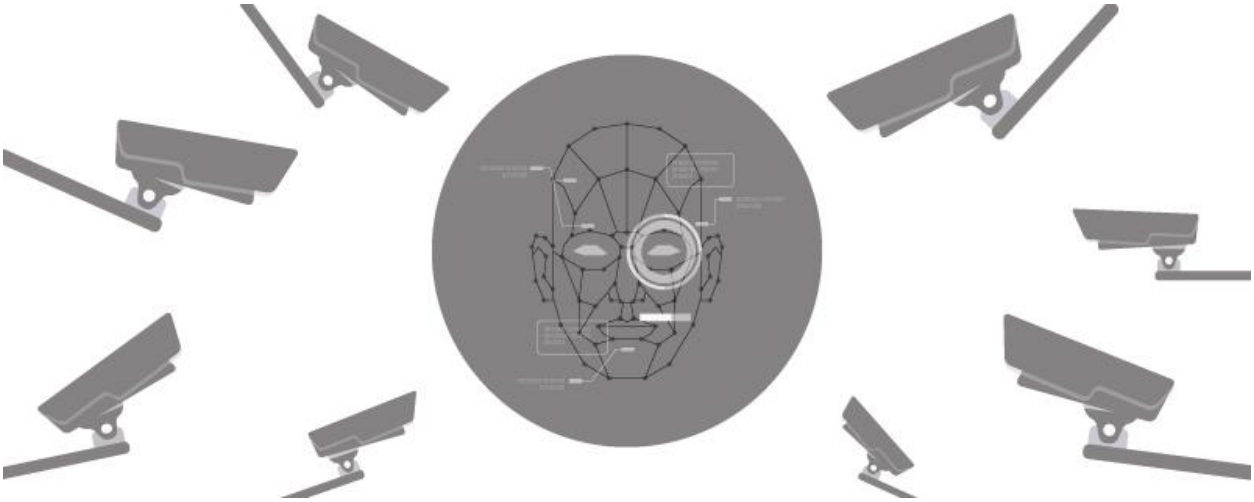

ANALIZA

Procene uticaja obrade na zaštitu podataka o ličnosti korišćenjem sistema video nadzora Ministarstva unutrašnjih poslova

SHARE FONDACIJA

PARTNERI SRBIJA

Beogradski centar za bezbednosnu politiku

Beograd,
Novembar, 2019.

Sadržaj

Rezime

Procena uticaja obrade na zaštitu podataka o ličnosti korišćenjem sistema video nadzora MUP-a **ne ispunjava ni formalne ni materijalne uslove propisane Zakonom o zaštiti podataka o ličnosti**. Shodno tome, Ministarstvo unutrašnjih poslova bi trebalo da do daljeg obustavi uvođenje sistema za pametan video nadzor.

MUP je u skladu sa Zakonom o zaštiti podataka o ličnosti izradio Procenu uticaja i, takođe u skladu sa propisanom procedurom, dokument dostavio Poverniku na mišljenje, što je pohvalna reakcija nadležnih na višemesečne zahteve stručne javnosti, posebno s obzirom na to da je novi Zakon stupio na snagu krajem avgusta, a da je Procena izrađena već u toku septembra. Uvidom u dokument, javnost je po prvi put zvanično upoznata sa konkretnim detaljima koji se tiču najavljenog sistema video nadzora, o kome su nas do sada, neformalno i često kontradiktorno, informisali jedino zvaničnici policije.

Nažalost, propuštena je prilika da se putem Procene uticaje odgovori na sva pitanja od interesa za javnost, kao i da se ispuni zakonska obaveza u formalnom i materijalnom smislu.

