Zbornik
Instituta za kriminološka i
sociološka istraživanja
2012/ Vol. XXXI / 2 / 85-101

Originalni naučni rad
UDK: 343.982:004.4

PRIMENA SAVREMENIH TEHNOLOGIJA U KONTROLI KRIMINALA*

Marina Kovačević-Lepojević*
Vesna Žunić-Pavlović*
Fakultet za specijalnu edukaciju i rehabilitaciju, Beograd

Uporedo sa tehnološkim napretkom i pojavom novih krivičnih dela, do promena dolazi i u oblasti društvene kontrole kriminala. Negativizacija pojma rizičnosti i širenje straha od kriminala doprinose negovanju podržavajućeg stava stručnjaka i građana o upotrebi savremenih tehnologija u cilju smanjenja potencijalne viktimizacije. Povreda osnovnih ljudskih prava prihvata se kao neminovna žrtva uz prividnu garanciju bezbednosti građana opredeljenih za takozvani život pod nadzorom.

Rad ima za cilj sagledavanje pozitivnih i negativnih aspekata primene savremenih tehnologija u kontroli kriminala. U radu su razmotrene konceptualne i praktične implikacije primene video nadzora, biometrijske identifikacije, prisluškivanja i nadzora nad elektronskom komunikacijom građana u kontroli kriminala. Preispitane su kritike stručne i laičke javnosti koje se odnose na pitanja zloupotrebe privatnosti, kršenja ljudskih prava, podsticanja marginalizacije, socijalne isključenosti, stigmatizacije, bezbednosne propuste posredstvom upotrebe savremenih tehnologija. U završnom delu date su preporuke za prevazilaženje uočenih nedostataka pri primeni predmetnih tehnologija.

* Ovaj tekst je nastao kao rezultat rada na projektu "Kriminal u Srbiji: fenomenologija, rizici i mogućnosti socijalne intervencije" (broj 47011) koji finansira Ministarstvo prosvete, nauke i tehnološkog razvoja RS.
* E-mail: marina.lepojevic@gmail.com.
* E-mail: zuniceva@eunet.rs.

Zbornik IKSI, 2/2012 – M. Kovačević-Lepojević, V. Žunić-Pavlović „Primena savremenih tehnologija u kontroli kriminala”, (str. 85-101)

KLJUČNE REČI: tehnologije / kriminal / video nadzor / biometrijska identifikacija / prisluškivanje

UVOD

Okruženje u kome se kriminal danas ispoljava, zahteva i promenu pristupa u kontroli kriminala. Značajne promene u vršenju i društvenoj reakciji na kriminal nastale su usled rapidnog razvoja tehnologije.

Tehnologija se danas smatra bitnim oruđem u vršenju kriminala i viktimizacije, s tim što se kod pojedinih tehnologija kao što su bezbednosne, razmere viktimizacije samo naslućuju s obzirom na manipulaciju velikom količinom podataka o ličnosti. Pri reagovanju na kriminal uz upotrebu tehnologija prednost se daje unapređivanju prakse preventivnog postupanja, mnogo manje sankcionisanju i tretmanu. Danas u tu svrhu koriste biometrijske tehnologije, video nadzor, tehnologije za nadzor nad komunikacijama i drugo. Klark smatra da su tehnologije doprinele promenama ne samo u reagovanju na kriminal, već i njihovom izučavanju (Clarke, 2004). Konvencionalnoj kriminologiji suprotstavlja se takozvana "nauka o kriminalu" koja mora biti mnogo primenljivija, sa akcentom na razumevanje kriminala umesto kriminalaca, momentalnu redukciju kriminala umesto dugotrajne socijalne reforme, redukovanje štete nanete žrtvama umesto pomaganja kriminalcima, problemski umesto teorijski orijentisana, usmerena promeni politike u kontroli kriminala (Clarke, 2004:56). Poslednjih godina "situaciona prevencija" prerasta u "nauku o kriminalu" (Knepper, 2009:58), odnosno najdirektnije proizilazi iz takozvane nauke o kriminalu, koja je isto ono što je i socijalna prevencija za tradicionalnu kriminologiju (Clarke, 2004:56). Situaciona prevencija kriminala podrazumeva identifikovanje, promenu i kontrolu faktora koji deluju u situaciji u kojoj se ispoljava kriminalno ponašanje (Cornish, Clarke, 2003). Godinama unazad ovaj pristup prepoznat je kao uspešan u prevenciji i redukovanju kriminala na specifičnim mestima (aerodromi, granični prelazi, javni prevoz, škole, zatvori, ulice).

Globalno širenje uticaja kapitalizma i industrijalizacije, posebno razvoj vojne industrije, doprinose ubrzanom razvoju bezbednosnih tehnologija u cilju unapređivanja kontrole i nadzora modernog društva. Iako bi danas pod okriljem neoliberalizma teorijski trebalo da ubiramo plodove oslobađanja uticaja države na ekonomiju, politički život, kulturu, pa i reagovanje na kriminal, u praksi je situacija nešto složenija. I pored predviđanja Gidensa (1998) da nadolazeći trend postmodernizma između ostalog neizostavno pretpostavlja oslobađanje uticaja države i humanizaciju tehnologija

odnosno bavljenje važnim etičkim i moralnim aspektima, empirijski podaci pokazuju suprotno. Naime, intervencionizam država, posebno u zemljama gde se "sloboda najglasnije izgovara" poput SAD u poslednjih nekoliko decenija povećao. Takva vrsta mešanja države je prema rečima autora dobila naglašeno klasni karakter, uz popularizaciju tehnologija koje služe za lakši nadzor građana (Navarro, 2007).

