreciat că orice interogare a unei baze de date conținând informații nepublice în afara atribuțiilor de serviciu care au justificat acordarea dreptului de acces la respectiva bază de date reprezintă o depășire a limitelor autorizării, însă nu echivalează cu un acces fără drept la sistemul informatic, în sensul art. 360 din Codul penal, fapta putând întruni elementele de tipicitate ale unei infracțiuni de serviciu.

Răspunsurile curților de apel Cluj, Brașov, Bacău, Alba Iulia, Oradea, Suceava și Târgu Mureș, precum și cele ale tribunalelor Covasna, Brașov, Buzău, Constanța și Tulcea cuprind doar mențiunea neidentificării, în jurisprudența acestora ori, după caz, a instanțelor din circumscripție, a unor hotărâri relevante pentru problema de drept ce face obiectul sesizării, iar, în plus, cel al Tribunalului Brașov face trimitere doar la aspecte de ordin teoretic generale, fără referiri concrete la chestiunea analizată.

În mod similar, Curtea de Apel Pitești și Tribunalul Prahova au făcut doar mențiunea identificării, la nivelul acestora, a unor decizii, respectiv sentințe ce privesc chestiunea de drept invocată, pe care le-au atașat răspunsului transmis.

Curtea de Apel Craiova nu a comunicat un punct de vedere.

V. **Punctul de vedere al Parchetului de pe lângă Înalta Curte de Casație și Justiție cu privire la problema de drept ce formează obiectul sesizării**

După ce a făcut referire la parcursul cauzei ce formează obiectul Dosarului nr. 4.710/105/2018 al Curții de Apel Ploiești, Secția penală și pentru cauze cu minori și de familie, precum și la dispozițiile legale considerate relevante în ceea ce privește obiectul întrebării prealabile, Parchetul de pe lângă Înalta Curte de Casație și Justiție a arătat că sesizarea instanței supreme nu îndeplinește cerințele referitoare la existența unei veritabile chestiuni de drept și a unei relații de dependență între răspunsul dat problemei invocate și soluționarea pe fond a cauzei, prevăzute de art. 475 din Codul de procedură penală, solicitând, pe cale de consecință, respingerea acesteia, ca inadmisibilă.

În acest sens s-a menționat că, potrivit jurisprudenței constante a Completului pentru dezlegarea unor chestiuni de drept în materie penală, atât în cazul în care vizează o normă de drept material, cât și atunci când privește o dispoziție de drept procesual, sesizarea în vederea pronunțării unei hotărâri prealabile este condiționată, sub aspectul admisibilității, de împrejurarea ca interpretarea dată de către instanța supremă să aibă consecințe juridice asupra modului de rezolvare a fondului cauzei.

Totodată, așa cum s-a statuat în practica aceluiași complet, sesizarea trebuie să conducă la interpretarea *in abstracto* a unor dispoziții legale determinate, iar nu la rezolvarea unor chestiuni ce țin de particularitățile cauzei (deciziile nr. 14 din 12 mai 2015, publicată în Monitorul Oficial al României, Partea I, nr. 454 din 24 iunie 2015; nr. 14 din 18 mai 2016, publicată în Monitorul Oficial al României, Partea I, nr. 460 din 21 iunie 2016; nr. 4 din 28 februarie 2017, publicată în Monitorul Oficial al României, Partea I, nr. 255 din 12 aprilie 2017; nr. 27 din 12 decembrie 2017, publicată în Monitorul Oficial al României, Partea I, nr. 65 din 22 ianuarie 2018), deci să vizeze exclusiv probleme de interpretare a legii, și nu elemente specifice, individuale, concrete, ale cauzei deduse judecății (Decizia nr. 5 din 10 februarie 2016, publicată în Monitorul Oficial al României, Partea I, nr. 183 din 11 martie 2016).

Ca atare, pentru a constitui o problemă de drept, premisa de la care se pornește în formularea întrebării ce reprezintă obiectul sesizării trebuie să își găsească izvorul în dispozițiile legale, și nu într-o stare de fapt, aplicarea legii la situația factuală, astfel cum aceasta a fost stabilită în baza probatoriului administrat, fiind atributul exclusiv al instanței învestite cu soluționarea cauzei (Decizia nr. 23 din 16 septembrie 2015, publicată în Monitorul Oficial al României, Partea I, nr. 824 din 4 noiembrie 2015).

Or, s-a subliniat de către parchet că, în cauză, prin întrebarea ce face obiectul sesizării, se solicită Înaltei Curți de Casație și Justiție să stabilească în ce măsură constituie infracțiunea de acces fără drept la un sistem informatic, prin depășirea limitelor autorizării, fapta persoanei care, fiind autorizată să acceseze o bază de date conținând informații nepublice, ulterior interogării acesteia nu efectuează acte specifice exercitării atribuțiilor de serviciu în legătură cu informațiile pe care le-a accesat, *punându-se, astfel, accent pe o împrejurare exterioară și ulterioară accesului propriu-zis, constând în nevalorificarea datelor accesate în cadrul activităților de serviciu*.

Făcând referire la condițiile de tipicitate obiectivă ale infracțiunii prevăzute de art. 360 din Codul penal, procurorul a arătat, însă, că, din perspectiva întrunirii acestora, nu interesează atitudinea ulterioară a autorului accesului cu privire la datele informatice interogate, ci conduita sa pe durata accesului și măsura în care prin respectiva conduită a respectat sau nu autorizarea acordată, de esența infracțiunii fiind ca accesul la sistemul informatic să se realizeze „fără drept”, sintagmă care, deși nu este definită în Codul penal, are semnificația atribuită prin dispozițiile art. 35 alin. (2) din Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției, astfel cum rezultă din considerentele Deciziei Curții Constituționale nr. 183 din 29 martie 2018, publicată în Monitorul Oficial al României, Partea I, nr. 486 din 13 iunie 2018, precum și ale Deciziei nr. 4 din 25 ianuarie 2021 a Completului pentru dezlegarea unor chestiuni de drept în materie penală, publicată în Monitorul Oficial al României, Partea I, nr. 171 din 19 februarie 2021.

Astfel, potrivit art. 35 alin. (2) din Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea

demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției, acționează fără drept inclusiv persoana care depășește limitele autorizării [lit. b)], analiza unei atari conduite presupunând, potrivit Ministerului Public, o dublă evaluare, atât a existenței autorizării, cât și a conținutului acesteia, care furnizează criteriile obiective în raport cu care se stabilește caracterul legitim sau nu al accesului la sistemul informatic.

Așadar, în ipoteza unei autorizări legale, cum este și cea din prezenta sesizare, s-a arătat că instanța verifică actul normativ care stabilește dreptul de a accesa sistemul informatic, limitele autorizării, așa cum rezultă din dispozițiile legale care reglementează competențele și activitățile ce pot fi desfășurate într-un anumit domeniu, și conduita materială a autorului pe durata accesului la sistemul informatic. În concret, în cauza în care a fost formulată întrebarea prealabilă, accesul la bazele de date reprezintă o formă de realizare a atribuțiilor de serviciu, astfel încât conținutul acestora și existența la momentul săvârșirii faptei a vreuneia dintre situațiile prevăzute de lege care reprezintă justificarea legală a accesului sunt limitele pe care instanța trebuie să le analizeze pentru a stabili dacă autorizarea a fost respectată.

Ca atare, s-a subliniat de către parchet că *o asemenea analiză este întotdeauna de natură factuală, deoarece presupune o evaluare în concret a datelor ce particularizează accesul și trebuie realizată de instanța învestită cu soluționarea fondului cauzei*, în contextul verificării tipicității obiective a faptei, din perspectiva elementului material al laturii obiective.

Mai mult, pornind de la împrejurarea că prevederile art. 360 din Codul penal reglementează o infracțiune de pericol, ce se consumă în momentul în care autorul, interacționând cu sistemul informatic, are posibilitatea de a beneficia de resursele lui, procurorul a menționat că *atitudinea ulterioară a acestuia în raport cu datele informatice accesate, în sensul folosirii lor sau nu în cadrul activității de serviciu, nu poate face obiectul acestei analize, deoarece respectiva conduită intervine după momentul consumării infracțiunii*, putând, în condițiile în care îmbracă o formă ilicită, indiferent de caracterul ei omisiv (făptuitorul nu valorifică datele, deși ar fi trebuit să o facă) sau comisiv (autorul folosește datele accesate în interes personal), să fie încadrată eventual într-o infracțiune distinctă (cum ar fi divulgarea informațiilor secrete de serviciu sau nepublice; abuz în serviciu; folosirea, în orice mod, direct sau indirect de informații care nu sunt destinate publicității ori permiterea accesului unor persoane neautorizate la aceste informații), punându-se, astfel, în discuție incidența instituției concursului de infracțiuni și nicidecum existența elementului material al infracțiunii de acces ilegal la un sistem informatic.

