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[1], Legea nr.135/2010 privind Codul de procedură penală[2], 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[3].

Astfel, la articolul 8, după alin.(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

[1] În continuare - Legea nr.14/1992.
[2] În continuare - Codul de procedură penală.
[3] În continuare - Legea nr.14/1992.

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 supra-vegherilor 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[4] 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.

[4] În continuare C.N.I.C.

Conform obiectului lor, circumstanțiat prin prevederile art.30[1] din Legea nr.304/2004, prezentele verificări privesc exclusiv modul de punere în aplicare a măsurilor de supraveghere tehnică, constând în interceptarea comunicațiilor, prevăzute în Codul de procedură penală. Nu sunt vizate măsurile de supraveghere prevăzute de Legea nr.51/1991 și nici aspecte punctuale, privind legalitatea administrării probelor (în speță, a celor rezultate ca urmare a măsurilor de supraveghere tehnică) într-un dosar de urmărire penală specific, acestea fiind atributul exclusiv al judecătorului care încuviințează măsura, al judecătorului de cameră preliminară ori, după caz, al instanței de judecată.

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.

C. CONSTATĂRILE PRECEDENTE

Raportul precedent a fost publicat pe pagina de internet a Înaltei Curți de Casație și Justiție la data de 14.08.2020, în urma verificărilor, fiind formulate, în esență, următoarele concluzii:

În perioada de referință 01.01.2020-30.06.2020, nu au intervenit elemente noi care să conducă la reconsiderarea concluziilor din raportul dat publicității în luna august 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.

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.).

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

(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 funcționează 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, 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.

După publicarea raportului precedent nu au intervenit noi împrejurări de fapt sau de drept care să justifice efectuarea verificărilor în mod anticipat faţă de intervalul uzual de 6 luni prevăzut de legiuitor.

D. DEFĂȘURAREA VERIFICĂRII ACTUALE

În raport cu concluziile și recomandările formulate prin raportul precedent, la data de 15.12.2020, 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 01.07.2020-31.12.2020, privind, în special, existența în perioada de referință a unor situații de atac informatic, avarii tehnice sau erori procedurale (inclusiv cele cauzate de operarea aplicațiilor informatice de către membrii personalului) în ceea ce privește activitatea de punere în executare a măsurilor de supraveghere tehnică și modul în care acestea au fost abordate și soluționate/remediate; modalitatea de monitorizare și evaluare a eficienței procedurilor și mecanismelor automate de prevenire a erorilor, rezultatele acestor evaluări și dacă s-au luat măsuri de updatare a echipamentelor, procedurilor de lucru sau a aplicațiilor informatice în vederea îmbunătățirii securității și eficienței acestora; existența unor proceduri de auditare a modului de răspuns a sistemelor informatice în condițiile de suprasolicitare tehnică sau de atac informatic; măsurile luate în perioada de referință (sau cu caracter permanent) pentru formarea profesională continuă a personalului implicat în aceste activități; evaluarea relațiilor instituționale dintre beneficiarii – organele de urmărire penală și Centrul Național de Interceptare a Comunicațiilor și existența unor dificultăți sau disfuncționalități de orice natură în ceea ce privește punerea în aplicare a solicitărilor formulate de către acestea, în conformitate cu legea; existența vreunei revizuiri a protocoalelor prevăzute la art.8 alin.(3) din Legea nr.14/1992 (strict în ceea ce privește organele judiciare); modalitățile concrete în care se asigură separarea circuitelor de date (sub aspectul echipamentelor, aplicațiilor informatice și a persoanelor implicate), 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 Centrului; necesitatea îmbunătățirii cadrului legislativ sau operațional; înregistrarea unor petiții sau sesizări de orice natură privind disfuncții în activitățile de punere în aplicare a măsurilor de supraveghere tehnică dispuse de organul de urmărire penală, procedura de cercetare a acestora și aspectele constatate 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 și a discuțiilor purtate cu această ocazie cu persoane din conducerea acestor instituții și a structurilor cu caracter tehnic constituite în cadrul acestora, precum şi a întâlnirii informale cu conducerea marilor parchete desfăşurate la sediul ÎCCJ la data de 29.01.2021.

