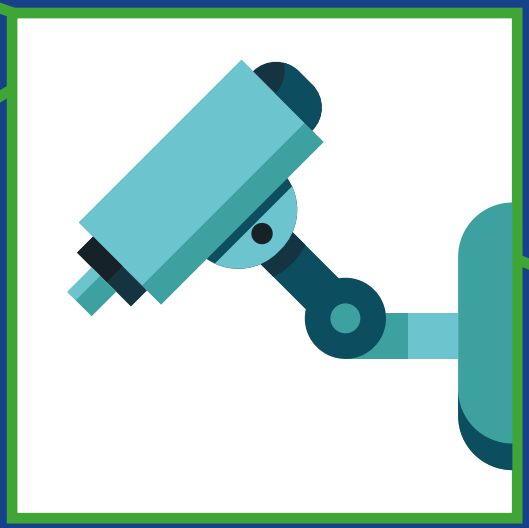
STUDIJA:

VIDEO NADZOR: SREDSTVO ZA UNAPREĐENJE BEZBEDNOSTI ILI KRŠENJE PRIVATNOSTI GRAĐANA?



PARTNERI SRBIJA

Ova studija slučaja je deo zajedničkih napora Centra za istraživanje, transparentnost i odgovornost (CRTA), Nacionalne koalicije za decentralizaciju (NKD), Beogradskog centra za bezbednosnu politiku (BCBP) i Partnera za demokratske promene Srbija da podstaknu veće učestvovanje građana u odlučivanju kroz projekat „Građani imaju moć" koji podržava Američka agencija za međunarodni razvoj (USAID). Stavovi izraženi u ovoj studiji slučaja isključivo su stavovi autora i ne odražavaju stavove USAID-a.

Autor:
Kristina Kalajdžić

Saradnici na istraživanju:
Uroš Mišljenović i Ana Toskić Cvetinović

Recenzent:
Blažo Nedić

Lektura i korektura:
Tamara Ljubović

Dizajn i prelom:
Dosije studio, Beograd

Izdavač:
Partneri Srbija

Za izdavača:
Ana Toskić Cvetinović

SADRŽAJ

Rezime 6
Uvod 8
Primeri neadekvatne upotrebe sistema za video nadzor u praksi 10
U korak sa svetom: kamere kao sredstvo za zaštitu ili legalni alat za kontrolu građana? 12
Projekat "SIGURAN GRAD" 13
Nedostatak pravnog okvira 16
Ovlašćenja za uspostavljanje i korišćenje sistema za video nadzor 17
Zaštita ličnih podataka i upotreba sistema za video nadzor 18
Zaključci i preporuke 22

REZIME

Praksa uspostavljanja i korišćenja sistema za video nadzor u Srbiji odlikuje se manjkom transparentnosti procesa i nedovoljnom usklađenošću ovih aktivnosti za Zakonom o zaštiti podataka o ličnosti i drugim propisima. Potreba za boljim regulisanjem oblasti video nadzora javlja se kao posledica više primera u kojima su ovakvi sistemi na pogrešan način korišćeni u Srbiji.

Pitanje opravdanosti uvođenja sistema za video nadzor javnih površina postalo je aktuelno početkom 2019. godine kada su predstavnici Ministarstva unutrašnjih poslova informisali javnost o namerama da započnu projekat "Siguran grad". Kako je tada najavljeno, projekat podrazumeva masovnu obradu podataka o ličnosti građana Srbije korišćenjem opreme za video nadzor, što uključuje i korišćenje softvera za prepoznavanje lica. Javnost ni danas nema pouzdanu informaciju o broju kamera i lokacijama na kojima će kamere biti postavljene, a izostala je i stručna analiza o opravdanosti uvođenja ovakvog sistema za video nadzor.

Primeri iz sveta ukazuju da države neretko koriste sisteme video nadzora kao sredstvo za masovno praćenje građana umesto za svoju osnovnu svrhu, što je zaštita bezbednosti. Ove vrste tehnologija pored posledica po privatnost građana, imaju i potencijalne implikacije na druga prava, kao što su pravo na slobodu govora i okupljanja. Ako smo svesni da nas posmatraju, manje ćemo biti slobodni da iznosimo svoje stavove i/ili šetamo ulicama mirno izražavajući protest protiv odluka koje donose javne institucije i ljudi koji njima upravljaju.

Šire posmatrano od pitanja (zlo)upotreba sistema za video nadzor, više puta se dešavalo da podaci u posedu službi bezbednosti i drugih organa javne vlasti postaju javno dostupni i koriste se u svrhe diskreditacije aktivista ili političkih protivnika. Šta nam garantuje da će se podaci prikupljeni korišćenjem sistema za video nadzor koristiti odgovornije?

UVOD

Video nadzor je sistem koji se sastoji od kamera za video nadzor kao i opreme za skladištenje, prikazivanje i dalju obradu video materijala.[1] Sa napretkom tehnologije i razvojem različitih softvera i aplikacija, ovi uređaji imaju sve više tehničkih mogućnosti, pa je i njihova upotreba sve kreativnija. Iako prvobitno zamišljeni za zaštitu ljudi i imovine, danas se kamere koriste za razne namene, pa tako zahvaljujući njima i uz pristup internetu možete ići u virtualne turističke ture muzeja, ili u realnom vremenu posmatrati šta se dešava na ulicama npr. Amsterdama.

Kada neko opljačka banku, na osnovu video nadzora policija može brže da identifikuje učinioca i liši ga slobode. Možemo reći da je to pobeda moderne tehnologije i kamera za video nadzor. Međutim, kamere su uključene i snimaju i kada niko ne vrši krivična dela. Kamere snimaju građane dok kupuju, voze, šetaju gradom ili piju kafu u bašti omiljenog kafića. Razvoj tehnologija za nadzor i njihova pristupačnost doveli su do toga da se ove tehnologije koriste kako od strane država tako i privatnih subjekata. Iako je namena ove tehnologije pre svega bezbednost ljudi i imovine, zloupotrebe su moguće i dešavaju se neretko.

Strah od zloupotreba sistema za video nadzor javlja se pre svega zato što ne znamo ko nas sve potencijalno snima i šta se dešava sa tim snimcima. Ovaj strah raste još više kada se uzme u obzir da oblast video nadzora nije dovoljno pravno regulisana u Republici Srbiji, i da državni organi, a u prvom redu oni koji su zaduženi za bezbednost građana i države nisu dovljno transparentni prilikom uvođenja novih sistema video nadzora. Tako je javnost u Beogradu ostala uskraćena za informacije kako će izgledati novi pametni video nadzor koji je najavilo Ministarstvo unutrašnjih poslova tokom 2019. godine. Iz nekoliko obraćanja ministra unutrašnjih poslova saznali smo da je u Beogradu planirano postavljanje video nadzora koji uključuje softvere za prepoznavanje lica, a da se broj kamera čije je postavljanje planirano kreće između 1.000 i 2.000.[2] Ovaj projekat MUP-a i grada Beograda nazvan "Siguran grad", prema dokumentima dostupnim javnosti treba da unapredi bezbednost u glavnom gradu.

