

ROMÂNIA
CURTEA DE APEL ---
SECȚIA PENALĂ ȘI PENTRU CAUZE CU MINORI ȘI DE FAMILIE

Dosar nr. --

ÎNCHIEIERE
Ședința publică din data de 14 iunie 2021
Instanța constituită din:
Președinte --
Judecător --
Judecător --
Grefier --

Ministerul Public a fost reprezentat de procuror ----- din cadrul Parchetului de pe lângă Curtea de Apel ---

Pe rol pronunțarea asupra solicitării formulate de apelantul -- inculpat -----, în sensul sesizării Înaltei Curți de Casație și Justiție cu privire la pronunțarea unei hotărâri prealabile pentru dezlegarea unei chestiuni de drept.

Dezbaterile asupra modului de formulare a solicitării și cu privire la condițiile de admisibilitate a sesizării Înaltei Curți de Casație și Justiție - Completul pentru dezlegarea unor chestiuni de drept în materie penală, conform dispozițiilor art. 475 și 476 C.proc.pen., au avut loc la termenul de judecată din data de 08 iunie 2021, pozițiile procesuale și susținerile părților fiind consemnate în încheierea de ședință de la acel termen de judecată, dată la care instanța a stabilit pronunțarea asupra solicitării formulate pentru astăzi, când a hotărât următoarele:

CURTEA,

Deliberând cu privire la condițiile de admisibilitate în vederea sesizării Înaltei Curți de Casație și Justiție - Completul pentru dezlegarea unor chestiuni de drept în materie penală, conform dispozițiilor art. 475 și 476 C.proc.pen., constată următoarele:

La termenul de judecată din data de 08 iunie 2021, instanța de control judiciar, sesizată cu judecarea apelului formulat inculpatul --- împotriva sentinței penale nr. 247 din 28.09.2020 pronunțate de Tribunalul ---, a supus dezbaterii părților posibilitatea de a sesiza Înalta Curte de Casație și Justiție - Completul pentru dezlegarea unor chestiuni de drept în materie penală, pentru pronunțarea unei hotărâri prin care să dea o rezolvare de principiu unei chestiuni de drept, vizând dispozițiile art. 360 alin.(1) din Codul penal, respectiv 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

Obiectul cauzei:

Prin sentința penală nr. ---/---, pronunțată de Tribunalul --- în dosarul nr. ----- s-au dispus următoarele măsuri:

"În baza art. 360 alin. 1, 2 și 3 C.p., cu aplic. art. 35 alin. 1 C.p. cu aplic. art. 396 alin. 2 C.pr.Pen. condamnă pe inculpatul ---, (...) pentru savarsirea infracțiunii de acces ilegal la un sistem informatic în formă continuată (177 acte materiale), la pedeapsa de 2 (doi) ani închisoare.

În baza art. 91 C.pen., dispune suspendarea executării pedepsei de 2(doi) ani închisoare aplicată inculpatului sub supraveghere și stabilește un termen de supraveghere de 2 ani, conform dispozițiilor art. 92 C. pen.

În baza art.93 alin.(1) C.pen. obliga inculpatul --- ca pe durata termenului de supraveghere să respecte următoarele măsuri de supraveghere:

- a) să se prezinte la Serviciul de Probațiune ---, la datele fixate de acesta;*
- b) să primească vizitele consilierului de probațiune desemnat cu supravegherea sa;*
- c) să anunțe, în prealabil, schimbarea locuinței și orice deplasare care depășește 5 zile;*
- d) să comunice schimbarea locului de muncă;*
- e) să comunice informații și documente de natură a permite controlul mijloacelor sale de existență.*

În baza art.93 alin. (2) lit.b) C.pen. impune inculpatului să execute următoarea obligație: să frecventeze un program de reintegrare socială derulat de Serviciul de Probațiune --- .

În baza art.93 alin.(3) C.pen.,pe parcursul termenului de supraveghere, inculpatul va presta o muncă neremunerată în folosul comunității pe o perioadă de 60 de zile lucrătoare, în cadrul Administrației Parcului Memorial Constantin Stere sau a Centrului Județean de Cultura ---.

În baza art. 91 alin. (4) C.pen. atrage atenția inculpatului asupra disp. art. 96 C. pen.

În baza art. 274 alin. 1 c.p.p., obligă inculpatul la plata cheltuielilor judiciare avansate de stat în cuantum de 2000 lei.”

Pentru a hotărî astfel, Tribunalul --- a reținut, în esență, următoarea situație de fapt:

În calitate de agent șef adjunct de poliție în cadrul Poliției - --- - Secția --, la data de 25.12.2013, ora 02:45:53, inculpatul ----- a accesat, fără drept (respectiv cu depășirea împuternicirii primite), un sistem informatic, respectiv bazele de date administrate de D.R.P.C.I.V. și D.E.B.A.P.D. (sisteme informatice la care accesul este permis numai prin introducerea unui user-name și a unei parole, deci prin intermediul unor proceduri), folosind user-name-ul și parola pe care le putea folosi pentru a accesa aceste sisteme informatice numai în exercitarea atribuțiilor de serviciu ca polițist, în scopul obținerii de date informatice, și anume datele de identificare ale autoturismului detinut de numitul -----, șeful Poliției -----, și datele acestuia de stare civilă, nu în exercitarea atribuțiilor de serviciu, ci în interes personal.

La aceeași dată, ora 02:46:44, inculpatul --- a accesat, fără drept (respectiv cu depășirea împuternicirii primite), un sistem informatic, respectiv baza de date administrate de D.R.P.C.I.V. (sistem informatic la care accesul este permis numai prin introducerea unui user-name și a unei parole, deci prin intermediul unor proceduri), folosind user-name-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 identificare ale autoturismelor detinute de ----, nu în exercitarea atribuțiilor de serviciu, ci în interes personal.

La data de 05.12.2014, ora 11:42:52, inculpatul --- a accesat, fără drept (respectiv cu depășirea împuternicirii primite), un sistem informatic, respectiv bazele de date administrate de D.R.P.C.I.V. și D.E.B.A.P.D. (sisteme informatice la care accesul este permis numai prin introducerea unui user-name și a unei parole, deci prin intermediul unor proceduri), folosind user-name-ul și parola pe care le putea folosi pentru a accesa aceste sisteme informatice numai în exercitarea atribuțiilor de serviciu ca polițist, în scopul obținerii de date informatice, și anume datele de stare civilă ale numitilor -----, șeful Poliției -----, -----, soția acestuia și -----, fiul acestora, și datele de identificare ale autoturismelor detinute de sus numitii, întrunesc elementele constitutive ale infracțiunii prevăzute de art. 360 alin. 1, 2 și 3 C.pen., cu aplicarea art. 35 alin. 1 C.pen. (6 acte materiale).