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 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**

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, 01.07.2020-31.12.2020, 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.

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. În acest context, în următorul raport se impune a fi examinat şi modul concret de funcționare a cooperării dintre parchete şi structurile Poliţiei Române, la nivel teritorial, pentru punerea în executarea a măsurilor de supraveghere constând în interceptarea comunicaţiilor.

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 prin intermediul echipamentelor din 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 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 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 și prevenirea eventualelor erori umane**

În perioada de referință nu au fost înregistrate situații de atac informatic 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 politici și standarde de securizare a accesului. La nivelul CNIC au fost efectuate proceduri de atac informatic (simulări) asupra unor aplicații din cadrul SNIC, datele astfel colectate fiind menite să crească securitatea unor parametri operaționali. Trimestrial sunt întocmite rapoarte privind starea de securitate a sistemului, iar acesta este supus unor auditări interne periodice.

Efectele negative ale avariilor tehnice ale echipamentelor sunt prevenite prin monitorizarea permanentă a stării de funcționare a sistemelor de către administrator (CNIC) și remedierea de urgență a defecțiunilor. În perioada de referință au existat situații de suprasolicitare tehnică a echipamentelor, care au îngreunat temporar sistemul în ceea ce privește transferul de date dintre CNIC și beneficiari, însă fără pierderi de interceptare(CNIC). La nivelul unităților de parchet nu s-au înregistrat deficiențe în ceea ce privește stabilitatea și siguranța echipamentelor tehnice utilizate (DNA). Ori de câte ori au existat disfuncționalități în procesul de exploatare a echipamentelor, administratorul sistemului -CNIC- a asigurat suport tehnic și a intervenit cu celeritate, în condiții de anonimizare și fără riscul alterării conținutului (PÎCCJ).

O altă modalitate de asigurare a securității informațiilor este upgradarea periodică a SNIC în funcție de evoluțiile tehnologice, atât sub aspect hardware, cât și software, cât și în funcție de modificările intervenite în infrastructura tehnică a furnizorilor de comunicații electronice, asigurându-se astfel creșterea eficienței și securității sistemului.

Totuși, acest proces de evoluție tehnologică trebuie dublat de un set de măsuri cu privire la formarea adecvată a personalului și adaptarea procedurilor operaționale, ritmul tuturor acestor tipuri de măsuri trebuind să fie similar. Astfel, s-a constatat că în perioada de referință au fost semnalate unele erori de operare, cu precădere în zona activității de marcare, generate tocmai de procesul de upgrade al echipamentelor și aplicațiilor informatice folosite, erori care au fost analizate, evaluate și eliminate de către specialiștii CNIC, fără a fi afectat procesul de interceptare din punct de vedere al conţinutului sau al accesului neautorizat.

Urmare a procesului de actualizare, în special sub aspectul procedurilor de marcare a criteriilor de interceptare în centrala unui furnizor de servicii de telefonie mobilă, s-a obținut simplificarea procesului și creșterea siguranței în utilizarea aplicației, fiind instalată pe stațiile de lucru ale ofițerilor de poliție o aplicație prin intermediul căreia se facilitează accesul la informațiile privind metodologia de marcare și sunt generate rapoarte de lucru (PÎCCJ).

Avantajul faptului că aplicația informatică dedicată se bazează pe procese automatizate constă tocmai în detectarea și semnalizarea către operator a oricărei erori detectate, erorile putând apărea în principal în procesul de introducere în aplicație a datelor din autorizațiile de interceptare. În acest sens, CNIC a pus la dispoziția autorităților judiciare instrumente automatizate de limitare a erorilor materiale, care au fost apreciate ca având o eficiență crescută (DIICOT).

La nivelul unităților de parchet se asigură monitorizarea constantă a modului de funcționare a acestor mecanisme automate de limitare a erorilor umane sau tehnice, iar echipamentele și procedurile utilizate au fost evaluate ca fiind eficiente și fiabile (DNA).