Nameću se pitanja u kojoj meri su rizici, onako kako ih danas percipiramo, produkovani i koji su pravi dometi proklamovane brige za bezbednost građana i unapređivanja nacionalne sigurnosti država. Autori se slažu da u današnjem društvu, popularno nazvanom društvu rizika, ljudi u velikoj meri žive život sa "strahom kao pogledom na svet" (Svensen, 2008:57). Iako je reč rizik prvobitno mogla da ima i pozitivno i negativno značenje, u aktuelnim društvenim prilikama najčešće se svodi na sinonim za opasnost. Prema tome, niko nije bezbedan, bez obzira na društveni status i druge razlike. Autori razmatraju tezu o gradovima kao izvorima straha koji su prvobitno podizani da zaštite stanovnike od spoljnih opasnosti. Građanima su na raspolaganju različite tehnologije koje bi trebalo da ih zaštite, ali i obezbeđuju praćenje i nadzor različitih aspekata njihovog života, pa je kako Svensen (2008) primećuje nadziranje građana intenzivnije i ekstenzivnije nego ikada ranije i sve veći deo privatnih života postaje vidljiv za nevidljive posmatrače. Međutim, pitanje je koliko je svojevrsna žrtva privatnosti prihvatljiva građanima i koliko su tehnologije po sebi rizične. Klark je još sedamdesetih godina predvideo društvo u kome niko neće znati da li se svaki njegov pokret posmatra, svaka reč sluša, ili će pak svi znati da je to tako, ali je izvesno da niko neće videti nikakvo zlo u tome (Klark, 2009:197).

Rad je predmetno usmeren na različite aspekte primene savremenih tehnologija u kontroli kriminala. Cilj rada predstavlja analiza primene video nadzora, biometrijske identifikacije, prisluškivanja i praćenja elektronske komunikacije, izdvajanje negativnih posledica primene uz pružanje smernica za njihovo prevazilaženje.

PRIMENA SAVREMENIH TEHNOLOGIJA U KONTROLI KRIMINALA

Stručnjaci smatraju da su biometrijska identifikacija, video nadzor, skeniranje i nadzor nad komunikacijama najzastupljenije bezbednosne tehnologije čija primena izaziva uvek aktuelne polemike u savremenom društvu (Pavone, Esposti, 2012).

Video nadzor u svom tehnološki najnaprednijem obliku (CCTV) predstavlja britanski nacionalni simbol za situacionu prevenciju kriminala. Maja 2008. godine britanska pop grupa *Get Out Clause* snimila je spot putem CCTV

sistema.[1] Sa uvođenjem video nadzora započelo se šezdesetih godina u bankama i prodavnicama u Velikoj Britaniji i SAD pretežno radi osiguravanja kapitala, ekonomskih i političkih interesa, smanjenja straha od kriminala kod građana. Tokom devedesetih godina Velika Britanija je potrošila dve trećine godišnjeg budžeta na uvođenje video nadzora, a posebno posle 1993. godine nakon pogibije dvojice desetogodišnjih dečaka od teroriste IRA u Bišopgejtu (Bishopgate) (Knneper, 2009). Uočene su znatne razlike u rasprostranjenosti, razvoju i zakonskoj regulativi video nadzora među različitim državama i gradovima Evrope (Kovačević-Lepojević, Žunić-Pavlović, 2012). Primena video nadzora na javnim mestima u Srbiji posredno je regulisana specifičnim propisima. U cilju unapređenja funkcionisanja sistema video nadzora saobraćajnica i raskrsnica u Beogradu, a u skladu sa *Zakonom o bezbednosti saobraćaja na putevima*, doneta je *Obavezna instrukcija o uslovima korišćenja i održavanja sistema video nadzora gradskih saobraćajnica i raskrsnica za grad Beograd*. Ove odredbe regulišu pravo pristupa podacima, procedure preuzimanja snimaka iz arhive, odgovornost organizacionih jedinica PU za grad Beograd i preciziraju način održavanja sistema. *Zakon o sprečavanju nasilja i nedoličnog ponašanja na sportskim priredbama* propisuje obaveze organizatora da obezbedi tehničku opremu za praćenje i snimanje ulaska i ponašanja gledalaca na sportskom objektu. Prema *Zakonu o igrama na sreću,* priređivač je dužan da obezbedi neprekidan audio-video nadzor stolova i aparata za igru, ulaza i izlaza u igračnicu, igrača i posetioca, kao i da dokumentaciju o neprekidnom snimanju čuva deset dana, a po nalogu Uprave i duže. Prema *Zakonu o zaštiti državne granice*, granična policija je ovlašćena da, radi vođenja evidencija, prikuplja lične podatke putem različitih tehničkih sredstava, pa i putem video nadzora. U Republici Srbiji ne postoje propisi kojima se reguliše primena video nadzora u školama i ustanovama za izvršenje krivičnih sankcija, već se konkretno o primeni odlučuje na nivou pojedinačnih institucija (Kovačević-Lepojević, Žunić-Pavlović, 2012). Video nadzor zaposlenih u Srbiji takođe nije posebno regulisan.

Biometrijske tehnologije omogućavaju automatsku identifikaciju osobe na osnovu njenih bioloških karakteristika i ponašanja (Johnson, 2004:90). Principi na kojima se zasniva biometrijska identifikacija su: univerzalnost (svi ljudi poseduju biometrijske karakteristike), distinktivnost (ljudi se međusobno razlikuju po svojim biometrijskim karakteristikama), permanentnost (biometrijske karakteristike se ne menjaju tokom života), jednostavnost primene (lako je izvršiti biometrijsku identifikaciju uz malu mogućnost greške)