La data de 14.02.2014, ora 00:51:50, inculpatul --- a accesat, fără drept (respectiv cu depășirea împuternicirii primite), un sistem informatic, respectiv bazele de date administrate de D.R.P.C.I.V. și D.E.B.A.P.D. (sisteme informatice la care accesul este permis numai prin introducerea unui user-name și a unei parole, deci prin intermediul unor proceduri), folosind user-name-ul și parola pe care le putea folosi pentru a accesa aceste sisteme informatice numai în exercitarea atribuțiilor de serviciu ca polițist, în scopul obținerii de date informatice, și anume datele de identificare ale autoturismului detinut de numitul ----, șeful ---- din cadrul Poliției -----, și

datele acestuia de stare civilă, nu în exercitarea atribuțiilor de serviciu, ci în interes personal.

La data de 30.12.2014, ora 00:11:07, inculpatul --- a accesat, fără drept (respectiv cu depășirea împuternicirii primite), un sistem informatic, respectiv baza de date administrată de D.E.P.A.B.D., (sistem informatic la care accesul este permis numai prin introducerea unui user-name și a unei parole, deci prin intermediul unor proceduri), folosind user-name-ul și parola pe care le putea folosi pentru a accesa acest sistem informatic numai în exercitarea atribuțiilor de serviciu ca politist, în scopul obținerii de date informatice, și anume datele de stare civilă ale numitului -----, ziarist, nu în exercitarea atribuțiilor de serviciu, ci în interes personal.

La data de 20.01.2014, ora 21:55:29, inculpatul --- a accesat, fără drept (respectiv cu depășirea împuternicirii primite), un sistem informatic, respectiv baza de date administrată de D.E.P.A.B.D., (sistem informatic la care accesul este permis numai prin introducerea unui user-name și a unei parole, deci prin intermediul unor proceduri), folosind user-name-ul și parola pe care le putea folosi pentru a accesa acest sistem informatic numai în exercitarea atribuțiilor de serviciu ca politist, în scopul obținerii de date informatice, și anume datele de stare civilă ale numitului -----, lucrător de poliție în cadrul B.C.C.O. -----.

La data de 05.11.2014, ora 15:54:39, a accesat, fără drept (respectiv cu depășirea împuternicirii primite), un sistem informatic, respectiv baza de date administrată de D.E.P.A.B.D., (sistem informatic la care accesul este permis numai prin introducerea unui user-name și a unei parole, deci prin intermediul unor proceduri), folosind user-name-ul și parola pe care le putea folosi pentru a accesa acest sistem informatic numai în exercitarea atribuțiilor de serviciu ca politist, în scopul obținerii de date informatice, și anume datele de stare civilă ale numitului -----, lucrător de poliție în cadrul I.P.J. -----, nu în exercitarea atribuțiilor de serviciu.

La data de 10.11.2014, în intervalul orar 09.00 – 16.00, inculpatul --- a accesat, fără drept (respectiv cu depășirea împuternicirii primite), un sistem informatic, respectiv bazele de date administrate de D.E.P.A.B.D. și D.R.P.C.I.V., (sisteme informatice la care accesul este permis numai prin introducerea unui user-name și a unei parole, deci prin intermediul unor proceduri), folosind user-name-ul și parola pe care le putea folosi pentru a accesa aceste sisteme informatice numai în exercitarea atribuțiilor de serviciu ca politist, în scopul obținerii de date informatice, și anume datele de stare civilă ale persoanelor nominalizate în rechizitoriu, nu în legătura cu exercitarea atribuțiilor de serviciu.

La data de 19.11.2014, în intervalul orar 11:06-11:12, inculpatul --- a accesat, fără drept (respectiv cu depășirea împuternicirii primite), un sistem informatic, respectiv baza de date administrată de D.E.P.A.B.D. (sistem informatic la care accesul este permis numai prin introducerea unui user-name și a unei parole, deci prin intermediul unor proceduri), folosind user-name-ul și parola pe care le putea folosi pentru a accesa acest sistem informatic numai în exercitarea atribuțiilor de serviciu ca politist, în scopul obținerii de date informatice, și anume datele de stare civilă ale numitorilor --- lucrător în cadrul Institutiei Prefectului – S.P.C.R.P.C.I.V.; ---, lucrător în cadrul Institutiei Prefectului – S.P.C.R.P.C.I.V., --- fiica acesteia, --- fostul sot al acesteia; --- seful S.P.C.R.P.C.I.V., ---, fostul sot al acesteia, --, fiul acestora; --- – lucrător în cadrul Institutiei Prefectului – Serviciul Pasapoarte; --- – lucrător în cadrul I.P.J. ---, nu în exercitarea atribuțiilor de serviciu

La data de 09.01.2015, în intervalul orar 09:25-09:30, inculpatul --- a accesat, fără drept (respectiv cu depășirea împuternicirii primite), un sistem informatic, respectiv baza de date administrată de D.E.P.A.B.D. (sistem informatic la care accesul este permis numai prin introducerea unui user-name și a unei parole, deci prin intermediul unor proceduri), folosind user-name-ul și parola pe care le putea folosi pentru a accesa acest sistem informatic numai în exercitarea atribuțiilor de serviciu ca politist, în scopul obținerii de date informatice, și anume datele de stare civilă ale numitorilor ---, lucrător în cadrul I.P.J. --; ---, lucrător în cadrul I.P.J. ---; ---, lucrător în cadrul I.P.J. --; ---, lucrător în cadrul I.P.J. --; --, lucrător în cadrul I.P.J. --, nu în exercitarea atribuțiilor de serviciu.

La data de 19.01.2015, în intervalul orar 22:45-23:50, inculpatul --- a accesat, fără drept (respectiv cu depășirea împuternicirii primite), un sistem informatic, respectiv baza de date administrată de D.E.P.A.B.D. (sistem informatic la care accesul este permis numai prin introducerea unui user-name și a unei parole, deci prin intermediul unor proceduri), folosind user-name-ul și parola pe care le putea folosi pentru a accesa acest sistem informatic numai în exercitarea atribuțiilor

de serviciu ca politist, în scopul obtinerii de date informatice, si anume datele de stare civilă ale numitilor ---, lucrător în cadrul I.P.J. --; --, lucrător în cadrul I.P.J. ..; --, lucrător în cadrul I.P.J. ---; --, seful -- de Politie --; --, lucrător în cadrul I.P.J. --; --, lucrător în cadrul I.P.J. --; --, lucrător în cadrul I.P.J. --; --, lucrător în cadrul I.P.J. --; --, lucrător în cadrul I.P.J. ---; --, lucrător în cadrul I.P.J. ---; --, lucrător în cadrul I.P.J. ---; --, lucrător în cadrul I.P.J. ---, nu în exercitarea atributiilor de serviciu.

