KRIMINALISTIČKO-OBAVEŠTAJNI RAD I TRADICIJA GRAĐANSKIH I LJUDSKIH PRAVA

*Aleksandar Fatić**

APSTRAKT

Trendovi u razvoju savremenog ukupnog policijskog rada su metodološki značajno različiti u odnosu na njegov tradicionalni oblik. Klasični policijski rad, koji je suštinski reaktivnog karaktera, gotovo sasvim je ustupio mesto proaktivnom policijskom radu, koji se još naziva i „policijskim radom rukovođenim obaveštajnim radom" (*intelligence-led policing*) i proističe iz prirode savremenih bezbednosnih pretnji, pre svega organizovanog kriminala i terorizma. Proaktivni policijski rad, sam po sebi, donosi brojna pitanja u odnosu na tradicionalni domen građanskih i ljudskih prava. On se zasniva na aktivnom i često agresivnom prikupljanju podataka u odnosu na osobe koje niti su osuđivane za krivično delo, niti u trenutku prikupljanja informacija čine neko krivično delo. Stoga je mogućnost zloupotrebe proaktivnog policijskog rada izuzetno izražena, a otvaraju se i brojna pitanja u vezi sa integritetom čuvanja i upotrebe prikupljenih podataka. Autor u tekstu raspravlja neka od navedenih pitanja, locirajući ih pre svega u sferu novih metodologija za borbu protiv organizovanog kriminala koje se razvijaju primarno u SAD. Pitanja o ljudskim pravima se u tom kontekstu sagledavaju kao jedna od varijabli savremenog „bezbednosnog društva". Tekst pozicionira ovo pitanje u kontekstu fenomena „sekuritizacije" društvenog diskursa. U tekstu se raspravlja pitanje do koje mere su argumenti zagovornika „sekuritizacije" opravdani, a u kojoj meri je ograničavanje ljudskih prava prihvatljivo ako se ima u vidu percepcija povišenog stepena pretnje od organizovanog kriminala.

Ključne reči: kriminalistički obaveštajni rad, klasični bezbednosni obaveštajni rad, raspolaganje obaveštajnim materijalom, politička hijerarhija, tradicionalna prava na privatnost.

Primena obaveštajnih metoda u radu policije u borbi protiv organizovanog kriminala podrazumeva značajne kontroverze, koje se pre svega tiču potrebe da se jasno razdvoji obaveštajni materijal dobijen klasičnim bezbednosnim obaveštajnim

* Autor je naučni savetnik u Institutu za međunarodnu politiku i privredu, Beograd.

radom od onog dobijenog kriminalističkim obaveštajnim radom. Sama metodologija prikupljanja ovog materijala u bezbednosnom i kriminalističkom kontekstu najčešće je identična, ali tretman materijala mora biti dramatično različit kada je reč o ova dva tipa službi. Problematika tretmana ovog tipa obaveštajnog materijala je predmet posebne diskusije ovog autora na drugom mestu, a cilj ove analize biće posebne karakteristike dominantnog modela kriminalističko-obaveštajnog rada danas i njihove posledice za integritet društva. Reč je o modelu presretanja komunikacija, koji se smatra intruzivnim, nametljivim obaveštajnim metodom izvedenim iz poznatog tipa bezbednosnog obaveštajnog rada koji se običajno naziva Sigint (*Signals Intelligence*).

Sigint u tradicionalnom bezbednosnom kontekstu

Sigint predstavlja svaki oblik presretanja komunikacija koji se zasniva na tehnologiji elektromagnetnog polja, uključujući tu sve radijske i elektronske komunikacije. On uključuje specifične oblike obaveštajnog materijala do kojih se dolazi, poput elektronskog obaveštajnog materijala (Elint) ili presretanja komunikacija telefonom (Comint). Sigint se obično razdvaja od obaveštajnog rada zasnivanog na upotrebi agenata kao izvora informacija (*Human Intelligence* — Humint) ili upotrebe savremene opreme za mapiranje i geografski nadzor, poput špijunskih satelita (*Image Intelligence* — Imint). Iako su se tradicionalno i Sigint, i Imint, i Humint koristili pre svega u bezbednosnom kontekstu vojnih i paravojnih operacija, danas se sve ove forme obaveštajnog rada primenjuju i u kriminalističkom obaveštajnom kontekstu u borbi protiv organizovanog kriminala. Čak se i Imint danas u SAD koristi za lociranje kretanja transporta oružja, ljudi ili droge, za mapiranje puteva organizovane trgovine ukradenim automobilima, kao i za praćenje terorističkih grupa. Presretanje elektronskih komunikacija ili telefonskih razgovora danas je široko rasprostranjeno u policijskom radu protiv organizovanog kriminala, a neretko se neopravdano i nelegitimno koristi i kao najlakši način suzbijanja i drugih, klasičnih oblika kriminaliteta, iako za to nije namenjen i time se krši princip minimalizma u upotrebi policijskih ovlašćenja, o čemu će biti reči pri kraju ovog teksta.

