ASUPRA UNOR METODE SPECIALE DE INVESTIGAŢII ŞI DE PREVENŢIE MODERNE ÎN PROCEDURILE PENALE

Serghei PÂNTEA

Ministerul Afacerilor Interne

Abstract: *Realitatea socială arată că o pondere considerabilă a infractorilor fac uz de tehnologiile moderne, sunt în pas cu cele mai noi schimbări în domeniu, ceea ce îngreunează mult activitatea de prevenire, relevare şi combatere a infracţiunilor. Se propun două instrumente în ajutorul organelor de urmărire penală şi de investigaţie care, îmbracă forma măsurilor speciale de investigaţii de natură dublă, cu funcţie mixtă, şi pot în opinia noastră contribui decisiv la prevenirea şi combaterea eficientă a anumitor categorii de infracţiuni; fortificarea probatoriului penal; determinarea unor categorii de subiecţi să renunţe la activitatea infracţională iniţiată şi/sau deja în desfăşurare*

***Cuvinte cheie*:** *Justiţie, proceduri penale, probe, măsuri speciale de investigaţii, prevenire*

Materiale şi metode. La elaborarea cercetării a fost consultat cadrul normativ naţional, legislaţia şi practica altor state, resursele în materie internaţională. De asemenea, a fost cercetată literatura de specialitate în domeniul prevenirii criminalităţii şi investigării infracţiunilor, cu trimiterile şi explicaţiile de rigoare. În acest sens, menţionăm în special autorii *Al. Monteith, A. Thomson, Th. Chittum, T. Macaulay* ale căror contribuţie apreciem drept substanţială. Lucrarea ştiinţifică este suplimentată de o analiză comprehensivă care permite argumentarea necesităţii elaborării a două metode, de natură dublă, cu funcţie mixtă, de prevenire şi investigare a infracţiunilor. Suportul teoretic şi ştiinţific este comprehensiv, fiind aplicată metoda logică şi metoda sistemică de cercetare.

De la general la particular. *"În ceea ce priveşte justiţia şi supremaţia legii, o jumătate de măsură de prevenire, valorează mai mult decât o măsură întreagă de vindecare... Prevenirea este primul imperativ al justiţiei"*[1, p.4].

Realitatea socială arată că o pondere considerabilă a infractorilor fac uz de tehnologiile moderne, cunosc schimbările în domeniu, ceea ce îngreunează activitatea de relevare şi combatere a infracţiunilor.

Punct de pornire a cercetării este formularea propunerilor şi argumentarea necesităţii intervenţiei legislative. Astfel, cele două metode propuse vin în ajutorul organelor de aplicare a legii şi sunt, după noi utile, pentru situaţii cum ar fi atunci când, deşi este identificat suspectul, probatoriul este insuficient; atunci când nu există certitudinea că făptuitorul urmăreşte cu adevărat satisfacerea presupusei *intenţii criminale*; prevenirea survenirii unor consecinţe prejudiciabile; precum şi alte ipoteze. Aceste instrumente îmbracă forma metodelor de natură dublă, cu funcţie mixtă care, în opinia noastră, pot contribui decisiv la prevenirea anumitor categorii de infracţiuni; fortificarea probatoriului penal; determinarea unor categorii de subiecţi să renunţe la activitatea infracţională iniţiată şi/sau deja avansată, altele.

Formele conceptuale ale acestor metode sunt:

1. Deconectarea controlată a unor servicii de comunicaţii electronice determinate;
2. Obstrucţionarea, bruierea sau interferenţa controlată a unor servicii de comunicaţii electronice.

Să modelăm câteva situaţii inspirate din practica organelor de aplicare a legii [2]: (1) o persoană, despre care există anumite informaţii că distribuie droguri, utilizează aplicaţii moderne de comunicare *(pentru organizare, dirijare, comunicare, schimb de informaţii, etc.)*. Drogurile sunt ascunse în spaţii cu acces public, fără a interacţiona direct cu cumpărătorul, iar prin intermediul aplicaţiei, suspectul îşi reclamă oferta, transmite locaţia cu drogul ascuns iar cumpărătorul, achită pentru cantitatea de drog solicitată prin intermediul terminalelor electronice de plată; (2) alerta presupusă sau reală de detonare a unui exploziv de la distanţă; (3) dirijarea unor activităţi infracţionale din locaţii cu regim de supraveghere *(penitenciare, locuri de detenţie provizorie, etc)*.

