(ZLO)UPOTREBA INFRASTRUKTURE INFORMACIONO KOMUNIKACIONIH TEHNOLOGIJA U KONTEKSTU KONTROLE DRUŠTVENIH RIZIKA*

Dalibor Petrović
Univerzitet u Beogradu – Saobraćajni fakultet

Sadržaj: *Savremeno društvo se, sve češće, tretira kroz sintagmu rizično društvo pod čime se misli na to da tradicionalni društveni kao i institucionalni mehanizmi društvene sigurnosti sve manje vrše svoju očekivanu funkciju, ostavljajući pojedinca prepuštenog rastućim rizicima savremenog načina života. U tom kontekstu informaciono-komunikacione tehnologije (IKT) imaju protivrečnu ulogu omogućavajući, s jedne strane, dalju modernizaciju društva, ali čineći, s druge strane, njegove segmente izložene potpuno novim rizicima. Imajući ovo u vidu cilj rada je da se ukaže na ulogu infrastrukture IKT kako u proizvodnji, tako i u prevenciji i kontroli društvenih rizika. Posebna pažnja biće posvećena mogućnostima zloupotrebe infrastrukture IKT u cilju nadgledanja i kontrole aktivnosti korisnika IKT, bilo da su u pitanju pojedinci, organizacije ili države u celini.*

Ključne reči: *Nadzor, IKT, rizici, infrastruktura, poverenje*

1. Uvod

U drugoj polovini XX veka dolazi do bujanja različitih paradigmi koje za svoj predmet imaju tumačenje transformacije savremenih društava. Međutim, za razliku od temeljne društvene transformacije predmodernih društva, tokom koje dolazi do suštinske promene društvene reprodukcije života, u savremenom dobu takvi procesi imaju «puzajući» karakter. Promene izviru svuda oko nas i mi ih kao takve prepoznajemo ali njihovi uzroci ne leže u revolucionarnoj ili eksplozivnoj transformaciji društvenih sistema i njihovih institucija, kakav je bilo slučaj sa nastankom industrijskog društva. Međutim, iako su nove paradigme društvene promene manje ili više različite, jedna konstanta počinje da se nazire. Reč je o novim informaciono-komunikacionim tehnologijama (IKT) koje prožimaju različite društvene podsisteme, od političkog, preko ekonomskog do kulturnog. U zavisnosti od toga koje efekte ovih tehnologija želimo da analiziramo ove društvene teorije nose različite nazive, od društva znanja, preko umreženog društva do

* Ovaj tekst je rezultat rada na projektu br. 36022, koji se realizuje uz finansijsku podr ku Ministarstva prosvete, nauke i tehnolo kog razvoja Republike Srbije.

informacionog društva. Poslednjih nekoliko decenija, takođe, pojavljuju se nove paradigme, koje u svoje središte stavljaju društvene rizike koji se generišu kao posledica ljudskih aktivnosti, bilo da govorimo o ekološkim rizicima ili nasuprot tome terorizmu ali i paradigme koje govore o novoj konstelaciji društvene moći kao posledica stvarnog ili lažnog pokušaja kontrole pomenutih rizika [1]. Ovde pre svega imamo u vidu teorije nadziranog društva (*surveillance society*) koje svoju ekspanziju doživljavaju upravo u doba masovnog širenja upotrebe IKT, o čemu ćemo u nastavku više govoriti.

2. Nadzirano društvo

Naravno, nije ni malo slučajno zašto teorije o nadziranom društvu svoj procvat doživljavaju krajem XX-og i početkom XXI-og veka, i zašto to koincidira sa razvojem IKT. Nove IKT, kao i u mnogim drugim sferama, revolucionisale su mogućnosti državne ali i svake druge kontrole i nadzora nad građanima. Pomenimo samo razvoj audio i video nadzora (CCTV), izum senzora za detektovanje pokreta ili toplote tela, optičke naprave za noćni nadzor, elektronsko tagovanje, biometrijske uređaje, softvere za nadgledanje komunikacije na internetu koji su u stanju da čitaju email poruke, uključuju personalne web kamere i mikrofone, detektuju lica na fotografijama, i još mnoge druge. Ipak, pogrešno je na nadzor u modernom društvu gledati samo u kontekstu zloupotrebe moći ili pak isključivo kao posledicu širenja novih IKT. Zapravo, reč je o modernom proizvodu organizovanih praksi i želja za efikasnošću, kontrolom i koordinacijom koje datiraju najmanje 400 godina unazad, a svoju ekspanziju doživljavaju sa nastankom modernih država [2, 3]. Gidens ističe da upravo nadziranje predstavlja jedan od četiri osnovna stuba na kojima počivaju moderne države definišući ga kao nadgledanje delovanja podanika države u okviru političke sfere, iako njegov delokrug uveliko prevazilazi ovu sferu. Nadziranje može biti direktno ili, kroz kontrolu informacija, indirektno [4]. Iako je Gidens mišljenja da je kontrola informacija daleko razvijenija od direktnog nadgledanja sa razvojem novih IKT čini se da i ova druga dimenzija nadzora sve više dolazi do izražaja, o čemu ćemo upravo govoriti u nastavku.