[1] http://www.youtube.com/watch?v=W2iuZMEEs_A

(Jain et al., 2000). Sistemi identifikacije razvijaju se i usložnjavaju velikom brzinom od onih tradicionalnih - ono što znamo (šifra, PIN) ili imamo (token, identifikaciona kartica), do modernog sistema - ono što sami jesmo (fizičke karakteristike) (Pfitzmann, 2009). Od biometrijskih identifikatora najčešće se primenjuju uzimanje otisaka prstiju, prepoznavanje lica i prepoznavanje zenica oka, a nešto ređe se za identifikaciju koriste geometrije šake, mrežnjača oka, lični potpis, glas, prokrvljenost ručnog zgloba, način hoda, miris, struktura uha i drugo. U zavisnosti od toga da li je osoba svesna procesa identifikacije u konkretnom slučaju ona može biti pasivna (na primer, prepoznavanje lica) i aktivna (na primer, prepoznavanje zenice oka) (Pfitzmann, 2009). Različite situacije zahtevaju primenu različitih sistema za identifikaciju, ali se preporučuje njihovo kombinovanje u cilju obezbeđivanja zaštite na više nivoa, jer postoji mogućnost da se osoba ne identifikuje ili da se pogrešno identifikuje (Miller, 1994). Otisak prsta se za identifikaciju koristi još 7000 godina pre nove ere o čemu svedoče zapisi Asiraca i Kineza, mada nema dokaza da su korišćeni na univerzalnom nivou. Za identifikovanje kriminalaca koristi se od osamdesetih godina 19. veka, pre svega u Argentini, zatim Velikoj Britaniji, da bi se šezdesetih godina 20. veka počelo sa pravljenjem elektronske baze otisaka prstiju (Gorman, 1998). Baza biometrijskih podataka SAD sadrži 70 miliona otisaka prstiju osoba koje su identifikovane kao kriminalci, 34 miliona građana i 73 000 osoba koje su okarakterisani kao teroristi (FBI, 2012). Prepoznavanje lica pretpostavlja poređenje i preko velikog bioloških karakteristika na licu (na primer, razmak između očiju, oblik brade, jagodica i slično). Prepoznavanje lica je međunarodno prihvaćeno kao primarna biometrijska karakteristika u pasošima građana, dok se otisak prsta može koristiti opciono kao sekundarni biometrijski podatak. Kao deo biometrijskih podataka lične karte u Srbiji prema *Zakonu o ličnoj karti* nalaze se fotografija, otisak prsta i potpis (član 7), dok *Zakon o putnim ispravama* (član 24) predviđa fotografiju i potpis kao sadržaj pasoša.

DNK profilisanje se ne vrši automatski, ima najveću preciznost i mnoge druge specifičnosti, pa se u radovima neretko izdvaja kao posebna kategorija. Prva i do danas najveća nacionalna baza DNK profila pod nazivom *The National DNA Database* osnovana je aprila 1995. godine u Velikoj Britaniji. Sadrži DNK profile izolovane iz bioloških uzoraka sa tri izvora: sa mesta zločina, od osumnjičenih i od volontera uz pristanak na jednokratnu upotrebu biološkog uzorka ili njegovo trajno zadržavanje. Pripadnici policije takođe ostavljaju svoje DNK profile od 2002. u sklopu obavezne procedure kao deo baze pod nazivom *Police Elimination Database*, dok ih oni zaposleni pre tog perioda ostavljaju na dobrovoljnoj bazi radi sprečavanja kontaminiranja mesta zločina (Williams et al., 2004).

Raspolaže sa preko pet miliona DNK profila (NDNAD, 2010:6). Predviđeno je da se u nacionalnom DNK registru Srbije nađu biološki materijali punoletnih osuđenih na kazne zatvora preko godinu dana i maloletnika osuđenih na najteža krivična dela. Predviđa se postojanje još tri registra: arhiva bioloških materijala osumnjičenih i okrivljenih za vreme trajanja krivičnog postupka, registar nestalih lica i forenzički DNK registar u kome će se čuvati svi biološki tragovi pronađeni na mestu zločina koji se ne poklapaju sa postojećim DNK tragovima u arhivama osuđenih i okrivljenih (Politika Online, 2012).

Prisluškivanje, praćenje elektronske komunikacije, pretraživanje baza podataka o ličnosti i neovlašćeno zadržavanje podataka se smatra posebno ugrožavajućim sredstvom za unapređivanje nacionalne i globalne sigurnosti, posebno ukoliko se ne vrši na osnovu odobrenja suda, već u takozvane preventivne svrhe. Nakon terorističkih napada 11 septembra 2001, Ministarstvo odbrane SAD promovisalo je *Total Information Awareness System* (TIAS) koji je nastao u cilju pravovremenog detektovanja, klasifikovanja i identifikovanja aktivnosti terorista i predupređivanja terorističkog akta. TIAS integriše tri aktivnosti: automatski prevod jezika, pretragu podataka i prepoznavanje obrazaca od značaja i adekvatnu koordinacija službi i brzo donošenje odluka. Tim putem, pretražuje se telefonska, radio, elektronska i komunikacija licem u lice, ali i knjige, video i audio zapisi i druga dokumenta (Stevens, 2003). *Zakon o krivičnom postupku Republike Srbije* kao i zakonodavstvo većine evropskih zemalja sadrži odredbe koje se tiču mera tajnog nadzora i snimanja komunikacije koja se obavlja putem telefona ili drugih tehničkih sredstava ili nadzor elektronske ili druge adrese osumnjičenog i zaplenu pisama i drugih pošiljki (član 166). Naredbu iz člana 167. stav 1. ovog zakonika izvršava policija, Bezbednosno-informativna agencija ili Vojno-bezbednosna agencija. O sprovođenju tajnog nadzora komunikacije sačinjavaju se dnevni izveštaji koji se zajedno sa prikupljenim snimcima komunikacije, pismima i drugim pošiljkama koje su upućene osumnjičenom ili koje on šalje dostavljaju sudiji za prethodni postupak i javnom tužiocu na njihov zahtev. Poštanska, telegrafska i druga preduzeća, društva i lica registrovana za prenošenje informacija dužna su da državnom organu koji izvršava naredbu (BIA, VBA, MUP) omoguće sprovođenje nadzora i snimanja komunikacije i da, uz potvrdu prijema, predaju pisma i druge pošiljke. Po završetku tajnog nadzora komunikacije organ iz člana 168. stav 1. ovog zakonika dostavlja sudiji za prethodni postupak snimke komunikacije, pisma i druge pošiljke i poseban izveštaj koji sadrži: vreme početka i završetka nadzora, podatke o službenom licu koje je nadzor sprovelo, opis tehničkih sredstava koja su primenjena, broj i raspoložive podatke o licima obuhvaćenim nadzorom i ocenu o