În scopul asigurării securității informatice a sistemelor utilizate și a eliminării riscului unor erori umane s-a menținut infrastructura concepută pe baza principiilor de separare a rețelelor și a resurselor de calcul și de stocare existente, controlul accesului prin reguli explicit definite, inspecția traficului prin sisteme de prevenire și detectarea intruziunilor, protecția la vulnerabilități, scanare anti-malware și acordarea de permisiuni pornind de la principiul celor mai mici drepturi (PÎCCJ).

Accesul la echipamentele necesare procesului de punere în aplicare a măsurilor de supraveghere tehnică s-a realizat în condiții securizate, existând o monitorizare și o auditare periodică a stării de securitate a sistemului (DIICOT).

Cu toate acestea, procesul de monitorizare și de prevenire a erorilor umane în operarea aplicațiilor informatice dedicate apare ca fiind mai riguros organizat în cadrul CNIC decât în cazul structurilor tehnice constituite la nivelul parchetelor. Sistemul de monitorizare implementat la nivelul CNIC pare a avea preponderent rol preventiv, fiind astfel conceput încât să prevină posibilitatea de eroare/avariile tehnice, iar incidentele sunt riguros documentate, în cadrul unui registru special, în timp ce în cadrul structurilor tehnice constituite la nivelul structurilor de parchet se

intervine punctual, pentru remedierea eventualelor erori, la momentul apariţiei acestora. Sub acest aspect, considerăm că se impune o mai mare rigurozitate în ceea ce privește documentarea incidentelor, indiferent de natură (eroare umană, avarie tehnică etc.) și a modului de intervenție pentru rezolvarea acestora în cadrul structurilor specializate ale parchetelor, precum şi o monitorizare continuă, cu scop preventiv a modului de funcţionare a sistemelor şi echipamentelor proprii.

3. **Separarea fluxurilor de date și asigurarea accesului <u>exclusiv</u> al organelor judiciare la datele colectate în urma procesului de interceptare a comunicațiilor ca măsură de supraveghere tehnică**

Ca urmare a preocupărilor manifestate în ultimii ani din spațiul public în ceea ce privește modul de accesare și valorificare a datelor colectate prin interceptarea comunicațiilor în baza autorizării acestei măsuri de supraveghere tehnică, prezentele verificări au vizat în mod expres separarea circuitelor 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.

Datele furnizate de către toate instituțiile implicate și aspectele rezultate în urma vizitelor efectuate personal de către președintele ÎCCJ la sediile acestora sunt convergente sub aspectul 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 specializare pentru punere 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, în sens fizic, echipamentele de interceptare din cadrul CNIC sunt aceleași pentru toți utilizatorii, acestea depinzând de livrarea traficului de către operatorii de telecomunicații, la nivel logic (software), separarea pe autorități este realizată integral: procese separate, zone de stocare a traficului distincte, acces partajat din aplicații. Fiecare autoritate este complet autonomă, își marchează în sistemul centralizat țintele proprii și are propriul administrator în aplicația de exploatare a

conținutului sesiunilor interceptate, având posibilitatea să creeze noi utilizatori și să acceseze conținutul sesiunilor aparținând țintelor proprii.

Operațiunile tehnice derulate pentru a da eficiență actelor de autorizare a măsurii prevăzute la art.138 alin.(1) lit.a) C.p.p. în cadrul Serviciului tehnic al PÎCCJ sunt îndeplinite doar de către ofițeri de poliție judiciară, direct și nemijlocit, prin intermediul echipamentelor tehnice deținute și utilizate de către Parchetul General. Conținutul datelor colectate este primit în format criptat pe echipamentele proprii, extras și transferat pe suport optic către lucrătorii proprii, care au acces la comunicațiile interceptate în baza unor reguli riguros stabilite. Punerea în executare a măsurilor și consemnarea rezultatelor obținute constau într-o succesiune de operațiuni puse în practică de mai mulți ofițeri de poliție judiciară, accesul la datele cauzei și la informațiile rezultate de interceptare fiind limitat în fiecare stadiu la cele absolut necesare, pe baza principiului nevoii de a cunoaște. Accesul în sisteme este securizat și logat, iar rezultatul supravegherii (suport optic și proces-verbal de export al datelor) se transmit beneficiarului în plic închis. Transcrierile comunicațiilor sunt întocmite în unic exemplar, exclusiv de către ofițerii de poliție judiciară din cadrul serviciului, în baza repartizării procurorului șef serviciu și a procurorului de caz și se transmit acestuia din urmă în plic închis. În sfârșit, documentele de autorizare a interceptării sunt păstrate la procurorul șef al Serviciului tehnic, iar în evidențele structurii nu sunt indicate numele persoanei interceptate, numere de telefon sau starea de fapt care a justificat autorizarea măsurii (PÎCCJ).