Primena Siginta je u celini najprisutnija tema u obaveštajnom diskursu danas, uključujući i sistematske analize obaveštajnih operacija, pa se toj temi stoga mora obratiti posebna pažnja kada je reč o njenoj primeni u kriminalističko-obaveštajnom kontekstu.[1] Popularnost Siginta proističe iz lakoće i bezbednosti

[1] Videti primera radi: Cees Wiebes, *Intelligence and the War in Bosnia 1992–1995*, Lit Verlag, Münster, 2003.

njegove primene i iz njegovog velikog potencijala u prikupljanju širokog spektra informacija o različitim temama. U današnjoj literaturi jasno su prepoznate kako dobre, tako i loše strane Siginta, koje se moraju imati u vidu prilikom donošenja strateške odluke o njegovoj manje ili više širokoj primeni u kriminalističko-obaveštajnom radu. Ovde će stoga biti nešto detaljnije razmotrene prednosti i mane Siginta kako bi se formirao kontekst za izvođenje zaključaka o bitnim elementima njegove policijske primene.

Pozitivne karakteristike Siginta kao metode prikupljanja obaveštajnog materijala

1. Primena presretanja komunikacija upotrebom elektromagnetnog polja pre svega lišava obaveštajnu službu i operativce gotovo svih rizika sa kojima se oni tradicionalno suočavaju prilikom prikupljanja podataka korišćenjem drugih metoda, posebno Huminta. Postavljanje prislušnog uređaja (kada je to potrebno, a danas često nije, jer je signal moguće „uhvatiti" u vazduhu) je bezbedno, omogućava da se komunikacijama pristupi iz udobnosti kancelarije ili operativne stanice, sa velike udaljenosti, bez ikakvog rizika po bezbednost operativca, pa i bez rizika za otkrivanje praćene komunikacije. Na ovaj način se postiže pre svega visok stepen bezbednosti, ali se omogućava i procesuiranje komunikacije uz dovoljno vremena i pažnje, što je inače problem kada se operativno deluje u realnim situacijama u kojima vlada napetost. Ukratko, Sigint postavlja obaveštajnog operativca u potpuno superiornu poziciju u odnosu na subjekta koji se prati.
2. Informacije do kojih se dolazi presretanjem komunikacija su obično objektivne, to jest nisu prejudicirane ličnim stavovima agenta, što je često slučaj pri Humintu, niti odnosima agenta sa subjektima praćenja. Takođe, one ne podležu organizacionim, političkim i drugim predrasudama.
3. U nekim slučajevima primena Siginta omogućava da se izbegne jedno od osnovnih pravila obaveštajnog rada, a to je da se svaka informacija proverava iz najmanje dva izvora. Poznato je da je postupanje na osnovu informacije koja nije proverena mnogo puta dovelo do ozbiljnih negativnih posledica, kako bezbednosnih, tako i političkih, slično postupanju na osnovu takozvane sirove obaveštajne informacije ili materijala, bez prethodne analize i kritičkog sagledavanja u svetlu drugih informacija. Kada je reč o transkriptima presretnutih komunikacija, oni ponekad, ali ne uvek, mogu biti toliko uverljivi da se mogu koristiti bez potrebe da se dodatno proveravaju na osnovu informacija dobijenih Humint-om ili Imint-om. Reč je, očigledno, o velikoj

prednosti ove vrste prikupljanja obaveštajnih podataka, jer se na ovaj način omogućava značajna ušteda vremena i resursa obaveštajne službe.