Raportat la toate aceste considerente, Parchetul de pe lângă Înalta Curte de Casație și Justiție a concluzionat că aspectul depășirii limitelor autorizării nu poate fi stabilit *in abstracto*, întrucât concluzia existenței sau inexistenței unei astfel de ipoteze este diferită, în funcție de circumstanțele particulare ale fiecărei cauze, și că ceea ce se solicită, în realitate, de către instanța de trimitere nu este interpretarea de principiu a unei dispoziții legale, ci lămurirea unei situații concrete, ce face obiectul procesului aflat pe rolul Curții de Apel Ploiești, Secția penală și pentru cauze cu minori și de familie, prin formularea sesizării tinzându-se, de fapt, la rezolvarea conflictului de drept penal dedus judecății și, implicit, la soluționarea de către instanța supremă a fondului cauzei, în sensul de a stabili dacă fapta ce face obiectul acuzației penale este sau nu prevăzută de legea penală, lucru inadmisibil din perspectiva prevederilor art. 475 din Codul de procedură penală.

VI. **Opinia specialiștilor consultați asupra chestiunii de drept ce formează obiectul sesizării**

În conformitate cu dispozițiile art. 476 alin. (10) raportate la cele ale art. 473 alin. (5) din Codul de procedură penală, a fost solicitată specialiștilor în drept penal opinia asupra problemei supuse examinării.

Centrul de cercetări în Științe penale din cadrul Facultății de Drept a Universității de Vest din Timișoara a opinat, sub aspect formal, că, deși sesizarea este deficitar formulată, sunt îndeplinite condițiile de admisibilitate ale acesteia, prevăzute de art. 475 din Codul de procedură penală, putând fi decelată finalitatea demersului realizat, iar, în ceea ce privește fondul chestiunii de drept supuse examinării, că, în interpretarea dispozițiilor art. 360 alin. (1) din Codul penal privind accesul ilegal la un sistem informatic, în cazul persoanelor care pot interoga oricând o bază de date conținând informații nepublice, o asemenea interogare fără efectuarea ulterioară a unor acte specifice exercitării atribuțiilor de serviciu în legătură cu interogarea realizată nu reprezintă o depășire a limitelor autorizării decât dacă interogarea s-a făcut cu neobservarea cadrului legal privind efectuarea acesteia, inclusiv neurmarea procedurilor prealabile privind autorizarea și legitimarea specifică în vederea realizării unei atari interogări.

În argumentarea acestei opinii, după prezentarea unor considerații de natură teoretică cu privire la conținutul normei de incriminare a faptei de acces fără drept la un sistem informatic, s-a arătat, în esență, că interpretarea textului art. 360 alin. (1) din Codul penal în sensul rezolvării chestiunii de drept cu care Înalta Curte de Casație și Justiție a fost sesizată impune o structurare a analizei pe două elemente, și anume observarea standardului protecției datelor cu caracter personal care ar fi lezat prin comiterea respectivei fapte, ce trebuie avut în vedere și prin raportare la speța în care a fost formulată întrebarea prealabilă, și înțelesul noțiunii de „autorizare/depășirea limitelor autorizării” prin prisma prevederilor legale care guvernează activitatea funcționarului care a fost deferit judecății în cauza aflată pe rolul instanței de trimitere.

Astfel, cu privire la primul element, s-a făcut o amplă referire la cuprinsul dispozițiilor legale incidente în materie, cu trimitere la art. 34 și art. 35 alin. (2) din Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției, la art. 2 lit. d) din Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului, la pct. 17 din preambulul aceleiași directive, la art. 10 din Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date și la art. 1, 4 și 5 din Legea nr. 238/2009 privind reglementarea prelucrării datelor cu caracter personal de către structurile/unitățile Ministerului Administrației și Internelor în activitățile de prevenire, cercetare și combatere a infracțiunilor, precum și de menținere și asigurare a ordinii publice, în vigoare la momentul comiterii faptelor, dar în prezent ambele abrogate (prin Legea nr. 129/2018 și, respectiv, prin Legea nr. 363/2018), precum și la art. 1 alin. (1) și (2) și art. 2 din Legea nr. 363/2018 privind protecția persoanelor fizice referitor la prelucrarea datelor

cu caracter personal de către autoritățile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale și combaterii infracțiunilor sau al executării pedepselor, măsurilor educative și de siguranță, precum și privind libera circulație a acestor date, concluzionându-se, pe baza acestora, că protecția datelor cu caracter personal reprezintă un suprastandard ce este prevăzut pentru exercitarea oricărui tip de activitate, excepțiile fiind limitativ și restrictiv prevăzute de lege.

În acest context s-a subliniat că orice prelucrare a datelor cu caracter personal, chiar dacă este realizată de către agenți care au recunoscute astfel de atribuții, trebuie să se desfășoare potrivit unor proceduri legale, în îndeplinirea competențelor prevăzute de actele normative, fără abuzuri sau derapaje. Astfel, motivul instituirii la nivel european și național a unui asemenea standard este strâns legat de protejarea drepturilor omului, iar orice excepție trebuie să aibă prevăzute garanții suficiente de care persoanele ale căror libertăți ar putea fi încălcate să poată să uzeze în apărarea drepturilor lor.

Referitor la cel de-al doilea element de analiză, legat de înțelesul noțiunii de „autorizare/depășirea limitelor autorizării", dată fiind calitatea subiectului activ din cauza în care a fost formulată întrebarea prealabilă, s-a făcut trimitere la conținutul textelor legale care guvernează activitatea polițistului [art. 41—43 din Legea nr. 360/2002 privind Statutul polițistului; art. 17 alin. (2), art. 19 alin. (3) și art. 22 din Hotărârea Guvernului nr. 991/2005 pentru aprobarea Codului de etică și deontologie al polițistului; art. 4 din anexa la Dispoziția Inspectoratului General al Poliției Române nr. 101 din 13 decembrie 2007], concluzionându-se că, potrivit reglementărilor în materie, agentul de poliție are obligația verificării și respectării permanente a cadrului legal în ceea ce privește desfășurarea activității sale.

De asemenea, pornindu-se de la înțelesul dat noțiunii de „acces la un sistem informatic" în cuprinsul Raportului explicativ al Convenției Consiliului Europei asupra criminalității informatice (Budapesta, 2001) și al art. 138 alin. (3) din Codul de procedură penală, s-a arătat că, în situația în care un astfel de sistem este protejat prin măsuri de securitate, accesul se face de către făptuitor pe baza unor credențiale (instrumente de autentificare) cunoscute anterior.

Totodată, s-a subliniat că atât timp cât utilizarea credențialelor și accesarea sistemului/bazei de date informatice se pot realiza doar în condițiile prevăzute de lege și doar cu parcurgerea unei proceduri specifice ce presupune efectuarea anterioară a unor acte proprii exercitării atribuțiilor de serviciu în legătură cu accesarea/interogarea efectuată, neîndeplinirea acestora excedează accesării legale a sistemului. Astfel, accesarea „cu drept" presupune nu numai existența posibilității generale recunoscute de lege de a accesa sistemul în baza credențialelor primite în vederea îndeplinirii atribuțiilor de serviciu, ci și a procedurilor specifice referitoare la exercitarea acestor atribuții în concret. Ca atare, s-a apreciat că legalitatea accesării trebuie analizată strict, atât prin prisma competențelor și atribuțiilor de serviciu prevăzute de lege, cât și prin prisma procedurilor instituite de lege privind îndeplinirea concretă a acestor atribuții și îndatoriri de serviciu.

Dacă, însă, s-a parcurs procedura specifică prevăzută de legislația specială (de exemplu, informarea prealabilă prevăzută de art. 4 din Legea nr. 238/2009 ori sesizarea șefului ierarhic privind comiterea unor fapte de corupție de către colegii de serviciu), faptul că, ulterior accesării, informațiile obținute nu sunt utilizate, nefiind importante pentru îndeplinirea atribuțiilor de serviciu, nu are relevanță, fapta de a accesa baza de date în temeiul credențialelor obținute neconstituind în acest caz infracțiunea de acces ilegal la un sistem informatic.

