R O M Â N I A
ÎNALTA CURTE DE CASAŢIE ŞI JUSTIŢIE
CABINET PREŞEDINTE

Nr. 1302 din 30 august 2021

RAPORT
privind verificarea efectuată de președintele Înaltei Curți de Casație și Justiție în temeiul art.30[1] 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. 30[1] 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. 30^1 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 supravegherilor 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.(1^1) din Codul de procedură penală: „Pentru realizarea activităţilor prevăzute la art.138 alin.(1) lit. a)-d), procurorul, organele de cercetare penală sau lucrătorii specializaţi din cadrul poliţiei folosesc nemijlocit sistemele tehnice şi proceduri adecvate, de natură să asigure integritatea şi confidenţialitatea datelor şi informaţiilor colectate."

B. LIMITELE ȘI OBIECTIVELE VERIFICĂRII

Din interpretarea coroborată a dispozițiilor art.30^1 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 supravegherii 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 05.02.2021, în urma verificărilor, fiind formulate următoarele concluzii:

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, cadrul legislativ aplicabil a rămas stabil, asigurând funcționarea platformei partajate reprezentată de CNIC, în vederea punerii în aplicare a măsurilor de supraveghere tehnică constând în interceptarea comunicațiilor.

Sub aspect tehnic, rolul administratorului sistemului cu privire la toate aspectele ținând de funcționarea echipamentelor hardware și de aplicațiile tehnice folosite rămâne în continuare important, însă gradul de autonomie tehnică și tehnologică a structurilor specializate din cadrul parchetelor în raport cu administratorul sistemului crește în mod progresiv, pe măsură ce marile parchete sunt dotate cu echipamente adecvate și poate fi încadrat/specializat suficient personal pregătit pentru a prelua toate provocările de ordin tehnic pe care le ridică aceste activități. Această aspecte nu afectează însă punerea efectivă în executare a măsurilor de supraveghere tehnică, care se realizează de organele de urmărire penală în mod autonom, folosind infrastructura platformei unice partajate și, după introducerea datelor, în principal prin procese automatizate.

Din această perspectivă, trebuie urmărită dezvoltarea capacităților tehnice ale structurilor specializate ale parchetelor și încadrarea cu personal specializat suficient, astfel încât independența funcțională și operațională a organelor de urmărire penală în ceea ce privește aceste activități de obținere a probelor să fie dublată de o capacitate tehnică completă, indiferent dacă ea urmează să fie asigurată în cadrul fiecărui mare parchet în parte sau printr-o structură comună.

În perioada de referință a fost asigurată securitatea informatică a sistemelor, aplicațiilor informatice și fluxurilor de date specifice. Cu toate acestea, contextul internațional actual (caracterizat prin riscuri crescute legate de securitatea informatică și prin raportarea mai multor cazuri de acces neautorizat la date confidențiale sau de

colectare nelegală de date sau metadate în diferite scopuri) îndreptățește păstrarea și pe viitor a unui nivel ridicat de vigilență sub aceste aspecte.

CNIC a asigurat actualizarea echipamentelor și a aplicațiilor folosite prin raportare la evoluțiile tehnologice, în special noile tehnologii implementate de operatorii/furnizorii de servicii de comunicații și a asigurat asistență pentru parchetele beneficiare în ceea ce privește implementarea acestor modificări. Personalul Centrului Național de Interceptare a Comunicațiilor și persoanele care își desfășoară activitatea în cadrul structurilor speciale constituite în cadrul ÎCCJ, DNA și DIICOT au beneficiat de asistență și formare profesională pentru utilizarea adecvată a acestora. Este recomandat să se păstreze sincronizarea dintre ritmul de upgradare/modificare a echipamentelor și aplicațiilor folosite și acela privind instruirea personalului relevant (din cadrul unităților de parchet și CNIC), în vederea prevenirii oricărei forme de eroare umană în gestionarea sistemului.

Mecanismele automatizate de prevenire a erorilor sunt și trebuie să rămână dublate de forme de monitorizare cu intervenție umană, care să permită verificarea corectitudinii introducerii, colectării, exportării, transcrierii etc. datelor colectate, cu asigurarea confidențialității acestor operațiuni și cu respectarea principiului nevoii de a cunoaște în fiecare stadiu al operațiunilor.