4. U vezi sa prethodnom prednošću, Sigint je, zbog osobina tehnologije koja se pri njemu koristi, brzo raspoloživ krajnjim korisnicima. Presretnute e-mail komunikacije, radio ili telefonski razgovori, mogu se gotovo u realnom vremenu elektronskim putem preneti na velike udaljenosti i staviti na raspolaganje donosiocima odluka u udaljenim krajevima sveta. Američka Nacionalna bezbednosna agencija (*National Security Agency* — NSA) ima danas najrazvijeniji i najobuhvatniji sistem elektronskog praćenja sa globalnim dosegom, tako da je u stanju da presreće praktično sve vrste komunikacija u bilo kom delu sveta i da taj materijal koristi sa minimalnim odlaganjem u stizanju do krajnjeg korisnika.
5. Presretanjem komunikacija dobija se velika količina informacija koje se odnose na očekivani predmet, ali često i na druge značajne teme (poput drugih krivičnih dela u kriminalističko-obaveštajnom kontekstu), što je jedinstvena osobina koju nema obaveštajni materijal do koga se dolazi upotrebom agenata ili tehnologije za imidžing. Stoga je informativna vrednost materijala dobijenog Sigintom obično znatno veća od drugog obaveštajnog materijala. Poznati su primeri kada je policija, korišćenjem Siginta u kriminalističko-obaveštajnom kontekstu, prateći, recimo, organizovanu trgovinu zabranjenom robom u okviru delatnosti organizovane kriminalne grupe dolazila do informacija o pripremi ubistava. Time se tada otvaralo pitanje o načinu na koji je trebalo intervenisati radi sprečavanja ubistva, a da se pri tome ne kompromituje čitava operacija praćenja organizovanog šverca ljudi, oružja ili droge. Reč je o opštoj osobini Siginta da neselektivno omogućava pribavljanje informacija o svemu onome o čemu subjekti komuniciraju, pri čemu se ponekad ne može pretpostaviti šta može biti rezultat takvog praćenja komunikacija.
6. Pozitivna osobina Siginta je i da „nikada ne spava", to jest da može stalno biti u funkciji. Kada je reč o Humintu, situacija je sasvim drugačija. Jedan agent ne bi trebalo da bude aktivan duže vreme u kontinuitetu; on se mora odmarati kako fizički, tako i obaveštajno i strateški. Kada se ponovo aktivira, bilo bi idealno da se to čini u odnosu na druge subjekte, pa i u drugom geografskom prostoru, uz što veću vremensku udaljenost od prethodnog aktiviranja, kako bi se izbeglo otkrivanje. Sa Sigintom, nema potrebe za odmaranjem, i informacije se, neprimećeno, prikupljaju u kontinuitetu.
7. Sigint je moguće vrlo jednostavno „fokurisati na subjekt", pa i na više različitih subjekata u kratkom vremenskom intervalu. Kada se plasira agent u neku

sredinu, ta taktika zahteva vreme za pripremu, priliku, logističku podršku, obezbeđivanje pomoći u slučaju opasnosti, a svi ti elementi podrazumevaju da mora prvo postojati fokus na nekom subjektu (npr. neka osoba ili grupa), a tek potom se gradi struktura koja stoji iza agenta poslanog u tu sredinu. Kada agenta treba povući, to često nije jednostavno, jer bi bilo upadljivo i moglo bi dovesti do reakcije subjekata koja, u nekim situacijama, može poništiti veliki deo vrednosti informacija koje je agent prikupio. Naročito je komplikovano plasirati agenta u neku drugu sredinu u kratkom vremenskom periodu. Sigint omogućava da se, uz postojanje odgovarajućih tehnoloških kapaciteta (neke obaveštajne službe, pre svega u SAD, imaju tehnološke mogućnosti da praktično presreću sve komunikacije globalno) promeni fokus za svega nekoliko sati i prate komunikacije neke druge grupe. Reč je o velikoj prednosti Siginta u odnosu na Humint u smislu fleksibilnosti fokusa.

8. Često su podaci do kojih se dolazi primenom Siginta takvi da donose neuporedivo veću korist od bilo kakvih informacija koje pribavljaju agenti. Možda je najočigledniji primer „razbijanje" zaštitne šifre za šifrirane komunikacije. Kada se to jednom postigne, ukoliko je neprimetno, a šifru je moguće promeniti u vrlo kratkom roku, dobija se spektar informacija visoke vrednosti.
9. Odnos Siginta prema Humintu je često povoljan u smislu troškova, jer investicija u opremu i obuku kadrova daje dugoročne povratne rezultate zbog velike količine informacija koje se kontinuirano mogu nabavljati.

Slabosti Siginta

1. Obaveštajni materijal do koga se dolazi presretanjem komunikacija je, po pravilu, u demokratskim društvima klasifikovan visokim stepenom zaštite informacija, što znači da se automatski stavlja na raspolaganje samo vrlo uskom krugu političkih i bezbednosnih donosilaca odluka. Ta činjenica, kao i protokoli koji regulišu restrikcije u raspodeli ovakvog materijala, često dovode do toga da relevantne informacije dobijene Sigintom ne dospevaju, ili bar ne dospevaju dovoljno brzo, do operativaca na terenu koji bi mogli da deluju na sprečavanju bezbednosne pretnje. Upravo to je bila slabost obaveštajnog rada pre 11. septembra 2001. godine, pa se pokazalo da su neka upozorenja o pripremi terorističkih napada na SAD u centrale obaveštajnih agencija i drugih bezbednosnih struktura stigle dan ili dva nakon što je napad izvršen. Restriktivnost u raspolaganju Sigintom je deo demokratske organizacije društva, ali istovremeno može ograničiti njegovu vrednost za operativno delovanje.