VII. **Examenul jurisprudenței în materie**

VII.1. **Jurisprudența relevantă a Înaltei Curți de Casație și Justiție**

VII.1.1. Din perspectiva hotărârilor obligatorii, menite să asigure unificarea practicii judiciare și care prezintă semnificație sub aspectul chestiunii ce formează obiectul întrebării prealabile, a fost identificată Decizia nr. 4 din 25 ianuarie 2021 a Înaltei Curți de Casație și Justiție, Completul pentru dezlegarea unor chestiuni de drept în materie penală, publicată în Monitorul Oficial al României, Partea I, nr. 171 din 19 februarie 2021, prin care s-a statuat că „Fapta de a deschide și utiliza un cont pe o rețea de socializare deschisă publicului, folosind ca nume de utilizator numele unei alte persoane și introducând date personale reale care permit identificarea acesteia, întrunește două dintre cerințele esențiale ale infracțiunii de fals informatic prevăzute de art. 325 din Codul penal, respectiv cea ca acțiunea de introducere a datelor informatice să fie realizată fără drept și cea ca acțiunea de introducere a datelor informatice să aibă ca rezultat date necorespunzătoare adevărului".

În cuprinsul considerentelor acesteia (paragraful X.2.A) s-a stabilit că, „Spre deosebire de Legea nr. 161/2003, care, în art. 35 alin. (2), reglementa înțelesul sintagmei «fără drept», Codul penal, deși a preluat toate infracțiunile din titlul III — *Prevenirea și combaterea criminalității informatice* al cărții I — *Reglementări generale pentru prevenirea și combaterea corupției* din Legea nr. 161/2003, precum și o parte din definițiile date unor noțiuni («sistem informatic», «date informatice»), nu cuprinde o dispoziție similară.

Având însă în vedere împrejurarea că prevederile art. 35 alin. (2) din Legea nr. 161/2003 nu au fost abrogate, ele continuă să aibă relevanță juridică din perspectiva incriminărilor preluate în noul Cod penal. Aceasta este poziția unitară a doctrinei, precum și a practicii judiciare și aceeași interpretare o regăsim și în jurisprudența Curții Constituționale. Astfel, efectuând controlul de constituționalitate cu privire la dispozițiile art. 360 din Codul penal referitoare la infracțiunea de acces ilegal la un sistem informatic, Curtea Constituțională precizează că infracțiunea a fost preluată din Legea nr. 161/2003 și explică cerința ca făptuitorul să acționeze fără drept prin referire la art. 35 alin. (2) din același act normativ, reținând că «chiar dacă Codul penal nu a preluat toate definițiile din Legea nr. 161/2003, aceasta rămâne în continuare un reper pentru înțelegerea elementelor de conținut ale infracțiunii criticate» (Decizia nr. 183 din 29 martie 2018, publicată în Monitorul Oficial al României, Partea I, nr. 486 din 13 iunie 2018).

Rezultă, așadar, că cerința ca acțiunea de contrafacere sau alterare a datelor informatice să fie realizată fără drept are semnificația atribuită prin dispozițiile art. 35 alin. (2) din Legea nr. 161/2003, respectiv «(…) acționează fără drept persoana care se află în una din următoarele situații:

a) Nu este autorizată, în temeiul legii sau al unui contract;

b) Depășește limitele autorizării;

c) Nu are permisiunea, din partea persoanei fizice sau juridice competente, potrivit legii, să o acorde, de a folosi, administra sau controla un sistem informatic ori de a desfășura cercetări științifice sau de a efectua orice altă operațiune într-un sistem informatic.»

În mod evident, dispozițiile art. 35 alin. (2) din Legea nr. 161/2003, comune unor incriminări distincte, trebuie analizate prin prisma elementului material al laturii obiective a fiecărei infracțiuni care are atașată această cerință esențială și pentru care textul este aplicabil."

VII.1.2. În ceea ce privește deciziile de speță, Direcția legislație, studii, documentare și informatică juridică din cadrul Înaltei Curți de Casație și Justiție a comunicat, prin Adresa nr. 981 din 28 iunie 2021, că nu a identificat practică judiciară cu privire la problema de drept care formează obiectul sesizării în vederea pronunțării unei hotărâri prealabile, aceeași constatare rezultând și în urma documentării prealabile întocmirii prezentului raport, realizată la nivelul Secției penale a instanței supreme.

VII.2. **Jurisprudența națională relevantă în materie**

În materialul transmis de curțile de apel au fost identificate două hotărâri judecătorești relevante pentru problema de drept ridicată în speță, și anume:

2.1. Sentința penală nr. 2.519 din 8 decembrie 2017 a Tribunalului București, Secția I penală, definitivă prin Decizia penală nr. 685/A din 17 mai 2018, pronunțată de Curtea de Apel București, Secția a II-a penală, în Dosarul nr. 7.618/3/2017, prin care inculpatul M.A. a fost condamnat la pedeapsa închisorii pentru comiterea infracțiunilor de acces ilegal la un sistem informatic, prevăzută de art. 360 alin. (1), (2) și (3) din Codul penal, și de divulgare a informațiilor secrete de serviciu sau nepublice, prevăzută de art. 304 alin. (1) din Codul penal, reținându-se, în esență, în fapt, că, la solicitarea telefonică a coinculpatului P.G., a accesat cu depășirea limitelor autorizării bazele de date pentru evidența persoanelor, evidența pașapoartelor și evidența auto, scopul nefiind unul în interes de serviciu, ci acela de a-i transmite solicitantului faptul că nu figurează urmărit național/internațional, în condițiile în care acesta din urmă fusese identificat de autoritățile franceze ca fiind autorul unei infracțiuni de furt pe raza orașului Paris. Ca atare, în urma accesării bazelor de date, inculpatul M.A. i-a comunicat celuilalt acuzat că nu figurează urmărit la nivel național, putând pătrunde pe teritoriul României.

2.2. Sentința penală nr. 192 din 15 iulie 2020 a Tribunalului Prahova, Secția penală, definitivă prin Decizia penală nr. 868 din 22 iulie 2021, pronunțată de Curtea de Apel Ploiești, Secția penală și pentru cauze cu minori și de familie în Dosarul nr. 2.207/105/2019, prin care inculpata T.A.I. a fost condamnată la pedeapsa închisorii pentru comiterea infracțiunilor de acces ilegal la un sistem informatic, prevăzută de art. 360 alin. (1) și (2) din Codul penal, cu aplicarea art. 35 alin. (1) din Codul penal, de operațiuni ilegale cu dispozitive sau programe informatice, prevăzută de art. 365 alin. (2) din Codul penal, cu aplicarea art. 35 alin. (1) din Codul penal, și de divulgare a informațiilor secrete de serviciu sau nepublice, prevăzută de art. 304 alin. (1) din Codul penal, cu aplicarea art. 35 alin. (1) din Codul penal, reținându-se, în esență, în fapt, că, în calitate de agent de poliție în cadrul Inspectoratului de Poliție al Județului Prahova, a utilizat fără drept, în modalitatea depășirii limitelor autorizării, conturile de acces și celelalte date de logare/parole de acces ale colegilor săi de serviciu și a accesat în mod repetat baza de date a Direcției pentru Evidența Persoanelor și Administrarea Bazelor de Date, pentru a consulta datele unor persoane în privința cărora nu exista o lucrare sau un dosar penal în curs, deși interogarea respectivei baze de date nu se putea realiza decât în anumite condiții și doar pentru îndeplinirea atribuțiilor de serviciu, și nu în scopuri personale; ulterior, anumite informații astfel obținute au fost divulgate de inculpată fratelui său.

VII.3. **Jurisprudența relevantă a Curții Constituționale**

3.1. Decizia nr. 183 din 29 martie 2018, publicată în Monitorul Oficial al României, Partea I, nr. 486 din 13 iunie 2018, prin care s-a respins, ca neîntemeiată, excepția de neconstituționalitate a dispozițiilor art. 360 alin. (3) din Codul penal, reținându-se, în considerente, că, potrivit art. 35 alin. (2) din Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției, „prin persoană care acționează fără drept se înțelege persoana care nu este autorizată, în temeiul legii sau al unui contract, persoana care depășește limitele autorizării sau persoana care nu are permisiunea, din partea persoanei fizice sau juridice competente, potrivit legii, să o acorde, de a folosi, administra sau controla un sistem informatic ori de a desfășura cercetări științifice sau de a efectua orice altă operațiune într-un sistem informatic. (…) Chiar dacă Codul penal nu a preluat toate definițiile din Legea nr. 161/2003, aceasta rămâne în continuare un reper pentru înțelegerea elementelor de conținut ale infracțiunii criticate, iar practica și jurisprudența anterioară își păstrează actualitatea, întrucât noua reglementare nu aduce modificări conținutului infracțiunii" (paragrafele 27 și 28).

