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

Nr. 1314 din 14 august 2020

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 08.01.2020, fiind formulate următoarele *concluzii*:

Serviciul Român de Informații, în calitate de administrator unic al Centrului Național de Interceptare a Comunicațiilor, asigură cadrul tehnic necesar accesului nemijlocit 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, în condițiile în care, în urma verificărilor efectuate, președintele Înaltei Curți de Casație și Justiție a constatat următoarele aspecte:

- punerea în aplicare a măsurilor de supraveghere dispuse în procesul penal se realizează de fiecare autoritate judiciară în mod autonom, exclusiv prin personal propriu, direct, nemijlocit și independent, prin intermediul echipamentelor tehnice terminale pe care le deține și le utilizează în sediile proprii;

- organele judiciare nu desfășoară niciun fel de activitate specifică procedurii de punere în aplicare a măsurilor de interceptare a comunicațiilor la sediul Centrului Național de Interceptare a Comunicațiilor;

- în baza datelor conținute în actul de autorizare a interceptării pe care autoritatea judiciară le introduce în aplicațiile informatice, conținutul brut al comunicației este înregistrat, extras și transferat, în mod automatizat de la operatorul de comunicații în sistemul de stocare administrat de Centrul Național de Interceptare a Comunicațiilor, respectiv către beneficiari, fără posibilitatea vreunei intervenții umane din partea personalului Centrului pe fluxul de interceptare;

- comunicațiile sunt interceptate în condițiile și limitele cuprinse în actul de autorizare, astfel cum acestea au fost introduse în aplicațiile informatice de către autoritatea judiciară, căreia îi revine competența exclusivă de punere în aplicare a măsurilor de supraveghere; datele se stochează pe serverul general în formă criptată, pentru o perioadă limitată de timp, sunt expediate, în sistem complet automatizat, organului judiciar beneficiar, apoi sunt distruse automat;

- tehnic nu există posibilitatea înregistrării peste durata mandatului emis de judecător pentru că sistemul se închide automat la împlinirea termenului limită dispuse prin actul de autorizare. În ipoteza în care a existat o eroare la introducerea datelor în rețea, există un sistem automat de corectare a datelor, conform mandatului emis;

- sistemul informatic este conceput de așa natură încât să asigure ștergerea automată și ireversibilă a interceptărilor, ce sunt transmise în format criptat pe echipamentele proprii ale autorităților judiciare beneficiare;

- sistemul este configurat astfel încât să asigure pornirea și oprirea automată a interceptărilor la data și ora indicate în actul de autorizare, precum și imposibilitatea

ștergerii sau modificării de către operatorii de redare a conținutului unei convorbiri interceptate sau a altor date aferente acestora;

- Centrului Național de Interceptare a Comunicațiilor din cadrul Serviciului Român de Informații îi revin exclusiv atribuții specifice administratorului unic al sistemului, în sensul că: (i) stabilește procedurile și politicile de securitate ale rețelei locale instalate în spațiile proprii ale Ministerului Public și acordă sprijin și suport tehnic pentru buna funcționare a acestuia; (ii) oferă suport tehnic pentru instalarea și exploatarea echipamentelor tehnice și aplicațiilor informatice dedicate, precum și pentru soluționarea dificultăților tehnice ivite în această procedură total automatizată;

- personalul Centrului Național de Interceptare a Comunicațiilor: (i) nu interferează pe fondul activității autorităților judiciare de operare și gestionare a măsurilor de interceptare a comunicațiilor dispuse prin actele de autorizare emise în condițiile legii; (ii) nu are acces la conținutul comunicațiilor transferate automat de la operatorii de comunicații în sistemul de stocare administrat de Centrul Național de Interceptare a Comunicațiilor; (iii) nu are acces pe fluxul de interceptare în procesul tehnic de extragere și transferare către autoritatea judiciară beneficiară a traficului de voce și date interceptat;

- legăturile de comunicații dintre Centrul Național de Interceptare a Comunicațiilor din cadrul Serviciului Român de Informații și Parchetul de pe lângă Înalta Curte de Casație și Justiție, Direcția Națională Anticorupție, respectiv Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism, pe fondul accesului nemijlocit și independent la sistemele tehnice de interceptare, se desfășoară în limitele stabilite prin Protocolul nr.9331/2440/C/2016, încheiat în baza art. 8 alin.(3) din *Legea nr. 14/1992;*

- nu au fost identificate la acest moment 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*.

