

ROMÂNIA



ÎNALTA CURTE DE CASAȚIE ȘI JUSTIȚIE
160 de ani de activitate
CABINETUL PREȘEDINTELUI

Nr. 226 din 04 februarie 2022

RAPORT

**privind verificarea efectuată de președintele Înaltei Curți de Casație și Justiție
în temeiul art.30¹ din Legea nr. 304/2004 privind organizarea judiciară,
republicată, cu modificările și completările ulterioare**

A. CADRUL LEGAL AL VERIFICĂRII

O.U.G. nr.6/2016 privind unele măsuri pentru punerea în executare a mandatelor de supraveghere tehnică dispuse în procesul penal, Legea nr.304/2004 privind organizarea judiciară, Legea nr.14/1992 privind organizarea și funcționarea Serviciului Român de Informații, Legea nr.135/2010 privind Codul de procedură penală, Decizia Curții Constituționale nr.51/16.02.2016.

Prin O.U.G. nr.6/2016, a fost modificată și completată Legea nr.14/1992 privind organizarea și funcționarea Serviciului Român de Informații.

Astfel, la articolul 8, după alineatul 1, au fost introduse două noi alineate, după cum urmează:

„(2) Pentru relația cu furnizorii de comunicații electronice destinate publicului, Centrul Național de Interceptare a Comunicațiilor din cadrul Serviciului Român de Informații este desemnat cu rolul de a obține, prelucra și stoca informații în domeniul securității naționale. La cererea organelor de urmărire penală, Centrul asigură accesul nemijlocit și independent al acestora la sistemele tehnice în scopul executării supravegherii tehnice prevăzute la art. 138 alin. (1) lit. a) din Codul de procedură penală. Verificarea modului de punere în aplicare în cadrul Centrului Național de Interceptare a Comunicațiilor a executării acestor supravegheri tehnice se realizează potrivit art. 30¹ din Legea nr. 304/2004 privind organizarea judiciară, republicată, cu modificările și completările ulterioare.

(3) Condițiile concrete de acces la sistemele tehnice al organelor judiciare se stabilesc prin protocoale de cooperare încheiate de Serviciul Român de Informații cu Ministerul

Public, Ministerul Afacerilor Interne, precum și cu alte instituții în cadrul cărora își desfășoară activitatea, în condițiile art. 57 alin. (2) din Codul de procedură penală, organe de cercetare penală speciale.”

De asemenea, prin aceeași ordonanță de urgență, a fost modificată și completată Legea nr. 304/2004 privind organizarea judiciară, în sensul că a fost introdus art. 30¹ care dispune:

„(1) Semestrial sau ori de câte ori este nevoie, președintele Înaltei Curți de Casație și Justiție sau unul dintre judecătorii anume desemnați de către acesta verifică modul de punere în aplicare în cadrul Centrului Național de Interceptare a Comunicațiilor prevăzut de art.8 alin.(2) din Legea nr. 14/1992 privind organizarea și funcționarea Serviciului Român de Informații, cu modificările și completările ulterioare, a supravegheților tehnice realizate de organele de urmărire penală.

(2) Verificarea prevăzută la alin. (1) se face în condițiile prevăzute prin Regulamentul privind organizarea și funcționarea administrativă a Înaltei Curți de Casație și Justiție. Raportul întocmit cu ocazia verificărilor va fi făcut public, prin afișare pe site-ul oficial al Înaltei Curți de Casație și Justiție.”

În fine, potrivit art.138 alin.(1) lit.a) din Codul de procedură penală: „Constituie metode speciale de supraveghere sau cercetare următoarele: a) interceptarea comunicațiilor ori a oricărui tip de comunicare la distanță”, iar, potrivit art.142 alin.(1¹) din Codul de procedură penală: „Pentru realizarea activităților prevăzute la art.138 alin.(1) lit. a)-d), procurorul, organele de cercetare penală sau lucrătorii specializați din cadrul poliției folosesc nemijlocit sistemele tehnice și proceduri adecvate, de natură să asigure integritatea și confidențialitatea datelor și informațiilor colectate.”

B. LIMITELE ȘI OBIECTIVELE VERIFICĂRII

Din interpretarea coroborată a dispozițiilor art.30¹ din Legea nr.304/2004 și art.8 alin.(2) din Legea nr.14/1992, rezultă că legiuitorul a stabilit în sarcina președintelui Înaltei Curți de Casație și Justiție atribuția de verificare a cadrului operațional și tehnic menit a asigura accesul nemijlocit și independent al organelor de urmărire penală la sistemele tehnice ale Centrului Național de Interceptare a Comunicațiilor din cadrul Serviciului Român de Informații, în scopul executării, în condiții de legalitate, a supravegheții tehnice prevăzute la art. 138 alin. (1) lit. a) din Codul de procedură penală.

Așadar, activitatea de verificare reglementată prin Legea nr.304/2004 vizează exclusiv măsurile generale care au ca scop respectarea dispozițiilor legale privind accesul organelor de urmărire penală la sistemele tehnice ale Centrului Național de Interceptare a Comunicațiilor, în scopul punerii în aplicare a dispozițiilor art.138 alin.(1) lit.a) din Codul de procedură penală, nefiind rolul președintelui Înaltei Curți de Casație și

Justiție de a verifica legalitatea procedurilor sau a probelor obținute prin mijloace tehnice de supraveghere, atribut exclusiv al judecătorului de cameră preliminară sau, după caz, al instanței de judecată.

C. CONSTATĂRILE PRECEDENTE

Raportul precedent a fost publicat pe pagina de internet a Înaltei Curți de Casație și Justiție la data de 31.08.2021, în urma verificărilor, fiind formulate următoarele concluzii:

Atât ca urmare a verificărilor directe efectuate de către președintele ÎCCJ cât și a datelor furnizate de către administratorul și beneficiarii SNIC, s-a apreciat că trebuie menținută concluzia din rapoartele precedente, privind faptul că, în actualul cadru legislativ, operațional și tehnic, este asigurat accesul direct și nemijlocit al organelor de urmărire penală la comunicațiile interceptate, iar activitățile specifice de urmărire penală sunt derulate doar de către personal din cadrul organelor judiciare.

În respectiva perioada de referință, nu au fost înregistrate disfuncționalități care să pericliteze punerea în executare a măsurilor de interceptare dispuse de organele judiciare, nu au fost semnalate situații de acces neautorizat în sistem, fiind asigurată deplina funcționalitate a acestuia sub aspect tehnic și al securității cibernetice.

Cadrul legislativ și operațional a rămas stabil, sunt implementate atât mecanisme cibernetice de separare a fluxurilor de date, cât și reguli operaționale clare, care exclud, în cazul administratorului și al fiecărui beneficiar, posibilitatea accesării altor date decât acelea generate, în condițiile legii, cu privire la ”țintele” proprii. Deși, în anumite cazuri, unitățile de parchet teritoriale sunt nevoite să apeleze pentru punerea în aplicare a măsurilor de supraveghere tehnică la sprijinul structurilor tehnice specializate ale Poliției Române (ca urmare a volumului ridicat de lucrări la nivelul structurilor tehnice din cadrul marilor parchete), și în aceste cazuri sunt aplicabile aceleași reguli și proceduri de realizare a activității de interceptare, precum și garanțiile tehnice și procedurale aferente, care sunt unice și au fost stabilite de către administratorul sistemului.

În raport și de recomandările din raportul aferent perioadei precedente, s-a remarcat creșterea rigurozității în materia jurnalizării (documentării) incidentelor (avarii tehnice, introducerea eronată a datelor etc.), atât prin implementarea unei noi versiuni a aplicației Help Desk, cât și prin bune practici stabilite la nivelul marilor parchete, în ceea ce privește supracontrolul uman al mecanismelor automatizate de limitare a erorilor, precum și pentru logarea și documentarea eventualelor erori materiale și a modului de remediere.

Rigoarea în folosirea echipamentelor și a aplicațiilor informatice este în continuare asigurată prin practici și proceduri operaționale unitare și garantată printr-un înalt grad de automatizare al sistemului.

Se asigură instruirea prealabilă a personalului specializat în raport cu orice modificare (upgradare) tehnică sau operațională, însă, cel puțin la nivelul unor unități de parchet apare drept importantă alocarea de resurse suplimentare, în special umane – specialiști/ofițeri de poliție judiciară special instruiți -, pentru gestionarea volumului ridicat de activitate.