Međutim, nije tako teško zamisliti scenario u kojem se ova ista oprema koristi za nezakonito praćenje ljudi, kao sredstvo pritiska na one koji žele da iskažu nezadovoljstvo radom institucija i nosilaca javnih funkcija, ili da koriste svoje pravo na organizovanje i okupljanje u javnom prostoru.

Analiza u nastavku odnosi se na ukazivanje na dosadašnje primere (zlo)upotreba sistema za video nadzor od strane organa javne vlasti, pravni okvir kojim je regulisana oblast video nadzora, i preporuke za bolje regulisanje ove oblasti, uz osvrt na uticaj ovih sistema na građanski aktivizam.

1 U zavisnosti od vrste i namene mogu posedovati mikrofone za snimanje, a sa uređajem za prenos slike biti povezani kablom ili bežično, itd.

2 N1, Stefanović: Hiljadu kamera sa softverima za prepoznavanje lica i tablica: http://rs.n1info.com/Vesti/a456247/Stefanovic-Hiljadu-kamera-sa-softverima-za-prepoznavanje-lica-i-tablica.html

PRIMERI NEADEKVATNE UPOTREBE SISTEMA ZA VIDEO NADZOR U PRAKSI

Obazrivost zbog upotrebe sistema za video nadzor javlja se kao posledica više primera u kojima su ovakvi sistemi na pogrešan način korišćeni u Srbiji. Tokom poslednjih nekoliko godina Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti (u daljem tekstu Poverenik) reagovao je na nekoliko pravno problematičnih slučajeva korišćenja video nadzora od strane organa javne vlasti. Jedan od slučajeva koji se ne odnosi na javno snimanje, već na korišćenje video nadzora unutar prostorija same institucije odnosi se na video nadzor korišćen u Klinici za psihijatriju Kliničkog centra Srbije. Nakon predstavki građana, Poverenik je sproveo nadzor u ovoj psihijatrijskoj ustanovi i utvrdio „da su kamere sistema video nadzora postavljene u svim prostorijama u kojima borave pacijenti, uključujući sobe, prostorije za dnevni boravak, prostorije za radnu terapiju i hodnike, čak, što je posebno delikatno, i u unutrašnjosti toaleta. Kao svrha ovakve obrade navedena je bezbednosna prevencija, sprečavanje samopovređivanja ili nanošenja povreda drugim licima od strane pacijenata i zaštita imovine Kliničkog centra, a potom i dokazivanje u slučaju incidentnih događaja, a kao pravni osnov navedene su odredbe Zakona o privatnom obezbeđenju."[3] U postupku nadzora još je utvrđeno da pacijenti nisu prethodno upoznati sa sprovođenjem video nadzora, odnosno ovom vrstom obrade njihovih ličnih podataka, niti institucija poseduje interne akte koji se odnose na procenu rizika i druge akte predviđene Zakonom o privatnom obezbeđenju čime bi ovakva obrada podataka bila zakonita. U saopštenju Poverenika povodom izvršenog nadzora stoji i da je praksa psihijatrijskih ustanova u ovom pogledu prilično neujednačena, te da postoje institucije ovog tipa u kojima se uopšte ne vrši video nadzor, dok postoje i one u kojima sistemi video nadzora postoje ali su ograničeni na određene prostorije[4].

Još jedan primer upotrebe video nadzora od strane organa javne vlasti koji je Poverenik ocenio kao sporan sa aspekta Zakona o zaštiti podataka o ličnosti,[5] je slučaj upotrebe tehnologija za video nadzor od strane Komunalne policije iz 2016. godine. Poverenik je utvrdio da Komunalna policija raspolaže sa oko 250 personalnih kamera, od kojih je 216 povezano sa uniformama komunialnih policajaca. U postupku nadzora Poverenik je konstatovao da Komunalna policija nema valjan pravni osnov za upotrebu ovih kamera, jer su akti na koje se pozivala Komunalna policija nižeg ranga od zakona koji jedini može biti pravni osnov za ovakvu obradu ličnih podataka. Uz to, prema navodima Poverenika, ti akti su direktno suprotni i odredbama Zakona o komunalnoj policiji kojima se uređuju mogućnosti i načini korišćenja tehnologije za video-nadzor prostora i objekata.[6]

Da je curenje video snimaka u javnost realna bojazan, pokazuje i primer iz 2019. godine, kada se snimak sa javne površine našao na crnogorskom tabloidu "Borba". U pitanju su snimci sa nadzornih kamera koji prikazuju strogi centar Beograda, 14. oktobra 2019. godine, uveče, kada je na promociji knjige gradskog menadžera Gorana Vesića, jedan primerak knjige i zapaljen. Prema pisanju tabloida "Borba", čije je delove članka preneo portal "N1", *opozicija je organizovano spalila Vesićevu knjigu… snimak* (snimak paljenja knjige) *navodno pribavljen uz pomoć "jedne od bezbednosnih službi sa prostora bivše Jugoslavije".*[7] Do danas nije razjašnjeno poreklo ovog snimka, odnosno nije utvrđeno kojom i čijom kamerom je snimak napravljen, ko je snimke preuzeo, a potom ih dostavio tabloidu.

Šire posmatrano od pitanja (zlo)upotreba sistema za video nadzor, više puta se dešavalo da podaci službi bezbednosti i drugih organa javne vlasti postaju javno dostupni i koriste se u svrhe diskreditacije političkih protivnika. Poznat je primer da su zdravstveni podaci jednog narodnog poslanika čitani tokom sednice Narodne skupštine, a koju je prenosio RTS.[8] Takođe, pokazalo se da je praksa telekomunikacionih provajdera/operatera bila takva da su službe bezbednosti imale pristup njihovim podacima o korisnicima, bez postojanja sudskih naloga i poštovanja drugih procedura,[9] te se postavlja pitanje da li bi sa podacima sa sistema za video nadzor bilo drugačije?

3 Poverenik, Saopštenja, Video nadzor u psihijatrijskim ustanovama mora biti zakonit i opravdan svrhom: https://www.poverenik.rs/sr/

4 Ibid.

5 Ovde se misli na prethodni Zakon o zaštiti podataka o ličnosti, usvojen 2008. godine, koji je bio na snazi sve do početka primene novog Zakona o zaštiti podataka o ličnosti, 21.08. 2019. godine.

6 Poverenik, Saopštenja, Upozorenje komunalnoj policiji - snimanje građana bez zakonskog osnova i bez jasne svrhe https://www.poverenik.rs/sr/

7 N1, Tabloidi objavili snimke s promocije Vesićeve knjige, Đilas tvrdi – montaža: http://rs.n1info.com/Vesti/a539217/Tabloidi-objavili-snimke-s-promocije-Vesiceve-knjige-Djilas-tvrdi-montaza.html

8 N1, Živković pokazao povredu zbog koje je oslobođen vojske: http://rs.n1info.com/Vesti/a279908/Kako-su-naprednjaci-dobili-tajne-podatke-o-Zivkovicu.html

9 SHARE fondacija, Nevidljive infastrukture: Elektronski nadzor i zadržavnje podataka sa mobilnih telefona: https://labs.rs/sr/nevidljive-infrastrukture-elektronski-nadzor-i-zadrzavanje-podataka-sa-mobilnih-telefona/

U KORAK SA SVETOM: KAMERE KAO SREDSTVO ZA ZAŠTITU ILI LEGALNI ALAT ZA KONTROLU GRAĐANA?