Međutim, nadziranje nije samo pitanje države i očuvanja njene sigurnosti i funkcionalnosti, već ono ulazi i u naš život postajući deo praksi koje svakodnevno, dobrovoljno ili ne, upražnjavamo. Pa tako, od dana kad novi član društva dođe na svet on, uz pomoć različitih bebi alarma a neretko i kamera, postaje predmet nadzora svojih roditelja, a kasnije vaspitača i nastavnika u vrtićima i školama. Zaposleni su pod nadzorom na svojim radnima mestima, od kartica putem kojih se registruje ulazak i izlazak u radne organizacije, preko nadgledanja njihove internet komunikacije, do javnog ili tajnog video nadzora. Ali ni izlazak iz stanova, škola, radnih organizacija nije trenutak kada se nadzor nad nama prekida. On se sofisticiranim sistemom kamera za nadzor brzine, pokreta ili prepoznavanje lica vrši dok se vozimo automobilom, koristimo javni prevoz, kupujemo u tržnim centrima ili naprosto koračamo ulicama grada. Ako ovome dodamo legalno ili nelegalno nadziranje naših komunikacionih naprava, mogućnost da neko čita naše email i sms poruke, gleda ili snima naše razgovore putem Skype-a ili čak da nas nadzire putem naših web kamera, jasno je da govorimo o tome da nadzirano društvo nije neka futuristička slika sveta koji je decenijama udaljen od nas već realni svet koji nas veća sada okružuje.

Iako organizovane prakse nadzora, kao što smo već istakli, postoje već nekoliko stotina godina unazad očigledno je da se u njegovom definisanju mora imati u vidu razvoj

novih tehnologija nadziranja čija je posledica ne samo efikasnije nadgledanje sumnjivih lica i aktivnosti već sveobuhvatnije nadgledanje praktično svih članova društva, bili oni sumnjivi ili ne [5]. Imajući to u vidu možemo se pozvati na Liona koji *definiše nadzor kao svrsishodno, rutinizirano, usmereno i sistematično prikupljanje ličnih podataka u cilju kontrole, opunomoćavanja, upravljanja, uticaja ili zaštite* [6]. Nadzor je *svrsishodan* zbog toga što se nadgledanje opravdava kao sredstvo ostvarivanja kontrole ili nekog drugog javno proklamovanog opšteg dobra. On je istovremeno i *rutina* zato što postoji kao deo svakodnevice svih nas. Takođe je i *sistematičan* zato što se izvodi i planira po nekom precizno utvrđenom protokolu. Pored toga, nadzor je i *usmeren*, zato što ima jasno definisan predmet nadgledanja, bilo da se radi o protoku informacija ili o nadgledanju pojedinaca čiji se podaci prikupljaju, pohranjuju, procesuiraju, itd.

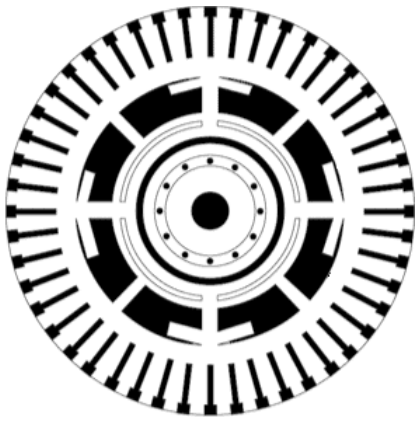
Kada je reč procesu nadgledanja tu se mogu izdvojiti tri glavne faze: društveno sortiranje, kategorizacija i targetiranje [2]. Društveno sortiranje se dešava svakodnevno i može se zapaziti u različitim sferama društvenog života: u oblasti potrošnje, rada, telekomunikacijama, u sferi nacionalne bezbednosti, izdavanju ličnih dokumenata. Kategorisanje podrazumeva sortiranje populacije po određenim kriterijumima i njihovo međusobno rangiranje. Države i institucije vrše ovakve kategorizacije stotinama godina unazad, od zdravstvenih pregleda i ocenjivanja do uniformisanja zatvorenika, vojnika, bolesnika. Jedna od primarnih kategorija državnog nadzora jesu građani, a jedan od najaktuelnijih primera kategorisanja su biometrijski dokumenti. Drugi primer su javni prostori kao i IKT infrastruktura koje se projektuje direktno u cilju što efikasnijeg nadgledanja ovih javnih prostora. Osim sortiranja i kategorisanja i targetiranje predstavlja još jedan način direktnog nadzora na pojedincima. Ovaj vid nadzora je posebno razvijen u marketinškim kampanjama i podstaknut masovnim otvaranjem profila na *online* platformama za društveno umrežavanje. Kroz targetiranje kompanije mogu pratiti navike i potrošnju konzumenata, analizirati njihovu potrošnju i planirati daleko personalizovanije marketinške kampanje.