svrsishodnosti i rezultatima primene nadzora. Prema članu 178 na obrazloženi predlog javnog tužioca sud može odrediti računarsko pretraživanje već obrađenih ličnih i drugih podataka i njihovo poređenje sa podacima koji se odnose na osumnjičenog i krivično delo. Po završetku računarskog pretraživanja podataka državni organ dostavlja sudiji za prethodni postupak izveštaj koji sadrži: podatke o vremenu početka i završetka računarskog pretraživanja podataka, podatke koji su pretraženi i obrađeni, podatke o službenom licu koje je sprovelo posebnu dokaznu radnju, opis primenjenih tehničkih sredstava, podatke o obuhvaćenim licima i rezultatima primenjenog računarskog pretraživanja podataka. Tajni nadzor i računarsko pretraživanje u Srbiji bez odluke suda smatra se neustavnim. Podaci koje prikupljaju internet pretraživači, sajtovi za socijalno umrežavanje i komunikaciju ne koriste se samo u komercijalne svrhe, već se smatraju vrlo aktuelnim za državne službe. Prema podacima kompanije *Google* u prvih šest meseci 2012. godine trideset zemalja je uputilo 20.938 zahteva za otkrivanje privatnih podataka o korisnicima, među kojima najviše SAD (7.969), Indija (2.319), Brazil (1.566), Francuska (1.546), Nemačka (1.533) i Velika Britanija (1.425) (Google Transparency Report, 2012).

KRITIKA PRIMENE SAVREMENIH TEHNOLOGIJA U KONTROLI KRIMINALA

Još od vremena kada su britanski kriminolozi "doneli svetu situacionu prevenciju" (Knneper, 2009:57), prisutan je skepticizam u vezi sa dometima koje ona može imati, a koji se sa tehnološkim razvojem još više povećao. Iako su tako nastale nove mogućnosti za primenu tehnologija u svetlu prevencije i redukcije kriminala, otvorila su se i mnoga pitanja o negativnim posledicama upotrebe. Tehnologije je trebalo da u prvobitnoj zamisli pomognu ljudima da stave svet pod svoju kontrolu i učine život predvidljivijim, ali je to izmaklo kontroli, stvoren je nekakav "odbegli svet", u kome opasnosti koje smo sami stvorili stvaraju podjednaku ili veću pretnju od onih koje nam dolaze spolja (Gidens, 2005:60). Smatra da rizik ima dvostruku oštricu kada je nauka u pitanju, da je blisko povezan sa inovacijom, pri čemu se sa razvojem tehnologije zapaža prelaz dominacije spoljašnjeg na dominaciju proizvedenog rizika (Gidens, 2005).

Politizacija i komercijalizacija razmatranih tehnoloških oruđa je nesporna. Diznilend pruža dobar primer za komercijalizaciju tehnologije u službi zabave, počevši od arhitekture, osoblja, voznog parka, animacija, organizacije

posetilaca, nevidljivog sistema, pri čemu je sve pod nadzorom. Pa se izraz "dizniizacija"[2] koristi da opiše procese planiranja prevencije kriminala u britanskim gradovima orijentisanih oko elektronskog nadzora (Knepper, 2009:68). Prema tome, planiranje prevencije je u službi obezbeđivanja zone sigurne kupovine i zabave. Autori opisuju hipokriziju američkog društva koje koristi frazu "nacionalne odbrane" za razvoj industrije i ojačavanje ekonomskih kapaciteta (Wade, 2007). Očigledno je da su biznis i industrija osnovni pokretači za uvođenje novih tehnologija u svakodnevni život i kontrolu kriminala. Kriminolozi prirodno moraju uzeti učešće u evaluaciji i poboljšanju bezbednosti pomažući da se zaštite zaposleni i klijenti od viktimizacije (Clarke, 2004). Smatra se da su jaki privedni interesi upleteni u održavanje ili povećanje straha stanovništva. Međutim, nije izvesno da li osećanje ugroženosti doprinosi primeni bezbednosnih mera ili obrnuto. Autori smatraju da se oni međusobno pojačavaju, odnosno da osećanje ugroženosti stanovništva povećava primenu bezbednosnih tehnologija, koje utiču na dalje stimulisanje straha (Svensen, 2008). Kako primećuje Garland (2001:194-5) primena nauke i tehnologije u kontroli kriminala zapravo predstavlja "novu kulturu kontrole kriminala", promovisanu od strane političkih i kulturnih vrednosti kasnog modernizma, gde intenzivnija regulacija i kontrola samo doprinose da građani budu manje tolerantni, kao i znatno isključiviji i nepoverljiviji. Ono što prouzrokuje strah nisu samo teroristi koji se nalaze na nekom određenom mestu, već i medijsko izveštavanje o tome koliko su oni opasni, što se kasnije koristi da se opravdaju neke mere za obezbeđivanje sigurnosti građana. Savremene metode izveštavanja definitivno utiču na povećavanje svesti o riziku, pa i preuzimanje kontrole nad definisanjem i regulisanjem rizika (Tompson, 2003). Na primer, u SAD se sredstva za obezbeđenje od terororizma zasnivaju na broju terorističkih ciljeva, što daje podstrek državama da izveste o što većem broju ciljeva, pa su se na listi tako našle i prodavnice sladoleda, đevreka i slično (Svensen, 2008).

Deo kritika odnosi se na produbljivanje raslojavanja, socijalne isključenosti, stigmatizacije, marginalizacije i nejednakosti u društvu, izostajanje socijalne zaštite. Smatra se da je neoliberalna ideologija odgovor dominantnih klasa na uspeh koji su postigli radnička klasa i seljaci, posle II svetskog rata i sedamdesetih i da je ekonomska i socijalna politika tome doprinela, odnosno mehanizmi poput deregulacije tržišta rada, prometa robe i usluga, privatizacija javnih službi, promocija individualizma i komercijalizma i drugo (Navarro, 2007). Prema tome, u duhu neoliberalne ideologije samo pojedinac može biti problematičan po rođenju, socijalizaciji, moralnom