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

(i) acordarea unei atenții deosebite atât pregătirii profesionale a personalului specializat din cadrul celor trei autorități judiciare, cât și procedurilor operaționale menite a limita pe cât posibil erorile umane ce pot surveni în gestionarea aplicației;

(ii) efectuarea unei auditări periodice a modului în care sunt respectate instrumentele automatizate de limitare a greșelilor/derapajelor ce pot surveni în procesul de exploatare a aplicației informatice;

(iii) menținerea unor înalte standarde de securitate informatică la nivelul Centrului Național de Interceptare a Comunicațiilor, inclusiv prin efectuarea unor operațiuni de auditare internă permanentă a sistemului;

(iv) evaluarea permanentă a modului de funcționare a compartimentelor specializate prin raportare la cele mai înalte standarde de rigoare impuse de exploatarea și actualizarea aplicației informatice.

D. DEFĂȘURAREA VERIFICĂRII

În raport cu concluziile și recomandările formulate prin raportul precedent, la data de 30.07.2020, 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 01.01.2020-30.06.2020, privind, în special, monitorizarea și auditarea procedurile operaționale instituite la nivelul Centrului în vederea eliminării/limitării posibilității apariției unor erori umane în gestionarea aplicațiilor informatice folosite, dacă au fost constatate astfel de incidente în activitatea Centrului și, în caz afirmativ, modul în care acestea au fost gestionate și dacă s-au implementat măsurile necesare pentru evitarea recurenței acestora; evaluarea eficienței instrumentelor automatizate de limitare a erorilor în procesul de utilizare a aplicației informatice și dacă s-a constatat că acestea sunt efectiv apte să prevină astfel de incidente; asigurarea securității informatice a sistemelor utilizate în activitatea Centrului Național pentru Interceptarea Comunicațiilor; măsurile luate în perioada de referință sau cu caracter permanent pentru formarea profesională continuă a personalului implicat în activitatea Centrului, precum și privind instruirea personalului (lucrători de poliție judiciară) din cadrul structurilor special create în cadrul PÎCCJ, DNA și DIICOT; modul de desfășurare a relațiilor instituționale dintre organele de urmărire penală și Centru și eventualele dificultăți întâmpinate; dacă protocoalele prevăzute la art.8 alin.(3) din Legea nr.14/1992 (strict cu referință la organele judiciare) au suferit revizuiri în perioada de referință și, în caz afirmativ, o scurtă descriere a motivelor care au impus modificarea acestora; aprecierea organelor de urmărire penală beneficiare cu privire la modul de funcționare a sistemelor și procedurilor care asigură punerea în executare a măsurilor de supraveghere tehnică și dacă este asigurată cerința impusă de Curtea Constituțională ca administrarea probelor să fie asigurată exclusiv de persoane care au calitatea de organe de urmărire sau de cercetare penală; orice alte chestiuni relevante din perspectiva obiectului verificărilor prevăzute de lege.

Pentru a se asigura contextul complementar și non-repetitiv al verificărilor efectuate de către președintele Înaltei Curți și, având în vedere și contextul creat de pandemia de COVID-19, prezentele verificări au avut drept obiective principale evaluarea modului de funcționare în concret a aplicațiilor informatice folosite în legătură cu activitatea Centrului Național pentru Interceptarea Comunicațiilor, separarea și administrarea autonomă de către organele de urmărire penală a fluxurilor de date generate de punerea în aplicare a unor măsuri de supraveghere tehnică și asigurarea securității acestuia (din punct de vedere al garantării securității informatice a sistemelor, a prevenirii posibilității intervenirii unor erori umane în gestionarea acestora, a folosirii unor mecanisme informatice automatizate de prevenție și din perspectiva formării continue

a personalului implicat), precum și stabilitatea și respectarea cadrului legal, primar și derivat, care reglementează organizarea generală a acestor activități tehnico-judiciare. În cadrul verificărilor care vor privi semestrul al doilea 2020 urmează a se reexamina în mod direct modul de organizare și de funcționare a structurilor specializate și a Centrului, care au făcut obiectul raportului precedent, prin vizite desfășurate la sediul Centrului și la sediile celor trei mari unități de parchet menționate.

E. CONSTATĂRILE VERIFICĂRII

Având în vedere aspectele constatate anterior, 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, din cadrul căruia își desfășoară activitatea Centrul Național de Interceptare a Comunicațiilor, precum și dispozițiile legale incidente în materie, au rezultat următoarele:

1. Cadrul legal și procedurile operaționale

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 stabilește, 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, 01.01.2010-30.06.2020, 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.

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 a patru autorități de interceptare, trei fiind administrate și utilizate de către autoritățile judiciare, și cea de-a patra de către Serviciul Român de Informații.