3. Infrastruktura IKT u službi nadziranog društva

Pre više od dva veka nastaje prvi sistematski razrađen i dizajniran pristup nadziranja ljudi u različitim institucijama poput zatvora, bolnica, škola, sanatorijuma, poznat pod nazivom *Panoptikon*. Ovde je reč o za to doba specifičnom arhitektonskom rešenju, poznatog filozofa Džeremi Bentama (*Jeremy Bentham*) koji se bazira na mogućnost nadzora svih jedinica iz jedne jedine centralne tačke zdanja. Ovakav vid kontrole se obično predstavlja u formi zatvora gde se u njegovom centru nalazi kula a ćelije su raspoređene u kružnoj formi oko nje. Svaka ćelija je vidljiva iz kule dok zatvorenici nikada ne mogu videti da li se neko nalazi u kuli i nadgleda ih (Slika 1). Osnovni principi ovakvog rešenja je stalna vidljivost nadziranog i nevidljivost onog koji nadzire. Međutim, ovaj model nije prikladan samo za zatvore već se može primenjivati i u drugim institucijama poput bolnica ili škola, odnosno u svim institucijama čije funkcionisanje na ovaj ili onaj način zavisi od nadzora i kontrole članova ovih institucija.

Doktrinu panopiticizma aktuelizovao je sedamdesetih godina XX veka, u svojoj knjizi „Nadzirati i kažnjavati“, Mišel Fuko [7]. Fuko ističe da je glavni efekat *Panoptikona* izazivanje osećanja konstantne vidljivosti koja osigurava automatsko funkcionisanje moći. Ovo se postiže na nekoliko načina. Prvo, smanjenjem broja ljudi koji nadziru, čime ono postaje efikasnije jer se sa istim brojem nadzirača može povećati

broj nadziranih. Drugo, time što postoji stalna pretnja da nadzirač može da se umeša u bilo kom trenutku, čime se stvara osećaj konstantnog pritiska zbog čega nadziranje vrši svoju funkciju i pre nego što se prekršaj desi. Treće, nadzor se nikada ne prekida, on se vrši spontano i tiho, stvarajući mehanizam čiji efekti slede automatski, odnosno jedan za drugim. I na kraju, zato što bez i jednog fizičkog instrumenta, osim arhitekture i geometrije, deluje direktno na nadzirane pojedince.



Slika 1. *Panoptikon*

Iako danas ovakav vid arhitekture nije sveprisutan, doktrina panopticizma ostaje na snazi. Sada ulogu urbanističke zamenjuje tehnološka infrastruktura koja omogućava neuporedivo efikasniji nadzor nego što ga je Bentam ikada mogao zamisliti. IKT infrastruktura sada obezbeđuje permanentno i skriveno nadziranje, a simboličku funkciju kule za nadzor preuzimaju različite bezbednosne agencije širom sveta. Primena IKT dovodi ideal nevidljivosti nadzirača da savršenstva ujedno proširujući svoj obuhvat kao nikada do sada [5].

