**CANDIDAT COD 1011 HOTĂRÂREA nr. 26**

R O M Â N I A

CURTEA DE APEL **………**- SECŢIA **………**

Dosar nr. **………**

(**………**)

***ÎNCHEIERE***

Şedinţa din camera de consiliu din: **………**

***Judecător de drepturi şi libertăţi:* CANDIDAT COD 1011**

*Grefier:* **………**

Ministerul Public - P.I.C.C.J. - Direcţia de Investigare a Infracţiunilor de Criminalitate Organizată şi Terorism a fost reprezentat de procuror **………*.***

Pe rol soluţionarea cererii formulate de P.I.C.C.J. – Direcţia de Investigare a Infracţiunilor de Criminalitate Organizată şi Terorism – Structura …… – Secţia ……….., în dosarul nr. ........, privind confirmarea ***ordonanţei*** nr. ........ emisă la data de 30.10.2019, ora 20:30 prin care s-a dispus ***autorizarea, cu titlu provizoriu*,** pe o durată de ***10 ore,*** de la data de ***….10.2019, ora 20:30*** până la data de ***31.10.2019, ora 06:30, a accesului în sistemele informatice şi interceptarea comunicaţiilor ori al oricărui tip de comunicare la distanţă privind laptop-ul marca ….., cu seria …….; SNID: …… şi telefoanele mobile identificate în locuinţă, aparţinând suspectului A.........***

Fără citarea părţilor.

Referatul cauzei a fost făcut de grefierul de şedinţă, după care,

**Reprezentantul Ministerului Public**, având cuvântul, pune concluzii de admitere a cererii şi, în consecinţă, de confirmare a ordonanţei emise la data de ….10.2019 ora 20:30 în dosarul de urmărire penală nr. ........, în sensul celor menţionate în referat.

***JUDECĂTORUL DE DREPTURI ŞI LIBERTĂŢI,***

***Deliberând asupra cererii formulate, constată:***

Prin adresa nr. ........, înregistrată pe rolul Curţii de Apel B........– Secţia …… la data de ….., sub nr. …..), P.I.C.C.J. – D.I.I.C.O.T.- Structura …….. – Secţia ………, solicită confirmarea ***ordonanţei*** nr. ........ emisă la data de .....10.2019, ora 20:30 prin care s-a dispus ***autorizarea, cu titlu provizoriu*,** pe o durată de ***10 ore,*** de la data de ***30.10.2019, ora 20:30*** până la data de ***31.10.2019, ora 06:30, a accesului în sistemele informatice şi interceptarea comunicaţiilor ori al oricărui tip de comunicare la distanţă privind laptop-ul marca ……, cu seria ………; SNID: …….. şi telefoanele mobile identificate în locuinţă, aparţinând suspectului A.........***

Prin referatul cu propunere de confirmare, se arată că, la D.I.I.C.O.T. a fost înregistrată sesizarea formulată de S.T.S., cu privire la faptul că persoane necunoscute care, prin beneficiul libertăţii de a accesa Sistemul Naţional Unic pentru apeluri de urgenţă -112 (SNUAU), apelează în mod continuu numărul unic de urgenţă 112, prin intermediul unui terminal telefonic fără serviciu, afectând în mod fundamental infrastructura critică ce deserveşte SNUAU pe raza mun. B........şi a jud. I…. şi punând în pericol grav accesul la numărul unic de urgenţă 112, vulnerabilitatea fiind efectivă şi generând imposibilitatea de alertare a agenţiilor specializate de intervenţie la urgenţele semnalate în care se află sau se pot afla toţi cetăţenii din aria mun. B........şi jud. I…...