De asemenea, la nivelul structurilor tehnice proprii, constituite la nivelul parchetelor, securitatea datelor colectate prin măsuri de interceptare a comunicațiilor se asigură prin utilizarea exclusiv de stații de lucru dedicate acestor activități, care sunt instalate în spații cu acces limitat și controlat, prin respectarea unor reguli stricte în ceea ce privește fluxul de lucru și circuitul documentelor, precum și prin faptul că rezultatele punerii în aplicare a măsurii de supraveghere (atât suporturile de date, cât și datele pe suport de hârtie) sunt expediate în plicuri sigilate, fiind destinate exclusiv procurorului care efectuează urmărirea penală (DNA).

În cadrul DIICOT, datele obținute în urma procesului de interceptare sunt transmise în mod automat și nemijlocit, printr-un canal criptat, către echipamentele tehnice proprii, rețelele dedicate interconectării cu CNIC fiind protejate și separate fizic de celelalte rețele ale instituției. Sesiunile rezultate din fluxul de interceptare sunt repartizate spre ascultare lucrătorilor de poliție judiciară special desemnați sau delegați de procurorul de caz, iar accesul este limitat doar la sesiunile alocate, logările făcându-se în mod individual. Accesul la exportul sesiunilor este permis doar lucrătorilor de poliție judiciară care gestionează din punct de vedere tehnic interconectarea și fixează informațiile pe suporți optici sau magnetici, pentru a fi transmise organului de urmărire penală, iar transcrierile se realizează de către lucrători de poliție judiciară delegați în cauză de către organul de urmărire penală (DIICOT).

Deși modalitatea actuală de lucru asigură autonomia funcțională și operațională totală a organelor de urmărire penală în privința punerii în aplicare a măsurilor de supraveghere tehnică constând în interceptarea comunicațiilor, ca urmare a caracterului limitat al resurselor umane și materiale disponibile la nivelul structurilor tehnice ale parchetelor, totuşi, toate aspectele tehnice esenţiale, upgrade-urile de software şi instruirea personalului sub raportul operării sistemelor şi aplicaţiilor necesită asistența CNIC.

Această situaţie este generată, pe de o parte, de prevederile legale care consacră calitatea CNIC de administrator al sistemului, dar şi de resursele umane şi tehnice necesare pentru administrarea sistemelor şi aplicaţiilor informatice folosite. Capacitatea tehnică a parchetelor ar trebui extinsă astfel încât toate operaţiunile tehnice legate de propriile echipamente şi de gestionarea (actualizare, remediere erori, teste de funcţionare sau cu privire la securitatea informatică) aplicaţiilor informatice la nivelul parchetelor să fie gestionate din punct de vedere tehnic integral la nivel intern, însă acesta reprezintă un proces evolutiv, care progresează pe măsura achiziționării echipamentelor disponibile și a încadrării/instruirii de personal corespunzător pregătit.

Totuși, se impune mențiunea că dotarea corespunzătoare și efectuarea activităților de interceptare presupune anumite constrângeri de ordin material, precum și asigurarea relației cu operatorii/furnizorii de servicii de comunicații, aspecte care sunt eficient gestionate la momentul actual prin existența unui intermediar unic – CNIC – în relația cu aceştia. Ca urmare a acestor constrângeri, se impune a fi analizat dacă sistemul actual, care vizează practic dezvoltarea a trei sisteme autonome (PÎCCJ, DNA, DIICOT) poate fi considerat eficient ori ar putea fi analizată de către instituțiile implicate posibilitatea constituirii unei structuri judiciare unice, care ar putea obține mai ușor finanțarea necesară, după modelul agențiilor autonome existente în alte state.