Digitalizacija nadzora je po Grahamu i Vudsu važna iz dva razloga [8]. Prvo, ona obezbeđuje nadgledanje, razvrstavanje prioriteta i prosuđivanje koje se dešava na širokom geografskom području uz veoma kratko vremensko odlaganje. Drugo, dozvoljava neprestano sortiranje, identifikovanje, uspostavljanje prioriteta i praćenje pojedinaca, ponašanja i karakteristika određene populacije u realnom vremenu. To znači da digitalizacija dovodi do automatizacije samog nadzora. Ono što je ključno, rad ljudskih operatera se pomera sa direktnog posredovanja i diskrecije na dizajniranje, programiranje, nadgledanje i održavanje polu ili u potpunosti automatizovanih sistema za nadzor. Ovo je važno i zbog toga što su digitalne tehnologije za nadzor izuzetno fleksibilne i ambivalentne. S jedne strane, sistem može biti dizajniran da izvrši društveno isključivanje bazirano na automatizovanom procenjivanju društvenih ili ekonomskih vrednosti. S druge strane, isti sistem može biti programiran tako da pomaže prevazilaženje društvenih barijera i procesa marginalizacije različitih društvenih grupa. Pored toga, digitalno nadziranje je sveobuhvatnije u odnosu na tradicionalno i u sebi sadrži različite mere, koje mu omogućavaju da bude intenzivnije i ekstenzivnije. Njegova pažnja sad je proširena sa nadgledanja osoba na nadgledanje sistema i mreža [5].

Infrastruktura IKT se upotrebljava za društveni nadzor na najmanje tri nivoa [9]:

1. Nadziranje javnih prostora

2. Nadziranje komunikacija

3. Nadziranje tela

Nadziranje javnih prostora sofisticiranim sistemom kamera za nadzor (CCTV) predstavlja najuočljiviji vid nadzora. Gde god da se okrenemo kamere su oko nas: na bankomatima, u ulazima zgrada, na saobraćajnicama, parkovima, trgovima, u tržnim centrima, itd. Može se pretpostaviti da većina ljudi sa odobravanjem gleda na sistem video nadzora jer imaju u vidu njegovu osnovnu funkciju prevencije kriminalnih dela, čime se povećava osećaj sigurnost građana. Sa druge strane, postoji bojazan da će daljim razvojem i usavršavanjem ovog sistema naša privatnost biti potpuno narušena. Ovo je realna bojazan kada se zna da već sada postoje sistemi video nadzora opremljeni softverima za detekciju lica i pokreta; detekciju gužve i protoka ljudi, detekciju nedostajućih objekata, prepoznavanje lica, prepoznavanje registarskih tablica, targetiranje, pozicioniranje i praćenje subjekata i objekata, analizu ponašanja i prepoznavanje anomalija.

Drugi, praktično nevidljiv, ali možda i delotvorniji vid nadzora odvija se kroz upotrebu softvera za nadgledanje komunikacije putem interneta i mobilnih telefona ali i transporta. Jedan od najkorišćenijih alata je *paket za dubinsku inspekciju* (*Deep Packet Inspection-DPI*) koji služi za nadgledanje saobraćaja na internetu. Ovaj alat funkcioniše tako što pregleda pakete koji dolaze i odlaze sa računara ili druge komunikacione naprave analizirajući svih sedam slojeva podatkovnih paketa. Na ovaj način dobijaju se podaci koji se nalaze u nazivu (*header*) i sadržaju (*payload*) paketa, kao što su protokoli, aplikacije, URL, sadržaj medija, teksta, brojeva kreditnih kartica itd. Drugi metod nadgledanja je targetiranje vozila ili određenih komunikacionih naprava putem različitih softvera, kao što su trojanci. Kada ovi softevri dospeju do sprave oni kreiraju tajni ulaz u sistem (*backdoor to the system*) omogućavajući pregled i analizu sadržine „inficirane" sprave. Ovi softveri su u stanju da nadgledaju sistem, lozinke, slikaju ekran, po potrebi uključuju i isključuju web kameru ili mikrofon, manipulišu datotekama, itd. Kada govorimo o savremenoj infrastrukturi za nadziranje komunikacije onda se neizostavno moraju pomenuti tajnoviti programi za anonimno prikupljanje podataka kao što su američka PRIZMA i britanska TEMPORA. Bez pretenzije da ulazimo u tehničke pojedinosti za koje nismo stručni i služeći se jednostavnim rečnikom možemo ih opisati kao programe za prikupljanje i obradu digitalnih metapodataka velikog obima [14].