[2] Engleski izraz "Disneyisation"

deficitu i slično. Sigurnost tako može biti ugrožena samo od strane "opasnih kriminalaca (niže klase)" ili pak terorista zanemarujući pritom uticaj globalnog kapitalističkog sistema i državnih politika što podržava Marksovu tezu o održavanju dugoročnog interesa kapitala (Kanduč, 2009:67-69). Međutim, na primeru skandinavskih zemalja gde se kriminal ne može objasniti siromaštvom, nepovoljnim socioekonomskih statusom, klasnim razlikama, slabom obrazovnom politikom i nezaposlenošću, može se videti kako je model situacione prevencije kriminala kompatibilan sa merama socijalne zaštite (Knepper, 2009). Međutim, i prenaglašavanje socijalne zaštite može biti stigmatizujuće po pojedince, odnosno marginalizovane i posebno ranjive slojeve društva. Autori primećuju da socijalne službe od klijenata traže detaljne privatne podatke, očekuju kooperaciju u smislu promene vrednosti, stavova, ponašanja. Zatim, deo pojedinaca ne kontaktira dobrovoljno socijalne službe rehabilitacionog ili drugog karaktera, već po odluci suda i slično (Knepper, 2009). Prema tome, ne može se unapred reći koliko će konkretno neka bezbednosna tehnologija biti disciplinujuća i stigmatizujuća po pojedinca, sve zavisi od načina primene. Na primeru video nadzora autori objašnjavaju da sočivo, kablovi, rekorder i drugi tehnički delovi neophodni za funkcionisanje video nadzora nemaju po sebi ni socijalnu ni kriminološku dimenziju, dok se ne smeste u odgovarajući kontekst (Norris, McCahill, 2006:30).

Postavlja se pitanje mogu li bezbednosne tehnologije imati bezbednosne propuste. Pri primeni pojedinih bezbednosnih tehnologija, pre svega biometrijskih tehnologija može doći do greške pri identifikaciji, do pogrešnog prepoznavanja ili do neprepoznavanja osobe. Najveća mogućnost greške je kod prepoznavanja lica, srednja kod prepoznavanja zenice oka, potpisa, glasa i geometrije šake, a najmanja kod otiska prsta (Luis-Garcia et al., 2003: 2543). S godinama biološke katrakteristike bivaju teže prepoznatljive, a postoji rizik i da je usled nekih povreda na radu, sredinskih uticaja, genetskih faktora ili starenja došlo do izvesnih promena koje vode, na primer do neprepoznavanja otiska prsta (Jain et al., 2000). Mali broj ljudi nema zenicu, dok slepima može biti teško da upere pogled u kameru da bi ih identifikovali, kao i onima sa tremorom očiju (PRISE, 2007). Istraživanjem kvaliteta sistema video nadzora u Londonu u četiri različita konteksta utvrđena je svojevrsna tehnološka neefikasnost prema kojoj se dve trećine postojećih sistema oslanja na fiksne kamere, bez digitalnog snimka i mogućnosti za kompjutersku obradu slike i nedovoljno operatera zaduženih za nadzor (Norris, McCahill, 2006).

Na osnovu biometrijskog podatka mogu biti dobijeni i neki privatni podaci. Na primer, na osnovu zenice oka može se otkriti podatak da li je osoba

koristila PAS, trudnoća ili uzrast, pri prepoznavanju lica uočiti emocionalno stanje, dok se putem DNK profilisanja raspolaže najosetljivijim informacijama o osobi (Van der Ploeg, 2005). Na primer iz genetičkog materijala osobe, može se otkriti njeno poreklo ili boja kose, pri čemu se kako nauka napreduje povećava se broj dostupnih informacija koje se tim putem mogu saznati. Tim putem prikupljene informacije mogu poslužiti kao osnov za diskriminaciju osobe koja je nosilac DNK profila od interesa i njenih srodnika. U slučajevima kada se DNK profil sa mesta zločina ne poklapa sa profilima skladištenim u bazi podataka, pretraživanje se vrši po principu "približnog" poklapanja, uz očekivanje da se u bazi nalazi neko od bliskih srodnika osumnjičenog (roditelj, dete ili sibling). Ova tehnika u istrazi se primenjuje još od 2002. godine, na osnovu koje je identifikovan tada već preminuli ubica i silovatelj Joe Kappen čija DNK je pronađena na telima tri žrtve (Cartney, 2006). Skladištenje DNK profila donosi mnoga pitanja kao na primer da li treba čuvati podatke osumnjičenih pre optuženja, optuženih pre utvrđivanja krivice, osuđenih nakon odsluženja kazne, da li se biometrijski podaci koriste samo u svrhe za koje su namenjene, ko ima pristup podacima i drugo. Važeći britanski propisi o funkcionisanju nacionalne baze DNK profila sadrže odredbe koje se tiču vremena skladištenja genetičkog materijala: neograničeno zadržavanje kod odraslih osuđenih lica; šestogodišnje zadržavanje kod osumnjičenih, ali ne i osuđenih; neograničeno zadržavanje kod maloletnih izvršilaca teških krivičnih dela ili višestrukih učinilaca; petogodišnje zadržavanje kod maloletnika osuđenih za jedno lakše krivično delo; šestogodišnje zadržavanje kod šesnaestogodišnjaka i sedamnaestogodišnjaka koji su bili osumnjičeni, ali ne i osuđeni za teško delo; trogodišnje zadržavanje kod maloletnika koji su bili uhapšeni, ali ne i osuđeni; dvogodišnje zadržavanje kod osumnjičenih za terorizam nakon isteka mere kontrolisane slobode; i uništavanje DNK profila koji je dat volonterski odmah nakon ispunjenja svrhe davanja (NDNAD, 2009/10:11).

Može se reći da rezultati istraživanja ne potvrđuju popularnost primene savremenih tehnologija u bezbednosne svrhe. Podaci o efektivnosti primene video nadzora u redukciji kriminala su prilično neusaglašeni i u najvećoj meri zavise od prirode nadzora, karakteristika okruženja, kulturnog konteksta, vrste krivičnog dela, od toga da li se koristi izolovano od drugih preventivnih intervencija, koliki je period praćenja, kakva je podrška sredine, u odnosu na koje vrste krivičnog dela se merenje vrši i drugo. Podaci o smanjenju kriminala nakon uvođenja video nadzora se prilično razlikuju, a izmerena redukcija se kreće od 7% do preko 50% u pojedinim studijama (Žunić-Pavlović, Kovačević-Lepojević, 2010). Zajednički zaključak većine evaluacija je da ova mera daje bolje rezultate kada je u pitanju prevencija imovinskih krivičnih dela (posebno bezbednost vozila), kao i unapređivanje bezbednosti u javnom prevozu i