4. **Asigurarea pregătirii continue a personalului implicat**

CNIC a asigurat atât forme periodice cât și forme ad-hoc de informare și perfecționare a personalului specializat din cadrul celor trei autorități judiciare beneficiare (PÎCCJ, DNA, DIICOT), în scopul cunoașterii procedurilor operaționale, a evitării erorilor umane și a prezentării și asimilării upgrade-urilor intervenite cu privire la sistemele sau aplicațiile informatice folosite. După upgradarea soluției de interceptare/marcare de către operator, aceasta este testată și implementată împreună cu specialiștii CNIC, are loc instruirea utilizatorilor cu privire la noua aplicație și este colectat feedback-ul acestora cu privire la eventualele soluții pentru îmbunătățirea acesteia.

În cadrul Parchetului de pe lângă Înalta Curte de Casație și Justiție (PÎCCJ) a fost elaborat și diseminat la parchetele din teritoriu un set de instrucțiuni cu privire la modalitatea în care se efectuează interceptarea comunicațiilor persoanelor

încarcerate, cu privire la care s-au încuviințat astfel de măsuri de supraveghere tehnică. În contextul epidemiologic actual formarea personalului a fost asigurată prin studiul instrucțiunilor de utilizare și a elementelor de noutate, informări transmise de către CNIC în format electronic, scurte sesiuni de instruire cu reprezentanți CNIC, la momentul instalării/upgradării și configurării aplicațiilor informatice și organizarea de ședințe de lucru în cadrul Serviciului tehnic al PÎCCJ.

La nivelul unităților de parchet au fost prelucrate cu personalul implicat în activitatea de punere în executare a măsurilor de supraveghere tehnică materialele întocmite de către CNIC cu privire la măsurile tehnice și umane necesar a fi respectate pentru limitarea vulnerabilităților (DNA).

Prin notificările și instrucțiunile cu caracter tehnic primite din partea CNIC cu privire la modificările aduse de operatorii de telefonie mobilă asupra soluțiilor de interceptare s-a asigurat un flux de lucru fără întreruperi în procesul de punere în executare a măsurilor de supraveghere tehnică (DIICOT).

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 fiind foarte bune (DNA, DIICOT), desfășurându-se cu respectarea limitelor de competență și a cerinței de asigurare a confidențialității operațiunilor efectuate (PÎCCJ).

Există reguli standardizate privind modalitate de utilizare a SNIC, iar problemele tehnice și de securitate au fost analizate în cadrul unor întâlniri/grupuri de lucru cu reprezentanți ai organelor judiciare. Pentru soluționarea unor probleme tehnice în regim de urgență au fost constituite echipe tehnice comune. Deși chestiunile vizate au fost probleme de ordin tehnic, fiind normală cooperarea dintre administratorul sistemului și beneficiari, din perspectiva istoricului alegațiilor manifestate în spațiul public legat de astfel de aspecte, considerăm că ar fi preferabilă autonomizarea completă din punct de vedere tehnic a structurilor tehnice constituite în cadrul parchetelor, astfel încât acestea să aibă mijloacele materiale și umane necesare pentru rezolvarea internă a oricăror incidente de ordin tehnic legate de funcționarea sistemelor proprii.

Prevederile protocolului nr.9331/2016 nu a fost revizuit în perioada de referință și niciuna dintre instituțiile consultate nu a semnalat necesitatea unor modificări ale dispozițiilor acestuia, actualul conținut al protocolului apărând astfel ca fiind apt să asigure realizarea scopului pentru care a fost încheiat.

6. Propuneri formulate cu privire la îmbunătățirea cadrului legislativ și operațional

În cadrul procesului de consultare și informare declanșat de către președintele ÎCCJ în vederea efectuării verificărilor, CNIC a arătat că ar fi necesară optimizarea cadrului legislativ național aplicabil domeniului de referință, în sensul promovării/introducerii unor prevederi care să definească în mod explicit și exhaustiv toate categoriile de operatori/furnizori de servicii de comunicații electronice, astfel încât obligațiile stipulate prin lege să devină opozabile inclusiv companiilor furnizoare de mijloace moderne de comunicare.