Se arată că, potrivit *O.U.G. nr. 34/2008* privind organizarea şi funcţionarea Sistemului naţional unic pentru apeluri de urgenţă, aprobată cu modificări şi completări de Legea nr. 160/2008, S.T.S. a fost desemnat drept administrator al Sistemului naţional unic pentru apeluri de urgenţă, conform art. 4 alin. 2., acest sistem fiind înfiinţat şi având drept scop furnizarea către cetăţeni a Serviciului de urgenţă 112, asigurând preluarea apelurilor de urgenţă de la cetăţeni şi, după caz, transmiterea acestora către agenţiile specializate de intervenţie, în vederea asigurării unei reacţii imediate, uniforme şi unitare pentru soluţionarea urgenţelor. SNUAU este un ansamblu integrat de aplicaţii, echipamente şi reţele de comunicaţii şi tehnologia informaţiei, care realizează puncte publice de acces al cetăţeanului la agenţiile specializate de intervenţie şi care permite răspunsul adecvat urgenţei semnalate. Interfaţa publică de acces este realizată prin integrarea în cadrul sistemului, la nivelul fiecărui judeţ, a centrului unic pentru apeluri de urgenţă cu dispeceratele agenţiilor specializate de intervenţie.

***În fapt***, se reţine că, în perioada iunie - octombrie 2019, persoane necunoscute au profitat şi profită de capabilităţile unor terminale mobile, prin intermediul cărora au apelat şi apelează în continuare nr. unic de urgenţă 112.

Astfel, în această perioadă de timp, s-a identificat o creştere a numărului acestui tip de apeluri la nivelul Centrului unic integrat pentru apeluri de urgenţă B….-I……, de trei ori mai mare faţă de perioada similară a anului trecut, acest număr neobişnuit de mare de apeluri fiind cauzat de utilizarea unui terminal mobil care a fost identificat de către operatorul X…. S.A. cu cartela SIM IMSI ………. Acest terminal mobil a beneficiat de servicii de la operatorul Y…… S.A. până la nivelul lunii iunie 2019, iar în acest moment nu are asociat nici un serviciu de telefonie, conform informaţiilor furnizate de operatorul Y….. S.A. \*

Se arată că, în urma unei analize de ordin tehnic efectuate la nivelul S.T.S. asupra codurilor de localizare ale numerelor de trunchi, a rezultat faptul că apelurile au fost şi sunt generate, în continuare, din celule din toate reţelele mobile din zona T….., locaţie aflată în

municipiul B........şi că cea mai mare parte ale apelurilor o reprezintă apeluri deconectate înainte de a putea fi procesate de către operatoarele Centrului unic integrat pentru apeluri de urgenţă Bucureşti-llfov.

Respectivele apeluri sunt rutate automat prin numerele de trunchi dedicate, prin intermediul operatorilor de comunicaţii electronice, pe zona dedicată pentru urgenţe, fiind introduse şi identificate de SNUAU drept apeluri de urgenţă, însă apelurile care au fost preluate nu au indicat elemente precise de identificare, ci doar au relevat sunete de tip metalic, neinteligibile.

De asemenea, în argumentarea propunerii, se arată că analiza efectuată de operatorul X….. S.A. a statuat faptul că, în perioada iunie- septembrie 2019, prin reţeaua respectivului operator s-au transferat peste 75.000 de apeluri cu nr. de trunchi de la terminalul mobil dotat cu cartela SIM IMSI ….., operatorul Z….. S.A. confirmând traficul excesiv generat de respectivul terminal mobil, numărul apelurilor iniţiate fiind de aproximativ 5.000 de apeluri pe zi. S-a constatat că numărul mare de apeluri blochează sistemul, deoarece capabilităţile tehnice ale acestuia sunt limitate, iar procesarea apelurilor nu poate fi selectivă, prin prisma faptului că operatorii SNUAU au obligaţia legală de a procesa fiecare apel de urgenţă imediat ce acesta este efectuat.

Potrivit art. 8 din OUG nr. 34/2008, în cadrul SNUAU, Centrele unice pentru apeluri de urgenţă au, printre altele, ca atribuţii principale: primirea şi înregistrarea automat a apelurilor de urgenţă comunicate prin telefon, radio, dispozitive automate de anunţare, semnalizare, alarmare ori prin alte mijloace, precum şi analizarea, direcţionarea şi transmiterea operativă a apelurilor de urgenţă la dispeceratele de urgenţă, precum şi la autorităţile competente, în funcţie de natura evenimentelor şi de consecinţele acestora, pe baza unui index al incidentelor stabilit de toate structurile specializate în soluţionarea urgenţelor.