2. Drugo ograničenje Siginta, takođe u demokratskim društvima, odnosi se na normativne restrikcije na upotrebu informacija koje on sadrži. Primera radi, u obaveštajnim strukturama je tokom druge polovine prošlog veka bilo rašireno pravilo da prva rečenica u svim Sigint izveštajima upozorava korisnike (mali broj njih na vrhu državne hijerarhije) da se na osnovu informacija sadržanih u izveštaju ne sme postupati, čak ni da bi se sprečila bezbednosna pretnja, ukoliko bi takvo postupanje moglo otkriti izvor informacija. Drugim rečima, ako Sigint sadrži rezultate praćenja elektronskih komunikacija neke grupe, i postupanje po nalazima tog praćenja bi grupi ukazalo da je bezbednosna struktura u stanju da čita njenu šifru, postupanje bi bilo često zabranjeno da grupa ne bi promenila šifru ili modus komunikacije, čime bi obaveštajna agencija naglo postala „gluva" u odnosu na grupu.

   Oktobra 1995. godine, australijska služba za Sigint, *Defence Signals Directorate* (DSD), presrela je šifrovanu komunikaciju indonezijske vojske iz koje se videlo da se sprema ubistvo pet australijskih novinara uhapšenih u Istočnom Timoru. Ova informacija nije prosleđena australijskom premijeru, jer je DSD pretpostavio da bi on nešto preduzeo ili bi čak javno obznanio da ima takvu informaciju, čime bi se možda sprečilo pogubljenje novinara, ali bi se istovremeno Indonežanima otkrilo da DSD može da ih „sluša". Svih pet novinara je ubijeno. Sličnih primera ima još tokom proteklih decenija u selektivnoj upotrebi Siginta.[2]

3. Sigint često nije predmet poverenja u tradicionalnim obaveštajnim sistemima čija kultura se zasniva na Humint-u. Primera radi, tokom Hladnog rata bilo je uobičajeno da se nalazi dobijeni Sigintom tretiraju kao nedovoljno pouzdani za operativno postupanje dok se ne potvrde Humintom.

4. U savremenim uslovima Sigint se smatra, nasuprot prethodnom iskustvu, jedinim pouzdanim izvorom informacija, pa se zanemaruje Humint. To dovodi do problema u interpretaciji elektronski dobijenog obaveštajnog materijala koji, iako u nekim slučajevima može biti gotov obaveštajni proizvod, to ipak uglavnom nije i zahteva procesiranje, obradu i interpretaciju da bi se na osnovu njega moglo postupati. To procesiranje podrazumeva stavljanje tog materijala u odgovarajući kontekst. U bar dva slučaja pripreme NATO saveza ili Varšavskog ugovora za manevre tokom Hladnog rata, koje je detektovao sistem Siginta druge strane, gotovo da je došlo do izbijanja ozbiljnog nuklearnog sukoba, jer su nalazi Siginta, bez odgovarajuće kritičke

[2] Cees Wiebes, *Intelligence and the War in Bosnia 1992–1995*, op. cit., p. 225.

interpretacije, shvaćeni kao indikacija pripreme napada druge strane. U obaveštajnoj literaturi ovaj fenomen isključivog oslanjanja na Sigint se ponekad naziva „snobizam Siginta" ili „sindrom zelenih vrata".