saobraćaju uopšte. Daleko slabiji rezultati su zabeleženi u prevenciji nasilnih krivičnih dela (Žunić-Pavlović, Kovačević-Lepojević, 2010). Istraživanja pokazuju da sistem za prepoznavanje lica na aerodromima funkcioniše sa 50% uspešnosti u prepoznavanju, a postoje podaci da se na javnim mestima tim putem ostvaruje redukcija kriminala za 20-40% (Bowyer, 2004). Iako je popularnost Nacionalne baze podataka Velike Britanije velika, teško je izmeriti koliko ona doprinosi redukciji kriminala, pa kako primećuju autori na desetogodišnjicu uspostavljanja baze još nema dostupnih nezavisnih evaluacija koji bi njenu popularnost opovrgli ili opravdali (Williams et al., 2004). U izveštaju o radu NDNAD (2003/04:23) ukazuje se na podatak da se samo 17% od prijavljenih krivičnih dela forenzički obradi, 5% od obrađenih mesta zločina pruži DNK podatke za skladištenje u bazu, što predstavlja 0,85% od ukupno izvršenog kriminala. Obrađena mesta zločina su u periodu od 1998. do 2009. donela 182.277 razrešenih krivičnih dela, pri čemu su osumnjičeni priznavali druga krivična dela za koja nisu postojali DNK tragovi u 121.888 slučajeva (NDNAD, 2008/09:35). Govoreći o ogromnim sredstvima koja se ulažu u prisluškivanje i procena da manje od 1% presretanih poruka ima bilo kakav značaj za nacionalnu bezbednost Klark (2009:204) smatra da efikasnost u oblasti nacionalne odbrane nikada nije bila važan kriterijum primene. Dalje, svega nešto preko 6% novca koji se godišnje uloži u nacionalnu odbranu i vojnu industriju, potroši se na kontrolu kriminala na federalnom, državnom i lokalnom nivou i da možda zbog toga ima toliko mnogo ratova i kriminala (Klark, 2009). Rezultati istraživanja stavova građana Evropske unije o primeni bezbednosnih tehnologija pokazuju da su se oni najnegativnije izjašnjavali o upotrebi tehnologija sa kojima imaju najmanje dodira, kao što je uređaj za skeniranje do gole kože ili tehnologija koje najviše zadiru u privatnost kao što je centralizacija biometrijskih podataka u registre. Autori smatraju da bi trebalo razmotriti primenu alternativnih tehnologija baš zbog slabe efektivnosti na primer video nadzora ili pojedinih biometrijskih identifikatora (Jacobi & Holst, 2007). Sa druge strane, postoje krupni metodološki problemi u merenju očekivanih rezultata bezbednosnih tehnologija, kao na primer nedostatak kontrolnih varijabli ili mešanje efekata više primenjenih mera. Takođe, teško je izmeriti koliko je osoba odustalo od izvršenja dela usled primene bezbednosnih tehnologija i koji su efekti izmeštanja kriminala. Očekuje se da bi prikladne evaluacije doprinele boljem razumevanju potrebe za korišćenjem bezbednosnih tehnologija i olakšali njihovu primenu.

ZAKLJUČAK

Smatra se da je koordinacija slobode, odnosno privatnosti i bezbednosti neophodna za srećan i dostojanstven život i da se svako uvećanje

slobode prirodno tumači kao umanjenje bezbednosti i obrnuto (Bauman, 2009). Iza naglašavanja potrebe za bezbednošću mogu stajati ekonomski razlozi, dok iza aktuelizacije za slobodom i privatnošću mogu stajati politički interesi ili obrnuto. Svensen smatra da ne postoji objektivno merilo prihvatljivog nivoa rizika, gornja granica koliko se bezbednosti može zahtevati, uvek se mogu preduzeti jos neke mere koje će smanjiti slobodu građana i odraziti se negativno na kvalitet života (Svensen, 2008).

Velika verovatnoća da bi podrška građana u pravcu uvođenja bezbednosnih tehnologija bila veća kad bi učestvovali u odlučivanju o primeni, što bi prema rečima Baumana (2009:49) bilo tumačeno kao svojevrsno "praktikovanje slobode". Autor zapaža da ako bi se ponudile mogućnosti čak i za povećanje slobode koje bi bile nametnute, retko bi bile shvaćene kao pravedne, upravo zbog načina na koji je do njih došlo. Kao primer iz domaćeg konteksta može poslužiti projekat uvođenja elektronskih ličnih karata sa biometrijskim podacima o kome se nije mnogo raspravljalo u javnosti, čak je i oprema kupljena pre usvajanja zakona (Šabić, 2008). *Zakon o ličnoj karti* predvideo je biometrijske lične karte, a *Zakon o putnim ispravama* biometrijske biometrijske pasoše. S obzirom na invazivnost DNK profilisanja i činjenicu da se u Srbiji ide u susret uvođenju DNK registra, treba uvažiti preporuke stručnjaka (Williams et al., 2004:126) o neophodnosti šire javne debate pre započinjanja projekta. Javna debata može biti shvaćena i kao način na koji možemo Gidensovim rečnikom "ukrotiti rizik" (Gidens, 2005:61).

Zapaža se da u Srbiji trenutno nema relevantnih institucija ni adekvatne regulative pomoću kojih bi se na neki način pratile tehnološke promene u oblasti kontrole kriminala, ali i ublažile neke od štetnih posledica primene. I pored najsavremenije tehničke zaštite ljudski faktor neminovno može doprineti mnogim bezbednosnim propustima kako zbog nedovoljne obučenosti, tako i zbog nepažnje, zloupotrebe položaja i slično. Podizanje kulture obezbeđenja podataka o ličnosti u Srbiji pretpostavlja uspostavljanje odnosa u kome za one koji se bave obradom i zaštitom podataka stoji obaveza da se redovno bave analizom stanja, procenom pretnji i rizika, definisanjem procedura zaštite u svojim internim aktima i kontinuiranom obukom zaposlenih. Preporučuje se praćenja na tri nivoa - utvrđivanje činjenica o tome ko je i kada ažurirao podatke, zatim ko je i kada pristupio podacima i šta je menjao i koliko (Šabić, 2009:37,39). Ukoliko nije moguće obezbediti posebne propise, na primer, o primeni biometrijskih tehnologija ili video nadzora, Zakon o zaštiti podataka o ličnosti neminovno treba dopuniti rešenjima koja se odnose na pomenuta pitanja. *Direktiva 95/46/EC* Evropskog parlamenta predviđa da podaci o ličnosti treba da budu