Najsofisticiraniji sistemi za nadzor su oni koji se odnose na prepoznavanje biometrijskih karakteristika kao i skeneri za telo. Međunarodno udruženje za identifikovanje definiše biometriku kao pojam i aktivnost koje se odnose na merenje i analizu karakteristika živih bića [15]. Uopšteno govoreći, najkorišćeniji biometrijski parametri su otisci prstiju i dlanova, lica, zenice, oblik glave, vene na rukama i glasovi. Jedna od najvažnijih biometrijskih tehnika nadgledanja jeste prepoznavanje lica (*facial recognition*). Ovaj softver funkcioniše tako što se prvo mere fizičke karakteristike i osobine posmatrane osobe na osnovu kojih se pravi šablon (*template file*), nakon čega se ovaj šablon upoređuje sa postojećim fotografijama posmatrane osobe. Pored tehnika za prepoznavanje lica sve više u primenu ulaze i takozvani skeneri za telo (*body scanners*), ali je njihova upotreba usled etičkih pitanja, ali i mogućeg ozračivanja nadziranih osoba, još uvek kontroverzna.

4. Nadzor i njegovi društveni efekti

U kultnoj knjizi *Filosofija palanke,* Radomir Konstatinović zapaža da se tiranija palanke ogleda kroz tiraniju uvida u sve aktivnosti njenih žitelja, odnosno da u palanci vlada tiranija apsolutne javnosti svega [10]. Savremena društva, zahvaljujući sve savršenijim sistemima za nadzor, počinju da nalikuju palankama, bivajući sve više izložena tiraniji javnosti, odnosno zahtevu za potpunim uvidom u sve radnje njihovih članova. Iako je nesumnjivo da nadzor i kontrola imaju svoje društveno-pozitivne funkcije postavlja se pitanja gde treba povući granicu kada je reč o domašaju novih tehnologija nadzora. Kao što je tokom šezdesetih godina XX veka prevladala svest da trka u nuklearnom naoružanju može dovesti do fizičkog nestanka sveta i da je kao takvu treba staviti pod međunarodnu kontrolu, tako bi i danas trebalo da prevlada svest o potrebi globalne kontrole sredstava za nadzor budući da posledice, od nivoa svakodnevnog života pojedinaca do međudržavnih odnosa mogu biti isto tako pogubne.

Gubitak privatnosti je samo jedna od posledica pojačanog nadzora na koji se obraća najviše pažnje budući da zadire direktno u svakodnevni život pojedinaca. Međutim, kada se perspektiva podigne sa individualnog na nivo društva kao celine još je opasnije to što nadziranje podstiče sumnju [2]. Kada u jednom društvu poverenje, koje je vezivno tkivo svakog društva, ustupi mesto nepoverenju, odnosno sumnji, onda još jedino sila može to društvo održati na okupu. Ali i ona ne zadugo.

Bezbroj je primera kojima se može ilustrovati koliko je poverenje bitno za funkcionisanje svakodnevnog života, od poverenja u komšiju da neće zloupotrebiti ostavljeni ključ dok su vlasnici stana na letovanju, preko poverenja da će vaspitačica zaista brinuti o bebama u jaslicama do poverenja u druge učesnike u saobraćaju da će poštovati saobraćajnu signalizaciju i neće ugroziti svoju i bezbednost ostalih učesnika u saobraćaju. Upravo zbog toga što postoji sumnja i strah od rizika koji nas okružuju, poverenje predstavlja važan društveni i psihološki fenomen i kao takvo čini jedan od osnovnih elemenata za funkcionisanje svake društvene zajednice. Sa razvojem modernih društava, sa sve širom podelom rada, pa sam tim i sve većom međuzavisnošću društva u celini kao i njegovih segmenata, raste i uloga poverenja kao integrativnog društvenog faktora. Međutim, kada društveni rast i razvoj prevaziđu okvire koje je moguće jednoznačno definisati i kontrolisati onda se ono pretvara u svojevrsno *rizično društvo* [1], dok *apriorno* poverenje, pogotovo u apstraktne elemente društvenog života, postaje osnov funkcionisanja modernog društva.

Štompka, definiše *poverenje kao ulog koji se tiče potencijalnih budućih akcija drugih* [11]. U skladu sa tim dva osnovna elementa poverenja su: *verovanje* i *privrženost*. Nasuprot tome, *nepoverenje* predstavlja skup negativnih očekivanja spram akcija drugih i uključuje odbrambenu privrženost. Po Štompki poverenje ima tri osnovne dimenzije: *relacionu* - koja nastaje kao posledica društvenih odnosa, *psihološku* - koja nastaje kao posledica impulsa da se veruje, i *kulturološku* - koja nastaje kao posledica makro-strukturnih faktora. Gidens shvatanja poverenja kao *pouzdanje u relijabilnost neke osobe ili sistema, koje se odnosi na dati niz ishoda ili događaja pri čemu to pouzdanje izražava veru u poštenje ili ljubav druge osobe ili u ispravnost apstraktnih principa (tehničkog znanja)* [4]. Ovde nam je posebno važan poslednji deo ove definicije budući da je, po Gidensu, jedan od osnovnih preduslova modernizacije upravo poverenje u *apstraktne*