De asemenea, aspectele privind necesitatea reglementării situației modalităților atipice de comunicație a rezultat și din discuțiile purtate cu unii reprezentanți ai parchetelor.

Propunerea formulată constituie apanajul exclusiv al legiuitorului, includerea sau nu a acestor servicii puse la dispoziția utilizatorilor în categoria acelora care pot face obiectul interceptării în cadrul unor măsuri de supraveghere tehnică depinzând de definiția legală a noțiunilor de comunicație electronică și operator/furnizor de servicii de comunicații electronice. Interpretarea în concret a acestor noțiuni nu intră în competența președintelui Înaltei Curți, ci, în fiecare caz în parte, face obiectul aprecierii suverane din partea judecătorului învestit cu soluționarea unei cereri de încuviințare a unor măsuri de supraveghere tehnică – judecătorul de drepturi și libertăți sau instanța de judecată – ori cu aprecierea legalității probelor obținute prin astfel de măsuri – judecătorul de cameră preliminară sau instanța de judecata.

În linii generale însă, trebuie remarcat că interesele sociale ținând de buna desfășurare a procesului penal și de înlesnirea obținerii de probe pentru stabilirea adevărului judiciar trebuie întotdeauna corelate cu necesitatea respectării drepturilor fundamentale ale cetățenilor și asigurarea caracterului minimal și absolut necesar al ingerinței statului în ceea ce privește exercițiul acestora, astfel cum sunt circumstanțiate aceste valori prin jurisprudența Curții Europene a Drepturilor Omului și a Curții Constituționale, precum și prin hotărârile Curții de Justiție a Uniunii Europene, în special cele referitoare la protejarea confidențialității datelor cu caracter personal și la obligațiile care revin operatorilor de astfel de date, inclusiv furnizorii de servicii de telecomunicații, administratorii paginilor web sau a serviciilor de tip cloud etc.

În sfârșit, reprezentanții DNA au arătat că este necesară o îmbunătățire a cadrului legislativ și în ceea ce privește relația cu furnizorii/operatorii de servicii de comunicații și obligațiile care le revin acestora cu privire la solicitările organelor judiciare.

7. Petiții/sesizări privind disfuncții în activitatea de punere în aplicare a măsurilor de supraveghere tehnică

În pofida persistenței în spațiul public a unor mesaje privind folosirea excesivă a acestor mijloace de obținere a probelor, a implicării serviciilor secrete sau a valorificării nelegale a datelor rezultate din astfel de interceptări, niciuna dintre instituțiile implicate nu a raportat primirea unor petiții privind disfuncții sistemice legate de punerea în aplicare a măsurilor de supraveghere tehnică.

Orice nereguli cu caracter punctual pot fi invocate în cadrul procedurilor judiciare, drepturile eventualelor persoane vătămate prin astfel de fapte fiind astfel protejate, fie prin existența posibilității legale a invalidării mijloacelor de probă astfel obținute, fie prin angajarea răspunderii juridice a persoanelor responsabile

O posibilă explicație a contradicției dintre împrejurarea că, în concret, nu au fost semnalate deficiențe sistemice în ceea ce privește activitățile de interceptare a comunicațiilor, dispuse în cadrul unor măsuri de supraveghere tehnică și percepția, nu întotdeauna pozitivă, la nivelul opiniei publice, asupra folosirii acestor mijloace de probă, ar putea-o constitui tocmai neasigurarea în mod eficient al accesului cetățenilor la informațiile cu caracter general relevante, ceea ce conduce la un grad redus de cunoaștere cu privire la cazurile și modalitatea în care pot fi dispuse astfel de măsuri, modul în care ele sunt puse în aplicare, garanțiile procedurale care sunt instituite pentru fiecare fază a procedurii, de la momentul încuviințării și până la posibila valorificare a interceptărilor în cadrul unui proces penal etc.