prikupljani uz pristanak osoba, samo onda kada je to neophodno, isključivo za svrhu za koju se prikupljaju uz predviđanje neophodnih mera zaštite podataka. Saglasno evropskim propisima o zaštiti podataka o ličnosti treba osigurati da se podaci koriste u skladu sa svrhom prikupljanja (na primer, komercijalna, administrativna ili forenzička), samo kada je to nužno i pod posebno propisanim uslovima. Poverenik za informacije od javnog značaja je više puta izveštavao javnost o slabosti Zakona o tajnosti podataka Republike Srbije; Zakon o vojnim službama je proglašen neustavnim u odredbama da je prisluškivanje bilo moguće bez odluke suda; i pokrenuta je procedura za ocenu ustavnosti Zakona o krivičnom postupku Republike Srbije u odredbama kojim se policiji omogućava pristupanje listinzima o komunikacijama građana bez odluke suda. Godišnjom kontrolom Poverenika i Ombudsmana evidentirano je preko million slučajeva nezakonitog zadiranja u privatne komunikacije građana od strane bezbednosnih službi na godišnjem nivou (Šabić, 2012).

Međutim, čini se da ne samo građani, već i stručnjaci angažovani na pitanjima kontrole kriminala još uvek nedovoljno koriste pozitivne potencijale tehnologija, pa posledično društveno vidljivije postaju negativne strane primene. Autori naslućuju da bi izbor između slobode i bezbednosti mogao biti lažan. Klark (2009:189) smatra da ne postoji izbor između slobode i bezbednosti, da ćemo imati ili oboje ili nijedno, a da se ravnoteža može postići samo izbegavanjem represije. Treba priznati da čovek u izvesnom smislu uvek kasni za tehnologijom, zaostaje u razumevanju i nikad nije u stanju da sagleda sve posledice neke nove tehnologije koja se evidentno razvija brže od kulture zaštite podataka o ličnosti. Posebnu pažnju treba pružiti edukaciji medija koji izveštavaju o potencijalnim doprinosima i opasnostima koje bezbednosne tehnologije nose.

U studiji koja je rađena u Španiji otkriveno je da građani nisu raspoloženi da nekritički ustupe svoju privatnost zarad više sigurnosti, pri čemu su svesni političke manipulacije konceptom nacionalne bezbednosti i borbe protiv terorizma. Prema autorima ove studije (Pavone & Pereira, 2009:123), građani su ukazali na potrebu za "boljom" bezbednošću, a ne za "više" bezbednosti što je ujedno i glavni zaključak ovog rada. Nije nužno menjati slobodu, odnosno privatnost za bezbednost. Autorke smatraju da možemo imati i jedno i drugo ukoliko se angažujemo oko adekvatnog obezbeđivanja tim putem prikupljenih podataka o ličnosti.

LITERATURA

(1) Bauman, Z. (2009). *Fluidni život*. Novi Sad: Mediterran publishing.

(2) Cartney, C. (2006). The DNK expansion programme and criminal investigation. *British Journal of Criminology*, 46 (1), 175-192.
(3) Clarke, R. V. (2004). Technology, criminology and crime science. *European Journal on Criminal Policy and Research,* 10 (1), 55–63.
(4) Cornish, D., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decision: A reply to Wortley's critique of situational crime prevention. *Crime Prevention Studies,* 16 (1), 41-96.
(5) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal L 281 , 23/11/1995 P. 0031 – 0050,* Retrieved November 16., 2012. from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
(6) FBI (2012). *Integrated Automated Fingerprint Identification System*. Retrieved November 16., 2012. from http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis
(7) Garland, D. (2001). *The Culture of Control: Crime and Social Order in Contemporary Society*. NewYork: Oxford University Press.
(8) Gidens, E. (1998). *Posledice modernosti*. Beograd: Filip Višnjić.
(9) Gidens, E. (2005). *Odbegli svet*. Beograd: Stubovi kulture.
(10) Google Transparency Report (2012). *Google Transparency Report – User Data Requsts.* Retrieved November 24., 2012. from http://www.google.com/transparencyreport/userdatarequests/?p=2012-06
(11) Gorman, L. (1998). Overview of fingerprint verification technologies. *Elsevier Information Security Technical Report*, 3 (1), 42-64.
(12) Hempel, L., & Topher, E. (2004). *CCTV in Europe.* Berlin: Centre for Technology and Society.
(13) Jacobi, A., & Holst, M. (2007). *Synthesis Report - Interview Meeting on Security Technology and Privacy*. Vienna: PRISE.
(14) Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification. *Communications of the ACM*, 43 (2), 91-98.
(15) Johnson, M. (2004). Biometrics and Treat to Civil Liberties. *Computer* [IEEE], 37 (4), 90-92.
(16) Klark, R. (2009). *Kriminalitet u Americi*. Beograd: Univrzitet u Beogradu, Pravni fakultet.
(17) Knepper, P. (2009). How Situational Crime Prevention Contributes to Social Welfare. *Liverpool Law Rev,* 30 (1), 57-75.
(18) Kovačević-Lepojević, M., Žunić-Pavlović, V. (2012). Primena video-nadzora u kontroli kriminala. *Specijalna edukacija i rehabilitacija,* 11 (2), 325-345.