La nivelul marilor parchete se manifestă preocupare pentru creșterea gradului de transparență, prin furnizarea unor informații de interes public, cu caracter general (în special date statistice), în principal prin intermediul rapoartelor de activitate. S-a apreciat că identificarea unor modalități de diseminare a acestor date care să permită un caracter mai actual al acestora și o mai bună periodicitate ar contribui atât la îmbunătățirea percepției publice asupra sistemului judiciar în general, cât și la ”demitizarea” acestor tehnici de investigație în conștiința publică. În acest context, s-a apreciat că ar putea fi generalizate bune practici precum cele implementate în perioada de referință la nivelul DIICOT.

Totodată, prin raportul sus-menționat, președintele Înaltei Curți de Casație și Justiție a formulat următoarele recomandări:

- (i) menținerea înaltului standard de securitate cibernetică în ceea ce privește echipamentele și aplicațiile informatice folosite pentru interceptare, precum și fluxurile comunicaționale securizate;
- (ii) păstrarea și actualizarea permanentă a procedurilor operaționale unitare, standardizate, însoțite de garanțiile tehnice și procedurale necesare, în ceea ce privește efectuarea tuturor operațiunilor legate de punerea în executare a măsurilor de interceptare. În mod special, aceleași reguli și garanții trebuie să fie aplicabile indiferent dacă măsura de interceptare este pusă în executare, din punct de vedere tehnic, printr-o structură specializată constituită la nivelul unității centrale de parchet sau, la nivel teritorial, cu sprijinul Poliției Române;
- (iii) menținerea regulii instruirii prealabile a personalului implicat, în cazul oricărei modificări/upgradări semnificative a sistemelor informatice/aplicațiilor folosite;
- (iv) documentarea riguroasă a avariilor/erorilor materiale și intervenția imediată pentru remedierea acestora, atât prin folosirea aplicației Help Desk cât și prin sistemele automatizate de limitare a erorilor, dublate de sisteme adecvate de monitorizare cu intervenție umană. Schimbul reciproc de bune practici la nivelul structurilor specializate ale marilor parchete și standardizarea celor care sunt considerate cele mai eficiente ar putea constitui o modalitate de acțiune în această direcție;

- (v) asigurarea, cu sprijinul celorlalte puteri ale statului, a resurselor adecvate pentru buna funcționare a sistemului, în contextul evoluțiilor tehnice recente și a accelerării procesului de digitalizare, în special prin asigurarea resursei umane specializate;
- (vi) continuarea procesului de transparentizare privind informațiile de interes public (în principal, date statistice) legate de această categorie de activități de investigare. Este recomandabilă analizarea și, eventual, standardizarea unor bune practici cu acest obiect implementate la nivelul DIICOT.

D. DEFĂȘURAREA VERIFICĂRII ACTUALE

În raport cu concluziile și recomandările formulate prin raportul precedent, la data de 05.01.2022, s-au transmis Parchetului de pe lângă Înalta Curte de Casație și Justiție, Direcției Naționale Anticorupție, Direcției de Investigare a Infraacțiunilor de Criminalitate Organizată și Terorism și Serviciului Român de Informații solicitări privind transmiterea datelor relevante legate de perioada de referință 01.07.2021-31.12.2021, privind, în special, descrierea pe scurt a modului în care se asigură separarea fluxurilor de date și se exclude posibilitatea accesării de către orice alți beneficiari ai CNIC a datelor interceptate la cererea unuia dintre aceștia; descrierea pe scurt a procedurilor de verificare a existenței și termenului de validitate a autorizației prevăzute de lege pentru efectuarea interceptărilor de comunicații; dacă în perioada de referință s-au înregistrat incidente de securitate, avarii/erori de natură tehnică sau materială în ceea ce privește punerea în executare a autorizațiilor de interceptate, proporția acestora relativ la totalul operațiunilor efectuate, modul în care au fost ele remediate, durata medie de remediere a deficiențelor constatate și măsurile luate pentru prevenirea reapariției acestora; modul și periodicitatea acțiunilor de formare profesională continuă a personalului CNIC, atât în ceea ce privește elementele de natură tehnică, dar și cu privire la respectarea legislației specifice și a procedurilor operaționale, precum și implicarea CNIC, în calitate de administrator al sistemului în pregătirea personalului specializat din cadrul structurilor tehnice ale marilor parchete sau din cadrul Poliției Române (DOS); orice dificultăți înregistrate în perioada de referință în ceea ce privește punerea în executare a măsurilor de supraveghere tehnică dispuse de organele judiciare, indiferent de natura acestora – resurse umane sau materiale, cadru legislativ, cooperare inter-instituțională etc.; dacă au avut loc modificări privind protocoalele încheiate între instituțiile abilitate în această materie sau dacă s-au formulat propuneri privind eventuala modificare a cadrului legislativ și stadiul actual al acestora; dacă în perioada de referință au fost documentate/reclamate situații de acces neautorizat în sistem sau au existat sesizări privind interceptări ale comunicațiilor efectuate neautorizat, în afara CNIC, și, în caz afirmativ și, în măsura în care astfel de situații sunt tehnic posibile, modul în care astfel de sesizări sunt cercetate și soluționate.

Marile unități de parchet au mai fost chestionate cu privire la împrejurarea dacă actuala modalitate de reglementare și de organizare a punerii în executare a măsurilor de supraveghere tehnică asigură accesul direct și nemijlocit al organelor de urmărire penală la datele interceptate, dacă securitatea sistemului și a gestionării acestor categorii de date sunt asigurate și dacă celeritatea procedurilor judiciare și respectarea drepturilor fundamentale ale persoanelor implicate sunt astfel garantate și s-a solicitat colectarea de date, pe baza experienței unităților de parchet din subordine, în special cele din afara Capitalei, cu privire la orice dificultăți sau diferențieri de natură tehnică sau procedurală în cazurile în care se procedează la punerea în executare a măsurilor de supraveghere tehnică prin structurile Poliției Române (DOS).

Informațiile transmise au fost clarificate în cadrul vizitelor directe efectuate de către președintele Înaltei Curți de Casație și Justiție în cadrul PÎCCJ, DNA, DIICOT și CNIC, în luna ianuarie 2021, și a discuțiilor purtate cu această ocazie cu persoane din conducerea acestor instituții și a structurilor cu caracter tehnic constituite în cadrul acestora. De asemenea, având în vedere că în cadrul colectării datelor pentru raportul precedent a rezultat că, în teritoriu, măsurile de interceptare a comunicațiilor sunt puse în executare într-o proporție semnificativă prin intermediul structurii tehnice specializate a Poliției Române – DOS, la data de 20.01.2022 a fost efectuată o vizită de documentare și în cadrul acestei structuri.

E. CONSTATĂRILE VERIFICĂRII

Având în vedere aspectele constatate personal de către președintele Înaltei Curți, datele furnizate prin chestionarele transmise Parchetului de pe lângă Înalta Curte de Casație și Justiție, Direcției Naționale Anticorupție, Direcției de Investigare a Infraacțiunilor de Criminalitate Organizată și Terorism și Serviciului Român de Informații, în cadrul căruia își desfășoară activitatea Centrul Național de Interceptare a Comunicațiilor, precum și constatările anterioare și dispozițiile legale incidente în materie, au rezultat următoarele:

1. Cadrul legal și procedurile operaționale

În perioada de referință cadrul legislativ și operațional a rămas stabil, nefiind înregistrate modificări pe plan legislativ sau în ceea ce privește Protocolul nr.9331/2016. O.U.G. nr.6/2016 a fost aprobată, fără amendamente, de către Parlament, legea de aprobare aflându-se în prezent în procedura de verificare a constituționalității, înainte de promulgare.

Astfel, Centrul Național de Interceptare a Comunicațiilor din cadrul Serviciului Român de Informații este desemnat prin lege cu rolul de a obține, prelucra și stoca informații în domeniul siguranței naționale în cadrul relației cu furnizorii de comunicații electronice destinate publicului (art.8 alin.(2) teza I din Legea nr.14/1992).

La cererea organelor de urmărire penală, Centrul Național de Interceptare a Comunicațiilor asigură accesul nemijlocit și independent al acestora la sistemele tehnice proprii în scopul executării supravegherii tehnice prevăzute la art. 138 alin. (1) lit. a) din Codul de procedură penală (art.8 alin.(2) teza a II-a din Legea nr.14/1992).