principe, odnosno *simboličke znake* i *ekspertske (tehničke) sisteme,* čije je funkcionisanje odvojeno od neposrednog konteksta delovanja. Praktično, svaki put kada uđemo u lift ili se vozimo avionom, mi naše ponašanje baziramo na neupitnom poverenju u funkcionisanje ovih apstraktnih principa ili tehničkih sistema. To ne znači da mi ovo činimo bez ikakvog osećaja nelagode, ali bez ovakvog, *apriornog*, poverenja bio bi nemoguć razvoj modernih društava. Mi praktično, prihvatajući benefite funkcionisanja apstraktnih principa, prihvatamo i uračunati rizik njihove upotrebe.

Poverenje je čvrsto vezano za nesigurnost koju sa sobom nosi budućnost i to pre svega kada je reč o ljudskom ponašanju a ne prirodi. Da bismo učinili budućnost sigurnijom mi možemo ponekad kontrolisati fenomen. Recimo čuvati zatvorenika da ne pobegne iz zatvora-tu poverenje nije ni potrebno niti očekivano. Ali tamo gde postoji određena nesigurnost vezana za budući ishod, tu nastaje prostor za poverenje. Značaj poverenja još više dolazi do izražaja u slučaju kada nemamo nikakvu kontrolu nad budućim događajima. Problem sa društvenim okruženjem je taj što ono funkcioniše u velikoj meri po obrascu nesigurnosti i nekontrolisanosti. S druge strane, potpuno nadziranje i kontrola eliminiše prostor za poverenje, zbog čega može doći do bumerang efekta odnosno razvijanja nepoverenja u same institucije. Tipičan primer bumerang efekta su prošlogodišnji protesti u Mariboru i kasnije čitavoj Sloveniji koji su započeli upravo kao reakcija na preterani nadzor u saobraćaju. Tadašnji gradonačelnik Maribora, koji je nakon građanskih protesta i nemira bio primoran da podnese ostavku, dogovorio se sa jednom privatnom kompanijom o tome da im ustupi nadzor i naplatu saobraćajnih prekršaja u zamenu za održavanje i modernizaciju saobraćajne signalizacije koju bi kompanija u narednom periodu preuzela na sebe. Budući da je za svaku kompaniju sticanje profita osnov poslovanja tako se i u ovom slučaju desilo da je kompanija instalirala veliki broj kamera za nadzor saobraćaja koje su samo u jednom danu zabeležile preko 5000 prekršaja. Kako je po ugovoru kompaniji trebalo da pripadne 92% novca od naplate kazni jasno je zašto im je bilo u interesu da registruju što više prekršaja. Naravno, ovako rigidno shvatanje saobraćajnih propisa i nadzor kome su bili izloženi, uz ogromnu dobit koju je trebalo da ostvari ova kompanija, izazvali su veliko negodovanje žitelja Maribora koji su nakon višenedeljnih protesta primorali gradske vlasti da raskinu ugovor sa ovom kompanijom, a gradonačelnika da podnese ostavku [16].

Primer Maribora je samo mikro slika onoga što bi se moglo desiti na globalnoj razini. Recimo, procene su da u Velikoj Britaniji postoji između 1.8 i 4.2 miliona kamera koje snimaju javne površine [12]. Iako se sistemi video nadzora sve više instaliraju pod izgovorom zaštite od terorizma u Velikoj Britaniji je u proteklih 10 godina od terorizma poginulo samo 53 osobe [14] dok je, s druge strane, recimo u saobraćaju je u istom periodu poginulo više od 26000 ljudi [17]. Iako bi se za Veliku Britaniju moglo pomisliti da je uređeno društvo i da ovi pokazatelji ne oslikavaju realno stanje kada je reč o globalnoj pretnji od terorizma, stvar je zapravo još drastičnija kada se ukupni brojevi uzmu u obzir. Naime, prema podacima za 2010. godinu na nešto više od 13000 ljudi koji su u celom svetu stradali u terorističkim napadima [18], dolazi čak više od milion ljudi koji su poginuli u saobraćajnim nezgodama [19]. Uprkos tome, sve veća sredstva se ulažu u javni nadzor pod izgovorom straha od terorizma zbog čega je opravdano postaviti pitanje da li je terorizam zaista toliko izražena pretnja ili je to samo izgovor za sve jači nadzor i kontrolu građana. Tim pre što ni kad je reč o prevenciji kriminala nakon uvođenja video nadzora situacija nije mnogo povoljnija, budući da različite studije

pokazuju da se stope kriminala nisu značajno ili čak i uopšte spustile nakon njegovog uvođenja [12].