1. **Procena uticaja ne ispunjava minimum propisanih zakonskih elemenata** naročito u delu koji se odnosi na inteligentni video nadzor, a koji izaziva najviše interesovanja i zabrinutosti domaće i strane javnosti. Metodologija izrade i struktura Procene uticaja nisu usaglašeni sa zahtevima Zakona:
    a. Ne postoji sveobuhvatan opis predviđenih radnji obrade podataka o ličnosti u slučaju inteligentnog video nadzora;
    b. nisu procenjeni rizici po prava i slobode lica na koja se podaci odnose;
    c. nisu opisane mere koje se nameravaju preduzeti u odnosu na postojanje rizika;
    d. delimično su opisane tehničke, organizacione i kadrovske mere u cilju zaštite podataka.
2. **Sporan je pravni osnov** za masovno korišćenje sistema za inteligentni video nadzor.
3. **Pozitivni efekti** na smanjenje kriminaliteta izneti u Proceni uticaja su **precenjeni** usled činjenice da su relevantna istraživanja i uporedna praksa korišćeni selektivno.

4. **Nije utvrđeno da je** upotreba inteligentnog video nadzora **neophodna** zarad javne bezbednosti, niti da je upotreba ovako invazivne tehnologije **proporcionalna** uzimajući u obzir rizike po prava i slobode građana.
5. Procena uticaja sadrži primere zemalja koje se umnogome oslanjaju na video nadzor, i prenebregava **rastući trend zabrane ili ograničavanja** ovakvih sistema u svetu, zbog prepoznatih rizika po prava i slobode građana.
6. Postoji veliki broj nedoumica i nelogičnosti oko korišćenja pametnog video nadzora zbog protivrečnih informacija iz Procene uticaja i izjava MUP-ovih zvaničnika u medijima.

Kontekst

Početkom 2019. godine, ministar unutrašnjih poslova Republike Srbije Nebojša Stefanović[1] i direktor policije Vladimir Rebić[2] najavili su u izjavama za medije postavljanje 1000 kamera na 800 lokacija u Beogradu. Javnost je tada saznala da će kamere nove generacije imati mogućnost korišćenja softvera za prepoznavanje lica i registarskih tablica vozila.

Nakon ovih izjava, civilni sektor je Ministarstvu unutrašnjih poslova poslao zahteve za pristup informacijama od javnog značaja, tražeći informacije o javnoj nabavci kamera, proceni uticaja na zaštitu podataka o ličnosti koju je neophodno izraditi u skladu sa novim Zakonom o zaštiti podataka o ličnosti, lokacijama kamera i druge informacije od javnog interesa. Između ostalog, traženo je dostavljanje kopije "istraživanja i analize događanja, pre svega krivičnih dela, na teritoriji grada Beograda", koje je direktor policije Rebić spominjao tokom gostovanja na RTS-u.

MUP je u odgovorima na zahteve naveo da su svi dokumenti u vezi sa javnom nabavkom video opreme zaštićeni stepenom tajnosti "poverljivo", dok tražene informacije o lokacijama i analizi nisu sadržane ni u jednom dokumentu, odnosno nosaču informacija, što je zakonski preduslov za ostvarivanje pristupa informaciji od javnog značaja.[3] Na pitanje da li je izvršena procena uticaja obrade na zaštitu podataka o ličnosti, MUP je odgovorio da još nije počela primena novog Zakona o zaštiti podataka o ličnosti, uz objašnjenje da su evidencije i obrada podataka o ličnosti sa video nadzora regulisani Zakonom o evidencijama i obradi podataka u oblasti unutrašnjih poslova.[4]

U odgovorima MUP-a nalaze se informacije o saradnji MUP-a i kineske kompanije Huawei na unapređenju informacionog i telekomunikacionog sistema kroz izradu rešenja za povećanje opšte bezbednosti građana u projektu "Sigurno društvo", o čemu su razgovori

[1] Stefanović: Hiljadu kamera sa softverima za prepoznavanje lica i tablica, N1, 30. januar 2019. Link: http://rs.n1info.com/Vesti/a456247/Stefanovic-Hiljadu-kamera-sa-softverima-za-prepoznavanje-lica-i-tablica.html

[2] Šta će i koga snimati 1.000 novih kamera po gradskim ulicama, RTS, 9. februar 2019. Link: http://www.rts.rs/page/stories/sr/story/125/drustvo/3415215/sta-ce-i-koga-snimati-1000-novih-kamera-po-gradskim-ulicama.html