În vederea alinierii capacităților de interceptare la noile tehnologii implementate la nivelul serviciilor de comunicații electronice și în contextul procesului de consultare cu privire la proiectul de act normativ prin care va fi transpus în legislația națională Codul European al Comunicațiilor Electronice, CNIC a formulat propuneri referitoare la obligația de a sprijini organele de aplicare a legii și organele cu atribuții în domeniul securității naționale, pentru punerea în executare a măsurilor de interceptare și înregistrare a comunicațiilor, prevăzute în actele de autorizare a restrângerii temporare a exercițiului unor drepturi și libertăți fundamentale, cu referire la operatorii de servicii de găzduire electronică cu resurse IP și furnizorii de servicii de comunicații interpersonale care nu se bazează pe numere. Proiectul se află în curs de adoptare.

Condițiile concrete de acces ale organelor de urmărire penală la sistemele tehnice ale Centrului Național de Interceptare a Comunicațiilor se stabilesc prin protocoale de cooperare încheiate între Serviciul Român de Informații și Ministerul Public, Ministerul Afacerilor Interne, precum și cu alte instituții în cadrul cărora își desfășoară activitatea organele de cercetare penală (art.8 alin.(3) din Legea nr.14/1992).

În luna decembrie 2016 a fost încheiat Protocolul privind cooperarea între Serviciul Român de Informații și Ministerul Public pentru stabilirea condițiilor concrete de acces la sistemele tehnice ale Centrului Național de Interceptare a Comunicațiilor, înregistrat sub nr.9331 din 7 decembrie 2016, respectiv nr.2440/C din 8 decembrie 2016 („Protocolul”).

Protocolul stabilește, în baza Legii nr.14/1992, modalitatea tehnică de cooperare între instituțiile anterior menționate și asigură, potrivit dispozițiilor art.12 din respectivul act, și accesul Direcției Naționale Anticorupție, respectiv al Direcției de Investigare a Infraacțiunilor de Criminalitate Organizată și Terorism la sistemele tehnice ale Centrului Național de Interceptare a Comunicațiilor în aceleași condiții stabilite convențional între cele două instituții semnatare.

În perioada de referință, 01.07.2021-31.12.2021, Protocolul nu a suferit modificări și se află în vigoare.

În acord cu dispozițiile art.8 alin.(3) din Legea nr.14/1992, Protocolul este un document public, fără regim de confidențialitate.

Potrivit art.3 din Protocolul sus-menționat, accesul Parchetului de pe lângă Înalta Curte de Casație și Justiție, al Direcției Naționale Anticorupție, respectiv al Direcției de Investigare a Infraacțiunilor de Criminalitate Organizată și Terorism din cadrul Ministerului Public, (denumite în continuare, în cuprinsul prezentului raport, „autorități judiciare”) la sistemele tehnice se realizează direct, nemijlocit și independent prin: (i) utilizarea aplicațiilor informatice de interceptare specifice; (ii) managementul țintelor, al mandatelor de supraveghere tehnică și al utilizatorilor

conectați la sistem din cadrul structurii; (iii) direcționarea semnalului interceptat și/sau recepționarea acestuia către/de către structuri stabilite de Ministerul Public; (iv) exportarea produselor interceptării prin intermediul aplicațiilor informatice specifice; (v) exploatarea traficului interceptat exclusiv din locațiile proprii și prin intermediul personalului specializat desemnat la nivelul fiecărei autorități judiciare.

În exercitarea acestor operațiuni, autoritățile judiciare, după publicarea în Monitorul oficial al României a Deciziei Curții Constituționale nr.51/2016, au luat următoarele măsuri de natură logistică:

- și-au constituit în sediile proprii, structuri specializate pentru punerea în executare a măsurilor de supraveghere tehnică având ca obiect interceptarea comunicațiilor; prin aceste structuri, autoritățile judiciare au devenit în mod treptat apte de a proceda în mod autonom, direct, nemijlocit și independent la punerea în executare în concret a măsurilor de supraveghere din locațiile proprii, separate din punct de vedere fizic de Centrul Național de Interceptare a Comunicațiilor;

- și-au achiziționat, instalat și configurat echipamentele tehnice terminale necesare pentru punerea în executare a măsurilor de supraveghere, fiind, sub acest aspect, complet autonome și independente de Centrul Național de Interceptare a Comunicațiilor;

- au alocat personal tehnic specializat pentru desfășurarea operațiunilor specifice procedurilor tehnice de punere în executare a măsurilor de interceptare a comunicațiilor ori a oricărui tip de comunicare la distanță;

- prin echipamentele achiziționate cele trei autorități judiciare și-au asigurat un acces separat și autonom la fluxul de informații supus interceptării și realizează în mod exclusiv punerea în aplicare a măsurilor de supraveghere în cauzele pe care le instrumentează, având posibilitatea tehnică să acceseze doar conținutul sesiunilor interceptate aparținând țintelor proprii.

Toate aceste măsuri au conferit fiecărei autorități judiciare posibilitatea ca, în mod complet autonom, să își marcheze în sistemul informatic centralizat țintele proprii și să aibă propriul administrator în aplicația de exploatare a conținutului sesiunilor interceptate.

Cu toate acestea, în condițiile unor resurse materiale și umane limitate, structurile specializate constituite în cadrul unora dintre marile unități de parchet (PÎCCJ, DIICOT) pot asigura punerea în executare în mod direct a măsurilor de supraveghere tehnică numai într-un număr limitat de cazuri (în special în ceea ce privește activitatea structurilor centrale). În acest scop, la nivel local, organele de urmărire penală beneficiază de asistența structurilor specializate ale Poliției Române, în special Direcția de operațiuni speciale, situație care se încadrează în prevederile art.138 alin.(1) lit.a) C.p.p., privind calitatea persoanelor care pot realiza activități de supraveghere tehnică, în vederea interceptării comunicațiilor. Și în aceste situații, în relația cu CNIC, se aplică aceleași reguli și proceduri de realizare a activității de interceptare, precum și garanțiile tehnice și procedurale aferente, care sunt unice și au fost stabilite de Serviciul Român

de Informații – în calitate de autoritate națională în materie – în cooperare cu operatorii și furnizorii de servicii de comunicații electronice care au obligația de a implementa în propriile rețele funcția legală de interceptare. Acestea se aplică în mod unitar la nivelul tuturor structurilor tehnice ale instituțiilor conectate la SNIC. La nivelul parchetelor/structurilor teritoriale, punerea în executare în astfel de situații se realizează, ca procedură unitară, în baza unor ordonanțe de delegare emise de procuror către structurile specializate ale Poliției Române, iar procedurile operaționale folosite de către lucrătorii specializați ai poliției oferă aceleași garanții tehnice pentru implementarea mandatelor de supraveghere tehnică.

Conform relațiilor furnizate de către aceasta, în cazul Direcției Naționale Anticorupție, măsurile de supraveghere tehnică sunt puse în aplicare exclusiv prin intermediul Serviciului Tehnic, din cadrul structurii centrale, fără implicarea structurilor teritoriale.

Potrivit Protocolului încheiat, Centrul Național de Interceptare a Comunicațiilor are atribuții limitate, care vizează:

- administrarea sistemului tehnic de stocare a conținutului comunicațiilor transferate de operatorii de comunicații în condițiile din actul de autorizare, introdus în sistem de autoritatea judiciară beneficiară;
- acordarea de suport tehnic autorităților judiciare atât în vederea instalării, configurării și exploatării echipamentelor și aplicațiilor informatice, cât și pentru rezolvarea disfuncționalităților ivite în procesul de utilizare a acestora, în condiții de anonimizare, și fără riscul alterării conținutului comunicațiilor;
- implementarea politicii și măsurilor de securitate informatică, precum și a unor mecanisme de autentificare, autorizare și criptare a conexiunilor de date între utilizatori și servere.

Procesele tehnice de interceptare a comunicațiilor sunt realizate în centrele operatorilor de telecomunicații, iar conținutul comunicațiilor interceptate este transferat în mod complet automatizat către sistemul de stocare administrat de Centrul Național de Interceptare a Comunicațiilor, fără vreo intervenție umană din partea personalului Serviciului Român de Informații.

Sistemul administrat de Centrul Național de Interceptare a Comunicațiilor asigură accesul simultan, autonom și independent al autorităților de interceptare administrate și utilizate de către autoritățile judiciare și de către Serviciul Român de Informații (în acest ultim caz, doar pentru mandatele de supraveghere prevăzute de Legea 51/1991, care, în limitele prescrise de art.30¹ din Legea nr.304/2004, care nu fac obiectul prezentelor verificări).

Fiecare autoritate judiciară este complet autonomă în gestionarea și utilizarea propriului flux de acces la sistemul tehnic al Centrului Național de Interceptare a Comunicațiilor.