Se impune ca monitorizarea corectitudinii operațiunilor efectuate de operatorii umani și modul de funcționare a proceselor automatizate să se facă într-o modalitate pro-activă, care să prevină posibilitatea apariției erorilor/avariilor, iar incidentele constatate, indiferent de natură (spre exemplu, eroare umană de introducere a datelor, avarie tehnică, bug-uri identificate în aplicațiile informatice dedicate etc.) să fie documentate în evidențe specifice, care să includă inclusiv modalitatea în care s-a intervenit în vederea soluționării incidentului respectiv.

La nivelul CNIC fluxurile de date aferente interceptărilor pentru care beneficiare sunt organele de urmărire penală sunt separate, niciunul dintre beneficiarii SNIC (inclusiv SRI) neputând vizualiza în sistem ”țintele” (sursa comunicațiilor monitorizate n.ns.) altor autorități și nici accesa conținutul sesiunilor interceptate în structurile proprii ale acestora.

La nivelul marilor unități de parchet datele interceptate la nivelul structurilor proprii sunt colectate, exportate și transcrise prin ofițeri de poliție judiciară proprii (neexistând nicio implicare din partea unor autorități terțe) și sunt puse doar la dispoziția organului de urmărire penală.

Din cauza numărului semnificativ de solicitări și ca urmare a caracterului limitat al resurselor materiale și umane disponibile la nivelul structurilor tehnice constituite în cadrul parchetelor, la nivel teritorial unele măsuri de supraveghere sunt puse în aplicare cu sprijinul structurilor Poliției Române (MAI), fiind necesar să existe proceduri uniforme și garanții adecvate privind securitatea cibernetică și respectarea dispozițiilor legale care reglementează relațiile dintre cele două instituții.

Nu au fost identificate în perioada de referință vulnerabilități în legătură cu depășirea atribuțiilor celor două părți semnatare ale Protocolului nr.9331/2440/C/2016, de natură a afecta dreptul de acces direct și independent al organelor de urmărire penală la sistemele tehnice în scopul executării supravegherii tehnice prevăzute la art.138 alin. (1) lit. a) din Codul de procedură penală.

Nu s-au înregistrat în perioada de referință petiții/sesizări privind deficiențe sistemice în ceea ce privește punerea în executare a măsurilor de supraveghere tehnică constând în interceptarea comunicațiilor, iar procedurile operaționale actuale apar drept compatibile cu respectarea principiilor legalității administrării probelor în procesul penal și al respectării drepturilor și libertăților fundamentale ale cetățenilor.

La nivelul percepției publice continuă să se manifeste unele preocupări legate de măsurile de supraveghere tehnică constând în interceptarea comunicațiilor, legate probabil atât de conotația negativă atașată acestor operațiuni încă din persioada regimului comunist, cât și de suspiciuni ridicate de-a lungul timpului cu privire la modul de valorificare a rezultatelor interceptării. Tocmai pentru că, într-un stat de drept, astfel de mijloace sunt simple mijloace de investigare a unor presupuse fapte penale, care pot fi folosite alături de alte mijloace probă și se dispun, respectiv se pun în executare, numai cu respectarea cerințelor prevăzute de lege, este esențială creșterea gradului de transparență și de informare a publicului cu privire la aspectele generale privind reglementarea și desfășurarea acestor operațiuni, în condiții de normalitate și de legalitate. Fără îndoială că asigurarea unui mai înalt grad de transparență trebuie conciliată cu caracterul secret al urmăririi penale și cu necesitatea protejării informațiilor ce pot avea caracter confidențial sau care ar fi susceptibile să afecteze cercetările penale, însă avem în vedere doar acele aspecte cu caracter absolut general, care însă să permită o evaluare corectă și o mai bună informare a opiniei publice cu privire la rolul acestor mijloace de investigare în cadrul procesului penal și asupra mecanismelor de control prevăzute de lege pentru garantarea legalității acestora.