Sistemi za video nadzor se koriste širom sveta, a procenjuje se da samo u Velikoj Britaniji ima između 4-6 miliona kamera. U Kini postoji preko 170 miliona kamera, a od prvih 10 gradova sveta po broju kamera, kineskih je čak osam, preostala dva su London (UK) i Atlanta (USA).[10] Krajem 20. i početkom 21. veka, kao rezultat ekonomske reforme, računarska i internet tehnologija veoma su se razvile u Kini. Danas su kamere koje poseduju tehnologiju prepoznavanja lica, internet nadzor i nadzor preko mobilnih aplikacija koje sakupljaju velike količine podataka o korisnicima, kao i dronovi najzastupljeniji mehanizmi koje koriste kineske vlasti za masovni nadzor svojih građana. Pored sistema za nadzor čiji je osnovni cilj, barem prema tvrdnjama vlasti širom sveta, zaštita bezbednosti, video nadzor obogaćen softverima za prepoznavanje lica koristi se i u komercijalne svrhe. Pa tako, preko *You Tube*-a možete gledati uživo snimke sa raznih lokacija u Amsterdamu i drugim delovima Holandije,[11] što je primer tzv. *online* turizma. U praksi to znači da se kao turisti možete šetati delovima Amsterdama dok se vaš lik uživo emituje preko *You Tube*-a, bez vašeg znanja i pristanka. U državi Florida softveri sa prepoznavanjem lica koriste se tokom fudbalskih utakmica (*Super Bowl*) takođe bez znanja ili pristanka gledalaca na stadionu.[12]

Tehnologija za prepoznavanje lica omogućava da se korišćenjem snimka lica nastalog na osnovu ove tehnologije, koji je dalje ukršten sa nekom evidencijom lica (npr: bazom podataka MUP-a koja sadrži evidenciju svih punoletnih građana Republike Srbije) utvrdi identitet konkretne osobe, ili obrnutom metodom, ubacivanjem fotografije konkretnog lica u softver za prepoznavanje lice utvrde sva mesta koja je osoba posetila, ili utvrdi njena trenutna lokacija.

O masovnom video nadzoru javnih površina u Beogradu, prvi put se ozbiljnije pričalo i pisalo krajem 2017. godine. Naime, mediji su preneli zapažanja građana da su se na više lokacija u Beogradu pojavile nove kamere. Kao dve institucije u čijoj bi nadležnosti moglo da se nađe uspostavljanje sistema video nadzora nad saobraćajnicama, od strane Poverenika, označene su Ministarstvo unutrašnjih poslova i Gradska uprava grada Beograda. Nakon toga usledile su kontradiktorne informacije upućene od strane zvaničnika: „Mediji su tako preneli izjavu sekretara Sekretarijata za vanredne situacije, da Gradskoj upravi nije poznato ko postavlja kamere, ali i izjavu gradskog menadžera koja upućuje na zaključak da ih postavlja upravo Grad, te da namerava da postavi još jedan veći broj kamera."[13]

Nadzor koji je nakon toga pokrenuo Poverenik nad ovim institucijama, otklonio je dilemu jer je u nadzoru utvrđeno da je u drugoj polovini 2017. godine od strane MUP-a izvršena zamena tehnički zastarelih kamera naprednijim kamerama nove generacije i veće rezolucije, na postojećem 61 kamernom mestu. Nije povećan broj lokacija kamernih mesta, ali su na određenim kamernim mestima dodate fiksne kamere (ukupno 47 kamera), što je tada obrazloženo potrebom bolje preglednosti, brže pretrage zabeleženog meterijala i efikasnijeg rasvetljavanja krivičnih dela.[14] Poverenik je ocenio da je MUP i pored nespornog pravnog osnova za navedenu obradu podataka o ličnosti, propustio da, pre instalacije navedenih kamera, na adekvatan način obavesti javnost o tome. Taj propust, uz novinske natpise i kontradiktorne izjave funkcionera, izazvao je nepotrebnu uznemirenost građana.

Projekat "SIGURAN GRAD"

Pitanje opravdanosti uvođenja sistema za video nadzor na javne površine postalo je aktuelno početkom 2019. godine sa najavama ministra unutrašnjih poslova Nebojše Stefanovića i direktora policije Vladimira Rebića da će u narednom periodu u Beogradu biti instalirano skoro 1.000 kamera za video nadzor na 800 lokacija, te da će ovi uređaji imati instalirane softvere za prepoznavanje lica (*facial recognition*) i registarskih oznaka/tablica. [15] Kao razlog za uvođenje ovakvog sistema navodi se bezbednost građana, odnosno pad kriminaliteta.

10 South China Morning Post, Cities in China most monitored in the world, report finds: https://www.scmp.com/news/china/society/article/3023455/report-finds-cities-china-most-monitored-world

11 You Tube: https://www.youtube.com/c/WebCamNL/?gl=NL

12 T. E. Boult, PICO: Privacy throught Invertible Cryptographic Obscuration: https://vast.uccs.edu/~tboult/PAPERS/Boult-PICO-preprint.pdf

13 Insajder, Poverenik: Ko i zašto postavlja kamere po Beograd: https://insajder.net/sr/sajt/vazno/9172/

14 Poverenik, Saopštenja, Video-nadzor - hronično neuređena oblast: https://www.poverenik.rs/sr/

15 N1. Direktor policije: Ne postoji mogućnost zloupotrebe kamera: http://rs.n1info.com/Vesti/a458949/Direktor-policije-Ne-postoji-mogucnost-zloupotrebe-kamera.html

"Reč je o sistemu inteligentnog video nadzora koji podrazumeva da se kamere visoke rezolucije postave na oko 800 lokacija u Beogradu, koje će nadgledati ulice, škole, sve one tačke koje su kolege iz MUP-a, na osnovu ozbiljno uradjenih elaborata i procene rizika, zaključile da je neophodno pokriti kamerama", rekao je Stefanović u sklopu uvodnog predavanja na temu "Savremene tehnologije u razvoju Ministarstva unutrašnjih poslova", koje je na Kriminalističko-policijskom univerzitetu održao povodom početka školske godine, 01. oktobra 2019.[16]

Ministarstvo unutrašnjih poslova odbijalo je da na zahtev novinara i istraživača dostavi informacije o procesu nabavke ovih uređaja, uspostavljanja sistema, i drugoj dokumentaciji koja bi potvrdila da su prilikom nabavke i procesa uspotavljanja sistema video nadzora ispoštovane sve zakonske procedure. U odgovoru na zahtev za slobodan pristup informacijama od javnog značaja koji je uputila SHARE fondacija, MUP između ostalog navodi: "da su svi dokumenti o javnoj nabavci opreme za video nadzor u Beogradu zaštićeni stepenom tajnosti "Poverljivo", a da tražene informacije o lokacijama (kamera) i analizi nisu sadržane ni u jednom dokumentu, odnosno nosaču informacija, što je zakonski preduslov za ostvarivanje pristupa informaciji od javnog značaja [17].