Niciuna dintre autoritățile judiciare și nici Serviciul Român de Informații nu poate să vizualizeze ori să acceseze ”țintele” sau operațiunile efectuate de una dintre celelalte autorități.

Deși separarea nu se poate realiza la nivel fizic, deoarece echipamentele de interceptare sunt aceleași pentru toți utilizatorii și depind de livrarea traficului de către operatorii de telecomunicații, totuși, la nivel logic, separarea pe autorități este realizată integral: procese separate, zone de stocare distincte ale traficului, acces partajat în aplicații.

Accesul la conținutul comunicației interceptate se realizează de fiecare autoritate judiciară, conform principiului necesității de a cunoaște, prin introducerea datelor în aplicațiile informatice instalate pe terminalele proprii, care asigură securitatea sistemului și accesul utilizatorilor autorizați la fluxul de comunicații ce formează obiectul măsurii de supraveghere. Prin urmare, astfel cum s-a constatat în cadrul tuturor verificărilor efectuate până în prezent, fiecare autoritate judiciară are acces exclusiv la datele care privesc ”țintele” (terminalele sau numerele de telefon ori conturile electronice cu privire la care s-au dispus măsuri de interceptare) proprii, după cum însuși administratorul sistemului – Centrul Național de Interceptare a Comunicațiilor – **nu are acces**, din punct de vedere tehnic ori prin personalul propriu, la datele interceptate ca urmare a măsurilor de supraveghere tehnică puse în executare de către respectivele entități judiciare. Mecanismele tehnice prin care se asigură această separare este descrisă în cadrul următoarei secțiuni din prezentul raport.

De altfel, conform aprecierii tuturor celor trei mari parchete consultate – Parchetul General, DNA și DIICOT, în actuala modalitate de reglementare și de organizare a punerii în executare a măsurilor de supraveghere tehnică, este asigurat accesul direct și nemijlocit al organului de urmărire penală la datele de interceptate, fiind totodată garantate celeritatea procedurilor judiciare și respectarea drepturilor fundamentale ale persoanelor implicate.

Spre exemplu, în cazul măsurilor de supraveghere tehnică puse în executare prin intermediul Serviciului tehnic constituit în cadrul Parchetului de pe lângă Înalta Curte de Casație și Justiție, această structură internă a Parchetului General utilizează în mod direct aplicațiile informatice de interceptare, pune în executare nemijlocit mandatele de supraveghere tehnică, manageriază țintele, exploatează traficul rezultat din interceptarea comunicațiilor, exportă produsul interceptării comunicațiilor și în expediază beneficiarului, totul de la sediu propriu, folosind echipamentele special achiziționate, exclusiv prin lucrători specializați aflați în subordinea unui procuror PÎCCJ, fără participarea altor instituții sau persoane care nu au calitatea de organe de urmărire penală.

În cazul măsurilor puse în executare cu sprijinul structurii tehnice specializate a Poliției Române (Direcția Operațiuni Speciale – DOS), accesul direct și nemijlocit la datele interceptate se realizează prin folosirea echipamentelor proprii ale organelor de poliție, autonome și independente de CNIC, configurate în rețeaua locală independentă de alte rețele publice și private și conectată la SNIC, utilizarea de aplicații informatice specifice, asigurarea managementului țintelor, al actelor de autorizare și al utilizatorilor

conecțați la sistem din cadrul DOS, exportarea traficului interceptat înregistrat prin aplicații specifice, inscripționarea acestuia pe suporturi optice și înaintarea cu adresă către unitățile beneficiare, exploatarea traficului interceptat exclusiv prin locațiile proprii și prin lucrătorii specializați din cadrul DOS, asigurarea accesului organelor de cercetare penală delegate la datele interceptate, în locațiile dedicate de la nivelul tuturor structurilor de operațiuni speciale (organizate în fiecare județ, iar polițiștii delegați au acces la traficul interceptat în sistem 24/24).

2. Separarea fluxurilor de date și asigurarea accesului exclusiv al organelor judiciare la datele colectate în urma procesului de interceptare a comunicațiilor ca măsură de supraveghere tehnică

În perioada de referință nu au survenit modificări legislative, operaționale sau tehnice care să conducă la modificarea concluziilor reținute sub aceste aspecte în rapoartele precedente, constatându-se că datele interceptate la solicitarea fiecăruia dintre beneficiarii sistemului sunt disponibile exclusiv organului de urmărire penală care a solicitat interceptarea și care este autorizat să le acceseze, în condițiile legii, cu excluderea posibilității stocării, accesării sau modificării acestora de către orice alte instituții sau persoane terțe, inclusiv personalul CNIC.

Interceptarea comunicațiilor se realizează prin interconectarea sistemului tehnic de interceptare cu centralele operatorilor de comunicații electronice, prin canale de comunicații separate, unice și criptate, care transportă semnalul interceptat în formă brută (pachete distincte de date). Acesta este translatat și agregat la nivelul platformei tehnice administrate de CNIC și transmis, **pe fluxuri distincte**, către fiecare beneficiar în parte, respectiv **numai către acel beneficiar care are din punct de vedere legal acces la datele respective în baza prevederilor actelor de autorizare a interceptării comunicațiilor**.

Atât preluarea traficului furnizat de operatorii de comunicații, cât și agregarea acestuia la nivelul sistemului tehnic de interceptare, respectiv transmiterea către beneficiari sunt, prin excelență, procese automatizate, desfășurate fără intervenție umană, fiind astfel exclusă posibilitatea accesului operatorilor umani din cadrul CNIC la datele interceptate la cererea uneia dintre autoritățile judiciare beneficiare.

În consecință, pe baza vizitelor directe efectuate de către președintele ÎCCJ în cadrul instituțiilor implicate, precum și având în vedere datele furnizate, se impune menținerea concluziei că actuala configurație și actuala modalitate de funcționare a SNIC asigură accesul nemijlocit și independent al organelor de urmărire penală în SNIC, în vederea punerii în aplicare a prevederilor actelor de autorizare a interceptării comunicațiilor solicitate în dosarele penale.

Configurația sistemului administrat de CNIC asigură funcționarea simultană a patru autorități independente, trei fiind administrate și utilizate de structurile judiciare (PÎCCJ, DNA, DIICOT). Autoritățile judiciare și-au constituit în sediile proprii

structuri specializate pentru punerea în aplicare a mandatelor de supraveghere tehnică având ca obiect interceptarea comunicațiilor, sens în care și-au achiziționat, instalat și configurat echipamentele terminale necesare în procesul de marcare și stocare și au încadrat/redistribuit personal tehnic căreia i-a fost acordată de către CNIC asistență tehnică de specialitate.

Nicio autoritate nu poate vizualiza în sistem țintele altor autorități și nici accesa conținutul sesiunilor interceptate în structurile proprii ale acestora. Deși separarea nu se poate realiza **din punct de vedere fizic** la nivelul operatorilor de comunicații, existând un singur canal de comunicații unidirecțional, iar echipamentele de interceptare sunt aceleași pentru toți utilizatorii și depind de livrarea traficului de către operatorii de telecomunicații, totuși, separarea pe autorități este integral asigurată la nivel logic – zone de marcare a țintelor separate, procese separate, partiționarea în mod distinct a zonelor de stocare a traficului și a accesului în aplicații.

Ca urmare, se impune menținerea concluziei anterioare privind faptul că folosirea platformei partajate (utilizarea aceluiași echipamente tehnice, dar cu separarea riguroasă a fluxurilor de date) permite maximizarea resurselor disponibile – echipamente, dar, mai ales, specialiști IT care să asigure întreținerea platformei și asigurarea unui înalt nivel de securitate cibernetică, în condițiile în care, din punct de vedere tehnic, datele interceptate vor fi puse la dispoziție doar organului de urmărire penală care are dreptul să le acceseze în baza autorizației prin care s-a dispus măsura de supraveghere.

Din punct de vedere al respectării cu strictețe a prevederilor mandatului de supraveghere tehnică, administratorul platformei partajate (CNIC) a pus la dispoziția autorităților conectate la sistem aplicații informatice de suport al procesului de marcare a criteriilor de interceptare, cu caracter unitar, care integrează funcții de verificare a existenței actului de autorizare și de validare a unor parametri tehnici obligatorii, care sunt destinați, în esență, să reducă posibilitatea de eroare umană în procesul de implementare a datelor și să furnizeze unele mecanisme automatizate de detectare a unor astfel de erori (de exemplu, pot fi semnalate neconcordanțele în ceea ce privește resursele de numerotație aplicate unui operator de comunicații oarecare. Aceste aplicații de suport includ și măsuri de verificare și control ale perioadei de valabilitate a autorizării legale (inclusiv sub aspectul semnalării automate a duratei/valabilității actului de autorizare), însă, potrivit datelor furnizate de către administratorul sistemului, procesul depinde în continuare, într-o mare măsură, de activitatea operatorilor care execută activități de marcare.