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

(i) evaluarea permanentă a cadrului legislativ și operațional și a tuturor aspectelor care se impune a fi îmbunătățite la nivelul tuturor instituțiilor implicate și formularea propunerilor adecvate;

(ii) asigurarea unui înalt standard de securitate informatică în ceea ce privește echipamentele și aplicațiile informatice folosite pentru interceptare, precum și fluxurile comunicaționale securizate;

(iii) sincronizarea ritmului procedurilor de îmbunătățire și actualizare a echipamentelor și aplicațiilor informatice folosite cu posibilitatea formării personalului implicat cu privire la noile funcții introduse, modificarea procedurilor operaționale etc. În mod specific, nicio modificare nu ar trebui să

devină operațională înainte ca întreg personalul implicat să fie pregătit în mod adecvat pentru implementarea acesteia;

(iv) continuarea monitorizării modului în care funcționează instrumentele automatizate de limitare a greșelilor/derapajelor ce pot surveni în procesul de exploatare a aplicației informatice și dublarea acestora cu sisteme adecvate de verificare cu intervenție umană, în fiecare stadiu al procedurilor, cu respectarea principiului nevoii de a cunoaște, în special prin specializarea personalului cu privire la anumite operațiuni/activități;

(v) documentarea riguroasă a incidentelor, indiferent de natura acestora (ex. eroare de introducere a datelor, chiar dacă este semnalată ca atare de mecanismul automatizat de identificare a erorilor, avarie tehnică, funcționare anormală a aplicației informatice etc.), prin intermediul unei forme de registru de incidente, care să evidențieze și modalitatea de intervenție pentru remedierea acestuia;

(vi) continuarea procesului privind asigurarea resurselor materiale și umane necesare sub aspectul autonomiei tehnice a structurilor constituite în cadrul marilor parchete;

(vii) monitorizarea și, dacă este necesar, implementarea unor proceduri și a unui mod de lucru uniform la nivelul parchetelor teritoriale în cazul în care măsurile de supraveghere tehnică sunt puse în aplicare cu sprijinul structurilor specializate ale Poliției Române, iar nu prin structurile tehnice constituite la nivelul PÎCCJ, DNA, DIICOT;

(viii) creșterea gradului de transparență, la nivel public, în ceea ce privește toate aspectele generale relevante legate de măsura de supraveghere tehnică constând în interceptarea comunicațiilor.

D. DEFĂȘURAREA VERIFICĂRII ACTUALE

În raport cu concluziile și recomandările formulate prin raportul precendent, la data de 06.07.2021, s-au transmis Parchetului de pe lângă Înalta Curte de Casație și Justiție, Direcției Naționale Anticorupție, Direcției de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism și Serviciului Român de Informații solicitări privind transmiterea datelor relevante legate de perioada de referință 01.01.2021-30.06.2021, privind, în special, existența în perioada de referință a unor incidente de securitate informatică, asigurarea intruirii prealabile a personalului în condițiile upgradării echipamentelor/aplicațiilor informatice folosite, monitorizarea modului de funcționare a instrumentelor automatizate de limitare a erorilor, stabilitatea cadrului legislativ și operațional, asigurarea unui nivel adecvat de transparență pentru informațiile cu caracter general legate de aceste activități, existența unor proceduri operaționale unitare, precum și a unor garanții adecvate în situația punerii în executare

a măsurilor de supraveghere tehnică cu sprijinul structurilor Poliției Române (DOS), situația actuală privind resursele materiale și umane necesare pentru asigurarea autonomiei tehnice a structurilor specializate din cadrul marilor parchete, modul de documentare a incidentelor, existența unor plângeri, petiții, sesizări legate de modul desfășurare a activităților de interceptare etc.

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 perioada iulie-august 2021, și a discuțiilor purtate cu această ocazie cu persoane din conducerea acestor instituții și a structurilor cu caracter tehnic constituite în cadrul acestora.

D. 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 Infracțiunilor 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. În contextul procesului de consultare cu privire la *proiectul de Lege pentru modificarea și completarea unor acte normative în domeniul comunicațiilor electronice și pentru stabilirea unor măsuri de facilitare a dezvoltării rețelelor de comunicații electronice*, SRI-CNIC a formulat propuneri pentru sincronizarea cadrului legislativ la evoluțiile tehnologice, în special în ceea ce privește serviciile și tehnologiile inovatoare de comunicații, precum WEB HOSTING.

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).