(19) Luis-Garcia, R., Alberola-L'opeza, C., Aghzoutb, O., & Ruiz-Alzolab, J. (2003). Biometric identi cation systems. *Signal Processing,* 83, 2539 – 2557.
(20) Miller, B. (1994). Vital signs of identity. *IEEE Spectrum,* 31 (2), 22–30.
(21) Navarro, V. (2007). Neoliberalism as a Class Ideology; Or the Political Causes of the Growth of Inequalities. In V. Navarro (ed.), *Neoliberalism, Globalization, and Inequalities: Consequences for Health and Quality of Life* (pp. 9-27). NewYork: Baywood Publishing Company.
(22) NDNAD (2003/04). The National DNK Database. *Annual report 2003/04.* Retrieved November 24., 2012. from *http://www.forensic.gov.uk/pdf/company/publications/annual-reports/annual-report-NDNAD.pdf*
(23) NDNAD (2008/09). The National DNK Database. *Annual report 2007-2009.* Retrieved November 24., 2012. from http://www.npia.police.uk/en/docs/NDNAD07-09-LR.pdf
(24) NDNAD (2009/10). The National DNK Database. *Eigth Report of Session 1*. London: House of Commons, Home Affairs Committee. Retrieved November 24., 2012. from http://www.publications.parliament.uk/pa/cm200910/cmselect/cmhaff/222/222i.pdf
(25) *Obavezna instrukcija o uslovima korišćenja i održavanja sistema video nadzora gradskih saobraćajnica i raskrsnica za grad Beograd*. Pristupljeno 26. maja 2011. sa http://www.srbija.gov.vesti php?id=152338.
(26) Pavone, V., & Esposti, S. D. (2012). Public assessment of new surveillance-oriented security technologies: beyond the trade-off between privacy and security. *Public Understanding of Science,* 21 (5), 1-16.
(27) Pavone, V., & Pereira, M. (2009). The privacy vs. security dilemma in a risk society: Insights from the PRISE project on the public perception of new security technologies in Spain. In J. Čas (Ed.), *Towards privacy enhancing security technologies – the next steps* (pp. 109-127). Vienna: PRISE.
(28) Pfitzmann, A. (2008). Biometrics – how to put to use and how not at all? *Trust, privacy and security in digital business,* 5185, 1-7.
(29) Politika Online (2012). *Biološki tragovi – najpouzdaniji.* Pristupljeno 10. septembra 2012. sa http://www.politika.rs/rubrike/Hronika/t48750.lt.html
(30) PRISE (2007). *Overview of Security Technologies*. Vienna: PRISE.
(31) Šabić, R. (2008). Biometrija, bezbednost i ljudska prava (transkript sa tribine). *Bezbednost Zapadnog Balkana*, broj 9-10, 33-71.

(32) Šabić, R. (2009). Zaštita naročito osetljivih podataka o ličnosti – neka otvorena pitanja. *Revija za bezbednost,* 3 (6), 34-40.
(33) Šabić, R. (2012). Neophodno je obezbediti punu zaštitu ustavnih garancija o tajnosti komunikacija (Saopštenje poverenika, 2. novembar 2012.). Republika Srbija, Poverenik za informacije od javnog značaja. Pristupljeno 24. novembra 2012. sa http://www.poverenik.rs/sr/saopstenja/1480-neophodno-je-obezbediti-punu-zastitu-ustavnih-garancija-o-tajnosti-komunikacija.html
(34) Stevens, G. M. (2003). *Privacy: Total Information Awareness Programs and Related Information Access, Collection and Protection Laws*. Report for Congress, March 21.
(35) Svensen, L. (2008). *Filozofija straha*. Beograd: Geopoetika
(36) Van der Ploeg, I. (2005). Biometric Identification Technologies: Ethical Implications of the Informization of the Body. *Bite Policy Paper no 1*.
(37) Wade, R. H. (2007). Should we wory about income in inequality? In V. Navarro (ed.), *Neoliberalism, Globalization, and Inequalities: Consequences for Health and Quality of Life* (pp. 95-119). NewYork: Baywood Publishing Company.
(38) Williams, R., Johnson, P., & Martin, P. (2004). *Genetic information and crime investigation.* Durham: University of Durham, England.
(39) Zakon o bezbednosti saobraćaja na putevima. *Službeni glasnik RS*, *br. 41/2009.*
(40) Zakon o bezbednosti saobraćaja na putevima. *Službeni glasnik RS*, *br.* 41/2009.
(41) Zakon o igrama na sreću. *Službeni glasnik RS*, *br. 84/2004.*
(42) Zakon o krivičnom postupku Republike Srbije. *Službeni glasnik RS, br.* 72/2011.
(43) Zakon o ličnoj karti. *Službeni glasnik RS, br. 62/2006, 36/2011*
(44) Zakon o putnim ispravama. *Službeni glasnik RS, br. 90/2007, 116/2008, 104/2009, 76/2010.*
(45) Zakon o sprečavanju nasilja i nedoličnog ponašanja na sportskim priredbama. *Službeni glasnik RS*, *br. 67/2003.*
(46) Zakon o zaštiti državne granice. *Službeni glasnik RS*, *br. 97/2008.*
(47) Žunić-Pavlović, V., & Kovačević-Lepojević, M. (2010). Mere javnog nadzora u službi prevencije kriminala. *Zbornik instituta za kriminološka i sociološka istraživanja, 29* (1-2), 31-49.

Zbornik IKSI, 2/2012 – M. Kovačević-Lepojević, V. Žunić-Pavlović
„Primena savremenih tehnologija u kontroli kriminala", (str. 85-101)

APPLYING MODERN TECHNOLOGIES IN CRIME CONTROL

Along with the technology progress, changes in perpetrating traditional crimes and emerging new criminal acts, major changes in crime control occurred. Negativization of the risk concept and spreading the fear of crime contribute to the supportive attitudes of experts and citizens on the use of modern technologies in order to reduce potential victimization. Violation of human rights is accepted as an inevitable effect along with the apparent guarantee the security of citizens that have determinated for so-called life under control.
The aim of this paper is the consideration of the negative aspects of the application of modern technologies in crime control. At first, conceptual and practical implications of the application of video surveillance, biometric identification, surveillance and monitoring of electronic communication will be analysed and some positive aspects will be stressed. Then, the expert's and public opinion regarding the issues of privacy and human right violation, encouraging marginalization, social exclusion, stigmatization through the use of modern technologies in crime control will be re-examined. Finally, the authors provide recommendations for overcoming the shortcomings in the application of mentioned technologies.

KEY WORDS: technology / crime / video surveillance / biometric identification / eavesdropping