3. Asigurarea securității sistemelor și prevenirea eventualelor erori

În perioada de referință nu au existat incidente legate de asigurarea securității cibernetice a sistemelor Centrului Național de Interceptare a Comunicațiilor (CNIC) sau ale autorităților judiciare beneficiare. De asemenea, în perioada de referință nu au

existat situații de acces neautorizat în sistem și nici nu au fost recepționate sesizări privind interceptări ale comunicațiilor efectuate neautorizat.

Standardul de securitate al sistemelor și al fluxurilor de comunicații apare ca fiind adecvat, iar posibilitatea accesării datelor în mod fraudulos este exclusă prin caracterul relativ închis al Sistemului Național de Interceptare a Comunicațiilor, precum și prin faptul că asupra sistemului se aplică o serie de măsuri (politici, concepte, standarde și ghiduri de securitate), prin care este asigurată securizarea accesului.

CNIC monitorizează permanent starea de funcționare a echipamentelor componente prin aplicații dedicate, sub supravegherea personalului de tură – 24/24h, iar situațiile de avarie tehnică sunt semnalizate în sistemul dedicat și remediate de urgență, fiind folosită și o aplicație dedicată – HelpDesk - de semnalare și rezolvare a disfuncționalităților de natură tehnică survenite la nivelul echipamentelor sau al rețelei de interceptare.

Aceleași politici și proceduri de securitate transmise de către administratorul sistemului sunt implementate și respectate, indiferent că punerea în executare a măsurilor de supraveghere tehnică se realizează prin structurile tehnice constituite la nivelul marilor parchete sau cu sprijinul structurii tehnice specializate a Poliției Române (DOS). În acest ultim caz, toate spațiile destinate punerii în executare și exploatare a actelor de autorizare sunt monitorizate și verificate zilnic de către personalul de tură, săptămânal se verifică integritatea fizică și modul de funcționare a sistemelor informatice, sunt actualizate aplicațiile antivirus, iar lunar se verifică integritatea sigiliilor aplicate pe echipamentele informatice. *Referitor la aplicația HelpDesk, DOS a semnalat că există cazuri când erorile și deficiențele semnalate prin intermediul acestei aplicații sunt rezolvate cu întârziere sau rămân în continuare cu statusul "În lucru". Aceste aspecte urmează a fi urmărite în mod specific în raportul următor, urmând a fi colectate date de la toate unitățile de parchet și CNIC, pentru a se verifica rezolvarea promptă a unor astfel de situații.*

Pentru prevenirea apariției unor erori în procesul de marcare/exploatare, inclusiv prin introducerea de către utilizatori a unor date eronate în sistemele informatice, CNIC a pus la dispoziția autorităților judiciare beneficiare instrumente automatizate de limitare a erorilor materiale și a optimizat procesele de asigurare a conformității procedurilor de marcare cu resursele de numerotație alocate operatorilor de comunicații electronice. Interceptarea este un proces automatizat, orice eroare detectată fiind semnalizată în cadrul aplicațiilor dedicate prin avertizarea componentei tehnice umane.

Conform informațiilor furnizate de către administratorului sistemului, în perioada de referință erorile umane au survenit cu frecvență redusă și doar în situații punctuale, fiind soluționate de cele mai multe ori fie prin implementarea în pattern, fie prin implementarea corectării erorii materiale, fără afectarea legalității procesului de interceptare. De asemenea, potrivit relațiilor furnizate de către Parchetul General, în perioada de referință activitatea de punere în executare a măsurilor de supraveghere tehnică s-a desfășurat fără a se înregistra dificultăți semnificative. S-au înregistrat, cu titlu de excepție, situații punctuale în care au fost identificate criterii incomplet sau

greșit indicate în actele de autorizare sau comunicarea cu întârziere a datelor solicitate furnizorilor de servicii de comunicații electronice destinate publicului. Aceste disfuncționalități punctuale au apărut în special în situația punerii în executare a măsurilor de interceptare de către unele structuri teritoriale de parchet cu sprijinul structurilor tehnice specializate ale Poliției Române (DOS). Este de remarcat că ele au fost semnalate doar la nivelul a două unități de parchet de pe lângă judecătoria, respectiv a patru unități de parchet de pe lângă tribunal și în situații strict determinate, fiind așadar vorba de situații izolate, reprezentând un procent redus din totalul măsurilor de supraveghere puse în executare cu sprijinul tehnic al Poliției Române – DOS. *Potrivit informațiilor comunicate de către respectiva structură a Poliției Române, rezultă totuși că o parte a situațiilor semnalate (identificarea unor criterii incomplete sau greșit indicate) pot fi remediate doar de către beneficiari (instanța/parchetul care a emis actul de autorizare), iar o altă parte, respectiv întârzierile înregistrate în unele cazuri, nu s-ar datora neapărat lucrătorilor de poliție, fiind utilizată în toate situațiile aplicația tehnică specifică.*

Perspectiva parțial diferită a instituțiilor implicate cu privire la cauzele deficiențelor punctuale semnalate în procesul de documentare a prezentului raport evidențiază importanța bunei cooperări instituționale, pe toate palierele, nu doar la nivel central, dar și, poate chiar în special, la nivel teritorial și considerăm că îndreptățește cel puțin două recomandări:

- În primul rând, este recomandabilă documentarea riguroasă a tuturor acestor disfuncționalități în vederea identificării măsurilor adecvate pentru prevenirea repetării lor pe viitor. *La nivelul DOS există încă din anul 2016 un registru de consemnare a erorilor, situațiilor și incidentelor care pot afecta procesul normal de lucru. Ar fi însă recomandabil ca acesta să nu conțină doar o simplă evidență a acestor situații, dar și date relevante privind modul și termenele în care acestea au fost remediate, precum și măsurile dispuse cu caracter preventiv, pentru viitor. La nivelul marilor parchete există modalități diferite de documentare a acestor erori, cea mai comprehensivă fiind aceea de la nivelul DIICOT.*

- În al doilea rând, este recomandabilă îmbunătățirea cooperării inter-instituționale la nivel local, oriunde se constată dificultăți, aceste situații impunându-se a fi atent centralizate și monitorizate de la nivelul conducerilor instituțiilor centrale. Se impune remarca că, urmare a vizitei de documentare la această instituție a rezultat că DOS asigură punerea în executare și exploatare a actelor de autorizare emise de/emise la solicitarea tuturor unităților de parchet, și acordă sprijin ca beneficiar secundar într-un număr foarte ridicat de situații – spre exemplu la 31.12.2021, activitatea de punere în executare și exploatare a actelor de autorizare la nivelul DOS (central și teritorial) s-a efectuat de un număr de 428 lucrători specializați, au fost înregistrate pe parcursul anului precedent 3274 de lucrări și au fost întocmite nu mai puțin de 416395 note de redare a convorbirilor de interes. Este de necontestat că structura tehnică specializată a Poliției Române deține resurse umane net superioare din punct de vedere numeric celor din cadrul structurilor tehnice constituite la nivelul

parchetelor, astfel încât este de așteptat ca un număr semnificativ de autorizații de interceptare, în special la nivel teritorial, să fie puse în executare de către unitățile de parchet prin intermediul acesteia, astfel încât ambele recomandări formulate în cele de preced rămân deosebit de relevante. Se impune mențiunea că, raportat la datele comunicate de către DOS și proporțional cu numărul de lucrări, resursele umane existente la nivelul direcției respective sunt apreciate ca insuficiente (de exemplu, media traficului interceptat pe lucrător a fost în cursul anului 2021 de 9,5 ore/lucrător/zi, depășind semnificativ norma normală de lucru de 8 ore/zi), iar unele dintre problemele cu care se confruntă parchetele sub aspectul posibilității valorificării la maximum a personalului încadrat sunt comune și DOS – spre exemplu, din polițiștii încadrați la nivelul direcției, 41 de lucrători nu dețin aviz de poliție judiciară, astfel încât nu pot fi folosiți în activitățile de punere în executare a actelor de autorizare; durata de timp lungă necesară pentru obținerea respectivului aviz a fost semnalată de către DOS ca o vulnerabilitate din această perspectivă.