Jedno od prvih pitanja koje se pojavilo u javnosti jeste koliko ovi sistemi zapravo pomažu u sprečavanju izvršenja krivičnih dela i lakšem pronalaženju učinilaca, i da li je struka prethodno izradila analizu - procenu koja dokazuje opravdanost uvođenja sistema za video nadzor.[18] Sa druge strane, postavilo se pitanje upotrebe odnosno zloupotrebe ovako prikupljenih podataka.[19] Kamere jednom kada se postave beleže sve u svom dometu, dakle ne samo učinioce krivičnih dela. Važno je znati zato ko sve ima pristup tim snimcima, kako se ti snimci čuvaju, koliko su zaštićeni od spoljne ili unutrašnje kompromitacije, koliko dugo se čuvaju i sl, jer smo više puta bili svedoci curenja u javnost snimaka sa nadzornih kamera.

Najzad, ovako masovan video nadzor potencijalno može da utiče i na druga prava i slobode građana, u prvom redu na slobodu govora i okupljanja. "Osećaj da možemo biti podvrgnuti nadzoru i praćenju može nas motivisati da izmenimo ponašanje, odnosno da nas obeshrabri i odvrati od nečega što je inače dozvoljeno, na primer, da odemo na protest ili iskažemo nezadovoljstvo u javnom prostoru na neki drugi način. Jasno je da razvijanje ovakvog straha ide u prilog onima protiv kojih bi građani mogli da izraze nezadovoljstvo. Pored toga, prikupljanje obimne količine podataka o velikom broju ljudi može dovesti do zloupotreba, usled neodgovarajuće kontrole i davanja prevelike moći onima koji nas nadziru, u ovom slučaju službenicima i rukovodiocima MUP-a."[20] Primer iz Rusije svedoči o tome - naime, ruska aktivistkinja za prava žena, podnela je tužbu protiv državnih organa u Rusiji, jer su kamere za prepoznavanje lica korišćene za njenu identifikaciju u aprilu 2018, kada je protestovala ispred zgrade parlamenta protiv zastupnika kojeg je nekoliko žena optužilo za seksualno uznemiravanje.[21]

O projektu "Siguran grad", najviše informacija javnost je saznala kroz studiju slučaja kompanije Huawei, koja je strateški partner Republike Srbije na ovom projektu. Kompanija Huawei je u promotivne svrhe na svom sajtu podelila neke detalje o hronologiji tog projekta – zapravo, širег projekta "Sigurno društvo", o kome su pregovori počeli još 2011. godine. Huawei je u studiji slučaja naveo da projekat treba da obuhvati eLTE tehnologiju, pametni video nadzor, sistem pametnog transporta, izgradnju data centara, itd. Nedugo nakon što su se u javnosti pojavili delovi njihove studije slučaja, ona je uklonjena sa sajta kompanije.[22]

Od prve najave predstavnika Ministarstva unutrašnjih poslova, grupa organizacija civilnog društva,

16 N1, Stefanović: Video nadzor - manje kriminala na ulicama Beograda: http://rs.n1info.com/Vesti/a530748/Stefanovic-Video-nadzor-manje-kriminala-na-ulicama-Beograda.html

17 SHARE fondacija, Da li su poznate lokacije novih kamera za nadzor i rizici po ustavna prava građana? https://www.sharefoundation.info/sr/da-li-su-poznate-lokacije-novih-kamera-za-nadzor-i-rizici-po-ustavna-prava-gradjana/

18 Saša Đorđević, Video nadzor ne čini čuda: https://pescanik.net/video-nadzor-ne-cini-cuda/

19 N1, Pametni video nadzor - svi mogu biti praćeni u svako vreme, rizici su ogromni: http://rs.n1info.com/Vesti/a545631/Krivokapic-o-pametnom-video-nadzoru.html

20 Uroš Mišljenović, Da li samo kriminalci treba da budu zabrinuti zbog video nadzora? https://otvorenavratapravosudja.rs/teme/ustavno-pravo/da-li-samo-kriminalci-treba-da-budu-zabrinuti-zbog-video-nadzora

21 Radio slobodna Evropa, Rusija: Tehnologija za prepoznavanje lica i suzbijanje protesta: https://www.slobodnaevropa.org/a/30205620.html

22 SHARE fondacija, Huawei zna sve o kamerama u Beogradu, i nije im teško da to i kažu! https://www.sharefoundation.info/sr/huawei-zna-sve-o-kamerama-u-beogradu-i-nije-im-tesko-da-to-i-kazu/

među kojima su i Partneri Srbija, nastojala je da isprati usklađenost procedura sa Ustavom Srbije i važećim zakonima, uprkos nedovoljnoj transparetnosti čitavog procesa. Važan deo ispitivanja zakonitosti najavljenog sistema nadzora, jeste i izrada procene uticaja ovog projekta na prava građana. Ministarstvo unutrašnjih poslova je, nakon intervencija civilnog sektora i Poverenika, ovaj dokument izradilo i dostavilo Povereniku[23] Na osnovu ovog dokumenta, SHARE Fondacija, Partneri Srbija i Beogradski centar za bezbednosnu politiku izradili su *Analizu Procene uticaja obrade na zaštitu podataka o ličnosti korišćenjem sistema video nadzora Ministarstva unutrašnjih poslova.*[24] Zajednički zaključak Analize je da procena uticaja MUP-a ne ispunjava ni formalne ni materijalne uslove propisane zakonom,[25] te da bi Ministarstvo unutrašnjih poslova trebalo da do daljeg obustavi uvođenje sistema za pametan video nadzor.[26] U ovoj Analizi tri organizacije posvećene zaštiti prava na privatnost građana konstatovale su da:

"Osnovno pitanje koje se postavlja u slučaju pametnog video nadzora jeste njegova neophodnost, srazmernost i efikasnost imajući u vidu invanzivnost ove mere. Stoga je na rukovaocu podacima, odnosno MUP-u, dodatna obaveza da dokaže neophodnost uvođenja ovakve mere, njenu srazmernost u odnosu na svrhu koja se želi postići, kao i efikasnost u ostvarenju ciljeva obrade podataka."[27]

Povodom najava MUP-a, o uvođenju pametnog sistema za video nadzor, bivši Poverenik, Rodoljub Šabić, izrazio je bojazan *"da u postojećim uslovima sistem osposobljen za brzu, automatsku identifikaciju lica svakog čija fotografija postoji u bazi fotografija MUP-a (dakle svih punoletnih i ne malog broja maloletnih gradjana) bude umesto za borbu protiv kriminala upotrebljavan, na primer, u svrhu kontrole kretanja političkih oponenata vlasti ili slično.* Šabić je, takođe, izjavio *da se postavlja pitanje u kojoj meri je prikrivanje lokacija kamera u skladu ili u suprotnosti sa ustavnim i zakonskim odredbama o snimanju i praćenju*."[28]

U proceni uticaja koju je izradio MUP stoji da će projekat postavljanja video nadzora nad saobraćajnicama biti urađen kroz 2 faze:

I faza (2017. god) - 100 kamera na 61 lokaciji tzv. inteligentni video nadzor sa video analitikom materijala, uključujući pretraživanje materijala po određenim pojmovima, prepoznavanje tablica;

II faza- 1000 kamera na 800 lokacija, po celom gradu Beogradu, koje poseduju softvere za prepoznavanje lica (*Facial Recognition* system).[29]

U proceni uticaja stoji i da ovaj sistem još uvek nije u funkciji. U izjavi Ministra unutrašnjih poslova iz januara 2019. godine, a koju je preneo dnevni list „Blic" navodi se da će ovaj sistem biti uspostavljen u naredne dve do tri godine i da će se širiti ka autoputu i magistralnim putevima.[30] U kasnijim izjavama ministra unutrašnjih poslova Nebojše Stefanovića, navodi se "*da će u Beogradu do kraja sledeće godine biti postavljeno 2.000 kamera*".[31]

Činjenica da građani do danas nisu obavešteni o procesu uspostavljanja pametnog video nadzora, a da ni udruženja građana nisu dobila informacije o planovima MUP-a povodom ovog projekta, uključujući i informacije o broju kamera, lokacijama na kojima će biti postavljene kamere, i vremenskom okviru u kom će se započeti sa korišćenjem tehnologije pametnog video nadzora, ukazuje da je došlo do ozbiljne povrede načela transparentnosti obrade podataka.[32]

23 MUP, Procena uticaja obrade na zaštitu podataka o ličnosti korišćenjem sistema video nadzora: https://www.sharefoundation.info/wp-content/uploads/MUP-Procena-uticaja-obrade-na-zastitu-podataka-o-licnosti-koriscenjem-sistema-video-nadzora.pdf

24 Share, Partneri Srbija i Beogradski centar za bezbednosnu politiku, Analizu Procene uticaja obrade na zaštitu podataka o ličnosti korišćenjem sistema video nadzora Ministarstva unutrašnjih poslova: https://www.sharefoundation.info/wp-content/uploads/Analiza_procene_uticaja_SHARE_Partneri-Srbija_BCBP.pdf

25 Ovde se misli na Zakon o zaštiti podaka o ličnosti

26 Partneri Srbija, MUP do daljeg da obustavi uvođenje sistema za pametan video nadzor: http://www.partners-serbia.org/mup-do-daljeg-da-obustavi-uvodenje-sistema-za-pametan-video-nadzor/

27 Ibid

28 Danas, Šabić: Moguće zloupotrebe takozvanih inteligentnih kamera za video nadzor: https://www.danas.rs/drustvo/sabic-moguce-zloupotrebe-takozvanih-inteligentnih-kamera-za-video-nadzor/.

29 MUP, Procena uticaja obrade na zaštitu podataka o ličnosti korišćenjem sistema video nadzora: https://www.sharefoundation.info/wp-content/uploads/MUP-Procena-uticaja-obrade-na-zastitu-podataka-o-licnosti-koriscenjem-sistema-video-nadzora.pdf

30 Blic, Beograđane će narednih godina na ulicama snimati još 1.000 kamera: https://www.blic.rs/vesti/beograd/beogradane-ce-narednih-godina-na-ulicama-snimati-jos-1000-kamera/ph4m512

31 Ovu izjavu preuzeo je portal Mondo, i objavio kao vest 30.07.2019: https://mondo.rs/Info/Beograd/a1208322/Nebojsa-Stefanovic-o-javnim-kamerama-u-Beogradu.html

32 Zakon o zaštiti podataka o ličnosti, član 5- Načela obrade ličnih podataka: https://www.paragraf.rs/propisi/zakon-o-zastiti-podataka-o-licnosti.html

NEDOSTATAK PRAVNOG OKVIRA

Oblast video nadzora nedovoljno je regulisana u Republici Srbiji. Donošenjem novog Zakona o zaštiti podataka o ličnosti propuštena je prilika da se ova oblast detaljnije reguliše, posebno imajući u vidu njene implikacije na privatnost građana. Pojedine odredbe koje se dotiču video nadzora rasute su u zakonima vezanim za rad policije i drugih službi bezbednosti, a uvođenje sistema za video nadzor, pored policije, povereno je, prema Zakonu o privatnom obezbeđenju, jedino još privatnim subjektima za obezbeđenje (koji moraju imati određene licence).

Ovlašćenja za uspostavljanje i korišćenje sistema za video nadzor

Prema Zakonu o policiji, zarad obavljanja policijskih poslova policija može vršiti nadzor i snimanje javnog mesta, korišćenjem opreme za video akustičke snimke i fotografisanje u skladu sa propisom o evidencijama i obradi podataka u oblasti unutrašnjih poslova.[33] U Zakonu o policiji se ne precizira šta se smatra video nadzorom, a ovu definiciju moguće je naći u Zakonu o evidencijama u oblasti unutrašnjih poslova, u članu 5, u kojem stoji: "sistem video-akustičkog snimanja (video-nadzor) jeste elektronski sistem za nadgledanje i snimanje situacija na nekom prostoru i prenos signala s kamera na predefinisanu lokaciju"[34].

U članu 52. Zakona o policiji koji se odnosi na snimanje na javnim površinama stoji da ovu aktivnost policija mora javno saopštiti, a da se podaci prikupljeni na ovaj načini moraju čuvati u propisnoj evidenciji, i da je rok za njihovo uništenje godinu dana. U Zakonu o policiji se na više mesta navodi da podaci koji se prikupljaju posredstvom video nadzora čuvaju u skladu sa propisima o evidencijama.

Pregledom člana 47. Zakona o evidencijama u oblasti unutrašnjih poslova, a koji se odnosi na evidencije u oblasti video-akustičnog snimanja uočava se neujednačenost ova dva propisa. Naime, u član 47. stoji da se "svi podaci prikupljeni korišćenjem opreme za video-akustičko snimanje čuvaju najkraće 30 dana, odnosno najduže pet godina, kada se pregledom prikupljenih podataka identifikuju lica, događaji i pojave koji zahtevaju preduzimanje mera i radnji iz nadležnosti Ministarstva".

U pogledu rokova čuvanja podataka ova dva propisa utvrđuju drugačije rokove. Ovo može biti posledica neujednačenosti propisa, ili činjenice da se evidencija propisana u članu 47. Zakona o evidencijama u oblasti unutrašnjih poslova, zapravo ne odnosi na evidencije na koje se referiše u članu 52. Zakona o policiji. Ukoliko je ovo drugo tačno, onda se postavlja pitanje kojim članom je regulisana evidencija koju policija vodi za aktivnost snimanja na javnim površinama (član 52. Zakona o policiji)?[35]

33 Zakon o policiji https://www.paragraf.rs/propisi/zakon_o_policiji.html

34 Zakon o evidencijama u oblasti unutrašnjih poslova: https://www.paragraf.rs/propisi/zakon-evidencijama-obradi-podataka-oblasti-unutrasnjih-poslova.html

35 Za više pogledati: Analizu Procene uticaja obrade na zaštitu podataka o ličnosti korišćenjem sistema video nadzora Ministarstva unutrašnjih poslova, str:16-17 : https://www.sharefoundation.info/wp-content/uploads/Analiza_procene_uticaja_SHARE_Partneri-Srbija_BCBP.pdf

Pored policije, i komunalna milicija u obavljanju poslova iz svoje nadležnosti ima ovlašćenja za audio i video snimanje, a u članu 25. Zakona o komunalnoj miliciji se navodi: "Komunalna milicija vrši audio i video snimanje javnog mesta, radi obavljanja komunalno-milicijskih poslova, korišćenjem opreme za video akustičke snimke i fotografisanje. Radi primene komunalno-milicijskih ovlašćenja, otkrivanja i rasvetljavanja prekršaja, kao i kontrole i analize postupanja komunalnih milicionara, komunalna milicija može vršiti audio i video snimanje njihovog postupanja"[36].