3.2. Decizia nr. 353 din 22 mai 2018, publicată în Monitorul Oficial al României, Partea I, nr. 650 din 26 iulie 2018, prin care a fost respinsă, ca inadmisibilă, excepția de neconstituționalitate a dispozițiilor art. 250 alin. (1) și art. 360 din Codul penal. În considerentele acesteia s-a menționat, cu referire la incriminarea reglementată de art. 360 din Codul penal, că „aceasta protejează relațiile sociale a căror bună desfășurare depinde de respectarea securității și integrității sistemelor informatice, precum și a securității, integrității și confidențialității datelor informatice; (…) Elementul material al acestei infracțiuni îl constituie, în principiu, acea operațiune de acces, fără drept, prin care se realizează o interacțiune funcțională cu sistemul informatic" (paragraful 31).

3.3. Decizia nr. 27 din 19 ianuarie 2021, publicată în Monitorul Oficial al României, Partea I, nr. 325 din 31 martie 2021, prin care, verificând din nou constituționalitatea dispozițiilor art. 360 alin. (1) din Codul penal, instanța de contencios constituțional a reluat argumentele inserate în considerentele deciziei sale anterioare, nr. 183 din 29 martie 2018, publicată în Monitorul Oficial al României, Partea I, nr. 486 din 13 iunie 2018.

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

Nu au fost identificate decizii relevante în problema de drept analizată.

IX. **Dispoziții legale incidente**

Codul penal

Art. 360. — Accesul ilegal la un sistem informatic

(1) Accesul, fără drept, la un sistem informatic se pedepsește cu închisoarea de la 3 luni la 3 ani sau cu amendă.

(2) Fapta prevăzută în alin. (1), săvârșită în scopul obținerii de date informatice, se pedepsește cu închisoarea de la 6 luni la 5 ani.

(3) Dacă fapta prevăzută în alin. (1) a fost săvârșită cu privire la un sistem informatic la care, prin intermediul unor proceduri, dispozitive sau programe specializate, accesul este restricționat sau interzis pentru anumite categorii de utilizatori, pedeapsa este închisoarea de la 2 la 7 ani.

Art. 181. — Sistem informatic și date informatice

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

(2) Prin date informatice se înțelege orice reprezentare a unor fapte, informații sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic.

Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției

Art. 35.

(…)

(2) În sensul prezentului titlu, acționează fără drept persoana care se află în una dintre următoarele situații:

a) nu este autorizată, în temeiul legii sau al unui contract;

b) depășește limitele autorizării;

c) nu are permisiunea, din partea persoanei fizice sau juridice competente, potrivit legii, să o acorde, de a folosi, administra sau controla un sistem informatic ori de a desfășura cercetări științifice sau de a efectua orice altă operațiune într-un sistem informatic.

Convenția Consiliului Europei privind criminalitatea informatică, adoptată la Budapesta la 23 noiembrie 2001, ratificată prin Legea nr. 64/2004

Art. 2. — Accesarea ilegală

Fiecare parte va adopta măsurile legislative și alte măsuri considerate necesare pentru a incrimina ca infracțiune, potrivit dreptului său intern, accesarea intenționată și fără drept a ansamblului ori a unei părți a unui sistem informatic. O parte poate condiționa o astfel de incriminare de comiterea încălcării respective prin violarea măsurilor de securitate, cu intenția de a obține date informatice ori cu altă intenție delictuală, sau de legătura dintre încălcarea respectivă și un sistem informatic conectat la alt sistem informatic.

Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului

Art. 2. — Definiții

În sensul prezentei directive, se aplică următoarele definiții:

(…)

(d) „fără a avea dreptul” înseamnă un comportament menționat de prezenta directivă, inclusiv accesarea, afectarea integrității sau interceptarea, fără autorizare din partea proprietarului sau a unui alt titular de drepturi, a sistemului sau a unei părți a acestuia, sau care nu este permis în temeiul legislației naționale.

Art. 3. — Accesarea ilegală a sistemelor informatice

Statele membre adoptă măsurile necesare pentru a garanta că accesarea cu intenție și fără drept a unui sistem informatic sau a unei părți a acestuia este incriminată atunci când este săvârșită prin încălcarea unei măsuri de securitate, cel puțin atunci când nu reprezintă un caz minor.

X. **Opinia judecătorului-raportor**

Opinia judecătorului-raportor a fost în sensul respingerii, ca inadmisibilă, a sesizării formulate de Curtea de Apel Ploiești, Secția penală și pentru cauze cu minori și de familie, apreciindu-se că nu sunt îndeplinite, în mod cumulativ, toate condițiile de admisibilitate reglementate de art. 475 din Codul de procedură penală. Astfel, s-a considerat că în cauză nu există o veritabilă problemă de drept care să necesite o dezlegare cu valoare de principiu din partea Înaltei Curți de Casație și Justiție, iar soluționarea pe fond a apelului cu care a fost învestită instanța de trimitere nu depinde de lămurirea chestiunii ce face obiectul sesizării.

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

În urma examinării sesizării formulate de Curtea de Apel Ploiești, Secția penală și pentru cauze cu minori și de familie, în vederea pronunțării unei hotărâri prealabile, a raportului întocmit de judecătorul-raportor și a problemei ce se solicită a fi dezlegată, constată următoarele:

Reglementând condițiile de admisibilitate a sesizării Înaltei Curți de Casație și Justiție în vederea pronunțării unei hotărâri prealabile pentru dezlegarea unei chestiuni de drept, legiuitorul a stabilit în art. 475 din Codul de procedură penală posibilitatea anumitor instanțe, inclusiv a curții de apel, învestită cu soluționarea cauzei în ultimă instanță, care constată, în cursul judecății, existența unei chestiuni de drept de a cărei lămurire depinde soluționarea pe fond a cauzei și asupra căreia instanța supremă nu a statuat încă printr-o hotărâre prealabilă sau printr-un recurs în interesul legii și nici nu face obiectul unui asemenea recurs, să sesizeze Înalta Curte de Casație și Justiție în vederea pronunțării unei hotărâri prin care să se dea rezolvare de principiu respectivei probleme de drept.

Ca atare, pentru a fi admisibilă o asemenea sesizare trebuie îndeplinite cumulativ mai multe cerințe, respectiv existența unei cauze aflate în curs de judecată în ultimul grad de jurisdicție pe rolul uneia dintre instanțele prevăzute expres de articolul anterior menționat, soluționarea pe fond a acelei cauze să depindă de lămurirea chestiunii de drept ce formează obiectul sesizării, iar 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.

Totodată, din economia dispozițiilor legale invocate 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.

În speță, se constată că este îndeplinită condiția privind existența unei cauze pendinte aflate în curs de judecată în ultimă instanță, Curtea de Apel Ploiești, Secția penală și pentru cauze cu minori și de familie, fiind învestită în Dosarul nr. 4.710/105/2018 cu apelul declarat de inculpatul I.L. împotriva Sentinței penale nr. 247 din 28 septembrie 2020 a Tribunalului Prahova, Secția penală, prin care s-a dispus condamnarea celui din urmă pentru săvârșirea infracțiunii de acces ilegal la un sistem informatic, în formă continuată, prevăzută de art. 360 alin. (1), (2) și (3) din Codul penal, cu aplicarea art. 35 alin. (1) din Codul penal, la pedeapsa de 2 ani închisoare, în condițiile art. 91 și următoarele din Codul penal.

De asemenea, chestiunea ce formează obiectul întrebării cu care a fost sesizată instanța supremă nu a primit o rezolvare printr-o hotărâre prealabilă sau printr-un recurs în interesul legii și nici nu face obiectul unui asemenea recurs, așa cum rezultă

din cuprinsul Adresei nr. 1.134/C/1.544/III-5/2021 din 2 august 2021 a Parchetului de pe lângă Înalta Curte de Casație și Justiție.

Celelalte cerințe impuse de art. 475 din Codul de procedură penală nu sunt însă îndeplinite în cauză, întrucât nu există o veritabilă problemă de drept care să necesite o dezlegare cu valoare de principiu din partea instanței supreme, iar soluționarea pe fond a apelului cu care a fost învestită Curtea de Apel Ploiești nu depinde de lămurirea chestiunii ce face obiectul prezentei sesizări.