La data de 20.04.2015, ora 11:25:50, inculpatul --- a accesat, fără drept (respectiv cu depășirea împuternicirii primite), un sistem informatic, respectiv baza de date administrată de D.E.P.A.B.D. (sistem informatic la care accesul este permis numai prin introducerea unui user-name si a unei parole, deci prin intermediul unor proceduri), folosind user-name-ul si parola pe care le putea folosi pentru a accesa acest sistem informatic numai în exercitarea atributiilor de serviciu ca politist, în scopul obtinerii de date informatice, si anume datele de stare civilă ale numitilor --, lucrător în cadrul I.P.J. --- si --, fiica acestuia, nu în exercitarea atributiilor de serviciu.

Pentru a hotărî condamnarea inculpatului --, Tribunalul --- a reținut următoarele:

În cursul anului 2015, Parchetul de pe lângă Curtea de Apel Ploiesti a fost sesizat de către numitii -- si --, prin două plângeri separate, cu privire la presupuse fapte penale comise de către ofiteri cu functii de conducere din cadrul I.P.J. ---.

Plângerea formulată de numitul -- a fost înregistrată sub nr. 135/P/2015, iar cea formulată de -- a fost înregistrată sub nr. --/P/--.

Ambii denuntători au precizat în plângeri domiciliile lor si codul numeric personal.

În urma cercetărilor efectuate în respectivele cauze a rezultat că faptele sesizate nu există dar si că plângerile care au stat la baza deschiderii celor două dosare penale nu au fost formulate de către sus-numitii, întrucât acestia nu își au domiciliul în județul --- si sunt persoane fără adăpost (fiind, deci, improbabil că acestia să dețină informatiile furnizate).

În aceste conditii, ordonantele procurorului din cadrul Parchetului de pe lângă Curtea de Apel Ploiesti care a dispus clasarea cauzelor au fost trimise si I.P.J. ---.

Prin urmare, organele de politie din cadrul I.P.J. --- -- B.C.I. s-au sesizat din oficiu cu privire la faptul că, în cursul anului 2015, un politist a formulat plângeri/denunturi penale cunoscând că faptele sesizate nu sunt reale, pentru formularea plângerilor utilizând ilegal informatiile existente în bazele de date ale Politiei Române sau în documentele oficiale care contineau date cu caracter personal ale numitilor -- si --, la care avea acces în virtutea functiei.

În continuare, organele de politie au efectuat verificări pentru a stabili dacă au fost accesate datele de stare civilă ale sus-numitilor, precum si user_name-ul sub care au fost accesate.

Orice functionar public care primeste dreptul de a accesa bazele de date administrate de Directia pentru Evidenta Persoanelor si Administrarea Bazelor de Date (D.E.P.A.B.D.) -- directie din cadrul Ministerului Afacerilor Interne, primeste un user_name (sau ID ori nume de utilizator) si o parolă, sub care accesează aceste baze de date.

Organele de politie din cadrul I.P.J. --- -- B.C.I. au stabilit că, printre functionarii publici care au accesat datele de stare civilă ale sus numitilor se află si inculpatul ---, agent sef adjunct de politie în cadrul Politiei -- -- Sectia --, acesta având numele de utilizator "---".

Examinând situatia interogărilor efectuate de către inculpat, organele de politie au constatat că acesta a accesat si datele de stare civilă ale altor lucrători de politie sau ale membrilor familiilor acestora.

Inculpatul --- este politist, având gradul de agent sef adjunct de politie, si își desfășoară activitatea în cadrul Inspectoratului Judetean de Politie --- -- Politia -- -- Sectia -- de Politie.

În perioada august 2014 - august 2017, acesta a detinut si functia de vicepresedinte al Sindicatului Politistilor si Vamesilor ---- -- Biroul Teritorial ---.

În vederea exercitării atributiilor legale de politist, inculpatul a fost autorizat să acceseze, numai pentru a consulta, bazele de date care contin date cu caracter personal. Pentru a le putea accesa, acesta a primit codul de identificare (user-name) "---".

Asa cum rezultă din declaratia inculpatului, în anul 2009 sau 2010 a întocmit mai multe rapoarte informative cu privire la presupuse relatii de prietenie dintre martorul ---, seful Politiei Municipiului

Ploiesti, si alte persoane, considerând că, de atunci, toate actiunile martorului (cele referitoare la inculpat) au fost doar pentru a se răzbuna.

Inculpatul nu a formulat nicio sesizare în acest sens si nu există nicio probă că, de-a lungul timpului, cms. sef de politie -- a întreprins vreo actiune altfel decât în conformitate cu legea (în sens larg) în scopul de a se răzbuna pe acesta.

În apărarea sa, inculpatul a arătat că, în jurul datei de 25.12.2013, ar fi primit o informatie conform căreia, cms. sef de politie --, seful Politiei --, ar fi primit, cu titlu de mită, un autoturism de la administratorul S---. Presupunând că această afirmatie a inculpatului ar fi fost adevărată, acesta, potrivit art. 41 lit. g din Lg. 360/2002, avea obligatia de a transmite informatia obtinută organelor judiciare competente să efectueze verificări cu privire la o astfel de faptă, se mai reține în motivarea sentinței penale apelate.

Totodata, potrivit art 19 alin 3 din Codul de etica si deontologie al politistului, aprobat prin HG nr 991/2005 „Politistul ia atitudine fata de actele de coruptie manifestate în cadrul institutiei, având obligatia de a informa superiorii si alte organe competente cu privire la cazurile de coruptie despre care a luat cunostinta”.

Cu toate acestea, inculpatul, în dorinta sa de a demonstra că --- comite ilegalități (tot în sensul larg al cuvântului), desi nu există nicio probă că sus-numitul a comis vreo faptă prevăzută de legea penală, a luat decizia să facă el însusi verificări pentru a stabili dacă informatia se confirmă sau nu (trebuie subliniat faptul că pornim de la premisa că sustinerea inculpatului că ar fi primit o asemenea informatie este reală, desi nu există nicio altă dată în acest sens).

În aceste conditii, la data de 25.12.2013, la ora 02:45:53, în timp ce se afla în timpul programului de lucru, efectuând schimbul III în cadrul Biroului de Ordine publică din cadrul Politiei ----, de pe calculatorul de serviciu, inculpatul a accesat bazele de date administrate de D.R.P.C.I.V. si a consultat datele de identificare ale autoturismului numitului ----, utilizând ca si criteriu de căutare numărul de înmatriculare al autoturismului.