La nivelul DNA și DIICOT nu au fost înregistrate incidente de securitate, avarii sau erori de natură tehnică sau materială în ceea ce privește punerea în executare a autorizațiilor de interceptare. Cele două parchete specializate folosesc în mod predominant entitățile tehnice proprii, constituite în cadrul structurilor centrale cu acces direct în cadrul platformei partajate.

Cel mai riguros mecanism de documentare și prevenire a erorilor care pot interveni în procesul de executare a măsurilor de interceptare există la nivelul DIICOT, existând un registru de monitorizare a sistemelor și aplicațiilor informatice, în care este analizat orice incident privind securitatea fizică a sistemelor informatice și orice risc de securitate INFOSEC și fiind efectuate controale bilunare privind securitatea și integritatea fizică, modul de funcționare a sistemelor informatice, precum și apariția oricărui incident în funcționarea sistemelor și aplicațiilor informatice. În raport și de aspectele punctuale raportate la nivelul câtorva structuri teritoriale din subordinea Parchetului General dar și de obligativitatea cu caracter general ca măsurile de supraveghere tehnică, ca orice măsuri restrictive de drepturi, să fie puse în aplicare cu maximă rigoare, recomandarea formulată prin raportul precedent, privind standardizarea și preluarea la nivel general a bunelor practici constatate sub aceste aspecte la structura tehnică din cadrul DIICOT se impune a fi menținută.

Și la nivelul Poliției Române- DOS, disfuncționalitățile tehnice de la nivelul tuturor structurilor de operațiuni speciale sunt centralizate la nivelul DOS-SET și semnalate către CNIC, pentru remediere, în principal prin intermediul aplicației HelpDesk, dar și telefonic. Cu privire la toate erorile și disfuncționalitățile se întocmesc procese-verbale.

4. Asigurarea resurselor necesare și pregătirea profesională continuă a personalului implicat

Toate operațiunile de optimizare/upgradare a funcției de interceptare, inclusiv obligația legală a operatorilor de comunicații electronice de a implementa soluțiile tehnice

respective în propriile rețele se desfășoară în colaborare cu specialiștii CNIC, având la bază un cadru oficial de desfășurare, documentat tehnic anterior implementării și urmat de sesiuni de pregătire tehnică. La fiecare actualizare sau upgradare are loc instruirea prealabilă a personalului angrenat în activitățile de punere în executare a actelor de autorizare a interceptării comunicațiilor. În cazul schimbărilor cu impact semnificativ, anterior intrării acestora în exploatare, utilizatorilor le sunt transmise atât noile proceduri în cadrul aplicațiilor, cât și toate elementele de noutate, iar periodic, sau ad-hoc, în funcție de necesități (spre exemplu în cazul modificărilor de personal intervenite în cadrul structurilor tehnice ale marilor parchete), se asigură îndrumare metodologică prin intermediul specialiștilor cu experiență ai CNIC.

Informațiile furnizate de către administratorul sistemului sub aceste aspecte au fost confirmate de toate cele trei mari parchete consultate. Mai mult, la nivelul Parchetului General a fost menționată organizarea, la nivelul Serviciului tehnic, de sesiuni de lucru în cadrul cărora se discută modificările legislative și deciziile Curții Constituționale care antamează reglementările referitoare la mijloacele probatorii, probe și procedee probatorii în materie de supraveghere tehnică. Având în vedere că astfel de măsuri administrative sunt destinate bunei cunoașteri a cadrului legal, procedural și operațional, legat de punerea în executare a acestui tip de măsuri de supraveghere tehnică, considerăm că ar fi recomandabilă extinderea lor la nivelul tuturor instituțiilor implicate.

Sub aspectul resurselor, rezultă din relațiile furnizate de către marile parchete că principala dificultate este legată de asigurarea resursei umane specializate, respectiv lucrători de poliție judiciară care să fie instruiți și special alocați acestor activități tehnice. Cu excepția DNA (care a arătat că, printr-o gestionare eficientă, a contracarat astfel de vulnerabilități), atât Parchetul General, cât și DIICOT au menționat că întâmpină dificultăți în ceea ce privește selectarea și detașarea ofițerilor de poliție judiciară în cadrul structurilor tehnice proprii.

Parchetul de pe lângă Înalta Curte de Casație și Justiție a identificat cauzele acestei situații în maniera diferită în care au fost reglementate condițiile de detașare a lucrătorilor de poliție judiciară ai Serviciului tehnic al PÎCCJ în raport de cele prin care se dispune detașarea polițiștilor la DNA și DIICOT, precum și în rezerva unităților de poliție de a aviza detașarea de la MAI a ofițerilor de poliție judiciară care au participat la procedurile organizate pentru ocuparea posturilor de la serviciul tehnic specializat al Parchetului General.

Cu toate că procedura de detașare a polițiștilor în cadrul DIICOT a fost astfel apreciată ca fiind mai lesnicioasă, conform datelor furnizate de DIICOT, această instituție întâmpină la rândul său dificultăți în procesul de selecție pentru structura tehnică proprie. Condiția ca lucrătorii de poliție detașați să aibă aviz de poliție judiciară a fost apreciată ca având un impact negativ semnificativ asupra bazei de selecție, mai ales atunci când, spre exemplu, ar fi necesară detașarea unor lucrători de poliție vorbitori ai unor limbi străine de interes operativ în investigațiile penale, dar mai puțin uzuale.

O a doua cauză a dificultății procesului de selecție a fost identificată de către DIICOT în cadrul legislativ insuficient adaptat, legea în vigoare neprecizând niciun termen în care trebuie soluționată de către MAI solicitarea parchetului de detașare a unui polițist, după cum angajatorul persoanei respective are și posibilitatea refuzului solicitării din orice motive pe care le găsește pertinente.

Având în vedere că toate verificările efectuate până în prezent au relevat că existența resursei umane specializate, bine instruite și care să beneficieze de o anumită stabilitate în cadrul structurilor tehnice ale marilor parchete, este vitală sub aspectul activităților de punere în executare a măsurilor de interceptare, plecând de la procesul de supervizare a măsurilor automatizate de prevenire a erorilor, de gestiune a aplicațiilor informatice specializate și până la activități specifice organului de urmărire/cercetare penală, precum valorificarea în mod optim a informațiilor obținute sau a unui anumit moment operativ, prin prezentul raport se va formula recomandarea privind îmbunătățirea cooperării inter-instituționale între parchete și Poliția Română, în vederea asigurării unor proceduri de detașare a lucrătorilor de poliție judiciară după reguli mai simple, mai uniforme și care să aibă un rezultat previzibil încă de la declanșarea procedurii de selecție.

5. Buna desfășurare a relațiilor interinstituționale și asigurarea punerii în executare, în mod prompt și eficient, a autorizațiilor de interceptare emise, după caz, de procuror (în mod provizoriu), judecătorul de drepturi și libertăți sau de instanța de judecată

Pentru perioada de referință nu au fost semnalate disfuncționalități sistemice în ceea ce privește punerea în executare a măsurilor de supraveghere tehnică la cererea organelor judiciare, relațiile instituționale dintre CNIC și marile parchete beneficiare desfășurându-se în condiții foarte bune. Cadrul legislativ și operațional a rămas stabil.

Situațiile particulare survenite la nivelul activității de interceptare au fost soluționate eficient, inclusiv prin intermediul sistemului de ticketing. CNIC a arătat că, pe baza feed-back-ului recepționat de la instituțiile beneficiare, a derulat activități de optimizare/modernizare a aplicației de semnalare și rezolvare a disfuncționalităților de natură tehnică survenite la nivelul echipamentelor sau a rețelei de interceptare.

Ca urmare a caracterului limitat al resurselor disponibile, în special resursa umană specializată, cu excepția DNA, în cazul căreia toate măsurile de supraveghere tehnică sunt puse în aplicare prin intermediul Serviciului tehnic, structură constituită la nivel central, în cazul Parchetului General și al DIICOT, la nivelul unităților de parchet teritoriale din subordine, o parte a măsurilor de interceptare sunt puse în executare cu asistența structurilor tehnice specializate ale Poliției Române (Direcția Operațiuni Speciale) și tot prin utilizarea platformei partajate furnizate de către CNIC. *Chiar și în ceea ce privește DNA, structura tehnică a Poliției Române – DOS a semnalat faptul că, în anul 2021, structurile teritoriale ale DOS au pus în executare și exploatare acte*

de autorizare emise în 18 dosare penale ale parchetului specializat și au acordat sprijin tehnic în 27 de dosare penale.