U ovlašćenjima Vojnobezbednosne agencije (VBA) i Vojnoobaveštajne agencije (VOA) stoji da službena lica VBA i VOA imaju pravo da koriste sredstva za osmatranje, snimanje, navigaciju i vezu, kao i da se koriste saobraćajnim sredstvom i sredstvom veze pravnog ili fizičkog lica, kao i da su državni organ ii druga pravna lica u obavezi da im pruže neophodnu pomoć radi izvršenja zadataka iz njihove nadležnosti.[37] Na sličan način su uređena i ovlašćenja Bezbednosno informativne agencije u pogledu snimanja. Ovde treba napraviti razliku, u odnosu na navedena ovlašćenja policije koja se odnose na dozvolu/mogućnost postavljanja i korišćenje kamera na javnim površinama i saobraćajnicama, dok se ovlašćenja bezbednosnih agencija odnose na tajno snimanje konkretnih lica (za koja mora postojati odgovarajuća dozvola nadležnog organa).

Pored organa unutrašnjih poslova, sisteme video nadzora mogu jedino uspostavljati i servisirati pravna lica koja vrše poslove privatnog obezbeđenja. U Zakonu o privatnom obezbeđenju, privatno obezebeđenje definiše se kao obezbeđenje koje obuhvata:

"pružanje usluga, odnosno vršenje poslova zaštite lica, imovine i poslovanja fizičkom i tehničkom zaštitom kada ti poslovi nisu u isključivoj nadležnosti državnih organa, kao i poslove transporta novca, vrednosnih i drugih pošiljki, održavanja reda na javnim skupovima, sportskim priredbama i drugim mestima okupljanja građana (redarska služba), koje vrše pravna lica i preduzetnici registrovana za tu delatnost."[38]

36 Zakon o komunalnoj miliciji https://www.paragraf.rs/propisi/zakon_o_komunalnoj_policiji.html

37 Zakon o Vojnobezbednosnoj agenciji i Vojnoobaveštajnoj agenciji, član 33- Posebna ovlašćenja: https://www.paragraf.rs/propisi/zakon_o_vojnobezbednosnoj_agenciji_i_vojnoobavestajnoj_agenciji.html

38 Zakon o privatnom obezbeđenju https://www.paragraf.rs/propisi/zakon_o_privatnom_obezbedjenju.html

U Zakonu se dalje navodi da ove poslove mogu vršiti pravna lica, preduzetnici i fizička lica koja imaju licencu za vršenje poslova privatnog obezbeđenja, izdatu od strane Ministarstva unutrašnjih poslova.

Ovako uspostavljena pravila za korišćenje sistema za video nadzor stvaraju probleme u praksi. Tako javne institucije (na primer škole), kada imaju potrebu za uspostavljanjem sistema za video nadzor, dužne su da se obrate privatnim subjektima koji su licencirani od strane MUP-a. Kada se uzme u obzir nedostatak svesti institucija o zaštiti privatnosti i nedovoljno poznavanje propisa iz oblasti zaštiti podataka o ličnosti, a za tako važan posao se angažuje privatna firma, postoji opravdana zabrinutost da li će kroz ugovorni odnos ovih subjekata biti pravilno regulisani rokovi čuvanja video snimaka, pristup video snimcima, odgovornost za curenje ili zloupotrebu video snimaka, itd.

Zaštita ličnih podataka i upotreba sistema za video nadzor

Iako je donošenje novog Zakona o zaštiti podaka o ličnosti bilo neophodno, dugoočekivano usvajanje ovog propisa izazvalo je negativne reakcije od strane stručne javnosti, a pre svega organizacija civilnog društva koje se bave zaštitom podataka o ličnosti.

Sa aspekta video nadzora, izostale su odredbe koje bi posebno regulisale oblast video nadzora, a koje su bile predviđene Modelom zakona koji je izradio Poverenik (Model zakona),[39] a koji Ministarstvo pravde nije uzelo u obzir prilikom izrade novog Zakona o zaštiti podataka o ličnosti. Članovi 37-42. Modela zakona uređivali su oblast uspostavljanja i sprovođenja video nadzora na javnim površinama, poslovnim prostorijama i privatnim prostorima, kao i obaveze koje su se odnosile na rukovaoce i obrađivače ovakve vrste ličnih podataka.[40]

Zatim, radi usklađivanja sa pravnim okvirom u Evropskoj uniji, u novi Zakon su uvedene odredbe i Opšte uredbe o zaštiti podataka o ličnosti i Policijske direktive

39 Model Zakona o zaštiti podataka o ličnosti: https://www.poverenik.rs/sr-yu/

40 Ibid.

Evropske unije. To za posledicu ima veliki broj izuzetaka koji se odnose na organe istrage i gonjenja, čime je tumačenje Zakona otežano, a data veća sloboda ovim organima prilikom obrade ličnih podataka. Međutim, upravo je Evropska komisija u komentarima datim na Nacrt Zakona o zaštiti podataka o ličnosti, naglasila da bi odredbe ova dva dokumenta trebalo preneti u nacionalno zakonodavstvo kroz dva odvojena zakona. Takođe, u svojim komentarima Evropska komisija navodi: "da postoji problem u načinu na koji su u jednom zakonskom tekstu usklađene odredbe dva važna akta – Policijske direktive i Opšte uredbe o zaštiti podataka. Konkretno, EK upozorava da „veliki broj izuzetaka čini da Nacrt zakona bude izuzetno komplikovan a time i manje transparentan." Ovde se misli na „više od 40 izuzetaka od opštih pravila" u vezi sa nadležnostima organa za sprečavanje, istragu i otkrivanje krivičnih dela, gonjenje učinilaca krivičnih dela, izvršenje krivičnih sankcija, uključujući sprečavanje i zaštitu od pretnji javnoj i nacionalnoj bezbednosti[41]".

Organima istrage i gonjenja ide u prilog i to što se u članu 40. Zakona, koji se odnosi na ograničenja od prava na informisanost o obradi podataka, ne navodi da ova prava građana mogu biti ograničena samo ako je to utvrđeno drugim (konkretnim, sektorskim) zakonima.[42] Propuštanjem da ovaj član bude preciziran javlja se opasnost da organi vlasti ili privatne kompanije koje rukuju podacima o ličnosti mogu da ograniče pravo na obaveštenost građana o obradi njihovih ličnih podataka, bez izričitog zakonskog ovlašćenja i po sopstvenom nahođenju.