Astfel, sub acest din urmă aspect, este de menționat că, în jurisprudența sa, Completul pentru dezlegarea unor chestiuni de drept în materie penală a statuat asupra înțelesului ce trebuie atribuit sintagmei „problemă de drept de a cărei lămurire depinde soluționarea pe fond a cauzei", arătând că *„admisibilitatea sesizării în vederea pronunțării unei hotărâri prealabile este condiționată atât în cazul în care vizează o normă de drept material, cât și atunci când privește o dispoziție de drept procesual de împrejurarea ca interpretarea dată de instanța supremă să aibă consecințe juridice asupra modului de rezolvare a fondului cauzei. Cu alte cuvinte, între problema de drept a cărei lămurire se solicită și soluția dată asupra acțiunii penale și/sau civile de către instanța pe rolul căreia se află cauza în ultimul grad de jurisdicție, trebuie să existe o relație de dependență, în sensul ca decizia Înaltei Curți pronunțată în procedura prevăzută de art. 476—477 din Codul de procedură penală să fie de natură a produce un efect concret asupra conținutului hotărârii din procesul principal, cerința pertinenței fiind expresia utilității pe care rezolvarea de principiu a chestiunii de drept invocate o are în cadrul soluționării pe fond a litigiului."* (Decizia nr. 11 din 2 iunie 2014, publicată în Monitorul Oficial al României, Partea I, nr. 503 din 7 iulie 2014).

Ulterior, considerentele Deciziei nr. 11 din 2 iunie 2014 au fost preluate de Înalta Curte de Casație și Justiție și în cuprinsul altor hotărâri date în procedura reglementată de dispozițiile art. 475 și următoarele din Codul de procedură penală, prin care au fost respinse, ca inadmisibile, sesizările cu care instanța supremă a fost învestită, relevante fiind deciziile nr. 17 din 1 septembrie 2014, publicată în Monitorul Oficial al României, Partea I, nr. 691 din 22 septembrie 2014; nr. 19 din 15 septembrie 2014, publicată în Monitorul Oficial al României, Partea I, nr. 769 din 23 octombrie 2014; nr. 24 din 6 octombrie 2014, publicată în Monitorul Oficial al României, Partea I, nr. 823 din 11 noiembrie 2014; nr. 7 din 17 aprilie 2015, publicată în Monitorul Oficial al României, Partea I, nr. 359 din 25 mai 2015; nr. 26 din 29 octombrie 2015, publicată în Monitorul Oficial al României, Partea I, nr. 77 din 2 februarie 2016; nr. 28 din 29 octombrie 2015, publicată în Monitorul Oficial al României, Partea I, nr. 912 din 9 decembrie 2015; nr. 1 din 25 ianuarie 2017, publicată în Monitorul Oficial al României, Partea I, nr. 152 din 28 februarie 2017; nr. 20 din 14 iunie 2017, publicată în Monitorul Oficial al României, Partea I, nr. 542 din 10 iulie 2017; nr. 9 din 19 iunie 2018, publicată în Monitorul Oficial al României, Partea I, nr. 696 din 9 august 2018; nr. 11 din 12 septembrie 2018, publicată în Monitorul Oficial al României, Partea I, nr. 907 din 29 octombrie 2018; nr. 14 din 26 septembrie 2018, publicată în Monitorul Oficial al României, Partea I, nr. 988 din 22 noiembrie 2018; nr. 7 din 21 martie 2019, publicată în Monitorul Oficial al României, Partea I, nr. 365 din 10 mai 2019; nr. 21 din 29 octombrie 2019, publicată în Monitorul Oficial al României, Partea I, nr. 981 din 5 decembrie 2019; nr. 21 din 7 iulie 2020, publicată în Monitorul Oficial al României, Partea I, nr. 118 din 4 februarie 2021; nr. 12 din 18 februarie 2021, publicată în Monitorul Oficial al României, Partea I, nr. 355 din 7 aprilie 2021; nr. 17 din 17 martie 2021, publicată în Monitorul Oficial al României, Partea I, nr. 514 din 18 mai 2021.

Rezultă, așadar, din modul de definire/caracterizare a acestei condiții de admisibilitate a sesizării consacrat în jurisprudența constantă a Completului pentru dezlegarea unor chestiuni de drept în materie penală că relația de dependență dintre interpretarea dată de Înalta Curte de Casație și Justiție, prin intermediul mecanismului de unificare a practicii judiciare reglementat de art. 475 și următoarele din Codul de procedură penală, și rezolvarea pe fond a cauzei se verifică prin aptitudinea respectivei interpretări de a produce un efect concret asupra conținutului hotărârii din procesul în care a fost formulată întrebarea prealabilă, un asemenea raport de conexitate neexistând în acele situații în care oricare ar fi dezlegarea dată problemei de drept de către instanța supremă, aceasta nu va avea nicio influență asupra soluției pe fond a litigiului.

Or, în cauză, pornind de la tiparul normei de incriminare a faptei de acces ilegal la un sistem informatic, astfel cum este configurat în cuprinsul art. 360 din Codul penal, se constată că lămurirea aspectului ce formează obiectul sesizării cu care a fost învestit Completul pentru dezlegarea unor chestiuni de drept în materie penală nu poate avea nicio înrâurire asupra deciziei ce va fi luată pe fondul apelului înregistrat pe rolul Curții de Apel Ploiești, ce presupune examinarea învinuirii aduse apelantului inculpat prin rechizitoriu și dezlegarea definitivă a raportului juridic penal dedus judecății, neexistând legătura de dependență necesară dintre chestiunea de drept supusă interpretării și modul de rezolvare a procesului penal în curs, cerută cu caracter obligatoriu de dispozițiile procesual penale incidente în această procedură (art. 475).

Astfel, preluând fără modificări semnificative conținutul normativ al infracțiunii prevăzute de art. 42 din Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției, art. 360 din Codul penal reglementează infracțiunea de acces ilegal la un sistem informatic, într-o variantă de bază, ce interzice accesul, fără drept, la un sistem informatic [alin. (1)], și două variante agravate, care constau în comiterea faptei descrise în alineatul (1) în scopul obținerii de date informatice [alin. (2)] ori cu privire la un sistem informatic la care, prin intermediul unor proceduri, dispozitive sau programe specializate, accesul este restricționat sau interzis pentru anumite categorii de utilizatori, respectiv prin încălcarea unor măsuri de securitate [alin. (3)].

Fiind o infracțiune de pericol, obiectul juridic special al acesteia este constituit din relațiile sociale ale căror naștere și dezvoltare sunt condiționate de siguranța/securitatea sistemelor și datelor informatice constând în asigurarea confidențialității, integrității și accesibilității acestora, fără ca textul de incriminare să protejeze patrimoniul persoanei sau alte valori sociale ce ar putea fi lezate printr-o acțiune distinctă înlesnită ca urmare a consumării accesului, caz în care fapta incriminată de dispozițiile art. 360 din Codul penal va avea natura unei infracțiuni mijloc ce urmează a fi reținută în concurs cu o altă infracțiune.

De altfel, în ceea ce privește sfera relațiilor sociale ocrotite prin norma de incriminare, în același sens s-au pronunțat și Curtea Constituțională în cuprinsul Deciziei nr. 353 din 22 mai

2018, publicată în Monitorul Oficial al României, Partea I, nr. 650 din 26 iulie 2018, paragraful 31, dar și literatura de specialitate (George Antoniu, Tudorel Toader și colaboratorii, *Explicațiile noului Cod penal,* vol. IV, Editura Universul Juridic, București, 2016, pag. 855; George Zlati, *Tratat de criminalitate informatică*, Editura Solomon, 2020, pag. 147—148; Georgina Bodoroncea, Valerian Cioclei și colaboratorii, *Codul penal, Comentariu pe articole*, art. 1—446, Ediția a 3-a revizuită și adăugită, Editura C.H. Beck, București, 2020, pag. 1670—1671), precum și practica judiciară, inclusiv cea a instanței supreme (Decizia penală nr. 1.739 din 3 mai 2010 a Înaltei Curți de Casație și Justiție, Secția penală, pronunțată în Dosarul nr. 761/64/2009).