În general, modul de acţiune a unor reprezentanţi ai organelor de aplicare a legii, s-ar putea rezuma la orientarea eforturilor spre identificarea metodelor de a sparge sau decripta sistemele aplicaţiilor sau dispozitivelor [3], efectuarea măsurilor speciale de investigaţii sau a unui complex de măsuri speciale şi activităţi procesuale care, ar permite acumularea probatoriului. Activităţile pot fi suplimentate cu activităţi de identificare, activităţi cu scopul dezamorsării explozivului *(dacă acesta identificat)*, alte cercetări deschise sau secrete.

Cunoscând faptul că, aplicațiile moderne sau dispozitivele sunt de regulă *dependente* de accesul la rețea *(inclusiv internet)*, iar interacțiunea se efectuează prin telecomunicații sau comunicații electronice, fiind de regulă inutile fără un astfel de acces, în baza autorizării *(după caz, procedura urgentă)* ar putea fi deconectate temporar de la rețea sau bruiate într-un anumit sector sau pe un dispozitiv determinat. Afirmativ, dacă ar exista o astfel de opțiune juridică. Se înțelege că, făptuitorul, va căuta după caz: să renunțe; să continue prin convorbiri nesecurizate de pe același aparat sau interacțiunea directă *(riscând să fie supus altor MSI)*; să continue infracțiunea utilizând un alt aparat; etc., ceea ce ar cauza inevitabil impedimente în timp, mijloace, resurse și conspirație. Deconectarea ar putea avea loc nu numai în privința unui aparat sau a unor servicii determinate, dar a unui complex de aparate; pe o arie determinată; privind cumul de servicii; în privința unui utilizator *(persoană, apartament, bloc locativ, etc)*. Și dacă infractorul renunță? Există și alte ipoteze în care, se poate avea în vedere utilizarea metodelor respective, cum ar fi închisorile pentru a preveni utilizarea telefoanelor mobile de contrabandă de către deținuți [4]; în cadrul operațiunilor tactice, cum ar fi executarea mandatelor judiciare; cazurile de luare de ostatici; altele.

Procesul penal înglobează întreaga activitate a organelor de urmărire penală și a instanțelor judecătorești. Acesta se consideră început din momentul sesizării sau autosesizării despre *pregătirea* sau *săvârșirea* unei infracțiuni [*s.n.a.*]. Din acest moment, în special activitatea organelor de urmărire penală are ca și scop legal *printre altele*, protejarea persoanei, societății și statului de infracțiuni, iar legea penală stabilind expres drept scop *prevenirea* săvârșirii de noi infracțiuni. În continuare, organele de urmărire penală au obligația de a lua toate măsurile necesare pentru *prevenirea* și *curmarea* infracțiunilor [*s.n.a.*]. Astfel, din economia dispozițiilor legii penale și procesual penale, această dublă funcție, de prevenire și combatere, trebuie să fie realizată în egală măsură.

Consiliul Europei, în *codul european de etică polițienească* stabilește că, printre obiectivele de bază ale poliției este asigurarea prevenirii infracțiunilor, lupta cu criminalitatea, și descoperirea infracțiunilor [5, p.5]. Acest document confirmă că, toate dimensiunile activității poliției sunt în importante.

Ministerul Afacerilor Interne, în principal prin intermediul Inspectoratului General al Poliției și Inspectoratului General al Poliției de Frontieră, exercită *printre altele*, funcția de *prevenire* a infracțiunilor [6], [7], ambele autorități fiind abilitate cu investigarea și urmărirea penală a infracțiunilor.

Potrivit unor autori, prin prevenirea criminalității trebuie înțeleasă activitatea, scopul căreia este lichidarea cauzelor generatoare [8, p. 217], precum și *stoparea activității infracționale* deja demarate. Alții susțin că, în însuși conținutul gnoseologic al acestei noțiuni este admisă o eroare logică formală: e imposibil să preîntâmpini ceea ce deja există. Așadar, prevenirea infracțiunilor este percepută preponderent prin prisma activităților desfășurate în afara procesului penal, astfel, rămâne uneori declarativă funcția de prevenire în cadrul proceselor penale, probabil cu excepția sesizărilor întocmite în conformitate cu art. 216-217 Cod de procedură penală și cazul infracțiunilor neconsumate. Deși sunt importante și deloc neglijabile, eforturile în domeniul prevenirii îmbracă cel mai des forma verificărilor, ședințelor sau campaniilor de informare, diseminarea materialelor informative, ținerea de prelegeri, alte activități de sensibilizare, spontane, sau organizate și planificate, la diferite niveluri *(local, sectorial, național),* după caz, cu implicarea diferitor entități *(neguvernamentale, parteneri internaționali)*.