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 cele trei autorități judiciare și nici Serviciul Român de Informații nu poate să vizualizeze ori să acceseze operațiunile efectuate de una dintre celelalte autorități.

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, atât cu privire la amenințări informatice specifice, cât și pentru prevenirea posibilității intervenirii unor erori umane**

În perioada de referință nu au fost semnalate incidente generate de erori umane în gestionarea aplicațiilor informatice destinate punerii în executare a activității de interceptare și înregistrare a comunicațiilor, nici la nivelul Centrului Național de

Interceptare a Comunicațiilor și nici la nivelul instituțiilor de parchet beneficiare. Conform informațiilor furnizate de marile parchete, procedurile operaționale aplicabile sunt permanent monitorizate, în vederea prevenirii apariției erorilor umane.

De altfel, riscul apariției unor erori umane în gestionarea aplicațiilor informatice utilizate a fost diminuat ca urmare a upgrade-urile hardware/software aplicate unor componente ale Sistemului Național de Interceptare a Comunicațiilor, integrarea unor noi soluții tehnice puse la dispoziție de operatorii de telecomunicații abonaților lor și actualizarea procedurilor operaționale instituite la nivelul CNIC. Astfel, a fost modificată și simplificată procedura de marcare a criteriilor de interceptare în centralele unui furnizor de servicii de telefonie mobilă, având ca efect reducerea timpului alocat acestui proces și creșterea siguranței în utilizarea aplicației. La solicitarea beneficiarilor, CNIC derulează un proiect care va permite simplificarea considerabilă a procesului de marcare în sistemul integrat de interceptare și înregistrare voce-date.

Pe de altă parte, în procesul de utilizare curentă a aplicațiilor informatice specifice s-a constatat că instrumentele automate de limitare a erorilor, completate cu măsuri procedurale, sunt apte să prevină producerea unor incidente pe zona restrângerii drepturilor și libertăților cetățenești (astfel, aplicația a semnalat eventuale neconcordanțe cuprinse în actul de autorizare, precum cele referitoare la necorelarea duratei pentru care s-a emis mandatul și data indicată ca fiind ultima zi de interceptarea sau erori materiale privind numărul de cifre dintr-un număr de telefon – suplimentarea sau lipsa uneia dintre acestea – PÎCCJ). În cadrul unităților de parchet, mecanismele automatizate sunt dublate de proceduri operaționale care să prevină posibilitatea apariției erorilor umane, existând, spre exemplu, procedeul dublei verificări a datelor introduse în sistemul informatic (DIICOT). Aplicația informatică folosită pentru punerea în executare a actelor de autorizare a folosirii măsurilor de supraveghere tehnică presupune etapizarea procesului, participarea mai multor persoane la implementarea datelor, unele având rolul verificării introducerii datelor de către operatorul anterior și avertizează utilizatorul în situațiile în care apar erori (PÎCCJ). Aplicația nu permite efectuarea interceptării comunicațiilor peste durata prevăzută în mandat, sistemul oprindu-se automat la expirarea duratei acestora, nu acceptă intervale mai mari decât durata maximă prevăzută în Codul de procedură penală și generează așa-numite coduri de integritate pentru a preveni intervenția asupra conținutului unei comunicări, întreg fluxul de date fiind criptat.

Niciuna dintre marile unități de parchet nu a semnalat cazuri de eroare umană în gestionarea aplicațiilor informatice specifice în perioada de referință.

În perioada de referință a fost asigurată securitatea și integritate sistemelor informatice folosite în raport cu amenințările informatice specifice, nefiind înregistrate incidente de securitate informatică. CNIC a asigurat actualizarea politicilor și a procedurilor de securitate și protecție ce trebuie implementate pe terminalele și echipamentele din compunerea rețelelor locale constituite în spațiile organelor

judiciare care pun în aplicare mandate de supraveghere tehnică, conectate la CNIC, iar la data de 02.06.2020 au fost transmise tuturor instituțiilor beneficiare *Procedurile de securitate și protecție*, conținând regulile de securitate privind rețelele informatice și de comunicații și reguli de securitate privind stațiile de lucru. Punerea în aplicare efectivă a acestor reguli de securitate informatică și tehnică s-a realizat prin analize comune CNIC-instituții beneficiare, în care a fost evaluat nivelul de conformare la aceste reguli și au fost stabilite măsurile care sunt necesare în continuare.