Elementul material al laturii obiective a variantei normative de bază a infracțiunii prevăzute de art. 360 din Codul penal (la care se raportează, de altfel, și cele două variante agravate) constă în acțiunea de acces la un sistem informatic, ce presupune o interacțiune la nivel logic cu respectivul sistem, direct și nemijlocit ori de la distanță, care să permită făptuitorului să beneficieze de resursele ori/și de funcțiile lui, iar cerința esențială atașată acestuia presupune ca activitatea incriminată să se desfășoare fără drept, adică, cu alte cuvinte, ilegal sau neautorizat.

Deși Codul penal a preluat, în capitolul VI — Infracțiuni contra siguranței și integrității sistemelor informatice din titlul VII al Părții speciale, toate infracțiunile din titlul III — Prevenirea și combaterea criminalității informatice al cărții I — Reglementări generale pentru prevenirea și combaterea corupției din Legea nr. 161/2003, precum și o parte din definițiile date unor noțiuni („sistem informatic", „date informatice"), nu a explicat și conținutul sintagmei „fără drept", precizarea semnificației acesteia regăsindu-se doar în cuprinsul art. 35 alin. (2) din cel din urmă act normativ menționat, care stabilește că o persoană acționează într-o atare modalitate (fără drept) atunci când se află în una dintre următoarele situații: a) nu este autorizată, în temeiul legii sau al unui contract; b) depășește limitele autorizării; c) nu are permisiunea, din partea persoanei fizice sau juridice competente, potrivit legii, să o acorde, de a folosi, administra sau controla un sistem informatic ori de a desfășura cercetări științifice sau de a efectua orice altă operațiune într-un sistem informatic.

Cu privire la aplicabilitatea, în actualul cadru normativ, a prevederilor art. 35 alin. (2) din Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției, prin Decizia nr. 4 din 25 ianuarie 2021 a Înaltei Curți de Casație și Justiție, Completul pentru dezlegarea unor chestiuni de drept în materie penală, publicată în Monitorul Oficial al României, Partea I, nr. 171 din 19 februarie 2021, s-a stabilit, prin raportare la împrejurarea că acestea nu au fost abrogate, că *„ele continuă să aibă relevanță juridică din perspectiva incriminărilor preluate în noul Cod penal.* Aceasta este poziția unitară a doctrinei, precum și a practicii judiciare și *aceeași interpretare o regăsim și în jurisprudența Curții Constituționale.* Astfel, efectuând controlul de constituționalitate cu privire la dispozițiile art. 360 din Codul penal referitoare la infracțiunea de acces ilegal la un sistem informatic, *Curtea Constituțională* precizează că infracțiunea a fost preluată din Legea nr. 161/2003 și *explică cerința ca făptuitorul să acționeze fără drept prin referire la art. 35 alin. (2) din același act normativ,* reținând că *«chiar dacă Codul penal nu a preluat toate definițiile din Legea nr. 161/2003, aceasta rămâne în continuare un reper pentru înțelegerea elementelor de conținut ale infracțiunii criticate»* (Decizia nr. 183 din 29 martie 2018, publicată în Monitorul Oficial al României, Partea I, nr. 486 din 13 iunie 2018). *Rezultă, așadar, că cerința ca acțiunea de contrafacere sau alterare a datelor informatice să fie realizată fără drept are semnificația atribuită prin dispozițiile art. 35 alin. (2) din Legea nr. 161/2003 (…). În mod evident, dispozițiile art. 35 alin. (2) din Legea nr. 161/2003, comune unor incriminări distincte, trebuie analizate prin prisma elementului material al laturii obiective a fiecărei infracțiuni care are atașată această cerință esențială și pentru care textul este aplicabil."*

Ca atare, având în vedere aspectele statuate, cu caracter obligatoriu, de Înalta Curte de Casație și Justiție prin intermediul mecanismului de unificare a practicii judiciare reglementat de art. 475 și următoarele din Codul de procedură penală, cerința esențială atașată elementului material al laturii obiective a variantei normative de bază a infracțiunii prevăzute de art. 360 din Codul penal nu poate fi interpretată decât prin prisma dispozițiilor art. 35 alin. (2) din Legea nr. 161/2003, accesul fără drept la un sistem informatic vizând inclusiv situația în care făptuitorul acționează cu depășirea limitelor autorizării.

Această ipoteză în care accesul se realizează fără drept presupune, prin definiție, preexistența unei autorizări legale sau contractuale care, în special în situația persoanelor ce pot interoga oricând o bază de date conținând informații nepublice, vizată de întrebarea prealabilă, stabilește întotdeauna și limitele impuse cu privire la interacțiunea agentului cu sistemul informatic. Astfel, autorul este autorizat să interacționeze la nivel logic cu respectivul sistem informatic, însă conținutul acestei interferențe depășește cadrul stabilit prin lege/ordonanță sau actele de reglementare secundară ori prin convenția care a permis-o, aspect de natură să translateze fapta comisă în sfera ilicitului penal.

Rezultă, așadar, că analiza depășirii limitelor autorizării implică, pe de o parte, stabilirea existenței autorizării legale sau contractuale, iar, pe de altă parte, determinarea conținutului acesteia, singurul în măsură să furnizeze criteriile obiective în raport cu care se poate concluziona asupra caracterului legal sau ilegal al accesului la sistemul informatic.

În acest sens, în cadrul examinării realizate, organul judiciar verifică, în baza actelor normative care reglementează competențele și atribuțiile de serviciu într-un anumit domeniu de activitate, a regulamentelor de ordin intern sau a clauzelor specifice din contractele de muncă și a prevederilor din fișele postului, limitele autorizării — ce pot privi, printre altele, în cazul persoanelor ce pot interoga oricând o bază de date conținând informații nepublice, la care se referă sesizarea instanței supreme, obiectul, durata, natura și scopul accesului, tipul de date ce pot fi prelucrate și categoriile de persoane vizate —, dar și conduita materială a agentului pe durata accesului la sistemul informatic, căci depășirea limitelor autorizării trebuie să aibă loc în acest interval de timp.

Așa cum s-a arătat, fiind o infracțiune de pericol, accesul fără drept la un sistem informatic, prevăzută de art. 360 alin. (1) din Codul penal, se consumă în momentul realizării elementului material al laturii obiective, respectiv al accesului, când autorul, interacționând la nivel logic cu sistemul informatic, beneficiază de resursele ori/și de funcțiile lui și când se produce urmarea imediată constând în lezarea relațiilor sociale privind siguranța/securitatea sistemelor și datelor informatice prin asigurarea confidențialității, integrității și accesibilității acestora,

fără să prezinte vreo relevanță în ceea ce privește caracterizarea faptei ca infracțiune conduita ulterioară a agentului în raport cu informațiile obținute prin accesarea sistemului informatic, sub aspectul folosirii sau nefolosirii lor ori al scopului în care au fost efectiv utilizate (în cadrul activității de serviciu sau fără legătură cu aceasta), deoarece aceasta intervine după momentul consumării infracțiunii.

Lipsa autorizării sau depășirea limitelor acesteia trebuie să vizeze accesul, și nu folosirea datelor informatice, fiind fără importanță modul sau scopul în care informațiile obținute prin această acțiune au fost utilizate ulterior consumării accesului sau dacă nu au fost folosite în cadrul unei anumite activități, motiv pentru care orice analiză sub acest aspect excedează operațiunii de stabilire a tipicității infracțiunii reglementate de art. 360 alin. (1) din Codul penal (în acest sens a se vedea George Zlati, *Tratat de criminalitate informatică*, Editura Solomon, 2020, pag. 236, 240—241).

Ca atare, atitudinea ulterioară a autorului, care nu se integrează în conținutul constitutiv al infracțiunii de acces ilegal la un sistem informatic, poate cel mult întruni elementele de tipicitate ale unei/unor alte infracțiuni, cum ar fi divulgarea informațiilor secrete de serviciu sau nepublice, prevăzută de art. 304 din Codul penal, abuz în serviciu, prevăzut de art. 297 alin. (1) din Codul penal, folosirea, în orice mod, direct sau indirect, de informații ce nu sunt destinate publicității ori permiterea accesului unor persoane neautorizate la aceste informații, prevăzută de art. 12 alin. (1) lit. b) din Legea nr. 78/2000 privind prevenirea, descoperirea și sancționarea faptelor de corupție, frauda informatică, prevăzute de art. 249 din Codul penal, pentru care, astfel cum s-a argumentat în dezvoltările anterioare, fapta incriminată de dispozițiile art. 360 din Codul penal va avea natura unei infracțiuni mijloc, singura problemă care se ridică în legătură cu conduita manifestată de agent după consumarea acestei din urmă infracțiuni fiind aceea a îndeplinirii condițiilor prevăzute de lege pentru existența pluralității sub forma concursului, fără nicio consecință cu privire la realizarea cerinței esențiale atașate elementului material al laturii obiective a infracțiunii de acces fără drept la un sistem informatic.