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 stabileşte, în baza Legii nr.14/1992, modalitatea tehnică de cooperare între instituţiile anterior menţionate și asigură, potrivit dispozițiilor art.12 din respectivul act, și accesul Direcției Naționale Anticorupție, respectiv al Direcției de Investigare a Infracțiunilor 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, 01.01.2021-30.06.2021, 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 Protocol, accesul Parchetului de pe lângă Înalta Curte de Casație și Justiție, al Direcției Naționale Anticorupție, respectiv al Direcției de Investigare a Infracțiunilor 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 executarea 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.

Se impune totuși remarca că, în condițiile unor resurse materiale (în special sisteme informatice specifice, rețele interne și mijloace de comunicație și de transmitere a datelor securizate etc.) și umane limitate, structurile specializate constituite în cadrul marilor unități de parchet (PÎCCJ, DNA, 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 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. În cazul Direcției Naționale Anticorupție, măsurile de supraveghere tehnică sunt puse în aplicare prin intermediul Serviciului Tehnic, 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 beneficiare;

- 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 conținutul 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, pentru mandatele de supraveghere prevăzute de Legea 51/1991, care, în limitele prescrise de art.30[1] din Legea nr.304/2004, 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.

2. **Asigurarea securității sistemelor și prevenirea eventualelor erori**

În perioada de referință nu au fost incidente de securitate informatică cu privire la sistemele Centrului Național de Interceptare a Comunicațiilor (CNIC) sau ale autorităților judiciare beneficiare.

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 - (care are în componență doar echipamentele de mediere ale operatorilor de comunicații, echipamentele de interceptare și beneficiarii SNIC), 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.

Prin intermediul noii versiuni a aplicației HelpDesk (de semnalare și rezolvare a disfuncționalităților de natură tehnică survenite la nivelul echipamentelor sau al rețelei de interceptare), operaționalizată începând cu data de 01.03.2021 la nivelul tuturor beneficiarilor externi conectați la SNIC, au fost implementate optimizări ale funcției de jurnalizare (logarea numărului și a duratei deranjamentelor). Totodată, în perioada de referință s-au realizat upgrade-uri cu privire la procedura de marcare a țintei unice, precum și optimizări privind sistemul iSigma și comunicațiile de tip roaming.

În perioada de referință, procedurile operaționale și mecanismele automate de prevenire a erorilor au fost monitorizate constant, având o eficiență crescută în limitarea erorilor umane. S-a efectuat monitorizarea și auditarea periodică a stării de securitate a sistemelor și instrumentelor folosite, atât la nivel fizic, cât și la nivelul aplicațiilor informatice dedicate. Niciuna dintre marile unități de parchet consultate nu a semnalat erori umane/greșeli în procesul de exploatare a aplicațiilor informatice.

La nivelul CNIC nu au fost înregistrate la nivelul sistemului tehnic de interceptare incidente de natură tehnică cu impact asupra activității de interceptare, iar, în contextul intensificării demersurilor de cooperare cu structurile conectate la serviciile și resursele SNIC, au fost stabilite și puse în aplicare reguli clare cu privire la procesul de identificare și implementare a criteriilor de interceptare, care au limitat semnificativ situațiile de implementare eronată a țintelor. Erori operaționale au fost semnalate de către CNIC doar în situații punctuale, fiind corectate cu operativitate și neavând impact semnificativ asupra procesului de punere în aplicare a actelor de interceptare a comunicațiilor.

Siguranța în operare a sistemului este garantată prin caracterul eminamente automatizat al acestuia, orice eroare detectată fiind semnalizată în cadrul aplicațiilor dedicate. Erorile în procesul de marcare/exploatare, inclusiv introducerea de către

utilizatori în sistemele informatice a unor date eronate sunt prevenite/limitate prin intrumente automatizate de limitare a erorilor materiale, în perioada de referință astfel de erori survenind 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. Mecanismele automatizate de corecție sunt dublate prin monitorizare umană(PÎCCJ), prin intermediul șefului serviciului tehnic specializat, precum și prin ofițerii de poliție judiciară în ale căror atribuțiuni de serviciu se regăsește validarea și respectiv verificarea datelor introduse anterior în sistem de către lucrătorul care a îndeplinit această sarcină la prelucrarea datelor din actul de autorizare sau în procedura de marcare.