5. Potreba za interpretacijom Siginta, u slučajevima kada sam obaveštajni materijal nije istovremeno i obaveštajni proizvod, često zahteva vreme. U nekim situacijama ni informacije dobijene Sigintom ne mogu biti na vreme pretvorene u operativno upotrebljive podatke da bi se sprečila bezbednosna pretnja.
6. Najznačajnija slabost Siginta je u činjenici da se njime dobijaju milioni informacija svakog dana, te da ni najrazvijene obaveštajne službe često ne mogu analitički da se izbore sa tolikom količinom materijala. Iako je sam obaveštajni materijal osnova obaveštajnog rada, kada njegova količina prevaziđe određene limite, on postaje prepreka. U svojoj knjizi Vibs (Wiebes) navodi reči admirala Mekonela (McConnell), direktora Nacionalne agencije za bezbednost SAD (NSA) 2005. godine, koji je, govoreći o tehnološkim kapacitetima NSA za Sigint – verovatno najvećim od svih obaveštajnih agencija u svetu, rekao: „Dobra vest je da ova agencija može dekodirati i analizirati milion poruka dnevno; loša vest je da treba odlučiti kojih milion poruka da dekodiramo od milijardi poruka koje presrećemo na globalnom planu".[3] U ovom kontekstu, Humint ima jasnu prednost, jer je dobro pozicionirani agent u stanju da pravi kritičke procene informacija, da ih selektuje na licu mesta i da ih prosleđuje i formuliše na načine koji olakšavaju njihovo dalje procesiranje.
7. Konačno, treba imati u vidu činjenicu da tipični subjekti interesovanja obaveštajnih agencija nisu tehnološki pasivni u odnosu na presretanje komunikacija Sigintom, pa je suprotstavljanje Sigintu prilično razvijeno. Neke metode tehničkog sprečavanja Siginta uključuju:
   (a) obezbeđivanje signala posebnim protokolima za upotrebu frekvencija, korišćenjem različitih metoda ometanja i elektromagnetnog „zamračenja" u vreme transmisije sopstvenog signala;
   (b) česte promene šifre kada je reč o šifriranim transmisijama;
   (c) upotreba „skokovite frekvencije", pri čemu se poruka emituje promenljivom frekvencijom koju može da „uhvati" samo legitimni primalac poruke, kome je unapred poznat strukturni model skakanja frekvencije, a svako ko poruku pokušava da presretne pri prvoj promeni frekvencije prosto gubi signal;

[3] Ibid., p. 227.

(d) upotreba „snop transmisije" (*burst transmissions*), pri čemu se iznenada, velika količina informacija emituje u signalu od svega nekoliko sekundi, koji potom odmah prestaje, čime se maksimalno smanjuje raspoloživo vreme za aktiviranje uređaja za presretanje i povećava protok informacija preko granice koja omogućava čitljivo „hvatanje signala";

(e) upotreba „raširenog spektra", pri čemu se informacija emituje istovremeno na više različitih frekvencija, pa presretanje jedne frekvencije daje samo nerazumljiv deo poruke;

(f) namerno emitovanje pogrešnih informacija sa ciljem da one budu presretnute;

(g) upotreba kriptografije, to jest kriptovanih poruka.

8. Treba naglasiti i da Sigint može služiti političkim ciljevima pojedinaca koji njime raspolažu, pogotovo kada se ima u vidu ekskluzivnost informacija koju protokoli za raspolaganje Sigintom obično podrazumevaju.

Zbog svega navedenog, Sigint je izuzetno osetljiv način prikupljanja obaveštajnih podataka, kako u klasičnom, tako i u kriminalističkom obaveštajnom radu. Međutim, njegova osetljivost u kriminalističkom obaveštajnom radu je još znatno veća nego u klasičnom obaveštajnom radu.

Specifičnosti i rizici kriminalističkog obaveštajnog rada

Za razliku od klasičnog bezbednosnog obaveštajnog rada, čiji je cilj prikupljanje obaveštajnog materijala koji, nakon obrade, omogućava operativno delovanje na zaštiti nacionalne bezbednosti (špijunaža i kontraspijunaža), kriminalistički obaveštajni rad služi za suzbijanje „mekih" pretnji bezbednosti, pre svega organizovanog kriminala i jednim delom terorizma. U borbi protiv terorizma se sve više koriste i vojne strukture i klasični bezbednosni obaveštajni rad, jer je terorizam svojom bitnom dimenzijom i pitanje za političke strukture. Organizovani kriminal, koji je legitiman predmet interesovanja kriminalističko obaveštajnih struktura, nije pitanje za političke strukture. Praćenje organizovanog kriminala, za razliku od praćenja subjekata interesovanja klasičnog obaveštajnog rada (stranih predstavništava, grupa, vojnih i diplomatskih misija, terorističkih grupa), odvija se isključivo na suverenoj teritoriji i strogo u skladu sa zakonom. Dok je klasični obaveštajni rad, pogotovo kada se primenjuje na teritoriji druge države, po definiciji delovanje van granica zakona, kriminalistički obaveštajni rad mora biti u celosti zakonit. Osim toga, kriminalistički obaveštajni rad podrazumeva sve standarde zaštite privatnosti i drugih građanskih i ljudskih prava. Stoga on, za

razliku od tradicionalnog bezbednosnog obaveštajnog rada, podrazumeva bitnu *selektivnost*. Ta selektivnost proističe iz činjenice da se kriminalističke obaveštajne metode primenjuju za suzbijanje organizovanog kriminala kada postoji jasnom sumnja da se priprema krivično delo, sa krugom osumnjičenih, i na osnovu naloga tužioca, istražnog sudije i predsednika Vrhovnog suda (u Srbiji), tako da se informacije do kojih se eventualno dođe primenom ovih metoda, van domena određenog nalogom, moraju tretirati kao poverljive.