Având în vedere toate aceste considerații teoretice, se apreciază că lămurirea chestiunii ce formează obiectul întrebării prealabile nu se repercutează în niciun fel și nu poate avea vreo înrâurire asupra deciziei ce va fi luată pe fondul apelului înregistrat pe rolul Curții de Apel Ploiești, ce presupune verificarea temeiniciei acuzației aduse apelantului inculpat prin rechizitoriu și dezlegarea definitivă a raportului juridic de drept penal dedus judecății, prin stabilirea întrunirii sau, după caz, a neîntrunirii condițiilor de tipicitate obiectivă ale infracțiunii de acces fără drept (prin depășirea limitelor autorizării) la un sistem informatic, prevăzută de art. 360 din Codul penal, pentru care acesta a fost trimis în judecată, neexistând legătura de dependență necesară dintre problema de drept supusă interpretării și modul de rezolvare a procesului penal aflat pe rolul instanței în ultimul grad de jurisdicție, aspect ce determină inadmisibilitatea sesizării pentru neîndeplinirea uneia dintre condițiile cumulative prevăzute de art. 475 din Codul de procedură penală.

Deopotrivă, în cauză nu este întrunită nici cerința referitoare la existența unei veritabile probleme de drept care să necesite o dezlegare cu valoare de principiu din partea Înaltei Curți de Casație și Justiție, căci, față de modul în care a fost formulată întrebarea prealabilă, sesizarea tinde la rezolvarea propriu-zisă de către instanța supremă a cauzei cu care curtea de apel a fost învestită, depășind astfel cadrul unei interpretări *in abstracto* a dispozițiilor legale.

Or, 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 deciziile nr. 6 din 2 martie 2016, publicată în Monitorul Oficial al României, Partea I, nr. 287 din 15 aprilie 2016; nr. 19 din 27 septembrie 2016, publicată în Monitorul Oficial al României, Partea I, nr. 874 din 1 noiembrie 2016; nr. 20 din 14 iunie 2017, publicată în Monitorul Oficial al României, Partea I, nr. 542 din 10 iulie 2017; nr. 27 din 12 decembrie 2017, publicată în Monitorul Oficial al României, Partea I, nr. 65 din 22 ianuarie 2018; nr. 5 din 21 martie 2019, publicată în Monitorul Oficial al României, Partea I, nr. 381 din 15 mai 2019; nr. 19 din 29 octombrie 2019, publicată în Monitorul Oficial al României, Partea I, nr. 108 din 12 februarie 2020), 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 (…). Hotărârile prealabile trebuie pronunțate numai în interpretarea și aplicarea dispozițiilor legale, constituind o dezlegare de principiu a unei probleme de drept. În egală măsură, sesizarea trebuie să vizeze exclusiv probleme de interpretare a legii, și nu elemente particulare ale cauzei deduse judecății”.*

Ca atare, instanța supremă a statuat că, pentru a fi admisibilă, sesizarea trebuie să vizeze interpretarea *in abstracto* a unor prevederi legale determinate, iar nu rezolvarea unor chestiuni ce țin de particularitățile cauzei, dar și că, pentru a exista o veritabilă problemă de drept, premisa de la care se pornește în formularea întrebării adresate Înaltei Curți de Casație și Justiție, în procedura reglementată de art. 475 și următoarele din Codul de procedură penală, trebuie să își găsească izvorul în dispozițiile legale, și nu într-o stare de fapt, aplicarea legii la o anumită situație factuală, astfel cum aceasta a fost stabilită în urma interpretării probatoriului administrat, fiind atributul exclusiv al instanței învestite cu soluționarea cauzei (deciziile nr. 16 din 22 mai 2015, publicată în Monitorul Oficial al României, Partea I, nr. 490 din 3 iulie 2015; nr. 23 din 16 septembrie 2015, publicată în Monitorul Oficial al României, Partea I, nr. 824 din 4 noiembrie 2015; nr. 28 din 29 octombrie 2015, publicată în Monitorul Oficial al României, Partea I, nr. 912 din 9 decembrie 2015; nr. 10 din 12 aprilie 2016, publicată în Monitorul Oficial al României, Partea I, nr. 348 din 6 mai 2016; nr. 14 din 18 mai 2016, publicată în Monitorul Oficial al României, Partea I, nr. 460 din 21 iunie 2016; nr. 27 din 12 decembrie 2017, publicată în Monitorul Oficial al României, Partea I, nr. 65 din 22 ianuarie 2018; nr. 9 din 19 iunie 2018, publicată în Monitorul Oficial al României, Partea I, nr. 696 din 9 august 2018).

Mai mult, s-a subliniat că rațiunea sesizării în vederea pronunțării unei hotărâri prealabile pentru dezlegarea unei chestiuni de drept nu este aceea ca judecata Înaltei Curți de

Casație și Justiție să se substituie celei a instanțelor de trimitere (Decizia nr. 26 din 29 octombrie 2015, publicată în Monitorul Oficial al României, Partea I, nr. 77 din 2 februarie 2016), rolul practicii și literaturii de specialitate fiind doar acela de a oferi repere acestora în ceea ce privește modul de aplicare a legii, cu precizarea expresă că adoptarea soluțiilor reprezintă atributul exclusiv al judecătorului (Decizia nr. 1 din 25 ianuarie 2017, publicată în Monitorul Oficial al României, Partea I, nr. 152 din 28 februarie 2017).

În cauză, însă, din modalitatea de formulare a întrebării adresate Completului pentru dezlegarea unor chestiuni de drept în materie penală, dar și din mențiunile inserate de instanța de trimitere în cuprinsul Încheierii de sesizare din 14 iunie 2021 rezultă că problema ce se solicită a fi lămurită nu este susceptibilă de a primi o rezolvare de principiu printr-o hotărâre pronunțată în condițiile art. 477 din Codul de procedură penală, atât timp cât nu vizează interpretarea *in abstracto* a dispozițiilor art. 360 alin. (1) din Codul penal, prin stabilirea, în general, a înțelesului sau conținutului normei de incriminare, ci doar aplicarea acesteia la cazul concret dedus judecății, în funcție de particularitățile speței rezultate din propria analiză a materialului probator administrat, cu scopul de a se identifica soluția ce trebuie adoptată în dosarul aflat pe rolul Curții de Apel Ploiești.

Astfel, ceea ce se solicită Înaltei Curți de Casație și Justiție este de a stabili dacă, „în cazul persoanelor care pot interoga oricând o bază de date conținând informații nepublice, o asemenea interogare neurmată de efectuarea ulterioară a unor acte specifice exercitării atribuțiilor de serviciu în legătură cu interogarea efectuată poate reprezenta o depășire a limitelor pentru care a fost acordată autorizarea”, respectiv dacă, în această situație particulară ce formează obiectul cauzei cu care a fost învestită instanța de trimitere, faptele imputate inculpatului întrunesc sau nu elementele de tipicitate obiectivă ale infracțiunii prevăzute de art. 360 alin. (1) din Codul penal privind accesul ilegal la un sistem informatic.

Or, așa cum s-a arătat anterior, analiza depășirii limitelor autorizării implică, pe de o parte, stabilirea existenței autorizării legale sau contractuale, iar, pe de altă parte, determinarea conținutului acesteia, singurul în măsură să furnizeze criteriile obiective în raport cu care se poate concluziona asupra caracterului legal sau ilegal al accesului la sistemul informatic.

În acest sens, în cadrul examenului realizat, organul judiciar verifică, în temeiul actelor normative care reglementează competențele și atribuțiile de serviciu într-un anumit domeniu de activitate, al regulamentelor de ordin intern sau al clauzelor specifice din contractele de muncă și al prevederilor din fișele postului, limitele autorizării, dar și conduita materială efectivă a agentului pe durata accesului la sistemul informatic, toate acestea constituind aspecte de natură strict factuală, ce diferă de la caz la caz, în funcție de particularitățile speței deduse judecății, și care urmează a fi stabilite de instanța învestită pe baza materialului probator administrat în cauză, care va fundamenta concluzia depășirii sau a nedepășirii respectivelor limite și, implicit, a caracterului legal ori ilegal al accesului, neputând fi determinate prin mecanismul prevăzut de art. 475 și următoarele din Codul de procedură penală repere și criterii general valabile în funcție de care curtea de apel să decidă asupra îndeplinirii cerinței esențiale atașate elementului material al laturii obiective a infracțiunii prevăzute de art. 360 alin. (1) din Codul penal.