S-au înregistrat progrese semnificative față de perioada de referință precedentă în ceea ce privește documentarea riguroasă a incidentelor operaționale (avarie tehnică, funcționare anormală a aplicației informatice etc) la nivelul structurilor tehnice specializate din cadrul parchetelor, atât prin implementarea noii versiuni a aplicației HELP DESK, care înregistrează automat incidentele care pot apărea (DNA), cât și prin implementarea unor bune practici proprii sub aceste aspecte, spre exemplu, prin crearea unui registru special (PÎCCJ), în care se consemnează, prin proces-verbal întocmit de către lucrătorul de poliție judiciară, orice dificultate apărută în procesul de punere în aplicare a unei măsuri de supraveghere tehnică. Mai mult, DIICOT a implementat în perioada de referință un sistem preventiv de monitorizare și de prevenire a incidentelor, prin crearea unui 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 (inclusiv posibile vulnerabilități/erori umane în gestionarea sistemului), dublat de controale periodice, bilunare, privind securitatea și integritatea fizică, modul de funcționare a sistemelor informatice și apariția oricărui incident în funcționarea sistemelor și aplicațiilor informatice.

Având în vedere caracterul restrictiv de drepturi al măsurilor de supraveghere tehnică, care impune maximă rigoare în privința modului de punere în aplicare a acestora, apare ca recomandabil ca bunele practici adoptate de către unele mari unități de parchet și descrise mai sus să fie extinse ca standard operațional pentru toate structurile tehnice specializate implicate în procesul de punere în aplicare a măsurilor de supraveghere tehnică.

3. 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, în special în raportul privind semestrul al II-lea 2020, prin care s-a efectuat o descriere succintă a mecanismelor prin care se asigură separarea fluxurilor de date la nivelul CNIC, astfel încât datele interceptate să fie 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.

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.

Folosirea platformei partajate (utilizarea aceloraşi echipamente tehnice , dar cu separarea riguroasă a fluxurilor de date) reprezintă o soluție care și-a dovedit eficiența în perioada scursă de la înființarea CNIC și care prezintă avantajul că permite valorificarea la maxim a resurselor tehnice și umane disponibile (specialiștii IT), în condițiile caracterului inevitabil limitat al acestor resurse, precum și asigurarea unui înalt nivel de securitate cibernetică.

În perioada de referință nu au fost constatate nici incidente tehnice semnificative și nici situații de acces neautorizat în sistem, gradul de stabilitate și securizare a sistemelor fiind astfel corespunzător.

Pe parcursul perioadei de referință se constată o creștere a capacității tehnice a structurilor specializate din cadrul marilor parchete, în special în contextul bunei

cooperări între acestea și cu administratorul platformei partajate, prin implementarea de noi facilități privind documentarea și prevenirea avariilor tehnice și erorilor, crearea/preluarea la nivelul parchetelor de bune practici privind prevenirea oricăror erori de operare și creșterea, la nivel general, a gradului de transparență în ceea ce privește furnizarea unor date generale, de interes public, cu privire la activitățile de interceptare.

4. Asigurarea resurselor necesare și a pregătirii continue a personalului implicat

Conform aprecierii Parchetului General, deși cadrul tehnic și legislativ actual asigură accesul nemijlocit și independent al organelor de urmărire penală la sistemele tehnice în scopul punerii în executare a măsurii prevăzute de art.138 alin.1 lit.a C.p.p., permițând punerea în aplicare a acestei măsuri în mod direct, prin personalul propriu care utilizează echipamentele tehnice deținute de parchet, autonomia tehnică a marilor parchete în materie de interceptare a comunicațiilor este condiționată de intervenția organelor legislative în vederea revizuirii dispozițiilor care reglementează obligațiile furnizorilor de rețele publice de comunicații electronice sau furnizorii de servicii de comunicații electronice destinate publicului, atribuțiile instituțiilor aflate în relație cu aceștia, precum și resusele logistice, umane și financiare alocate.