Zbog svega navedenog, realna je bojazan da naša privatnost nije dovoljno zaštićena. Taj strah opravdano raste kada organi javne vlasti, preko medija, najavljuju aktivnosti koje za posledicu imaju veliki uticaj na zaštitu ličnih podataka, kakav je slučaj sa uvođenjem sistema pametnog video nadzora. Iako, novi Zakon o zaštiti podataka o ličnosti ne sadrži posebne odredbe koje se odnose na video nadzor, na ovu oblast se odnose sve odredbe zakona kojima se uređuju pravila i standardi za obradu podataka o ličnosti. Prema načelima Zakona o zaštiti podataka o ličnosti, podaci o ličnosti se moraju obrađivati "zakonito, pošteno i transparentno", što znači da svaka obrada podataka o ličnosti mora biti vršena u skladu sa ovim Zakonom i drugim zakonima koji se bave materijom obrade ličnih podataka. Dalje, lični podaci se mogu obrađivati samo uz postojanje prethodno određene svrhe, izričite, opravdane i zakonite svrhe. Zakon predviđa brojne obaveze za rukovaoce i obrađivače, prava lica čiji se podaci obrađuju uključujući i pravo na sudsku zaštitu, kao i kaznene odredbe za rukovaoce i obrađivače, koji obrađuju podatke o ličnosti suprotno Zakonu.

Kada se razmišlja o uvođenju sistema za video nadzor, a posebno uvođenje softvera za prepoznavanje lica koji veoma invazivno zadiru u pravo na privatnost građana, važno je imati u vidu načelo minimizacije podataka koje je utvrđeno Zakonom o zaštiti podataka o ličnosti. Konkretno, potrebno je ustanoviti da li je u datom slučaju zaista neophodno postavljanje takvog jednog sistema video nadzora ili se svrha zbog koje se taj video nadzor postavlja može ispuniti i nekim manje invazivnim sredstvom po privatnost. U slučaju pametnog sistema za video nadzor čije je postavljanje planirano u Gradu Beogradu, svrha postavljanja nadzora je, prema dokumentima dostupnim javnosti, *povećanje bezbednosti građana i doprinos rasvetljavanju različitih slučajeva*

41 Za više pogledati saopštenje Partnera Srbija: Komentari EK o Nacrtu ZZPL konačno dostupni javnosti https://www.partners-serbia.org/komentari-evropske-komisije-o-nacrtu-zakona-o-zastiti-podataka-o-licnosti-konacno-dostupni-javnosti/

42 Partneri Srbija, Zadržati ustavnu garanciju prava građana u novom Zakonu o zaštiti podataka o ličnosti: http://www.partners-serbia.org/zadrzati-ustavnu-garanciju-prava-gradana-u-novom-zakonu-o-zastiti-podataka-o-licnosti/

iz domena bezbednosti učesnika u saobraćaju, kao i i iz domena opšte bezbednosti.[43] Na Ministarstvu unutrašnjih poslova koje je nosilac ove aktivnosti, bilo je da proceni da li se povećanje bezbednosti građana i otkrivanje slučajeva iz domena bezbednosti može postići drugim metodama koje bi imale manji uticaj na privatnost građana. Da li se ista svrha mogla postići i sa povećanim brojem patrola u prometnim delovima grada ili na mestima za koja je procenjeno da se saobraćajni propisi najčešće krše, ili postavljanjem "običnih" kamera, tj video nadzora koji u sebi ne sadrži softvere za prepoznavanje lica? Ozbiljna analiza Ministarstva unutrašnjih poslova o opravdanosti uvođenja ovako masovnog video nadzora javnih površina je izostala.

Izjave zvaničnika nisu otkrile ni da li je Ministarstvo unutrašnjih poslova sprovelo sve procedure koje prethode uspostavljanju pamentnog video nadzora, a na koje su obavezne prema Zakonu o zaštiti podataka o ličnosti. Iz saopštenja Poverenika[44] zaključuje se da Ministarstvo unutrašnjih poslova nije tražilo mišljenje Poverenika o uvođenju video nadzora, niti je pre najava uvođenja novog video nadzora izradilo procenu uticaja ovakve vrste obrade podataka na zaštitu podataka o ličnosti. Naime, u Zakonu o zaštiti podataka o ličnosti, u članu 54. stoji:

Ako je verovatno da će neka vrsta obrade, posebno upotrebom novih tehnologija i uzimajući u obzir prirodu, obim, okolnosti i svrhu obrade, prouzrokovati visok rizik za prava i slobode fizičkih lica, rukovalac je dužan da pre nego što započne sa obradom izvrši procenu uticaja predviđenih radnji obrade na zaštitu podataka o ličnosti.

Član 54. dalje propisuje da u slučaju da se obrada ličnih podataka odnosi na *sistematski nadzor nad javno dostupnim površinama u velikoj meri*, rukovalac je obavezan da izvrši procenu uticaja.

Tek nakon što je Poverenik izvršio nadzor (po sopstvenoj inicijativi), MUP je izradio i Povereniku dostavio dokument sa procenom uticaja obrade podataka na zaštitu podataka o ličnosti.[45]

Dakle, kod uvođenja sistema za video nadzor na javnom prostoru i u velikom obimu kakav je slučaj sa gore pomenutim primerom uspostavljanja sistema pametnog video nadzora, neophodno je sprovođenje procene uticaja takvog sistema na prava građana. Ukoliko takva procena pokaže da predviđena aktivnost ili projekat imaju velike posledice po pravo na privatnost građana, nosioci projekta (u ovom slučaju MUP) treba da prilagode projekat tako da se umanji njegov uticaj na privatnost i druga prava građana. Činjenica da je MUP izradu ove Procene započeo tek nakon što je preduzeo određene korake u primeni projekta, ukazuje da u ovoj instituciji nije postojala dovoljna svest o neophodnosti da se postupi u potpunosti u skladu sa obavezama iz Zakona o zaštiti podataka o ličnosti. Ovo podrazumeva da se na proaktivnoj osnovi prvo jasno definišu razlozi za uvođenje planiranog sistema nadzora, te da se na osnovu toga odrede obim, svrha i način prikupljanja i daljeg korišćenja podataka, zatim da se prepoznaju slabe tačke planiranog sistema za video nadzor sa stanovišta procedura i mera zaštite podataka, a potom i otklone rizici od nezakonite upotrebe podataka, ili barem da se takvi rizici svedu na najniži mogući nivo. Naknadni postupci MUP-a u tom pogledu svakako su dobrodošli, a o tome da li su oni dovoljni sa stanovišta obrade i zaštite ličnih podataka, odnosno da li će sistem dobiti zeleno svetlo za upotrebu, trebalo bi da odluči Poverenik kao organ nadležan za kontrolu primene Zakona o zaštiti podataka o ličnosti.