Caracterul confidențial al urmăririi penale vizează păstrarea secretului informațiilor într-un caz concret, însă acesta nu trebuie să justifice omisiunea informării pe deplin a cetățenilor cu privire la aspectele generale ținând de aceste activități cu caracter judiciar, care atrag o restrângere semnificativă a drepturilor fundamentale ale persoanelor vizate de aceste măsuri, ceea ce presupune ca orice persoană să fie pe deplin informată cu privire la procedurile aplicabile și la modalitatea în care datele care eventual sunt colectate la un moment dat în ceea ce o privește sunt protejate. Deopotrivă însă, accesul la informaţii cu caracter general privind aceste măsuri de supraveghere ar asigura şi informarea acestuia asupra necesităţii şi rolului unor astfel de mijloace de probă, în special în cadrul anumitor categorii de infracţiuni, care nici nu ar putea fi descoperite, documentate şi, în final, sancţionate în lipsa unor mijloace moderne de investigaţie.

La latitudinea legiuitorului şi după consultarea tuturor actorilor implicaţi, ar putea fi examinată oportunitatea valorificării sub acest aspect a experienței altor state democratice, în care există o formă de evidență (de tip registru național), actualizată în timp real, în ceea ce privește măsurile judiciare restrictive de drepturi și care permite informarea la orice moment a presei și a cetățenilor cu privire la elemente relevante pentru politica penală și procesual-penală a statului în cauză – numărul măsurilor dispuse și evoluția lui în timp, repartiția pe categorii de infracțiuni,

eficiența sau relevanța unor astfel de măsuri sub aspect probator, numărul autorizațiilor care au fost ulterior invalidate, costurile generate de punerea în aplicare a unor astfel de măsuri de supraveghere și raportul cost-eficiență la finalul procesului penal etc.

De asemenea, tot prin raportare la opţiunea legiuitorului şi în funcţie de practicile administrative şi resursele existente în cadrul departamentelor de comunicare ale marilor parchete, ar putea fi puse la dispoziţia publicului larg date statistice şi informaţii de interes general cu privire la condițiile și categoriile de infracțiuni pentru care pot fi dispuse astfel de măsuri, garanţiile prevăzute de lege cu privire la drepturile fundamentale ale persoanelor implicate, în special prin examinarea cererii de autorizare de către un judecător, prin limitarea duratei interceptărilor succesive, prin distrugerea celor care nu sunt folosite în cadrul procesului penal etc., furnizarea de date statistice relevante cu privire la numărul de solicitări, categoriile de infracțiuni pentru care au fost acordate autorizațiile, perioada medie de menținere a măsurilor, costuri şi orice alte elemente de natură a schimba percepţia unei părţi a publicului cu privire la acest mijloc de probă, care, în final, este doar unul dintre cele prevăzute de Codul de procedură penală, pentru stabilirea adevărului în cadrul procesului penal.

F. CONCLUZIILE VERIFICĂRII

În urma verificărilor efectuate, președintele Înaltei Curți de Casație și Justiție constată că, pentru perioada de referință 01.07.2020-31.12.2020, se impune a fi menținute concluziile formulate anterior, 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, 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 ţinând de funcţionarea echipamentelor hardware şi de aplicaţiile tehnice folosite rămâne în continuare important, însă gradul de autonomie tehnică şi tehnologică a structurilor specializate din cadrul parchetelor în raport cu administratorul sistemului creşte 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. Aceste 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 PÎCCJ, 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 informative 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 CNIC (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 în acest sens proceduri uniforme şi garanţii adecvate privind securitatea cibernetică şi respectarea dispoziţiilor legale care reglementează relaţiile dintre cele două instituţii.

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 perioada 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 de 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.

G. RECOMANDĂRI

Măsurile de supraveghere tehnică au o natură restrictivă de drepturi, trebuind 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 echilibrului necesar între cele două valori fundamentale enunțate. În acest sens, se impun 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.

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 01.01.2021-30.06.2021, în acord cu dispozițiile art.30^1 alin.(1) din Legea nr.304/2004.

București, sediul Înaltei Curți de Casație și Justiție, 04 februarie 2021

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