Osnovni problem u primeni kriminalističkog obaveštajnog rada proističe upravo iz navedene potrebe za selektivnošću, to jest iz činjenice da se daleko najveći deo ukupnog rada sastoji iz presretanja komunikacija (Sigint) i iz napetosti koja postoji između opšte osobine Siginta da je neselektivan po prirodi i zakonske obaveze da se njegovi rezultati, u kriminalističko-obaveštajnom kontekstu, tretiraju selektivno. Jedna od prednosti Siginta navedenih u prethodnom odeljku upravo je njegova neselektivnost, koja predstavlja pozitivnu stranu ove metode u klasičnom obaveštajnom radu. Presretanje komunikacija diplomatskog predstavništva neke zemlje za koju se pretpostavlja da ima neprijateljske namere prema zemlji domaćinu podrazumeva otvorenost za sve vrste informacija: ako se presretanjem komunikacija ustanovi da neki diplomata te zemlje švercuje retke vrste ptica iz zemlje domaćina umesto da se bavi špijunažom, i ta informacija je korisna za operativno delovanje na sprečavanju šverca ptica. Generalno posmatrano, od informacija do kojih se dolazi u klasičnom obaveštajnom radu se ne očekuje da budu prihvatljive u sudskom postupku, nego da budu operativno upotrebljive i da donesu korist u sprečavanju neke pretnje bezbednosti. Suprotno tome, u kriminalističko-obaveštajnom radu često je bitno da informacije budu prihvatljive u sudu, i cilj nije samo operativno sprečavanje pretnje bezbednosti (mada to svakako jeste jedan od ciljeva), već i zakonsko procesuiranje počinilaca dela organizovanog kriminala. Istovremeno, zakonska ograničenja, koja u načelu uopšte ne važe za klasični obaveštajni rad, jer se on odvija po definiciji u najvećoj meri van domena zakona, ne dopuštaju da se, primera radi, informacije koje se dobiju o nekoj javnoj ili političkoj ličnosti, a koje se ne odnose na organizovani kriminal niti na sumnju na osnovu koje je izdat nalog za presretanje komunikacije, koriste protiv te ličnosti.

Selektovanje informacija dobijenih metodom koji je, pre svega, tehnološki složen, zahteva skupu opremu i obučene kadrove, a pošto je po prirodi i neselektivan, stvara relativno obuhvatne probleme. Oprema kojom raspolažu manje zemlje, a koja se koristi za Sigint, obično je u rukama vojnih i civilnih obaveštajnih službi. Njeno stavljanje na raspolaganje policiji podrazumeva nabavku duple opreme, ali i obuku kadrova. U prelaznom periodu prirodno je da

isti kadrovi rukuju istom opremom za različite svrhe; kako za svrhe klasičnog obaveštajnog, tako i za svrhe kriminalističko-obaveštajnog rada. Ti kadrovi su obučeni za određene protokole i često se dešava da oni sa informacijama u celini postupaju na identičan način. Kada se ima u vidu činjenica da u klasičnom obaveštajnom radu rezultati Siginta dolaze na raspolaganje ličnostima na vrhu političke i bezbednosne hijerarhije, postaje jasan problem u tome da se u rukama istih ličnosti nađu i informacije dobijene kriminalističko-obaveštajnim radom. Dok jedan predsednik države treba da ima sve informacije u vezi sa pretnjama od terorizma, potpuno je neprihvatljivo da on raspolaže informacijama o presretanju komunikacija zbog sumnje na organizovani kriminal zajedno sa neselektivnim informacijama o javnim i političkim ličnostima. Takve informacije ne smeju biti dostupne bilo kojoj političkoj ličnosti.

Autonomija sistema za borbu protiv kriminala, uključujući i organizovani kriminal, u odnosu na politički sloj upravljača u društvu je od ključnog značaja. U tome se sastoji i osnovna razlika u upotrebi informacija dobijenih klasičnim obaveštajnim radom od onih dobijenih kriminalističkim obaveštajnim radom. Kriminalistički obaveštajni rad, tehnički obično istovetan klasičnom obaveštajnom radu, za razliku od njega, mora biti tajan u odnosu na najviši politički vrh jednog društva. Ne sme postojati način da neki političar dođe do obaveštajnih podataka prikupljenih u kontekstu kriminalističkog obaveštajnog rada, a za sve one u krivičnopravnom sistemu koji omoguće takvu distribuciju obaveštajnog materijala moraju se primenjivati drakonske sankcije. Samo na taj način moguće je održati razuman stepen integriteta kriminalističko-obaveštajnog rada.