Astfel, apelarea abuzivă şi repetată generează o afectare gravă a infrastructurilor critice care desen/esc SNUAU şi perturbă, în mod evident activitatea SNUAU prin indisponibilitatea serviciului, dar şi a agenţiilor specializate de intervenţie prin imposibilitatea de a interveni la urgenţele reale, responsabilitate care este atribuită în sarcina agenţiilor specializate de intervenţie, stabilite de lege, aceste acte şi fapte constituind ameninţări reale la adresa securităţii naţionale.

Mai mult, se arată că art. 6 din Legea nr. 92/1996 privind organizarea şi funcţionarea Serviciului de Telecomunicaţii Speciale, stipulează faptul că *„penetrarea,* ***întreruperea funcţionării*** *şi distrugerea* ***reţelelor de telecomunicaţii speciale***, *precum şi interceptarea comunicaţiilor în aceste reţele* ***constituie ameninţări la adresa siguranţei naţionale".***

Aşadar, prin ordonanţa nr. ….. din data de …...10.2019 s-a dispus începerea urmăririi penale sub aspectul săvârşirii infracţiunilor de ***perturbarea funcţionării sistemelor informatice*** prev. de art. 363 C.pen., ***operaţiuni*** ***ilegale cu dispozitive sau programe informatice*** prev. de art. 365 C.pen. şi ***acte de diversiune*** prev. de art. 403 C.pen.

Din verificările efectuate de către organele de cercetare penală delegate în cauză rezultă că apelurile initiate către număr unic de urgentă 112 prin intermediul terminalului mobil cu codul IMSI …. au fost efectuate de către persoane necunoscute aflate la adresa din Bd ……., B……..

Astfel, la data de …..10.2019, a fost efectuată percheziţia domiciliară la imobilul din B….., Bd. ……., în baza mandatului nr. …./…..10.2019 emis de Curtea de Apel B........- Secţia ……., ocazie cu care au fost identificate mai multe terminale mobile si dispozitive artizanale de natură a amplifica semnalul GSM, care iniţiau apeluri repetate către numărul unic de urgenţă 112, precum şi către alte numere de telefon, în imobilul respectiv fiind identificat numitul ***A........*(**fiul lui … şi …., născut la data de …., în P…., judeţul N….., domiciliat în oraş B1…., strada …….., judeţul N…., CNP : ….).

Prin ordonanţa din data de …..10.2019, s-a dispus efectuarea în continuare a urmăririi penale în cauză, faţă de suspectul ***A…..*,** sub aspectul săvârşirii următoarelor infracţiuni: ***perturbarea funcţionării sistemelor informatice*** prev. de art. 363 C.pen., ***operaţiuni ilegale cu dispozitive sau programe informatice*** prev. de art. 365 alin. 1 lit. a şi alin. 2 C.pen. şi ***acte de diversiune*** prev. de art. 403 C.pen., toate cu aplic. art. 38 C.pen..

***În fapt,*** s-a reţinut că, începând cu vara anului 2019, suspectul ***A…..*** a pus bazele unui plan infracţional elaborat, destinat compromiterii şi destabilizării infrastructurii informatice critice ce desen/eşte SNUAU, pe raza întregului mun. B…., dar şi a jud. I….., punând astfel în pericol grav accesul la numărul unic de urgenţă 112.

Ca şi modalitate de operare, suspectul a procedat la confecţionarea şi adaptarea unui întreg arsenal de dispozitive şi terminale mobile interconectate, echipamente şi programe informatice ce aveau să-i servească la săvârşirea infracţiunilor reţinute în cauză, respectiv fapte contra siguranţei şi integrităţii sistemelor informatice şi totodată contra securităţii naţionale.

Atacurile îndreptate asupra infrastructurii şi totodată a mijloacelor de telecomunicaţie SNUAU şi gestionate de STS, au debutat începând cu luna iunie 2019 de o manieră latentă, activităţile luând amploare la foarte scurt timp şi determinând în mod direct afectarea gravă a funcţionării infrastructurii critice şi implicit aducerea în stare de neîntrebuinţare parţială/întrerupere a funcţionării mijloacelor şi reţelelor de telecomunicaţie aferente, punându-se în pericol securitatea naţională:

Atacurile informatice continue au constat în utilizarea echipamentelor şi terminalelor mobile adaptate, la efectuarea de apeluri repetate, la foarte scurte perioade de timp (chiar la secundă), la număru unic de urgenţă 112, fapt.ce a condus la generarea unei suprasolicitări a acestui serviciu de comunicaţii electronice destinate publicului, serviciu ce asigură preluarea apelurilor de urgenţă de la cetăţeni, şi după caz, transmiterea acestora către agenţiile specializate de intervenţie, în vederea asigurării unei reacţii imediate, uniforme şi unitare pentru soluţionarea urgenţelor.