În acest context, în justificarea soluției de condamnare s-a menționat faptul că inculpatul cunostea numărul de înmatriculare al autoturismului sus-numitului cel puțin din data de 10.12.2013 (când, potrivit propriilor sustineri, în timpul serviciului, a observat o masină care nu circula prudent pe drumurile publice si, verificând datele de identificare ale autoturismului, utilizând ca si criteriu de căutare numărul de înmatriculare al acestuia, a stabilit că autoturismul respectiv era proprietatea numitului ----, afirmatie care, desi pare greu credibilă, totusi nu poate fi contracarață prin alte argumente).

În continuare, la ora 02:45:53, a consultat datele de identificare ale autoturismelor aparținând --- si a observat că autoturismul în cauză a aparținut anterior acestei societăți.

Consultând datele de identificare ale acestui autoturism, inculpatul a aflat codul numeric personal al proprietarului, adică al numitului ---.

Apoi, la ora 02:47:17, inculpatul a accesat bazele de date administrate de D.E.P.A.B.D., utilizând ca si criteriu de căutare codul numeric personal, si a consultat datele de stare civilă ale numitului ---.

Tot din declaratia inculpatului rezultă si că, în continuare, a efectuat si alte verificări pentru a stabili dacă informatia primită este veridică sau, dar nu a obtinut alte date, astfel că nu a transmis informatia organelor competente să efectueze verificări.

Ulterior, astfel cum reiese tot din declaratia inculpatului, în jurul datei de 05.12.2014, acesta ar fi primit o nouă informatie conform căreia cms. sef ---- urmează să primească, cu titlu de mită, diferite cadouri de la comerciantii care își desfășoara activitatea în zona Halelor Ploiesti. Desi inculpatul avea obligatia să transmită informatia obtinută organelor judiciare competente să efectueze verificări cu privire la o astfel de faptă, acesta a luat decizia să prelucrez informatia, adică să facă el însusi verificări pentru a stabili dacă informatia se confirmă sau nu.

Astfel, la data de 05.12.2014, la ora 11:42:52, în timp ce se afla în timpul programului de lucru, efectuând schimbul I la compartimentul de investigatii criminale din cadrul Politiei -----, inculpatul a accesat bazele de date administrate de D.E.P.A.B.D., utilizând ca si criteriu de căutare codul numeric personal (pe care îl cunostea cel puțin din data de 25.12.2013), si a consultat datele de stare civilă ale numitului -----.

În continuare, la ora 11:43:38, a accesat bazele de date administrate de D.R.P.C.I.V. si a consultat datele de identificare ale autoturismelor aflate în proprietatea sus-numitului.

În cadrul datelor personale ale numitului ----- sunt incluse si numele si codul numeric al sotie si copilului acestuia, astfel că din contul sus-numitului, utilizând ca si criteriu codul numeric personal, inculpatul a consultat datele de stare civilă si datele de identificare ale autoturismelor detine si de numita --- (sotia lui ---) si --- (fiul celor doi) la orele 11:43:53, 11:43:55, 11:45:16, 11:45:23 si 11:46:30.

Inculpatul a mai arătat că a actionat în acest mod pentru stabili ce autoturisme detine familia --- pentru ca, ulterior, să le urmărească si să vadă dacă, atunci când ajung la domiciliul lor, descarcă din masini bunurile primite de --- cu titlu de mită. Mai mult decât atât, inculpatul a declarat că a si verificat aceste aspecte, dar, întrucât nu a văzut să se fi descărcat din masini astfel de bunuri, a considerat că informatia nu se confirmă, astfel că nu a transmis informatia organelor competente să efectueze verificări.

Potrivit art. 41 lit. g din Lg. 360/2002, politistul este dator să informeze seful ierarhic si celelalte autorități abilitate cu privire la faptele de corupție săvârșite de alti politisti, de care a luat cunostință.

În situatia în care, potrivit celor sustinute de inculpat, acesta nu putea transmite informatia sefului ierarhic pentru a nu suporta repercusiuni (având în vedere că cel pe care îl viza informatia era chiar seful Politiei ---), conform celor mentionate mai sus, acesta trebuia să sesizeze organele judiciare competente să efectueze cercetări în astfel de cazuri, respectiv Directia Generală Anticorupție sau Directia Națională Anticorupție, se mai arată în considerentele sentinței apelate.

Prin urmare, presupunând că apărările inculpatului ar fi reale, instanța de primă jurisdicție a apreciat că toate activitățile sale mai sus expuse intră în sfera ilicitului penal, acesta actionând în acest mod din cauza stării conflictuale în care el considera că se află cu martorul ----, el nefiind competent să cerceteze astfel de fapte.

La data de 13.02.2014, inculpatul --- din cadrul Politiei ---- a efectuat serviciul la schimbul II, în intervalul orar 14.00-22.00.

După terminarea programului de lucru, la data de 14.02.2014, începând cu ora 00:42:05, folosind statia mobilă (care se află în permanentă în posesia politistului, chiar si după terminarea programului de lucru), a accesat baza de date aparținând D.R.P.C.I.V. si, folosind ca si criteriu de căutare numărul de înmatriculare al autovehiculului, a verificat datele de identificare ale mai multor autoturisme (-----), pentru a identifica autoturismul proprietatea numitului ----, comisar de politie, seful ----.

În urma verificărilor, inculpatul a stabilit că autoturismul proprietatea sus-numitului are nr. de înmatriculare ----, a consultat datele de identificare ale masinii, precum si codul numeric personal si adresa de domiciliul ale proprietarului, adică ale martorului ---.

Astfel cum rezultă din declaratia inculpatului, la data si ora mai sus indicate, a fost contactat de un coleg de-al său care i-a comunicat că numitul --- conduce, la acel moment, un autoturism, desi se află sub influenta băuturilor alcoolice. În aceste conditii, inculpatul a verificat numărul masinii si domiciliul lui ---- si s-a deplasat în acea locatie pentru a constata personal comiterea unei posibile contraventii.

Ulterior, inculpatul a revenit asupra declaratiei sale si a arătat că, desi terminase programul de lucru, încă se afla la sediul ---, când a auzit comunicându-se prin statie că au autoturism conduce sinuos pe drum. De asemenea, inculpatul a declarat că a auzit întregul nr. de înmatriculare al autoturismului prin statie, astfel că a fost întrebat de ce a verificat mai multe numere de înmatriculare până a ajuns la nr. de înmatriculare al autovehiculului lui ----. În aceste conditii, inculpatul si-a schimbat din nou declaratia, arătând că nu mai stie cu exactitate dacă a auzit prin statie întreg numărul de înmatriculare sau doar o parte din combinatiile de numere si cifre, dar că prin statie s-a comunicat că este un autoturism marca ---, de culoare neagră si din acest motiv a consultat datele de identificare ale mai multor autoturisme până a identificat autoturismul lui ----, care este un autovehicul marca ---, de culoare neagră.