Tehnologii, prevenția și combaterea infracțiunilor. Dezvoltarea tehnologiilor moderne de comunicare, diferitor aplicații *(What's up, Viber, Telegram, online-banking, portmonee electronice, etc.),* existența softurilor și platformelor de telefonie și IP accesibile, evoluția și modernizarea accelerată a tehnologiilor, emergența tehnologiei în domeniul criminalității și inevitabila convergență a tehnologiei cu criminalitatea, îngreunează activitatea organelor de urmărire penală și speciale de investigații, de relevare și combatere a infracțiunilor.

Acestea, suplimentate de volumul considerabil de muncă, complexitatea activităților realizate pentru a *documenta calitativ* o faptă, modalitatea imperfectă de apreciere și evaluare a activității *organelor de drept,* alte aspecte, determină afirmarea funcției de combatere în detrimentul prevenirii, mai cu seamă atunci când un proces penal este declanșat deja sau se efectuează verificări, fie deja s-au depus eforturi considerabile pentru acumularea probatoriului. Totodată, prevenirea infracțiunilor este percepută ca și sarcină a altor autorități și subiecți decât organele de urmărire penală sau de investigații, inclusiv din motivul precarității instrumentarului legal. Odată inițiat procesul penal, sunt depuse eforturi considerabile pentru identificarea suspectului, acumularea probatoriului, întreprinderea acțiunilor asiguratorii și aplicarea măsurilor preventive, nefiind alocat timp sau mijloace pentru *a influența* persoana să renunțe. În ceea ce ține de măsurile speciale de investigații, accentuăm că două condiții de fond pentru dispunerea și efectuarea acestora sunt: imposibilitatea realizării *scopului procesului penal (include prevenirea, s.n.a), existența temeiurilor de a presupune că poate fi prejudiciată considerabil activitatea de administrare a probelor*; precum și existența

bănuielii rezonabile cu privire la *pregătirea* sau *săvârşirea* unei infracţiuni grave, deosebit sau excepţional de grave. Nu întâmplător am menţionat că, cele două instrumente urmează să îmbrace anume forma măsurilor speciale de investigaţii în sensul Codului de procedură penală, deoarece după noi, adoptarea unei alte legi care să servească temei juridic măsurilor de prevenţie, fie calificarea acestora ca şi măsuri de prevenţie sau asiguratorii, sau alte forme, nu vor permite realizarea *funcţiei duble*. Situaţiile modelate ar putea explica scopul, iar din acest motiv, expunem aceste măsuri astfel:

1. Obstrucţionarea, bruierea sau interferenţa controlată limitată a telecomunicaţiilor sau unor servicii de comunicaţii electronice pe arii determinate *(geografic);*
2. Deconectarea controlată a unor telecomunicaţii sau servicii de comunicaţii electronice:
   a) la un dispozitiv determinat *(IMEI, număr de telefon, IP, WLAN, IMSI)*; sau
   b) a mai multor dispozitive aparţinând aceluiaşi utilizator sau pe un complex de dispozitive;
   c) al unui serviciu determinat *(internet, telefonie mobilă, fixă);* a) şi/sau b) şi/sau c):
      - pe intervale de timp; sau
      - pe celule (CSLI) [9, p.82; 10, p. 6]; sau
      - pe arii determinate (inclusiv geografic).

Obstrucţionarea, bruierea sau interferenţa controlată. Standardele în domeniu stabilesc printre altele că aceasta nu trebuie deterioreze dispozitivele, să nu colecteze şi să stocheze date, să nu interfereze cu operarea normală a serviciilor de urgenţă *(cum ar fi 112, alte servicii de urgenţă);* să poată fi conectate şi deconectate manual de operator; să nu fie afectaţi terţii sau să se afle despre existenţa acestora; altele multiple.

Rezoluţia ECOSOC [11, p.300] stabileşte printre altele că, Guvernele şi societatea civilă, inclusiv, acolo unde este cazul, sectorul corporativ, ar trebui să sprijine dezvoltarea programelor de prevenire a criminalităţii.