43 MUP, Procena uticaja obrade na zaštitu podataka o ličnosti korišćenjem sistema video nadzora: https://www.sharefoundation.info/wp-content/uploads/MUP-Procena-uticaja-obrade-na-zastitu-podataka-o-licnosti-koriscenjem-sistema-video-nadzora.pdf

44 Poverenik je sproveo postupak nadzora u vezi sa najavom postavljanja video-kamera od strane ministarstva unutrašnjih poslova: https://www.poverenik.rs/sr/

45 MUP, Procena uticaja obrade na zaštitu podataka o ličnosti korišćenjem sistema video nadzora: https://www.sharefoundation.info/wp-content/uploads/MUP-Procena-uticaja-obrade-na-zastitu-podataka-o-licnosti-koriscenjem-sistema-video-nadzora.pdf

ZAKLJUČCI I PREPORUKE

Nedostaci pravnog uređenja video nadzora u Srbiji otvaraju prostor za opravdan strah. Pravo na zaštitu privatnosti, odnosno pravo na zaštitu podataka o ličnosti, iako relativno dobro pravno uređeno u Srbiji, suprotstavljeno je interesima za zaštitu bezbednosti zbog kojih se ovakvi sistemi nadzora najčešće i uvode. Kada su napori za zaštitu bezbednosti uvođenjem sistema za video nadzor praćeni podjednakim naporima i da se zaštiti privatnost građana, ova dva interesa ne moraju biti nekomplementarna. Nažalost, u praksi se mnogo manje pažnje poklanja razvijanju pravila i procedura koji će osigurati zakonitu i etičnu upotrebu sistema za video nadzor. Hardver i softver koji se nalaze u infrastrukturi sistema video nadzora na prvi pogled su „bezgrešni" jer, navodno, ljudi mogu da pogreše a tehnologija ne. Ali, tim sistemima upravljaju ljudi, pa su moguće nepravilnosti u korišćenju kao posledica tri faktora: svesne zloupotrebe, neznanja ili nepažnje. Jednako važno je imati u vidu da ove „mašine" takođe prave ljudi i u njih ugrađuju principe rada koji nisu nužno etični. Naizgled neutralno izrađeni sistemi nadzora, u praksi su se pokazali kao sredstvo kontrole i praćenja posebnih kategorija stanovništva (etničkih manjina, siromašnih, aktivista i boraca za ljudska prava, itd).[46] Ovakve prakse osporavaju pretpostavku da su sistemi nadzora nepristrasni time što njima upravljaju algoritmi.

U demokratiji, uvođenje video nadzora nad javnim površinama mora ispunjavati standarde transparentnosti, a organi javne vlasti dužni su da javnost upoznaju sa planovima za uspostavljanje video nadzora pre njegovog uvođenja. Ovo obaveštenje javnosti mora uključivati i stručno obrazloženje zašto je jedan takav sistem neophodan i u kojoj meri on doprinosi povećanju bezbednosti građana. Studije pokazuju da uvođenje video nadzora nužno ne utiče na povećanje bezbednosti građana, jer se kriminal ili nasilje samo "preseli" u prostor koji nije pokriven kamerama.[47] Zato je nužno da uvođenju video nadzora pretho-

46 Slate, The color of Surveillance: https://slate.com/technology/2016/01/what-the-fbis-surveillance-of-martin-luther-king-says-about-modern-spying.html

47 T. E. Boult, PICO: Privacy throught Invertible Cryptographic Obscuration, str. 3: https://vast.uccs.edu/~tboult/PAPERS/Boult-PICO-preprint.pdf

di stručna analiza koja bi utvrdila koji su metodi prevencije najpogodniji za povećanje bezbednosti nekog prostora. Neodostatak svesti o važnosti zaštite privatnosti u jednom demokratskom društvu, lako nas može pretvoriti u "policijsku državu", u kojoj su ljudska prava trajno suspendovana na uštrb navodne zaštite bezbednosti građana. Zato ovakvi sistemi moraju ispunjavati standarde koje propisuje Zakon o zaštiti podataka o ličnosti.

Zabrinutost da video nadzor može da ima štetne implikacije po zaštitu ličnih podataka proizlazi i iz toga što organi javne vlasti u Republici Srbiji imaju nizak stepen usklađenosti postupanja i internih procedura sa domaćim propisima i međunarodnim standardima vezanim za zaštitu podataka o ličnosti, i u ovom slučaju odredaba drugih zakona koje se odnose na korišćenje sistema za video nadzora. Različiti organi javne vlasti za vršenje svojih ovlašćenja kao sredstvo mogu koristiti sisteme za video nadzor. Međutim kao u opisanom slučaju sa psihijatrijskim institucijama, njihove prakse nisu ujednačene, i često zavisi od čelnika konkretnih institucija.

Video nadzor pored posledica po privatnost građana, ima i potencijalne implikacije na druga prava, kao što su pravo na slobodu govora i okupljanja. Ako smo svesni da "nas" posmatraju, manje ćemo biti slobodni da iznosimo svoje stavove i/ili šetamo ulicama mirno izražavajući protest protiv odluka koje donose javne institucije i ljudi koji njima upravljaju. Zabrinjavaju informacije iz sveta da se ova vrsta tehnologije umesto za bezbednost koristi kao sredstvo za masovni nadzor građana i njihovo držanje pod "kontrolom". Aktivisti u Rusiji tvrde da se tehnologija prepoznavanja lica koristi kako bi se identifikovali ljudi koji su učestvovali u protestima, od kojih su mnogi održani bez dozvole vlasti.[48] Ovakva praksa u kombinaciji sa tendencijom da se propisima kojima se omogućava pravo na organizovanje i učestvovanje u protestima, ovo pravo sputava, preti da umanji prava građana da na ustavom zagaratovane načine izraze svoje nezadovoljstvo protiv odluka države i njenih organa.

Konačno, u državi u kojoj poverenje u institucije nije na visokom nivou, i gde se dešavaju zloupotrebe ličnih podataka, postoji bojazan da bi i sistemi za video nadzor mogli biti zloupotrebljeni od strane države.

Shodno prethodnom, preporuke za unapređenje pravila i prakse upotrebe sistema za video nadzor odnose se pre svega na:

- Pravno regulisanje sistema za video nadzor donošenjem zakona koji bi detaljno uređivao ovu oblast, uključujući i pravno uređivanje tehnologija za prepoznavanje lica.
- Usklađivanje uspostavljanja i korišćenja sistema za video nadzor sa Zakonom o zaštiti podataka o ličnosti.
- Prethodnu izradu analize koja bi dokazala da je uvođenje jednog ovakvog sistema neophodno zarad povećanja bezbednosti građana i imovine, uključujući i prethodnu analizu procene uticaja ovakvog sistema na zaštitu prava na privatnost građana.
- Povećanje transparentnosti rada organa javne vlasti prilikom uvođenja ovakvih sistema.
- Obezbeđivanje sistema zaštite kako bi podaci prikupljeni na ovaj način bili zaštićeni od potencijalne unutrašnje ili spoljne kompromitacije.
- Adekvatno regulisanje odgovornosti u slučajevima kada dodje do manipulacije ili zloupotreba podataka prikupljenih korišćenjem video nadzora u propisima koje donose organi javne vlasti, i u internim politikama i procedurama subjekata koji uspostavljaju i koriste sisteme video nadzora.

48 Radio slobodna Evropa, Rusija: Tehnologija za prepoznavanje lica i suzbijanje protesta: https://www.slobodnaevropa.org/a/30205620.html