Slična je situacija i sa nadziranjem komunikacija koje se poslednjih godina takođe intenzivira. S jedne strane, sami korisnici novih IKT ne vode dovoljno računa o zaštiti sopstvene privatnosti [13] dok, sa druge stane, bezbednosne agencije, pod izgovorom zaštite od kriminala, terorizma i sajber napada sprovode nadgledanje komunikacija neslućenih razmera. Ova tema se posebno aktuelizovala nakon Snoudenovih (*Edward Snowden*) otkrića 2013. godine o funkcionisanju američke i britanske službe za bezbednost [14]. Slično ovome, gotovo neverovatno zvuči informacija da komunikaciju na internetu u Kini nadzire ni manje ni više nego dva miliona cenzora [20].

Imajući sve ovo u vidu možemo se složiti sa autorima jednog izveštaja o razmerama i posledicama nadziranja koji ističu da postoje četiri ključna segmenta za razumevanje društvenih posledica nadziranog društva [2]:

1. *Privatnosti i anonimnost*- Jedno od ključnih pitanja koje se u nadziranom društvu postavlja je ko i pod kojim uslovima ima pravo na narušavanje anonimnosti i privatnosti pojedinaca koje čine važne elemente modernog života i rada. Jedan od najvećih izazova jeste kako prilagoditi postojeću regulativu tehničkim inovacijama i kako učiniti da regulativa prati njihov razvoj. Bez ovoga neće biti moguće uspostaviti balans između neophodnog nadzora i neprikosnovenog prava na anonimnost i privatnost.
2. *Društvena diskriminacija*-Intenzitet nadzora varira u odnosu na geografsko područje kao i u odnosu na društveni položaj, etničku pripadnost i pol. Nadzor, narušavanje privatnosti i zaštita privatnosti se razlikuju između grupa štiteći jedne i ugrožavajući druge. Međutim, ovde treba dodati da danas praktično niko nije siguran u nadziranom društvu budući da i najmoćniji ljudi današnjice, poput svetskih lidera nisu lišeni ove, u najmanju ruku neželjene, pažnje [21].
3. *Mogućnost izbora* -Kada sistem nadzora ima svoju infrastrukturu i kada je njegovo funkcionisanje zaodenuto u tehnološki misticizam veoma je teško prosečnom građaninu da ima bilo kakvu moć i uticaj na vršenje nadzora. Međutim pojedinci ne bi trebalo da budu sami u ovoj borbi već bi trebalo da računaju na pomoć specijalizovanih agencija i drugih vladinih tela koja se bave zaštitom privatnosti kao i na pomoć nezavisnih stručnjaka i nevladinih organizacija.
4. *Transparentnost*- S jedne strane, u oblasti državne uprave, poslovanju, organizaciji saobraćaja dolazi do sve intenzivnijeg širenja infrastrukture za nadzor, dok sa druge strane pojedinci i grupe nemaju jasnu predstavu o tome šta se dešava sa njihovim ličnim podacima, ko ih čuva i za koje namene.

5. Zaključak

U radu smo se bavili novom fazom u razvoju društvenog nadzora. Zahvaljujući eksplozivnom razvoju IKT, dolazi i do neslućenih mogućnosti nadzora zbog čega savremena društva sve češće definišemo kao nadzirana društva. Iako su strategije nadzora postojale praktično otkad postoje i moderne države, poslednja faza koju karakteriše sveprisutan nadzor preti da potpuno uništi temelje na kojima počiva svako društvo, a to su poverenje i solidarnost. Namesto nekadašnje građevinske infrastrukture, sada IKT infrastruktura omogućava postojanje modernog *Panoptikona*, strukture u kojoj ni jedan

građanin nije siguran da li je i kada predmet nečijeg nadzora. Problem je u tome što nema ubedljivih dokaza da intenziviranje nadzora dovodi do eliminisanja postojećih rizika. Pored toga, ne dolazi ni do povećanja osećanja sigurnosti građana, već upravo suprotno. Nadzor pobuđuje sumnju, sumnja traži dalji nadzor, koji još više povećava sumnju i tako u krug.