Totodată, inculpatul a declarat că, după ce a identificat în baza de date administrată de D.R.P.C.I.V. autoturismul proprietatea lui --, a plecat cu autoturismul de serviciu la domiciliul acestuia si l-a asteptat acolo, considerând că poate constata o contravenție sau o infracțiune.

Tribunalul a apreciat că accesul bazei de date aparținând D.R.P.C.I.V. a fost realizat fără drept, cu depășirea autorizării acordate, întrucât nu s-a realizat în exercitarea atribuțiilor de serviciu. Deși se consideră că polițistul se află tot timpul în exercitarea atribuțiilor de serviciu atunci când constată comiterea unei contravenții sau a unei infracțiuni, în această situație inculpatul nu a constatat personal o astfel de faptă. Din chiar declarația acestuia, rezultă că a aflat despre o posibilă infracțiune/contravenție de la alți polițiști, care puteau ei să o constate și motivul pentru care i s-a spus a fost acela că se afla într-o stare conflictuală cu comisarul --- încă din perioada în care acesta a fost adjunctul Secției --- de Poliție -- unde inculpatul a lucrat anterior.

În situația în care cea de-a doua declarație a inculpatului corespunde adevărului, se constată că presupusa faptă se dăduse deja în atenția polițistilor competenți, deci era constatată (fiind sesizată de dispecerul de serviciu prin stație).

De asemenea, s-a reținut că inculpatul putea, într-adevăr să constate comiterea faptei și apoi să efectueze toate verificările care se impuneau, și nu să consulte întâi adresa de domiciliul a sus-numitului și apoi să constate fapta.

Prin urmare, susținerile inculpatului nu au fost luate în considerare, prima instanță considerând că accesarea bazelor de date s-a făcut din spirit revanșard și nu civic.

La data de 30.12.2014, la ora 00:11:07, deși nu se afla în exercitarea atribuțiilor de serviciu, folosind stația mobilă, inculpatul a accesat bazele de date administrate de D.E.P.A.B.D. și, folosind ca și criteriu de căutare codul numeric personal, a consultat datele de stare civilă ale numitului ---, ziarist.

În urma verificărilor efectuate s-a stabilit că inculpatul, în exercitarea atribuțiilor de serviciu, nu a avut nicio lucrare în care ar fi trebuit să consulte datele de stare civilă ale sus-numitului, mai ales că la data accesării și consultării figura în pontaj liber.

Din declarația inculpatului rezultă că, la data și ora mai sus indicate, se afla în parcare blocului în care locuiește și i s-a părut că o persoană care se afla într-o mașină ca cea proprietatea lui --- îi făcea poze. În aceste condiții, a consultat datele de stare civilă ale numitului --- pentru a vedea dacă el îi face poze.

Presupunând că declarația inculpatului corespunde realității, prima instanță a apreciat că accesarea sistemului informatic și într-o atare situație a depășit limitele autorizării primite, întrucât nu s-a efectuat în exercitarea atribuțiilor de serviciu, ci în interes personal.

Ulterior, inculpatul a declarat că a accesat bazele de date întrucât a considerat că persoana care îl fotografiază este cel care, înainte cu câteva luni de acest moment, l-a amenintat cu moartea (urmând, probabil, ca ulterior să solicite ajutorul colegilor săi), ceea ce ar fi putut da o aparență de legalitate accesării sistemului informatic. Cu toate acestea, susținerea inculpatului nu a fost luată în considerare, întrucât acesta a folosit ca și criteriu de căutare codul numeric personal al numitului ---, deci datele de stare civilă ale acestuia a dorit să le consulte și nu ale vreunei alte persoane. De asemenea, inculpatul nu a consultat datele de identificare ale autoturismului văzut, acțiune care ar fi confirmat cea de-a doua declarație a acestuia, ci datele de stare civilă ale numitului ---, ceea ce conduce la concluzia că doar aceste date a vrut să le consulte.

De asemenea, în mai multe ocazii, inculpatul --- a accesat, fără drept (prin depășirea limitelor autorizării primite), un sistem informatic, respectiv bazele de date administrate de D.E.P.A.B.D., pentru a consulta datele de stare civilă ale unor lucrători de poliție sau ai membrilor familiilor acestora.

Astfel, în perioada august 2014-august 2017, inculpatul a detinut și funcția de vicepresedinte al Sindicatului Polițistilor și Vameșilor -- -- Biroul Teritorial ---.

Membri acestui sindicat pot direcționa 2% din impozitul pe venit în contul sindicatului, iar în acest scop trebuie să completeze formularul 230.

De asemenea, cu ocazia sărbătorilor de iarnă, în funcție de cerințele fiecărei filiale, sindicatul poate acorda cadouri copiilor membrilor de sindicat în vârstă de până la 14 ani. În acest scop, fiecare filială trebuie să comunice o listă cu membri și copiii acestora.

Pe de altă parte, trebuie menționat faptul că sindicatul nu a împuternicit niciun membru al său pentru a prelucra datele cu caracter personal stocate în bazele de date administrate de M.A.I. (evidența populației, evidența auto etc.).

Inculpatul a fost împuternicit de președintele filialei --- să centralizeze numărul de copii care urmează să primească cadouri și să depună la administrația fiscală formularele 230.

În aceste scopuri, inculpatul, folosind user-name-ul și parola acordate de I.P.J. ---, a accesat bazele de date administrate de D.E.P.A.B.D. și a consultat datele stare civilă ale mai multor lucrători de poliție sau membri familiilor lor.

Cu privire la situațiile de fapt expuse, prima instanță a constatat că accesarea sistemelor informatice care stochează datele personale ale sus-numiților și datele de identificare ale autoturismelor acestora de către inculpat s-a realizat fără drept, respectiv cu depășirea limitelor autorizării, întrucât user-name-ul și parola primite trebuiau folosite numai în exercitarea atribuțiilor sale de serviciu ca lucrător de poliție și nu ca membru al unui sindicat.

Astfel, pentru a garanta și proteja drepturile și libertățile fundamentale ale persoanelor fizice, în special a dreptului la viață intimă, familială și privată, legiuitorul a reglementat Lg. 677/2001, acest act normativ stabilind modalitățile în care datele cu caracter personal (orice informații referitoare la o persoană fizică identificată sau identificabilă) pot fi prelucrate de către operatorii de date cu caracter personal.

De asemenea, legiuitorul a definit și noțiunea de prelucrare a datelor cu caracter personal, aceasta desemnând orice operațiune sau set de operațiuni care se efectuează asupra datelor cu caracter personal, inclusiv consultarea unor astfel de date.