Cu referire specială la resursele umane, se constată că la nivelul tuturor celor trei mari parchete schemele de personal ale structurilor tehnice au rămas constante în perioada de referință, ceea ce a permis desfășurarea în condiții corespunzătoare a activităților tehnice specifice. Cu toate acestea, în special la nivelul DIICOT rezultă din datele furnizate situații de supraîncărcare a ofițerilor de poliție judiciară detașați în cadrul Biroului tehnic și de criminalistică, în raport cu volumul de activitate și cu complexitatea activităților tehnice și operaționale desfășurate, context în care conducerea DIICOT a reluat demersurile pentru detașarea unui număr suplimentar de specialiști. Se impune remarca că DIICOT este unitatea de parchet specializată pentru cercetarea unui important număr de infracțiuni al căror specific impune de obicei folosirea mijloacelor de supraveghere tehnică – infracțiunile săvârșite prin sisteme informatice, infracțiuni împotriva siguranței naționale etc. În al doilea rând, situația impusă de pandemia de COVID-19 a provocat un proces de digitalizare la nivel mondial și în toate domeniile vieții sociale, iar, ca urmare imediată, necesitatea consolidării capacităților tehnice și încadrarea cu un număr adecvat de specialiști a devenit evidentă la nivelul tuturor agențiilor judiciare și polițienești, la nivel mondial.

În acest context, apare drept vitală pentru desfășurarea în continuare, în bune condiții, a anchetelor judiciare care implică măsuri de supraveghere tehnică, asigurarea resurselor necesare pentru consolidarea autonomiei juridice și tehnice a marilor

parchetele și la nivel operațional, prin asigurarea echipamentelor necesare, precum și a numărului corespunzător de specialiști IT sau de ofițeri/agenți de poliție judiciară.

Se remarcă că din datele furnizate de către toate marile parchete, precum și de CNIC, punerea în executare a unei părți dintre măsurile de supraveghere tehnică (în special de către parchetele teritoriale) cu asistența structurilor tehnice specializate ale Poliției Române (D.O.S.) presupune respectarea acelorași garanții tehnice, procedurale și de securitate informatică, aceasta fiind impusă tocmai de volumul ridicat de activitate la nivelul structurilor tehnice de la nivel central. În cadrul verificărilor aferente următorului raport semestrial urmează ca structura tehnică din cadrul M.A.I. să facă obiectul unei vizite de documentare similare celei efectuate la nivelul celorlalți beneficiari judiciari ai CNIC.

Sub aspectul instruirii corespunzătoare a personalului implicat și în contextul recomandării formulate sub acest aspect prin raportul precedent, se constată că administratorul sistemului a asigurat în bune condiții pregătirea prealabilă a personalului angrenat în activități de punere în executare a măsurilor de interceptare, cu ocazia fiecărei actualizări a procedurilor operaționale folosite sau a upgradării sistemelor/aplicațiilor software. Pe lângă implementarea actualizărilor procedurale în aplicațiile specifice și transmiterea documentației actualizate, în cazul schimbărilor cu impact semnificativ, CNIC transmite prin circulară tuturor beneficiarilor principalele elemente tehnice cu caracter de noutate. De asemenea, prin noua versiune a aplicației HELPDESK, implementată la nivelul tuturor beneficiarilor a fost optimizată funcționalitatea de jurnalizare.

Instruirea ofițerilor de poliție judiciară din cadrul structurilor tehnice specializate ale marilor parchete a fost asigurată, în prealabil implementării unor modificări/upgrade-uri, atât prin comunicarea în scris a datelor de interes, cât și în mod direct, de către reprezentanții CNIC. Informările, notificările și instrucțiunile privind actualizările echipamentelor/aplicațiilor sunt furnizate permanent și prompt de către CNIC.

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 în ceea ce privește punerea în executare a măsurilor de supraveghere tehnică la cererea organelor judiciare, relațiile instituționale desfășurându-se în condiții foarte bune. Cadrul legislativ și operațional a rămas stabil.

6. Petiții/sesizări privind disfuncții în activitatea de punere în aplicare a măsurilor de supraveghere tehnică. Creșterea gradului de transparență din perspectiva furnizării unor informații de interes public

În perioada de referință nu s-au primit la nivelul marilor parchete petiții sau sesizări privind disfuncții în activitățile de punere în aplicare a măsurilor de supraveghere tehnică dispuse de organele de urmărire penală. Legalitatea mijloacelor de probă obținute prin folosirea măsurilor de supraveghere tehnică este cenzurată, în fiecare caz în parte, după caz, de către judecătorul de cameră preliminară sau de instanța judecătorească.