În cadrul activităţii infracţionale, pentru realizarea fluxului mare de apeluri, suspectul s-a folosit de terminale telefonice fără serviciu ce utilizau conform identificării terminalului de către operatorul X….. S:A, o cartelă SIM IMSI …….. Acest terminal mobil a beneficiat de servicii de la operatorul Y…… S.A. până la nivelul lunii iunie 2019, când nu ha mai fost asociat nici un serviciu de către operatorii de telecomunicaţii din România.

S-a reţinut că, deşi cartela SIM era inactivă, erau iniţiate apelurile către serviciul unic 112, cea mai apropiată antenă GSM preluând apelul, acesta fiind atribuit primului operator de telecomunicaţii din România disponibil. întrucât IMSI-ul respectiv nu este înregistrat la operatorii de telecomunicaţii ca fiind un număr activ/fără semnal, acesta primeşte astfel de la operator un număr de trunchi dedicat, ulterior, fiind redirecţionat automat pe zona dedicată pentru urgenţe, aceasta fiind prioritară în vederea preluării de către SNUAU. Acest număr de trunchi dedicat reprezintă un număr generic alocat de către fiecare operator de telecomunicaţii apelurilor/dispozitivelor ce nu sunt întregistrate în reţeaua lor. Acesta este dinamic, unui singur IMSI fiindu-i distribuit câte un număr de fiecare dată când iniţiază apel.

Astfel, acest IMSI-ul utilizat de suspect a fost raportat de mai mulţi operatori de telecomunicaţii din România, ca generând excesiv trafic în reţea, în cuprinsul referatului fiind redate, cu titlu exemplificativ situaţiile constatate şi raportate de firmele de telefonie.

De asemenea, în susţinerea propunerii, parchetul arată că, în urma efectuării percheziţiilor domiciliare, la adresa din ***B…., Bd. ……,*** s-a descoperit faptul că activitatea infracţională descrisă mai sus se derula în continuare, în mod flagrant, în acest sens fiind identificate în interiorul apartamentului un întreg arsenal de dispozitive şi terminale mobile interconectate, care apelau serviciul de urgenţă 112, precum şi alte numer de telefon, echipamente posibil create artizanal şi anume confecţionate şi destinate săvârşirii infracţiunilor reţinute în cauză, respectiv fapte contra siguranţei şi integrităţii sistemelor informatice şi totodată contra securităţii naţionale.

De asemenea, a fost identificat în stare de funcţionare un laptop marca …., cu seria ……; SNID: …….

Astfel, prin ordonanţa din data de …….10.2019, ora 20:30, în baza art. 141 C.pr.pen. rap. la art. 138 alin. 1 lit. a şi d C.pr.pen., art. 324 C.pr.pen., s-a dispus ***autorizarea cu titlu provizoriu*** pe o perioadă de 10 ore de la data de 30.10.2019, ora 20:30 până la data de 31.10.2019 ora 06:30 a *accesului în sistemele informatice şi interceptarea comunicaţiilor ori al oricărui tip de comunicare la distanţă privind laptop-ul marca ….,* cu seria S/N …..; SNID: …. *şi telefoanele mobile identificate în locuinţă,* aparţinând suspectului ***A........***(CNP ……).

Cât priveşte caracterul urgent al măsurilor de supraveghere dispuse în cauză, se arată că s-a avut în vedere faptul că datele informatice stocate în memoria volatilă a sistemului informatic şi probabilitatea ca datele informatice stocate pe sistemul informatic, să fie criptate astfel încât acestea nu mai pot fi recuperate ulterior şi că există riscul accesării ulterioare de la distanţă a sistemului infromatic şi ştergerea eventualelor probe stocate în memoria acestuia.

Nu în ultimul rând, se arată că, în urma punerii în executare a măsurii de supraveghere dispusă, au fost identificate anumite date informatice astfel cum rezultă din procesul - verbal ataşat la dosar. ***În drept,*** parchetul invocă dispoziţiile art. 141 alin. 3 C.pr.pen.