Astfel, Procedura privind accesarea și valorificarea principalelor baze de date/aplicații folosite de personalul Poliției Române care acționează în teren prevede ca principalele situații în care se accesează aplicațiile/bazele de date sunt:

- Legitimări pentru stabilirea/certificarea identității persoanelor suspecte, urmărite, dispărute, decedate, reținute, arestate sau detinute, persoanelor reclamate sau învinuitorilor, inculpaților
- Punerea în executare a mandatelor penale, sentințelor penale sau hotărârilor judecătorești
- Stabilirea identității persoanelor împotriva cărora au fost dispuse măsuri asigurătorii de către instanțele judecătorești
- Soluționarea cauzelor penale, petițiilor, lucrărilor diverse sau secrete
- Munca specială (întocmirea rapoartelor informative, documentare calificată a activității infracționale a persoanelor suspecte prin MS/DUI, întocmirea mapelor documentare, etc).

Potrivit art. 1 din Lg. 238/2009, angajații Ministerului Administrației și Internelor, care au calitatea de persoane împuternicite de către inspectoratele de poliție (operatori de date), pot prelucra automat și neautomat datele cu caracter personal, în exercitarea atribuțiilor legale, pentru realizarea activităților de prevenire, cercetare și combatere a infracțiunilor, precum și de menținere și asigurare a ordinii publice, cu aplicarea mai multor principii, printre care și cel al necesității (necesitatea de a cunoaște).

Pentru a putea prelucra datele cu caracter personal stocate într-un sistem informatic, operatorii de date cu caracter personal și împuterniciții acestora trebuie să acceseze respectivele sisteme informatice.

Pentru a accesa sistemele informatice administrate de D.E.P.A.B.D. și D.R.P.C.I.V., trebuie urmate anumite proceduri, respectiv folosirea unui user-name și a unei parole.

Pentru fiecare utilizator, administratorul aplicației stabilește un cont unic care să permită atât identificarea, cât și configurarea categoriilor de prelucrări la care are dreptul.

Pentru lucrătorii de poliție, identificarea în sistem se realizează prin introducerea unui cod de identificare (user-name), însoțit de introducerea unei parole. Codurile de identificare și parolele sunt unice și netransmisibile.

Așa cum rezultă din Lg. 238/2008, dar și dispozițiile I.G.P.R. și M.I.R.A. aplicabile în domeniu, lucrătorii de poliție au dreptul să acceseze bazele de date care conțin date cu caracter personal numai în exercitarea atribuțiilor de serviciu.

Astfel, art 4 din Anexa la Dispoziția inspectorului general al Poliției Române nr 101/13.12.2007 (Norme metodologice privind accesul la baza de date privind evidența populației) prevede ca

„interogarea bazei de date privind evidenta populatiei de catre politisti se efectueaza doar in scopul realizarii atributiilor de serviciu, daca sunt indeplinite conditiile prevazute de lege privind legitimitatea prelucrarii datelor cu caracter personal”.

Prin incheierea din data de 15 iulie 2020, în baza art 386 alin (1) C pr pen, instanța de primă jurisdicție, din oficiu, a dispus schimbarea încadrării juridice a faptelor pentru care a fost trimis în judecata inculpatul ---, din infracțiunile prevăzute de art. 360 alin. 1, 2 și 3 C.pen., cu aplicarea art. 35 alin. 1 C.pen. (2 acte materiale) – faptele din data de 25.12.2013, ora 02:45:53, art. 360 alin. 1, 2 și 3 C.pen. – fapta din data de 25.12.2013, ora 02:46:44, art. 360 alin. 1, 2 și 3 C.pen. – fapta din data de 20.01.2014, art. 360 alin. 1, 2 și 3 C.pen., cu aplicarea art. 35 alin. 1 C.pen. (2 acte materiale) – faptele din data de 14.02.2014, art. 360 alin. 1, 2 și 3 C.pen. – fapta din data de 05.11.2014, art. 360 alin. 1, 2 și 3 C.pen., cu aplicarea art. 35 alin. 1 C.pen. (134 de acte materiale) – faptele din data de 10.11.2014, art. 360 alin. 1, 2 și 3 C.pen., cu aplicarea art. 35 alin. 1 C.pen. (9 acte materiale) – faptele din data de 19.11.2014; art. 360 alin. 1, 2 și 3 C.pen., cu aplicarea art. 35 alin. 1 C.pen. (6 acte materiale) – faptele din data de 05.12.2014, art. 360 alin. 1, 2 și 3 C.pen. – fapta din data de 30.12.2014; art. 360 alin. 1, 2 și 3 C.pen., cu aplicarea art. 35 alin. 1 C.pen. (5 acte materiale) – faptele din data de 09.01.2015, art. 360 alin. 1, 2 și 3 C.pen., cu aplicarea art. 35 alin. 1 C.pen. (13 acte materiale) – faptele din data de 19.01.2015, art. 360 alin. 1, 2 și 3 C.pen., cu aplicarea art. 35 alin. 1 C.pen. (2 acte materiale) – fapta comisă la data de 20.04.2015, toate cu aplicarea art. 38 alin. 1 C.pen., **în infracțiunea prev de art.360 alin.1,2,3 cu aplic.art.35 alin.1 cod penal- 177 acte materiale.**

În drept, prima instanță a reținut că faptele reținute în sarcina inculpatului --- **înrunesc toate elementele constitutive ale infracțiunii prevăzute de art. 360 alin. 1, 2 și 3 C.pen., cu aplicarea art. 35 alin. 1 C.pen. (177 acte materiale).**

În opinia primei instanțe, accesul fără drept presupune inexistența unui temei legal sau contractual, precum și depășirea limitelor pentru care s-a dat autorizarea, atunci accesul nu s-a făcut în interes de serviciu, ci în interes personal.

Constatand, dincolo de orice indoiala rezonabila, în baza probelor administrate în cursul urmaririi penale și al cercetării judecatorești ca fapta exista, este infracțiune și a fost savarsita de inculpat, instanța de fond a dispus condamnarea acestuia pentru infracțiunea reținută în sarcina sa

Expunerea pe scurt a chestiunilor de drept:

Dispozițiile art. 360 alin. (1), (2) și (3) din Codul penal au următorul conținut:

(1) Accesul, fără drept, la un sistem informatic se pedepsește cu închisoare 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.