În raport și cu recomandările prevăzute în raportul precedent, în perioada de referință se remarcă o creștere a gradului de transparență privind informațiile de interes general legate de activitățile de interceptare a comunicațiilor, cu păstrarea confidențialității asupra aspectelor care ar putea permite eventual contracarea acestor tehnici speciale de investigare. Spre exemplu, Parchetul General pune la dispoziția societății, cu ocazia publicării raportului anual de activitate, informații generale privind supravegherea tehnică, însă fără detalii privind categoriile de infracțiuni, în principal ca urmare a faptului că Regulamentul de ordine interioară al parchetelor nu prevede colectarea acestor date. La rândul său, Direcția Națională Anticorupție furnizează publicului informații de interes general, neclasificate, privind modul de punere în aplicare a măsurilor de supraveghere tehnică în rapoartele anuale de activitate ale instituției. La nivelul Biroului tehnic și de criminalistică din cadrul DIICOT sunt întocmite lunar statistici neclasificate privind diferite elemente ce pot prezenta interes general – numărul măsurilor de supraveghere tehnică autorizate (defalcat măsuri autorizate de judecătorul de drepturi și libertăți și ordonanțe provizorii emise de procuror), tipul măsurilor de supraveghere tehnică autorizate etc.

Deși, din perspectiva bunei desfășurări a anchetelor penale, rezerva marilor parchete de a furniza informații privind activitățile de interceptare este desigur legitimă, trebuie făcută o distincție netă între informațiile prejudiciabile pentru folosirea în bune condiții a acestor tehnici de investigare și informațiile statistice, cu caracter general, care pot prezenta interes din perspectiva dreptului de ”control” al societății cu privire la activitatea oricăror entități publice. Mai mult, diversificarea și augmentarea conținutului datelor statistice furnizate, precum și, poate, folosirea unor modalități de aducere la cunoștință publică mai sintetizate și cu o mai mare peridiciotate decât un raport de activitate ar servi la creșterea gradului de încredere al publicului în activitatea judiciară și la contracararea mesajelor încă existente în spațiul public privind caracterul ”ocult” a unor astfel de mijloace de obținere a probelor. Este important ca societății să i se ofere suficiente informații pentru a percepe interceptarea comunicațiilor drept ceea ce este aceasta într-un stat de drept – un mijloc de obținere a probelor folosit atunci și numai atunci când este necesar pentru documentarea unor presupuse activități infracționale, în funcție de circumstanțele concrete ale fiecărei cauze în parte (natura

infracțiunii cercetate, modalitatea de săvârșire, imposibilitatea documentării consecințelor acesteia în altă modalitate etc. constituind elemente obiective care pot conduce la necesitatea folosirii acestor mijloace de anchetă).

În acest context, considerăm că ar putea fi examinate și la nivelul conducerilor celorlalte mari parchete bunele practici implementate la nivelul DIICOT privind diversificarea și ritmicitatea generării de rapoarte statistice privind aceste activități.

E. CONCLUZIILE VERIFICĂRII

Pe baza verificărilor directe efectuate de către președintele ÎCCJ 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 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, 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.

În raport și de recomandările din raportul precedent, se remarcă creșterea rigurozității în materia jurnalizării(documentării) incidentelor (avarii tehnice, introducere 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 special prin intermediul rapoartelor de activitate. 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, ar putea fi generalizate bune practici precum cele implementate în perioada de referință la nivelul DIICOT.

F. 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 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.

G. MĂSURI

Prezentul Raport este întocmit în 5 exemplare și se comunică Serviciului Român de Informații, Parchetului de pe lângă Înalta Curte de Casație și Justiție, Direcției Naționale Anticorupție, precum și Direcției de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism.

Potrivit dispozițiilor art. 30^1 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 01.07.2021-31.12.2021, în acord cu dispozițiile art.30^1 alin.(1) din Legea nr.304/2004.

București, sediul Înaltei Curți de Casație și Justiție, 30 august 2021

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