Și în aceste cazuri sunt aplicabile aceleași garanții tehnice, procedurale și de securitate informatică.

De altfel, DIICOT a menționat expres că nu au fost înregistrate dificultăți sau diferențieri de natură tehnică ori procedurale în cazurile în care s-a procedat la punerea în executare a măsurilor de supraveghere tehnică prin structurile Poliției Române, cu excepția unor anumite reticențe punctuale în punerea în executare a unor măsuri de supraveghere ambientală, situații remediate prin preluarea cazurilor de către Biroul tehnic și de criminalistică al DIICOT.

Din datele colectate de către Parchetul General, ca urmare a solicitării formulate de către președintele Înaltei Curți în procesul de documentare a prezentului raport, două parchete locale și patru parchete de tribunal au semnalat dificultăți punctuale în ceea ce privește punerea în executare a măsurilor de supraveghere în cadrul platformei CNIC cu sprijinul tehnic al DOS. *Cu privire la situațiile consemnate în continuare, atât Parchetul General, cât și Poliția Română – DOS au transmis ulterior clarificări suplimentare, acestea fiind redată, în esență, în paranteze, pentru fiecare caz în parte. Situațiile semnalate de către unitățile de parchet de la nivel teritorial au vizat următoarele aspecte:* – într-una dintre spețele instrumentate s-a constatat lipsa traficului pentru o perioadă de o zi , fiind suspicionată o deficiență tehnică a structurii de suport (*conform DOS, deficiența nu a fost sesizată în timp util, traficul interceptat trebuind exportat din sistem într-o perioadă de timp determinată, cunoscută tuturor beneficiarilor; s-au făcut demersuri către administratorul sistemului pentru dezvoltarea unei aplicații care să verifice automat exportarea traficului înregistrat*); o unitate de parchet a apreciat ca deficitară activitatea de interceptare a comunicărilor efectuate prin intermediul e-mail-ului (*din datele ulterioare comunicate de PICCJ și DOS rezultă însă că este mai degrabă vorba de o situație generală legată de particularitățile tehnice de interceptare a acestui tip de comunicare la distanță*) , cea de ascultare în timp real a sesiunilor, din cauza spațiului insuficient (*conform DOS, spații de lucru dedicate sunt amenajate în cadrul tuturor structurilor teritoriale*) și cea de redare a comunicărilor de interes pentru cauză; o altă unitate de parchet a învederat că există întârzieri semnificative în redactarea și transmiterea notelor de redare (*existența unor situații punctuale în care există întârzieri în redactarea și transmiterea notelor de redare a fost motivată de către DOS prin numărul ridicat de lucrări raportat la personalul existent, situație prezentată mai pe larg într-o secțiune precedentă*) și că informațiile rezultate din exploatare, într-o singură situație, ar fi fost diseminate în afara echipelor de lucru (*conform precizărilor transmise de către PÍCCJ, această situație a vizat de fapt o altă activitate de supraveghere tehnică decât interceptarea comunicațiilor, excedând obiectului verificării, iar potrivit Poliției Române – DOS / în urma verificărilor a rezultat că polițiștii din cadrul DOS nu au diseminat date și informații în afara cadrului stabilit de procuror. Situația a fost reținută în final în cadrul raportului, tocmai pentru că evidențiază importanța documentării și cercetării*

imediate a unor astfel de situații, tocmai în vederea întăririi cooperării și încrederii instituționale) ; o altă unitate de parchet a indicat o situație în care un criteriu (număr de telefon) nu a fost implementat, ceea ce a dus la pierderea unui moment operativ și a unei probe esențiale urmării penale (potrivit Parchetului General și DOS, în urma documentării suplimentare a cazului a rezultat însă parcurgerea etapelor procedurale privind marcarea țintei, situația semnalată apărând pe fondul unor modificări tehnice la un operator de comunicații, după care situația a fost remediată) ; într-un alt caz s-au semnalat situații în care s-a constatat lipsa sesiunilor audio pentru care se întocmiseră note de redare și transmiterea traficului exportat nesistematizat pe unități de timp, ceea ce îngreunează procesul de căutare a unei convorbiri(din punct de vedere tehnic, datele rezultate din punerea în executare a actelor de autorizare sunt sistematizate pe unități de timp, ele fiind transferate în mod automat din sistem); în sfârșit, un alt parchet a informat că, într-o speță, sesiunea audio a unei comunicații importante care fusese redată nu s-a regăsit pe traficul transmis procurorului, ceea ce a atras după sine imposibilitatea valorificării probei în dosarul penal.

În raport cu datele prezentate în cele ce preced, numărul unor astfel de situații în totalul operațiunilor tehnice desfășurate de DOS este infim, iar mare parte dintre situațiile relatate ar constitui mai degrabă expresia unei cooperări instituționale deficitare la nivel local, fiecare dintre instituțiile implicate având un punct de vedere parțial diferit cu privire la motivele pentru care s-a ajuns la aceste dificultăți. Dar, mai important, rezultă din datele furnizate de către Parchetul General și de către structura Poliției Române că s-au luat măsuri procedurale și operaționale pentru prevenirea unor astfel de situații – spre exemplu, în prezent, la nivelul DOS sunt implementate reguli privind monitorizarea permanentă a ordonanțelor de interceptare și a mandatelor de supraveghere tehnică, pentru ca în cazul în care țintele nu produc trafic în 24 de ore să fie înaintate pentru verificări suplimentare la unitatea de marcarea; exportul traficului înregistrat este verificat zilnic, în vederea constatării la timp a unor eventuale disfuncționalități tehnice; săptămânal se verifică corespondența dintre numărul de sesiuni exportate pentru o țintă, într-o anumită perioadă și numărul de sesiuni înregistrate în aplicația specifică de redare; pentru celeritate, actele de autorizare se primesc și prin mijloace electronice agreeate de beneficiari, iar consemnele pe momente operative sunt asigurate în regim 24/24, 7/7.

Parchetul General a subliniat că, în raport cu prevederile art.143 alin.2 C.p.p., care statuează în sarcina organelor de urmărire penală obligativitatea de a atașa procesului-verbal de redare o copie a suportului care conține rezultatul activităților de supraveghere tehnică, în situațiile punctuale în care sesiunile audio redade nu au existat pe suporturile optice pe care a fost livrat traficul interceptat în baza mandatului de supraveghere tehnică, comunicațiile de interes nu au fost folosite ca probe în respectivul dosar penal și nu au stat la baza luării deciziei cu privire la existența infracțiunii și a vinovăției persoanei cercetate. S/a mai învederat că aspectele sesizate de parchetele care au înregistrat astfel de situații au fost calificate drept incidente în legătură cu capacitatea operațională a organelor de urmărire penală și au făcut obiectul unor verificări detaliate.

Deși rezultă din datele de mai sus că toate aceste dificultăți reprezintă cazuri particulare, cu o pondere foarte redusă în totalul activităților tehnice desfășurate pentru punerea în executare a măsurilor de interceptare, gradul de rigoare care trebuie să caracterizeze punerea în executare a unei măsuri restrictive de drepturi impune ca fiecare incident în parte să fie riguros documentat și cercetat, atât sub aspectul stabilirii eventualelor responsabilități, cât și pentru a se preveni repetarea unor astfel de situații pe viitor. În acest sens, ar fi recomandabil ca toate aceste incidente să fie colectate, centralizate și monitorizate de la nivel central, eventual prin constituirea unui registru central de tipul celui deja utilizat de DIICOT pentru propria structură tehnică (din vizita de documentare rezultă că un astfel de registru există și nivelul DOS), ceea ce ar permite atât un grad ridicat de rigoare în tratarea acestora, cât și o "imagine" în timp real a dificultăților care pot apărea, fie din motive tehnice, fie operaționale, fie pur și simplu ca rezultat al insuficienței pregătiri a resursei umane specializate sau unei cooperări inter-instituționale deficitare. *Această evidență ar fi recomandat să cuprindă nu numai existența și descrierea unui anumit incident, dar și rezultatul cercetării cauzelor acestuia, modul în care a fost remediat/soluționat și termenul în care s-a reușit remedierea lui.*

De asemenea, este recomandabilă creșterea capacității tehnice a structurilor tehnice specializate din cadrul Parchetului General, DIICOT și DOS, limitată mai ales sub aspectul resurselor umane.