Problemele de drept care se ridică în legătură cu acest text de lege sunt următoarele:

Accesul fără drept presupune inexistența unui temei legal sau contractual, precum și depășirea limitelor pentru care s-a dat autorizarea, atunci accesul nu s-a făcut în interes de serviciu, ci în interes personal. Legea nu face nicio distincție cu privire la modul în care sunt încălcate măsurile de securitate (în cazul concret reținându-se că logarea la sistem s-a făcut pe baza introducerii numelui utilizatorului și parolei ce sunt înregistrate în sistem, care în momentul când sunt introduse sunt recunoscute și executate de programul informatic), fiind irelevant că parola de acces și user-ul folosite pentru autentificare sunt adevărate.

S-a reținut că aceste date au fost introduse de titularul dreptului de acces (inculpatul utilizând parola și user-ul atribuite în acest scop,) cu depășirea autorizării ce i-a fost dată (să fie utilizate în exercitarea atribuțiilor de serviciu, în interes de serviciu).

Deși actele normative menționate de prima instanță în motivarea soluției de condamnare se referă la situațiile în care accesul într-un sistem informatic are loc în exercitarea atribuțiilor de serviciu, în interes de serviciu, având în vedere natura funcției publice pe care inculpatul apelant o exercită, o definire limitativă a situațiilor în care accesul are loc în exercitarea atribuțiilor de serviciu, este practic imposibilă.

Procedura privind accesarea și valorificarea principalelor baze de date/aplicații folosite de personalul Poliției Române care acționează în teren prevede că *principalele situații* în care se accesează aplicațiile/bazele de date sunt:

- Legitimări pentru stabilirea/certificarea identității persoanelor suspecte, urmărite, dispărute, decedate, reținute, arestate sau deținute, persoanelor reclamate sau învinuitorilor, inculpaților;
- Punerea în executare a mandatelor penale, a sentințelor penale sau hotărârilor judecătorești;
- Stabilirea identității persoanelor împotriva cărora au fost dispuse măsuri asigurătorii de către instanțele judecătorești;
- Soluționarea cauzelor penale, petițiilor, lucrărilor diverse sau secrete;
- Munca specială (întocmirea rapoartelor informative, documentare calificată a activității infracționale a persoanelor suspecte prin MS/DUI, întocmirea mapelor documentare, etc).

Prin urmare, enumerarea situațiilor în care o persoană care exercită funcția publică de polițist are acces la un sistem informatic (aplicațiile sau bazele de date), nu are decât *un caracter exemplificativ*, fapt care îngreunează considerabil probatoriul necesar a fi administrat pentru a demonstra că o asemenea persoană a accesat fără drept un sistem informatic.

Fiind o trăsătură caracteristică comună a tuturor infracțiunilor informatice, cerința expresă ca fapta să fie comisă „fără drept” reflectă, în mod logic, posibilitatea ca o faptă în legătură cu un sistem informatic să nu fie întotdeauna considerată o infracțiune per se, ci și un act legitim sau justificat chiar dacă nu este incidentă una din cauzele care înlătură caracterul penal al faptei.

Înțelesul expresiei „fără drept” derivă obligatoriu din contextul în care aceasta este folosită și impune o analiză atentă a principiilor sau intereselor care, eventual, pot înlătura vinovăția făptuitorului.

Potrivit art. 35 alin (2) al Legii nr. 161/2003, acționează fără drept persoana care se află într-una din următoarele situații:

- nu este autorizată în temeiul legii sau al unui contract;
- depășește limitele autorizării;
- 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 ceea ce privește elementul material al laturii obiective, acesta va fi reprezentat de acțiunea propriu-zisă de accesare a unui sistem informatic, sub formele și modalitățile la care face trimitere norma de incriminare.

Chiar dacă prevederile din legea specială definesc caracterul ”fără drept” al operațiunilor de acest tip, dispozițiile art. 35 alin. (2) din Legea nr. 161/2003 nu sunt prevăzute și în Codul penal intrat în vigoare la data de 01 februarie 2014 și *deci nu pot completa norma de incriminare*. Chiar dacă dispozițiile art. 35 alin. (2) al Legii nr. 161/2003 pot constitui repere de ordin teoretic a căror utilizare nu poate afecta principiul legalității incriminării, întrucât transpun previzibil criteriile generale care permit aprecierea caracterului îndreptățit al unui act, noțiunea de acces fără drept se impune a fi raportată la fiecare categorie de persoane căror prin lege li se conferă un asemenea acces.

Accesul, în înțelesul dat de lege, desemnează intrarea în tot sau numai într-o parte a sistemului informatic. Metoda de comunicare – la distanță, inclusiv grație legăturii prin satelit sau nu, ori de aproape – nu prezintă importanță.

În forma sa cea mai simplă, accesul la un sistem informatic presupune o interacțiune a făptuitorului cu tehnica de calcul vizată prin intermediul echipamentelor sau diverselor componente ale sistemului vizat (sursă de alimentare, butoane de pornire, tastatură, mouse, joystick). Manipularea acestor dispozitive se transformă în solicitări către Unitatea Centrală de Prelucrare (UCP) a sistemului, care va procesa date ori va rula programe de aplicații în beneficiul intrusului.

Practica a demonstrat că, în marea majoritate a cazurilor de acces ilegal la sisteme de calcul, făptuitorul acționează pentru obținerea de date informatice, care poate să însemne:

captarea vizuală a acestora pe monitor;

intrarea în posesia unei imprimante alfanumerice (foaia de hârtie tipărită);

rularea unor programe sau aplicații care gestionează date informatice (ex. programe de administrare a bazelor de date într-o instituție, programe de poștă electronică etc.).

În condițiile art. 360 alin. (1) C.pen și ținând cont de explicațiile de mai sus, este evident că nu se va reține existența unei infracțiuni de acces ilegal dacă 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.

În cauză, s-a reținut de prima instanță că inculpatul apelant exercită funcția de lucrător operativ al Poliției Române, fiind încadrat la Biroul de Investigații Criminale, făcând parte din categoria persoanelor care pot interoga oricând o bază de date conținând informații nepublice, cu condiția ca această interogare să aibă loc în legătură sau în exercitarea atribuțiilor de serviciu, astfel cum sunt acestea definite cu titlu exemplificativ de actele infra legale menționate anterior.