În cadrul compartimentelor constituite în cadrul marilor unități de parchet s-au luat măsuri de securizare a sistemelor față de orice intruziune sau accesare neautorizate, fiind monitorizate spațiile de lucru și folosite soluții informatice corespunzătoare. Se utilizează o infrastructură folosită cu respectarea principiilor de separare a rețelelor și resurselor de calcul și de stocare existente, existența unor reguli de acces ferme și clare, se asigură inspecția traficului prin sisteme de prevenire și detectare a intruziunilor, protecție la vulnerabilități, scanare anti-malware și acordarea de permisiuni de operare având ca setare implicită principiul celor mai mici drepturi.

3. **Asigurarea pregătirii continue a personalului implicat și respectarea limitelor impuse de lege și de conținutul autorizației care stă la baza interceptării**

În perioada de referință s-a asigurat formarea și perfecționarea personalului implicat în administrarea sistemelor informatice și utilizarea aplicațiilor informatice specifice, în vederea asigurării de cunoștințe tehnice și operaționale actualizate, care să permită buna funcționare a sistemelor și asigurarea securității fluxurilor de date. Acestea s-au materializat în activități de instruire a personalului, la sediile structurilor de urmărire penală, cu privire la utilizarea noilor aplicații software implementate, furnizarea documentațiilor necesare pregătirii continue, organizarea unui curs online (webinar) pentru instruirea cu privire la unele facilități tehnice nou implementate, în luna mai 2020 și acordarea de asistență tehnică de către CNIC la solicitarea beneficiarilor. De asemenea, în luna iunie 2020 s-a desfășurat o reuniune la sediul PÎCCJ având ca obiect implementarea și dezvoltare procedurilor de securitate informatică.

4. **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**

Relația interinstituțională dintre unitățile de parchet beneficiare și CNIC s-a derulat cu respectarea limitelor de competență și a cerinței de asigurare a confidențialității operațiunilor efectuate (PÎCCJ).Nu au fost semnalate dificultăți sau disfuncții în ceea ce privește punerea în aplicare a solicitărilor formulate, în conformitate cu legea, de către organele judiciare. Conform datelor comunicate de către instituțiile beneficiare, asistența tehnică pentru remedierea deranjamentelor tehnice a fost acordată cu operativitate, iar organele judiciare au fost anunțate în prealabil în situațiile care au

necesitat oprirea temporară a unor echipamente sau aplicații pentru operațiuni de upgrade sau mentenanță.

Relațiile interinstituționale cu CNIC au fost apreciate pozitiv și de marile unități de parchet beneficiare, acestea arătând că a existat o preocupare permanentă a personalului Centrului în ceea ce privește rezolvarea dificultăților de ordin tehnic apărute și asigurarea exploatării optime a echipamentelor disponibile. De asemenea, soluțiile tehnice implementate și dezvoltate au creat posibilitatea ca, în mod complet autonom, autoritatea judiciară să gestioneze și să utilizeze un flux propriu de acces la sistemul tehnic de interceptare.

În cadrul unităților de parchet au fost constituite compartimente specializate, încadrate cu lucrători de poliție judiciară detașați, iar activitatea se efectuează prin intermediul echipamentelor tehnice terminale, care sunt independente de CNIC, permițând accesul autonom la fluxul de informații supuși interceptării. Lucrătorii de poliție judiciară sunt delegați de către organul de urmărire penală pentru a pune în executare măsurile de supraveghere tehnică, prin introducerea datelor necesare, cu respectarea limitelor trasate în mandatul de interceptare emis de judecător, în aplicațiile informatice dedicate. Lucrătorii de poliție judiciară întocmesc procesul verbal ce constituie mijloc de probă și demonstrează efectiv punerea în executare a măsurii de supraveghere tehnică prevăzută de art.138 alin.(1) lit.a C.p.p.. Conținutul brut al datelor ce au fost colectate ca urmare a măsurii tehnice autorizate de judecător este primit în format criptat, pe echipamentele proprii ale unităților de parchet, iar activitatea de fixare a traficului (sesiuni voce/date) este realizată tot de lucrători de poliție judiciară din cadrul structurilor specializate ale parchetelor. Toate unitățile de parchet consultate au apreciat că procedurile tehnico-operaționale actuale exclud posibilitatea participării vreunor persoane care nu au calitatea de organe de urmărire penală, iar accesul la datele colectate este autonom și actualizat.

F. CONCLUZIILE VERIFICĂRII

În urma verificărilor efectuate, președintele Înaltei Curți de Casație și Justiție constată că, în perioada de referință 01.06.2020-30.06.2020, nu au intervenit elemente noi care să conducă la reconsiderarea concluziilor din raportul dat publicității în luna ianuarie 2020.