U razvijenim zemljama odnos političke strukture i policijske profesije je regulisan po opštim pravilima koja uređuju status javne administracije u političkom sistemu. Na čelu svakog ministarstva, pa tako i ministarstva unutrašnjih poslova, stoje jedna ili dve osobe koje su politički imenovane, uključujući obično samog ministra i eventualno državnog sekretara ili pomoćnika ministra. Svi ostali zaposleni su profesionalno agnažovani. Između ministra, koji obično niti je stručan za policijski posao, niti zna način delovanja policije, i profesionalnih policajaca postoji hijerarhija koja je vrlo uslovna. Ministar donosi odluke iz domena opštih pitanja, obezbeđuje finansijske i materijalne uslove za rad policije, bavi se ključnim kadrovskim i materijalnim upravljačkim odlukama, i učestvuje u formulisanju opšte strategije rada ministarstva, ali on, u demokratskim državama, nema nikakva ovlašćenja da deluje kao nalogodavac prema policiji u operativnom delovanju. Drugim rečima, ministar nema pravo da se meša u tekuće policijske istrage (kod nas bi to bio pretkrivični postupak), da izdaje naloge za postupanje ili nepostupanje po nekom pitanju, pa čak ni da ima detaljan uvid u stanje nekog predmeta. Ministar,

ukratko, ne treba uopšte da bude ovlašćen da pristupa predmetima i da se njima na bilo koji način bavi. Samo na taj način se obezbeđuje da svaki policijski službenik, po unutrašnjoj hijerarhiji, bude odgovaran za postupanje po predmetima iz svog domena ovlašćenja i rada. Uz poštovanje tog principa, mogućno je zaštiti i obaveštajni materijal prikupljen kriminalističkim obaveštajnim radom od političke upotrebe, a i od uvida političkih ličnosti.

U nedovoljno razvijenim zemljama, poput Srbije, ministar unutrašnjih poslova ima ovlašćenje da deluje kao nalogodavac policiji. On, primera radi, može izdati nalog da policija neku osobu uhapsi ili urgirati da se neko procesuira, što je svojevrstan apsurd za svaku državu koja sebe vidi kao demokratsku. Ministar u nerazvijenim sistemima ima uticaj i ovlašćenja nad ministarstvom „po dubini", što obično znači da u dubinskim strukturama buja korupcija i neefikasnost, političke linije se štite i promovišu. Sve je znak da je profesionalnost na niskom nivou. U svakoj policiji, u kojoj ministar ima moć po dubini, nema ni približno dovoljno profesionalnosti za demokratske standarde.

Kada se ima u vidu činjenica da ovakvi nedovoljno efikasni sistemi danas raspolažu ovlašćenjima da koriste Sigint, ali i Humint i Imint, postaje jasno kakve to rizike podrazumeva na planu zaštite privatnosti i ličnih podataka, ali i na kakav drastičan način neizgrađen represivni institucionalni sistem ugrožava osnovne principe demokratskog poretka.

Opšta klima u svetu, koja se ponekad naziva trendom „bezbednosnog društva", u kome se mnoga tradicionalna građanska prava i slobode ograničavaju u korist jednog nametljivijeg modela policijskog i kriminalističko-obaveštajnog rada, pre svega zbog pretnje od terorizma, ali i organizovanog kriminala, pogoduje dodatnom razvijanju negativnih strana zastale ili propale tranzicije u institucionalnom kontekstu represivnog aparata u nekim zemljama. Tolerancija na sve agresivnije načine prikupljanja podataka o građanima, uz sve manje proceduralnih, pa i tehničkih organičenja i istovremeno nedostatak svesti i mehanizama za sprečavanje zloupotrebe takvih informacije od strane političkih aktera, omogućavaju da se, pod fasadom borbe protiv novih pretnji bezbednosti, praktično „sekuritizuje" celo društvo i da se, uz izgovor o potrebi za borbom protiv organizovanog kriminala i terorizma, suzi domen legitimnog prava na samoizražavanje, na kritički stav, na političke razlike, pa i na socijalni protest.

U primitivnim društvenim kontekstima koji nisu dovoljno napredovali u tranzicijama, postoji tendencija da se ovlašćenja koriste na maksimumu, i istovremeno postoji nerazumevanje smisla principa da se ona ne koriste kada nisu neophodna. Slično tome, postoji tendencija da se svi postupci opravdavaju time što su „u skladu sa zakonom", čak ikada su očigledno necelishodni i neprimereni

realnim životnim okolnostima. Mogućno je činiti veliku štetu društvu „u skladu sa zakonom", kao što je, takođe u skladu sa zakonom, moguće i dobro upravljati. Nedovoljno izgrađeni upravljački stavovi u represivnom sistemu, u kome se samo postojanje mogućnosti za korišćenje kriminalističko-obaveštajnog rada shvata i kao pravo da se on koristi uvek kada može biti od koristi, čak i kada je to samo prečica ka istim rezultatima koji se mogu postići na druge, manje problematične načine, podrazumevaju stanje u kome je kriminalističko-obaveštajni rad više štetan nego koristan za samo društvo. To je jedan od klasičnih paradoksa nedovršenih tranzicija u kojima modeli javne politike i tehnike borbe protiv pretnji bezbednosti, umesto da budu deo rešenja, postaju deo problema.