Primul instrument propus urmăreşte *printre altele* reducerea intruziunii în dreptul la viaţa privată, precum şi prevenirea infracţiunii. În cel de-al doilea caz, pe lângă cele expuse, ţinteşte ipotezele în care infractorii, *influenţează* victimele sau martorii, inclusiv din locurile de detenţie, precum şi cazurile în care în anumite locaţii sunt desfăşurate activităţi infracţionale, fără a avea posibilitatea identificarea suspectului în termen proxim sau curmarea infracţiunii, ipoteza de securizare a unui perimetru geografic determinat, precum şi alte ipoteze.

Deşi prin *Hotărârea CSFR nr. 2 din 02.08.2013*, s-a decis neadmiterea utilizării dispozitivelor care provoacă premeditat perturbaţii prejudiciabile *(dispozitive de bruiaj intenţionat)* considerăm că, aceasta nu se poate referi la activitatea organelor de aplicare a legii, care trebuie să poată facă uz de orice mijloace legale, inclusiv tehnice, pentru a preveni şi combate infracţiunile. În acest sens, nota informativă la hotărârea *prenotată* relevă că, singura excepţie de la interdicţie ar putea fi plasarea unor dispozitive de bruiaj, în contextul utilizării naţionale autorizate de către organele de forţă şi de securitate [12]. O situaţie similară se atestă în Recomandarea ECC (04)01 din 2004 [13]. Această excepţie se referă nu numai la utilizare, dar şi *la introducerea pe piaţă a unor astfel de dispozitive*.

Aşadar, deşi interdicţia bruiajului există în majoritatea statelor, aceste dispozitive pot fi utilizate cu anumite excepţii *(organele de aplicare a legii şi cele de securitate naţională)*. Exemplul Canadei [14, p.83] relevă că, dacă se urmăreşte scopul securităţii sau siguranţei, apărării naţionale, limitându-se la cea mai mică zonă fizică, cel mai mic număr de frecvenţe pentru atingerea obiectivelor interferenţei sau obstrucţionării, cea mai redusă durată, această metodă este permisă.

Ţinem să menţionăm că, aceste metode speciale urmează să fie aplicate doar pentru anumite categorii de infracţiuni expres stabilite din categoria celor grave, deosebit sau excepţional de grave, pentru a evita critici aduse în legătură cu utilizarea improprie pentru alte încălcări de legislaţie, inclusiv limitarea drepturilor la exprimare [15 p.9,18] (*exemplu, cazul protestelor sau măsurilor în masă, chiar şi la etapa de pregătire* [4, p.259]).

Argument. Protecţia vieţii private *(în diferitele sale forme)* este importantă, aceasta reprezintă doar una dintr-o multitudine de îndatoriri impuse statelor, printre care protejarea vieţii şi proprietăţii cetăţenilor, prevenirea activităţii criminale, şi de a proteja securitate naţionala [16, p.19]. Atunci când persoana este deconectată de la un serviciu *(ex. accesul la internet)*, acesta dispune de liberul arbitru, să renunţe la infracţiune sau să continue comunicarea spre ex. fără utilizarea *aplicaţiei criptate*. Până la urmă, păstrarea secretului poate fi perceput într-un final ca şi un exerciţiu de voinţă. Renunţarea la secretul sau dreptul la viaţa privată, cedarea sau divulgarea unei părţi din acest drept este discreţia titularului. Intruziune fizică, prin deconectare poate împiedica persoanele să acţioneze cum doresc, poate influenţa indivizii în comportamentul pe care îl aleg să-l prezinte, *fără a interveni în conţinutul acestora (s.n.a)*. Printre constatările în domeniul

confidențialității ca și autonomie, Proiectului ALADDIN a relevat că, deoarece activitățile de supraveghere nu doar colectează pasiv informații despre persoane, acestea pot servi pentru *a influența și a modifica, chiar constrânge, comportamentul indivizilor (s.n.a).* Fiind conștienți de observație, ei își pot schimba comportamentul în așa fel să evite consecințele negative percepute sau chiar să acționeze într-o manieră coercitivă (...) [16, p.15]. La verificarea testului rezonabilității și proporționalității intruziunii agenților statului, se va consulta în fiecare caz concret jurisprudența *CtEDO, CJUE* și bunele practici ale instanțelor străine, cum ar fi *cauza Katz* [9, p.86].