Cadrul legislativ și tehnic actual asigură accesul direct și nemijlocit al organelor de urmărire penală la comunicațiile interceptate, iar activitățile specifice de urmărire penală se derulează doar de către personal din cadrul organelor judiciare.

A fost asigurată securitatea informatică a sistemelor și aplicațiilor informatice folosite, iar personalul Centrului Național de Interceptare a Comunicațiilor și persoanele care își desfășoară activitatea în cadrul structurilor speciale constituite în cadrul PÎCCJ, DNA și DIICOT au beneficiat de asistență și formare profesională pentru utilizarea adecvată a acestora.

Din datele existente nu rezultă că ar fi avut loc incidente de securitate informatică, iar mecanismele, automatizate și/sau operate uman, de prevenire a erorilor de introducere a datelor și de asigurare a accesului la datele colectate strict pentru durata și în limitele autorizației de interceptare apar la acest moment a fi eficiente.

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.

Procedurile operaționale examinate în raportul anterior nu au suferit modificări și sunt compatibile cu respectarea principiile legalității administrării probelor în procesul penal și al respectării drepturilor și libertăților fundamentale ale cetățenilor.

La nivelul comunicării din spațiul public continuă să se manifeste preocupare privind modul de punere în aplicare a măsurii de supraveghere tehnică privind interceptarea comunicațiilor sau cu privire la posibilitatea efectuării unor astfel de operațiuni în mod fraudulos, fără autorizarea judecătorului. Din această perspectivă, este esențial ca toate instituțiile implicate să asigure accesul cetățenilor la informații cu caracter general privind modul de desfășurare și principiile aplicabile acestor operațiuni tehnico-juridice (imposibilitatea efectuării de interceptări în lipsa autorizării acestora conform legii, separarea fluxurilor de date astfel încât doar organele de urmărire penală să aibă acces la datele colectate în baza măsurilor de supraveghere tehnică prevăzute în Codul de procedură penală, instruirea personalului și mijloacele tehnice care garantează respectarea limitelor trasate prin mandat, necesitatea desfășurării acestor activități de investigare cu respectarea drepturilor fundamentale ale persoanelor vizate etc.).

Aspectele punctuale, privind legalitatea administrării probelor (în speță, a celor rezultate ca urmare a măsurilor de supraveghere tehnică) într-un dosar de urmărire penală exced din punct de vedere legal obiectului verificărilor efectuate de către președintele Înaltei Curți de Casație și Justiție, care se referă la reglementările, procedurile și acțiunile cu caracter general, fiind atributul exclusiv al judecătorului de cameră preliminară ori, după caz, al instanței de judecată.

G. RECOMANDĂRI

Chiar dacă nu au fost identificate deficiențe, în vederea respectării principiului legalității și menținerii unui standard ridicat de protecție a drepturilor și libertăților fundamentale ale cetățenilor, cu privire la care măsurile de supraveghere tehnică presupun anumite restrângeri, care trebuie să se limiteze la aspectele strict necesare, să fie proporționale și autorizate în condițiile legii, considerăm că se recomandă:

(i) continuarea și consolidarea procesului de pregătire profesională continuă, din punct de vedere tehnic și procedural, a personalului specializat din cadrul celor trei autorități judiciare sau a CNIC;

(ii) examinarea periodică și calibrarea procedurilor operaționale, includerea feed-back-lui furnizat de beneficiari și asigurarea corespondenței acestora cu procesul de upgrade a echipamentelor hardware sau a aplicațiilor tehnice folosite;

(iii) continuarea auditărilor periodice a modului în care funcţionează instrumentele automatizate de limitare a greșelilor/derapajelor ce pot surveni în procesul de exploatare a aplicației informatice;

(iv) menținerea unor înalte standarde de securitate informatică la nivelul Centrului Național de Interceptare a Comunicațiilor, inclusiv prin efectuarea unor operațiuni de auditare internă permanentă a sistemului, inclusiv cu simularea unor situații de suprasolicitare tehnică a echipamentelor sau de atac informatic, care să documenteze integritatea sistemelor și un înalt grad de securitate informatică;

(v) evaluarea permanentă a aspectelor care se impun a fi îmbunătățite la nivelul tuturor structurilor implicate.

H. 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 01.07.2020-31.12.2020, în acord cu dispozițiile art.30^1 alin.(1) din Legea nr.304/2004.

București, sediul Înaltei Curți de Casație și Justiție, 14 august 2020

Preşedintele
Înaltei Curţi de Casaţie şi Justiţie
Judecător
CORINA-ALINA CORBU