CRIMINAL INTELLIGENCE AND CIVIL AND HUMAN RIGHTS TRADITION

Methodology of development trends in modern policing is significantly different from traditional policing. Classical policing, being essentially reactive and activated only upon filing of a criminal report or detection of a crime committed, has almost entirely been replaced by a more proactive type of policing, also known as "intelligence-led policing". This new style of policing has been introduced due to the nature of modern security threats, such as organised crime and terrorism, shifting the focus from prosecution to crime prevention, given drastic effects that such threats may cause. The nature of proactive policing raises numerous issues concerning the traditional sphere of human and civil rights. Namely, this type of policing is based on an active and often aggressive process of intelligence gathering against persons who have no criminal record or persons who did not even commit any criminal offence whatsoever at the time of being subjected to this intelligence gathering. Hence, proactive policing, i.e. criminal intelligence, is highly likely to be abused and may raise various concerns over the integrity of use and retention of intelligence data collected in such a manner. This paper discusses some of the above issues, primarily new methods of fighting organised crime that have been developed mostly in the United States. In this context, human rights issues are regarded as one of the variables of modern "security society". The paper also discusses this issue in the context of "securitisation" of social discourse. The term "securitization" was invented by Ole Weaver, a Scandinavian theorist, to denote a tendency of modern political elites to associate all kinds of relations in a society with security concerns, with a view to justifying various forms of manipulation in the sphere of governance. The paper explores this issue and ask how reasonable Weaver's arguments may be and to what extent human rights restriction could be deemed acceptable, given the public perception of increasing threat posed by organised crime.

OBAVEŠTAJNA KRIMINALISTIČKA MREŽA: ORUĐE ZA KONTROLU ORGANIZOVANOG KRIMINALA

Dragan Manojlović[*]

APSTRAKT

Kriminalisti se ne interesuju za kriminalne pojave sâme po sebi, već za probleme koji su u vezi sa manifestacijom kriminalne pojave i refleksijom njene statističke slike u vrednovanju njihovog učinka. Ovakav pristup ima dalekosežne posledice sa više aspekata. Već krajem osamnaestog veka kriminalistička teorija i praksa je počela da napušta pojedinačni model kontrole kriminala nazvan „pecanje sa jednom udicom i jednim štapom ili više udica i više štapova" i krenula put kriminalističko-obaveštajnih mreža u kriminalnom miljeu. Jedan broj autora je tada zauzeo stanovište da je „jednom udicom moguće uloviti jednu krupnu ribu, a da je mreža ta koja omogućava ulov više krupnih, a često i predvodnika jata sa mnogo manjih, ali značajno velikih riba". Razume se, verujem, iako se to ne vidi u nas, da smo svesni da je „pojedinačno pecanje sa jedom udicom i jednim štapom, pa i sa više štapova" daleka prošlost, a da je obaveštajna mreža u kriminalnom miljeu efikasnije sredstvo.

Ključne reči: kriminalni milje, obaveštajna kriminalistička mreža, kontrola organizovanog kriminala, bezbednost.

Često se ističe u kriminalističko-obaveštajnim istraživanjima da je istorija kriminalnih delatnosti samo jedna od učiteljica. Ovo verovanje je ispravno samo ako mu ne izmiče jedna važna činjenica: svaki kriminalni događaj je jedinstven, različit od svih drugih. Stojeći tako u kriminalnim dosijeima (obaveštajnim analitičkim bazama) oni imaju i nešto što ih povezuje, *modus operandi*, *perseveranca* i dr. Šta nam sa aspekta kriminalističko-obaveštajnog rada govori sama činjenica da se pojave u kriminalnom miljeu ponavljaju?[1] Činjenica da se

---

[*] Autor je docent na Pravnom fakultetu Univerziteta u Novom Pazaru.

[1] Kriminalni milje obuhvata: a) prostor u više njegovih oblika; b) kriminalnu delatnost u svim njenim oblicima; c) kriminalno tržište; d) ilegalne ili legalne robe ili dobra i usluge; e) aktivne i pasivne učesnike u kriminalnoj delatnosti; f) kriminalni profit.