O asemenea analiză se impune a fi efectuată și de instanța de trimitere pentru a stabili existența autorizării legale sau contractuale a inculpatului de a accesa sistemele informatice ce stochează bazele de date interogate, precum și limitele unei atari autorizări și atitudinea materială a acestuia pe timpul interogărilor realizate, o astfel de evaluare concretă a datelor ce particularizează accesul, în contextul verificării tipicității obiective a infracțiunii, neputând fi făcută de Înalta Curte în procedura pronunțării unei hotărâri prealabile pentru dezlegarea unei chestiuni de drept întrucât s-ar ajunge la o deturnare a scopului pentru care aceasta a fost reglementată, respectiv acela de a asigura o practică unitară la nivelul instanțelor judecătorești prin interpretarea *in abstracto* a unor veritabile probleme de drept.

În realitate, răspunsul la problematica pe care o ridică curtea de apel este diferit în funcție de circumstanțele particulare ale fiecărei spețe, situație în care dezlegarea acesteia își pierde caracterul pur teoretic, fiind condiționată de analiza datelor concrete ale cauzei și tinzând, de fapt, la o rezolvare a fondului litigiului aflat în ultimul grad de jurisdicție.

De altfel, împrejurarea că sesizarea Completului pentru dezlegarea unor chestiuni de drept în materie penală nu a vizat interpretarea cu valoare de principiu a unei dispoziții legale, ci stabilirea incidenței acesteia la o situație de fapt concretă (diferită de cea expusă de tribunal), stabilită în urma propriei interpretări a materialului probator administrat, reiese și din „indicațiile” date de instanța de trimitere, după reformularea întrebării într-o variantă diferită de cea menționată de către inculpat, precizându-se, prin extinderea, în fapt, a conținutului acesteia, că „Se impune a fi stabilit (*n.n.* de instanța supremă) dacă în cazul acestei categorii de funcționari (*n.n.* persoanele care pot interoga oricând o bază de date conținând informații nepublice), va fi reținută o depășire a limitelor legale a autorizării în cazul unei situații de fapt în care interogarea bazei de date să fie considerată necesară, însă informațiile obținute în urma interogării să nu prezinte relevanță pentru exercitarea ulterioară a atribuțiilor de serviciu și nici să nu fie valorificate în scop extraprofesional de titularul parolei de acces la baza de date”.

Mai mult, cu prilejul dezbaterii (la termenul de judecată din 8 iunie 2021) cererii apelantului inculpat de sesizare a Înaltei Curți de Casație și Justiție, curtea de apel a pus în discuție, din oficiu, împrejurarea că aspectele care trebuie lămurite de Înalta Curte „ar trebui să aibă în vedere fișa postului pe care o avea inculpatul, faptul că se recunoaște un acces nerestricționat în baza de date, acces efectuat pe baza unei parole distribuite, precum și faptul că, în absența unor îndrumări specifice din fișa postului, verificarea periodică a acestei baze de date, neînsoțită de efectuarea altor lucrări ulterioare de specialitate, poate întruni condițiile de tipicitate a infracțiunii cu care instanța a fost sesizată”.

Așadar, se constată că ceea ce se cere în realitate în procedura prevăzută de art. 475 și următoarele din Codul de procedură penală nu este interpretarea *in abstracto* a normei de incriminare a faptei de acces fără drept la un sistem informatic, ci, transformând propria opinie cu privire la circumstanțele faptice concrete ale cauzei în ipoteză a întrebării, Curtea de Apel Ploiești solicită stabilirea întrunirii sau, după caz, a neîndeplinirii în speța particulară dedusă judecății a condițiilor de tipicitate obiectivă ale infracțiunii prevăzute de art. 360 alin. (1) din Codul penal, sub aspectul cerinței esențiale atașate elementului material, lucru inadmisibil din perspectiva normelor procesual penale indicate, astfel cum înțelesul acestora a fost configurat în

jurisprudența constantă a Completului pentru dezlegarea unor chestiuni de drept în materie penală.

În plus, din mențiunile inserate în Încheierea de sesizare din 14 iunie 2021, care, deși nu cuprinde opinia completului cu privire la aspectul ce formează obiectul întrebării, face referire la „problemele de drept care se ridică în legătură" cu art. 360 din Codul penal, rezultă că instanța de trimitere, în baza unei situații de fapt diferite de cea expusă de tribunal, și-a format deja o părere cu privire la modul de dezlegare a chestiunii cu care a sesizat Înalta Curte de Casație și Justiție, urmărind, în realitate, prin declanșarea mecanismului de unificare a practicii judiciare, o confirmare sau, dimpotrivă, o infirmare a soluției ce se prefigurează în cauza cu care a fost învestită, și nu o rezolvare de principiu a unei veritabile probleme de drept, prin pronunțarea unei hotărâri prealabile obligatorii, de la momentul publicării sale în Monitorul Oficial al României, Partea I, pentru toate instanțele. Or, așa cum a stabilit Înalta Curte, Completul pentru dezlegarea unor chestiuni de drept în materie penală, în cuprinsul Deciziei nr. 26 din 23 noiembrie 2017, publicată în Monitorul Oficial al României, Partea I, nr. 328 din 13 aprilie 2018, „procedura pronunțării unei asemenea hotărâri este condiționată (…) de existența unei chestiuni de drept de a cărei lămurire depinde soluționarea cauzei în care s-a dispus sesizarea, nefiind permis a se apela la acest mijloc legal în scopul de a primi de la instanța supremă rezolvarea în concret a speței", în același sens fiind și considerentele deciziilor nr. 5 din 13 februarie 2020, publicată în Monitorul Oficial al României, Partea I, nr. 258 din 30 martie 2020, și nr. 17 din 17 martie 2021, publicată în Monitorul Oficial al României, Partea I, nr. 514 din 18 mai 2021, ale aceluiași complet.

În consecință, raportat la toate argumentele expuse anterior se apreciază că nu sunt îndeplinite condițiile de admisibilitate reglementate de art. 475 din Codul de procedură penală constând în existența unei veritabile probleme de drept care să necesite o dezlegare cu valoare de principiu din partea Înaltei Curți de Casație și Justiție și a unei relații de dependență între lămurirea chestiunii supuse interpretării și soluționarea pe fond a cauzei cu care a fost învestită instanța de trimitere, motiv pentru care, în temeiul art. 477 din Codul de procedură penală, sesizarea formulată de Curtea de Apel Ploiești, Secția penală și pentru cauze cu minori și de familie va fi respinsă, ca inadmisibilă.

PENTRU ACESTE MOTIVE

În numele legii

DECIDE:

Respinge, ca inadmisibilă, sesizarea formulată de Curtea de Apel Ploiești, Secția penală și pentru cauze cu minori și de familie, prin care solicită pronunțarea unei hotărâri prealabile pentru dezlegarea de principiu a următoarei chestiuni de drept:

„În interpretarea dispozițiilor art. 360 alin. (1) din Codul penal privind accesul ilegal la un sistem informatic, în cazul persoanelor care pot interoga oricând o bază de date conținând informații nepublice, o asemenea interogare neurmată de efectuarea ulterioară a unor acte specifice exercitării atribuțiilor de serviciu în legătură cu interogarea efectuată poate reprezenta o depășire a limitelor pentru care a fost acordată autorizarea."

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, 29 septembrie 2021.

PREȘEDINTELE SECȚIEI PENALE A ÎNALTEI CURȚI
DE CASAȚIE ȘI JUSTIȚIE
judecător **DANIEL GRĂDINARU**

Magistrat-asistent,
Florin Nicușor Mihalache

EDITOR: PARLAMENTUL ROMÂNIEI — CAMERA DEPUTAȚILOR

„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 Biroului pentru relații cu publicul este:
Str. Parcului nr. 65, intrarea A, sectorul 1, București; 012329.
Tel. 021.401.00.73, e-mail: concursurifp@ramo.ro, convocariaga@ramo.ro
Pentru publicări, încărcați actele pe site, la: https://www.monitoruloficial.ro/brp/

Monitorul Oficial al României, Partea I, nr. 56/19.I.2022 conține 16 pagini. Prețul: 4 lei **ISSN** 1453—4495