Recomandări de intervenție legislativă. În scopul îmbunătățirii situației în domeniu, sugerăm următoarele propuneri principale de *lege ferenda*:

[1]. Completarea art. 132[2] din Codul de procedură penală **cu două litere: e[1]**) Deconectarea controlată a unor telecomunicații sau servicii de comunicații electronice; **e[2]**) Bruierea sau interferența controlată limitată a telecomunicațiilor sau unor servicii de comunicații electronice pe arii determinate;"

[2]. Modificarea subsecventă prin completare CPP *(spre exemplu art. 138[4], 138[5])* și *Legea nr. 59 din 29.03.2012 privind activitatea specială de investigații*;

[3]. Completarea *Legii nr. 241 din 15.11.2007 comunicațiilor electronice*, la alin. (7) art. 5, după cuvintele "comunicațiile electronice pot fi interceptate" cu sintagma "deconectate sau bruiate,".

[4]. Menționăm că, amendarea Codului Contravențional *(exemplu art. 251)* nu este necesară întru-cât, aceasta va constitui o măsură specială de investigație autorizată în conformitate cu legislația.

[5]. Deși de principiu, *HG nr. 100 din 09.02.2009*, nu are incidență asupra aparatelor de bruiaj sau deconectare, această hotărâre ar trebui modificată prin includerea altor mijloace speciale, fără a îngusta nomenclatorul la domeniul scopului expus, deoarece sunt mijloace maxim intruzive în drepturi și libertățile persoanei, și urmează un regim juridic și de evidență strict.

Bibliografie

1. UNODC, *Crime prevention assesment tool*, New York: United Nations, 2009 //Apud S/2004/616, para. 4.
2. Comunicat de presă: http://politia.md/ro/content/vindeau-droguri-prin-aplicatii-electronice-de-comuni care-trei-persoane-retinute, accesat la 22.01.2019;
3. Comunicate și surse deschise: noi.md/md/news_id/208333;slate.com/technology/2018/06/paul-manafort-how-did-fbi-access-whatsappmessages.html;**Ошибка! Недопустимый объект гиперссылки.**;www.bizlaw.md/2017/04/30/proiectul-de-lege-big-brother-analize-si-recomandari; altele;
4. Chittum Th., *Can You Hear Me Now? Cell Phone Jamming and the Tenth Amendment, Nevada Law Journal:* Vol. 13:Iss.1, 2012;
5. *Общественная безопасность и осуществление полицейских функций. Пособие по оценке систем уголовного правосудия*, New York: United Nations, 2010;
6. http://lex.justice.md/md/347675/, accesat la 28.02.2019;
7. http://lex.justice.md/md/378478/, accesat la 28.02.2019;
8. Bîrgău M., *Aspecte teoretico-aplicative privind prevenirea criminalității la etapa actuală în contextul dezvoltării sistemului național de drept,* Revista științifico-practică nr.2, Chișinău: IRIM, 2015;
9. Monteith Al., *Cell site location information: A catalyst for change in fourth amendment jurisprudence*, The Kansas Journal of Law and Public Policy, Vol. 27, No. 1.;
10. *În același sens* Thomson A., *Cellular Dragnet: Active Cell Site Simulators and the Fourth Amendment,* New York University School of Law, 2015
11. ECOSOC Res.1995/9, *Guidelines for coop. and tech. assistance in the field of urban crime prevention*
12. NI la proiectul hotărârii CSFR privind interzicerea importului, punerii la dispoziție pe piață și utilizarea dispozitivelor de bruiaj, accesibil: particip.gov.md/public/documente/141/ro_949_NotainfoHotarireCSFRdispozitivebruiaj28.06.20131.pdf
13. ECC Rec. (04)01 *with regard to forbidding the placing on the market and use of jammers in the CEPT member countries*, 13 Februarie 2004 cu modificările din 08 februarie 2013
14. Macaulay T., *A Review of Canadian Radiocommunications Law Around ''Jammers'',* Canadian Journal of Law and Technology, Vol 4 Nr. 1, 2005
15. Council of the EU, *EU Human Rights Guidelines on Freedom of Expression Online and Offline, Development of surveillance technology and risk of abuse of economic information*, 2014
16. Proiectul ALADDIN, Raportul D 3.1., *Protecția Datelor: Cadrul Etic, Social și Juridic*, 2018