F. CONCLUZIILE VERIFICĂRII

Pe baza verificărilor directe efectuate de către președintele ÎCCJ în cadrul vizitelor de documentare și a datelor furnizate de către administratorul și beneficiarii SNIC, se menține concluzia din rapoartele precedente, privind faptul că în actualul cadru legislativ, operațional și tehnic, **este asigurat accesul direct și nemijlocit al organelor de urmărire penală la comunicațiile interceptate, iar activitățile specifice de urmărire penală sunt derulate doar de către personal din cadrul organelor judiciare.**

În perioada de referință, nu au fost înregistrate disfuncționalități care să periclitizeze punerea în executare a măsurilor de interceptare dispuse de organele judiciare, nu au fost semnalate situații de acces neautorizat în sistem, fiind asigurată deplina funcționalitate a acestuia sub aspect tehnic și al securității cibernetice.

Cadrul legislativ și operațional a rămas stabil, sunt implementate atât mecanisme cibernetice de separare a fluxurilor de date, cât și reguli operaționale clare, care exclud, în cazul administratorului și al fiecărui beneficiar, posibilitatea accesării altor date decât acelea generate, în condițiile legii, cu privire la "țintele" proprii.

Nu s-au înregistrat în perioada de referință dificultăți sistemice în ceea ce privește punerea în aplicare a măsurilor de supraveghere tehnică dispuse de organele judiciare competente.

Deși, în anumite cazuri, unele unități de parchet teritoriale sunt nevoite să apeleze pentru punerea în aplicare a măsurilor de supraveghere tehnică la sprijinul structurilor tehnice specializate ale Poliției Române (ca urmare a volumului ridicat de lucrări la nivelul structurilor tehnice din cadrul marilor parchete), și în aceste cazuri sunt aplicabile aceleași reguli și proceduri de realizare a activității de interceptare, precum și garanțiile tehnice și procedurale aferente, care sunt unice și au fost stabilite de către administratorul sistemului. Unele unități teritoriale de parchet au semnalat dificultăți punctuale întâmpinate în aceste situații, care se impune a fi documentate, centralizate și rezolvate prin creșterea calității cooperării interinstituționale inclusiv la nivel local, instruirea corespunzătoare a personalului implicat și creșterea capacității administrative și tehnice, în special sub aspectul resursei umane specializate, a structurilor tehnice constituite în cadrul PÎCCJ și DIICOT.

Deși înaltul grad de automatizare a sistemului de interceptare asigură, pe de o parte, securitatea acestuia și partiționarea între zonele logice dedicate fiecărui beneficiar, iar, pe de altă parte, limitează și semnalează erorile în procesul de introducere a datelor etc., pregătirea continuă a personalului implicat, informarea permanentă a acestuia asupra oricăror upgrade-uri hardware/software și menținerea rigorii în ceea ce privește monitorizarea calității activității fiecărei persoane implicate rămân aspecte esențiale și trebuie asigurate la același nivel în cadrul tuturor entităților implicate.

G. RECOMANDĂRI

Măsurile de supraveghere tehnică sunt tehnici de investigare care prezintă și o latură restrictivă de drepturi, astfel încât trebuie să se limiteze la aspectele strict necesare, să fie proporționale și autorizate în condițiile legii. Ca urmare, procesul de punere în aplicare a acestora trebuie să se caracterizeze printr-un grad ridicat de rigurozitate, astfel încât, pe de o parte, să fie respectate toate garanțiile prevăzute de lege pentru fiecare cetățean, iar, pe de altă parte, să permită strângerea probelor necesare pentru stabilirea adevărului judiciar, fiind necesară asigurarea în permanență a justului echilibru între cele două valori fundamentale sus-enunțate. În acest sens, considerăm că se recomandă următoarele:

- (i) menținerea standardelor de securitate cibernetică în ceea ce privește echipamentele și aplicațiile informatice folosite pentru interceptare, precum și fluxurile comunicaționale securizate, în special în contextul amenințărilor semnalate în prezent la nivel internațional cu privire la creșterea numărului și complexității criminalității informatice;
- (ii) păstrarea și actualizarea permanentă a procedurilor operaționale unitare, standardizate, însoțite de garanțiile tehnice și procedurale necesare. În mod special, aceleași reguli și garanții trebuie să fie aplicabile indiferent dacă măsura de interceptare este pusă în executare, din punct de vedere tehnic, printr-o

structură specializată constituită la nivelul unității centrale de parchet sau, la nivel teritorial, cu sprijinul Poliției Române. În ultimul caz este recomandabilă întărirea cooperării inter-instituționale, în special la nivel teritorial, pentru rezolvarea dificultăților punctuale care pot apărea, în paralel cu sporirea capacității tehnico-administrative a structurilor tehnice proprii, constituite în cadrul marilor parchete;

- (iii) menținerea bunelor practici actuale privind instruirea prealabilă a personalului implicat, în cazul oricărei modificări/upgradări semnificative a sistemelor informatice/aplicațiilor folosite. Același nivel de pregătire profesională sub aspectul cunoașterii și a folosirii adecvate a echipamentelor și aplicațiilor informatice trebuie asigurat cu privire la toate structurile tehnice beneficiare. Considerăm recomandabilă extinderea bunelor practici constatate la nivelul Parchetului de pe lângă Înalta Curte de Casație și Justiție, cu privire la organizarea de sesiuni periodice, în care personalul specializat să fie instruit nu numai cu privire la aspectele tehnice, dar și în ceea ce privește evoluțiile juridice privind activitățile de interceptare, inclusiv modificările legislative sau deciziile Curții Constituționale;
- (iv) documentarea riguroasă a avariilor/erorilor materiale și intervenția imediată pentru remedierea acestora, atât prin folosirea aplicației Help Desk cât și prin sistemele automatizate de limitare a erorilor, dublate de sisteme adecvate de monitorizare cu intervenție umană. Schimbul reciproc de bune practici la nivelul structurilor specializate ale marilor parchete și standardizarea celor care sunt considerate cele mai eficiente ar putea constitui o modalitate de acțiune în această direcție. Generalizarea sistemului utilizat în prezent la nivelul DIICOT, care presupune existența unui registru general al incidentelor, dublat de controale periodice (bilunare) pentru prevenirea/remedierea aspectelor deficitare apare ca recomandabilă;
- (v) asigurarea, cu sprijinul celorlalte puteri ale statului, a resurselor adecvate pentru buna funcționare a sistemului, în contextul evoluțiilor tehnice recente și a accelerării procesului de digitalizare, în special prin asigurarea resursei umane specializate. Ca soluție pe termen scurt, este recomandabilă întărirea cooperării interinstituționale între Parchet și Ministerul Afacerilor Interne sub aspectul asigurării unui proces mai rapid și mai simplu de detașare a lucrătorilor de poliție judiciară în cadrul parchetelor, luându-se în considerare situația fiecărei instituții implicate în parte;
- (vi) documentarea riguroasă, la nivelul tuturor instituțiilor implicate, a oricăror dificultăți înregistrate la nivel teritorial, local în ceea ce privește punerea în executare a măsurilor de interceptare cu sprijinul structurilor tehnice specializate ale Poliției Române. Existența unei evidențe la nivel central ar fi recomandabilă atât pentru prevenirea/remedierea rapidă a acestei situații prin colaborare interinstituțională desfășurată la cel mai înalt nivel al instituțiilor

implicate, cât și pentru creșterea gradului de rigurozitate în aceste operațiuni și formarea profesională uniformă la nivelul personalului implicat.

H. MĂSURI

Prezentul Raport este întocmit în 6 exemplare și se comunică Serviciului Român de Informații, Parchetului de pe lângă Înalta Curte de Casație și Justiție, Direcției Naționale Anticorupție, Direcției de Investigare a Infrațiunilor de Criminalitate Organizată și Terorism și Ministerului Afacerilor Interne - DOS.

Potrivit dispozițiilor art. 30¹ alin. (2) teza finală din Legea nr. 304/2004 raportul se aduce la cunoștință publică, prin afișare pe site-ul oficial al Înaltei Curți de Casație și Justiție.

Președintele Înaltei Curți de Casație și Justiție va efectua pe viitor activități de verificare la Centrul Național de Interceptare a Comunicațiilor din cadrul Serviciului Român de Informații ori de câte ori noi împrejurări de fapt sau de drept o vor impune.

Următoarea activitate de verificare va privi perioada de referință 01.01.2022-30.06.2022, în acord cu dispozițiile art.30¹ alin.(1) din Legea nr.304/2004.

București, sediul Înaltei Curți de Casație și Justiție, 04 februarie 2022.

**Președintele
Înaltei Curți de Casație și Justiție
Judecător
CORINA-ALINA CORBU**