În absența unor formalități prealabile interogării propriu zise a sistemului informatic, având în vedere că persoanele care desfășoară asemenea activități precum cele reținute de prima instanță, beneficiază de o parolă și un user - name alocat în acest sens pentru un număr nedefinit de interogări ce pot fi operate inclusiv de pe un terminal mobil (deci pentru o situație operativă inopinată care poate interveni în activitatea operativă), *noțiunea de depășire a limitelor autorizării nu se poate stabili decât ulterior și, de regulă, în funcție de modul în care informațiile obținute în urma interogării bazei de date au fost valorificate.*

Spre exemplu, în jurisprudența recentă s-a reținut că "fapta inculpatului -- care, la data de 09.01.2017, la solicitarea prealabilă, telefonică, a inculpatului --, a accesat cu depășirea limitelor autorizării, în intervalul orar 08:09:19 - 08:11:28, bazele de date evidența persoanelor, evidența pașapoarte și evidența auto, scopul verificărilor nefiind unul în interes de serviciu, ci acela de a-i transmite persoanei solicitante faptul că nu figurează urmărită național/internațional, în condițiile în care aceasta fusese identificată de autoritățile franceze ca fiind autorul infracțiuni de furt consumat pe raza orașului Paris, în dauna ----, la data de 30.12.2016, întrunește elementele de tipicitate ale infracțiunii de acces ilegal la un sistem informatic, prev. și ped. de art. 360 alin. (1), (2) și (3) C. pen. [Tribunalul București, Sentința penală nr. 2519 din 8 decembrie 2017, www.rolii.ro]"

Prin urmare, atât în speța citată cât și în alte situații de acest gen în care acuzațiile au fost formulate față de persoane care au dreptul de interogare a bazelor de date în virtutea exercitării atribuțiilor de serviciu, noțiunea de "depășire a limitelor autorizării" a fost reținută numai prin raportare la acțiunile subsecvente interogării bazei de date în baza parolei și a user - name-ului oferit de angajator.

Accesarea ab inițio a unui sistem informatic de către asemenea persoane nu poate fi considerată ilegală atât timp cât respectivul sistem este în mod uzual folosit de către aceste categorii de funcționari (indiferent de perioada alocată acestei activități) chiar dacă datele informatice stocate sunt personalizate și semnalizate ca atare prin criptare ori protejare împotriva deschiderii/suprascrierii/modificării/restricționării accesului.

În consecință, dacă ulterior accesului la baza de date, va exista o acțiune în care informațiile astfel obținute sunt folosite, se va putea concluziona asupra unui acces ilegal sau, după caz, legal la baza de date, numai acțiunile ulterioare putând demonstra o eventuală depășire a limitelor autorizării, de natură să facă incidentă norma de incriminare. În lipsa unor acțiuni ulterioare ale persoanei față de care interogarea operativă a bazei de date este asigurată de lege, tocmai pentru exercitarea în condiții optime a atribuțiilor de serviciu, va interveni o problemă de aplicare a normei de incriminare, în sensul că lipsa de relevanță și lipsa valorificării ulterioare în exercitiul funcțiunii a informațiilor obținute în urma interogării bazei de date poate constitui un acces ilegal la sistemul informatic.

Cum noțiunile de "fără drept" sau "depășire a limitelor autorizării" nu sunt definite concret în legea penală prin raportare la condițiile de tipicitate ale infracțiunii prevăzute de art. 360 C.pen, se impune stabilirea ariei de aplicare a normei de incriminare prin raportare concretă la cazul persoanelor care pot interoga oricând o bază de date conținând informații nepublice, când o

asemenea interogare nu este urmată și de efectuarea ulterioară a unor acte specifice exercitării atribuțiilor de serviciu în legătură cu interogarea efectuată.

Se impune a fi stabilit dacă în cazul acestei categorii de funcționari, 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.

În concluzie, pentru stabilirea certă a condițiilor în care fapta incriminată de dispozițiile art. 360 alin. (1), (2) și (3) C.pen. întrunește condițiile de tipicitate obiectivă ale infracțiunii, se impune rezolvarea de principiu următoarelor chestiuni de drept, vizând dispozițiile art. 360 alin.(1) din Codul penal, respectiv:

„În interpretarea dispozițiilor art. 360 alin. (1) Cod 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?”

Examenul de admisibilitate a sesizării:

- instanța care sesizează Înalta Curte de Casație și Justiție este Curtea de Apel ---, investită 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 nu face obiectul unui recurs în interesul legii în curs de soluționare;
- relevanța chestiunii de drept: 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 alin. (1) C.pen,

Punctele de vedere ale procurorului și ale inculpatului asupra chestiunii de drept sesizate:

Procurorul a apreciat că nu sunt întrunite toate condițiile de legalitate pentru sesizarea Înaltei Curți de Casație și Justiție conform art.475 Cod procedură penală, deoarece, în prezenta cauză calea de atac a apelului a fost exercitată de inculpat pentru motive de netemeinicie a sentinței iar solicitarea acestuia se referă la modul de interpretare a probatoriului pentru stabilirea unei stări de fapt.

Inculpatul apelant ---, prin apărător ales, a fost de acord cu sesizarea Înaltei Curți de Casație și Justiție pentru pronunțarea unei hotărâri prealabile, depunând la dosar și note scrise în acest sens, lăsând însă la aprecierea instanței modul de formulare a întrebării adresate în procedura prevăzută de art. 475 și 476 din Codul de procedură penală

Punctul de vedere al completului de judecată asupra chestiunilor de drept sesizate:

Având în vedere că în calea de atac a apelului este criticată soluția primei instanțe de a se reține existența unei infracțiuni de acces ilegal la un sistem informatic, prin reținerea depășirii limitelor autorizării, exprimarea punctului de vedere ar putea fi considerată o antepronunțare cu privire la condițiile de tipicitate obiectivă ale infracțiunii deduse judecătii.

PENTRU ACESTE MOTIVE ÎN NUMELE LEGII, D I S P U N E:

Admite cererea formulate de apelantul inculpat ---.

În baza art.475 și a art.476 alin. (1) Cod procedură penală sesizează Înalta Curte de Casație și Justiție - Completul pentru dezlegarea unor chestiuni de drept în materie penală pentru pronunțarea

unei hotărâri prin care să dea o rezolvare de principiu următoarei chestiuni de drept, vizând dispozițiile art. 360 alin.(1) din Codul penal, respectiv:

„În interpretarea dispozițiilor art. 360 alin. (1) Cod 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?”.

Se vor atașa sesizării formulate:

- prezenta încheiere în copie certificată și în format anonimizat;
- sentința penală nr. 247 din data de 28 septembrie 2020 pronunțată de Tribunalul --- și Rechizitoriul nr. 247/P/2017 din data de 08 octombrie 2018 al Parchetului de pe lângă Curtea de Apel ---, în copii certificate, ca înscrisuri relevante;
- citativul cuprinzând identitatea și domiciliul părților.

Definitivă.

Pronunțată în ședință publică, astăzi 14 iunie 2021

Președinte,

Judecător

Judecător,

Grefier,

Red/tehn --- 5 ex., 16.06.2021

Dosar nr. -----

S.pen. -----

Tribunalul --- Secția penală

Jud. fond -----

Document care conține date cu caracter personal

Protejate de prevederile Regulamentului (UE) 2016/679!

Notificare nr.3113/2006