Potrebno je hitno staviti pitanje nadzora na dnevni red kao jedno od najvažnijih pitanja sa kojima moderna društva na početku XXI-og veka suočavaju. Postojeća regulativa nadzora nije dovoljno razvijena niti je u stanju da prati dinamične promene koje se na polju tehnologija odvijaju. Neophodno je donošenje zakona kojim bi se regulisalo pravo na privatnost u digitalnom dobu, odnosno ko, zašto, kako, putem kojih sredstava i pod kojim uslovima ima pravo da prikuplja podatke i nadgleda ponašanje građana. Međutim, budući da smo svedoci da mnoge bezbednosne agencije, svesno ili nesvesno krše postojeće zakone, potrebno je formirati civilna tela ili ojačati postojeća koja će se aktivno baviti ovim pitanjem. Na kraju, potrebno je edukovati javnost o neprikosnovenosti prava na anonimnost i privatnost bez obzira na rizike koje moderni život nosi.

Literatura

[1] U. Bek, *Svetsko rizično društvo-u potrazi za izgubljenom sigurnošću*, Akademska knjiga, Novi Sad, 2011.

[2] D. Wood, K. Ball, D. Lyon, C. Norris & C. Raab, "A Report on the Surveillance Society", *Surveillance Studies Network,* UK., 2006.

[3] M. Aaron, R. Van Brakel and D. Bernhard, "Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework", *Surveillance & Society*, Vol. 6(3): 213-232, 2009.

[4] E. Gidens, *Posledice modernosti*. Filip Višnjić, Beograd, 1998.

[5] G. Marx, "What's New About the "New Surveillance"? Classifying for Change and Continuity", *Surveillance & Society,* Vol.1(1): 9-29, 2002.

[6] Lyon, David. *Surveillance society*. Buckingham: Open University Press, 2001.

[7] M. Fuko, *Nadzirati i kažnjavati*, Prosveta, Beograd, 1997.

[8] S. Graham and D. Wood, "Digitizing Surveillance: Categorization, Space, Inequality", *Critical Social Policy,* Vol. 23(2): 227-248, 2003.

[9] E. Schlehahn, M. Hansen, J. Sterbik-Lamina& J.S. Samaniego, "Report on surveillance technology and privacy enhancing design", *Project: Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe, 2013.*

[10] R. Konstatinović, *Filosofija palanke*, Treći program, Beograd, 1969.

[11] P. Sztompka, *Trust: A Sociological Theory*. Cambridge University Press,2000.

[12] S. Germain, "A Prosperous 'Business': The success of CCTV through the eyes of international literature". *Surveillance & Society*, Vol. 11(1/2): 134-147. 2013.

[13] D. Petrović i N. Tomić, "Sigurnost podataka na on-line društvenim mrežama", *SymOrg, XII međunarodni simpozijum Fakuleta organizacionih nauka,* Zlatibor, jun 2010.

Izvori sa interneta:

[14]http://www.theguardian.com/world/2013/oct/03/edward-snowden-files-john-lanchester
[15] http://www.theiai.org/disciplines/biometrics/index.php
[16]http://www.b92.net/info/vesti/index.php?yyyy=2012&mm=11&dd=14&nav_category=167&nav_id=660096
[17]https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/239790/ras40001.xls
[18] http://amanpour.blogs.cnn.com/2013/01/15/more-americans-killed-by-guns-than-by-terrorists/
[19] http://apps.who.int/gho/data/node.main.CODWORLD?lang=en
[20] http://www.b92.net/tehnopolis/aktuelno.php?yyyy=2013&mm=10&nav_id=762290
[21]http://www.bbc.co.uk/news/magazine-24627187

Abstract: *Modern society is often seen as risk society entailing that the traditional social and institutional mechanisms of social security being less capable of performing its expected role and leaving the individual to growing risks of modern life. In this context, information and communication technologies (ICT) play a contradictory role. On one hand they enable further modernization of the society, while, on the other hand, they make its segments completely exposed to new risks. In line with this the aim of this paper is to highlight the role of the ICT infrastructure both in production and in the prevention and control of social risk. Special attention will be given to possibilities of ICT infrastructure misuse in order to monitor and control the activities of ICT users, whether in terms of individuals, organizations, or the state as a whole.*

Key words: *Surveillance, ICT, risks, infrastructure, trust*

MIS(USE) OF ICT INFRASTRUCTURE IN THE CONTEXT OF SOCIAL RISK CONTROL

Dalibor Petrović