Judecătorul de drepturi şi libertăţi constată că, în susţinerea propunerii, a fost ataşat dosarul de urmărire penală nr. ........ al Parchetului de pe lângă Înalta Curte de Casaţie şi Justiţie – D.I.I.C.O.T. – Secţia ……..

Cât priveşte competenţa materială de soluţionare a prezentei propuneri, analizând actele şi înscrisurile existente la dosar, judecătorul de drepturi şi libertăţi reţine incidenţa dispoziţiilor art. 38 alin. 1 lit. a C. pr. pen., raportat la infracţiunea pentru care se efectuează cercetări, respectiv **acte de diversiune,** prev. de art. 403 C.pen.

***Analizând actele şi lucrările dosarului*** de urmărire penală nr. ........ al Parchetului de pe lângă Înalta Curte de Casaţie şi Justiţie – D.I.I.C.O.T. – Secţia ………., judecătorul de drepturi şi libertăţi constată că, în cauză, sunt incidente disp. art. 141 alin. 4 C.pr.pen., fiind îndeplinite toate condiţiile prevăzute de art. 141 alin. 1 C.pr.pen.

Astfel, constată că a existat *urgenţa* de natură a justifica autorizarea provizorie a măsurii de supraveghere tehnică de către procuror, iar obţinerea mandatului de supraveghere tehnică, în condiţiile art. 140 C.pr.pen., ar fi determinat întâzierea identificării persoanei vizate. Sunt relevante, în acest sens, intervalul de timp scurt scurs între momentul dispunerii autorizării şi cel al supravegherii propriu-zise, precum şi circumstanţele concrete în care s-a realizat activitatea de supraveghere.

Din probele administrate, există indicii de săvârşire a unor fapte de natură penală de către persoana vizată, context în care măsurile de supraveghere tehnică dispusă, cu titlu provizoriu, au fost p*roporţionale* cu restrângerea drepturilor şi libertăţilor fundamentale, date fiind particularităţile cauzei, importanţa informaţiilor şi a probelor ce puteau fi astfel obţinute.

În contextul celor reţinute, în baza art. 141 alin. 4 C.pr.pen. va admite propunerea formulatăP.I.C.C.J. – D.I.I.C.O.T. – Structura …. – Secţia ……., în dosarul nr. .........

Astfel, va confirma ***ordonanţa*** nr. ........ emisă la data de .....10.2019, ora 20:30 prin care s-a dispus ***autorizarea, cu titlu provizoriu*,** pe o durată de ***10 ore,*** de la data de ***30.10.2019, ora 20:30*** până la data de ***31.10.2019, ora 06:30, a accesului în sistemele informatice şi interceptarea comunicaţiilor ori al oricărui tip de comunicare la distanţă privind laptop-ul marca …., cu seria S……..; SNID: ………. şi telefoanele mobile identificate în locuinţă, aparţinând suspectului A........*** (CNP ……..).

PENTRU ACESTE MOTIVE

ÎN NUMELE LEGII

DISPUNE:

În baza art. 141 alin. 4 C.pr.pen. admite cererea formulatăP.I.C.C.J. – Direcţia de Investigare a Infracţiunilor de Criminalitate Organizată şi Terorism – Structura ….. – Secţia ……., în dosarul nr. .........

Confirmă ***ordonanţa*** nr. ........ emisă la data de .....10.2019, ora 20:30 prin care s-a dispus ***autorizarea, cu titlu provizoriu*,** pe o durată de ***10 ore,*** de la data de ***30.10.2019, ora 20:30*** până la data de ***31.10.2019, ora 06:30, a accesului în sistemele informatice şi interceptarea comunicaţiilor ori al oricărui tip de comunicare la distanţă privind laptop-ul marca …., cu seria ……….; SNID: ………. şi telefoanele mobile identificate în locuinţă, aparţinând suspectului A........*** (CNP **………**).

Cheltuielile judiciare avansate de stat rămân în sarcina sa.

Definitivă.

Pronunţată în camera de consiliu azi, **………**, ora 18:20.

***Judecător de drepturi şi libertăţi Grefier***

**COD 1011………**