[3] Odgovor MUP-a na zahtev za informacije od javnog značaja, 7. mart 2019. Link: https://resursi.sharefoundation.info/wp-content/uploads/2019/03/Odgovor-MUP-7.3.2019..pdf

[4] Rešenje MUP-a o odbijanju zahteva za informacije od javnog značaja, 7. mart 2019. Link: https://resursi.sharefoundation.info/wp-content/uploads/2019/03/Resenje-MUP-7.3.2019..pdf

započeti 2011. godine. Iz odgovora smo takođe saznali da je MUP 2017. godine zaključio Sporazum o strateškom partnerstvu sa kompanijom Huawei za uvođenje eLTE tehnologija i rešenja za "bezbedan grad" u sistemima javne bezbednosti. Vlada Republike Srbije je 2016. godine zaključkom dala saglasnost na ovaj sporazum.

Istovremeno, na zvaničnom sajtu kompanije Huawei nalazila se studija slučaja sa detaljnim informacijama o postavljanju kamera za video nadzor u Beogradu i saradnji sa Ministarstvom unutrašnjih poslova Republike Srbije.[5] Studija predstavlja iscrpan opis saradnje kompanije Huawei i MUP-a koji u znatnoj meri protivreči informacijama dobijenim od Ministarstva. Huawei navodi da je Ministarstvu unutrašnjih poslova ponudio inteligentne sisteme video nadzora (IVS), sisteme inteligentnog transporta (ITS), unapređenu 4G mrežu (eLTE broadband trunking technology), unifikovane data centre i povezane komandne centre. Dodaje se i da je prvobitno instalirano devet test kamera na pet lokacija, uključujući sedište Ministarstva unutrašnjih poslova, sportsku arenu, tržni centar i policijsku stanicu. Huawei navodi da su u test fazi kamere uspešno obavile više funkcija, između ostalih preuzimanje video snimaka, njihovo kompresovanje, automatsko prepoznavanje registracionih tablica, analizu ponašanja, prepoznavanje lica, kao i dijagnostiku kvaliteta zvuka. U prvoj fazi projekta, instalirano je 100 video kamera visoke definicije na više od 60 ključnih lokacija i renovirani su komandni i data centar u Beogradu. Nedugo po objavljivanju teksta SHARE Fondacije sa informacijama iz studije slučaja, stranica je uklonjena sa zvaničnog sajta kompanije Huawei, ali je ostala sačuvana arhivirana verzija.[6]

Organizacije civilnog društva su takođe tražile uvid u dokumenta koja su potpisana sa kineskim partnerima, za koja smo saznali iz prvobitnog odgovora MUP-a, kao što su Memorandum o razumevanju zaključen između Ministarstva unutrašnjih poslova i kompanije Huawei i Sporazum o strateškom partnerstvu, kao i više dokumenata koje je MUP potpisao sa Ministarstvom javne bezbednosti NR Kine. Međutim, MUP je uskratio pravo na pristup traženim službenim dokumentima, navodeći da u zahtevima nisu dati

[5] Arhivirana verzija stranice "Huawei Safe City Solution: Safeguards Serbia" sa zvaničnog sajta kompanije Huawei, 22. mart 2019. Link: https://archive.li/pZ9HO

[6] Huawei zna sve o kamerama u Beogradu – i nije im teško da to i kažu! SHARE Fondacija, 29. mart 2019. Link: https://www.sharefoundation.info/sr/huawei-zna-sve-o-kamerama-u-beogradu-i-nije-im-tesko-da-to-i-kazu/

"precizni opisi" informacija koje se traže.[7] U međuvremenu, ministar Stefanović je tokom leta u novoj izjavi medijima rekao da će, umesto hiljadu, u Beogradu biti postavljeno 2000 kamera.[8]

Procena uticaja obrade na zaštitu podataka o ličnosti korišćenjem sistema video nadzora MUP-a dobijena je od Poverenika, na osnovu zahteva za pristup informacijama od javnog značaja. Mišljenje Poverenika je još uvek u izradi.

[7] Zarobljeni službeni dokumenti – šta je sve informacija od javnog značaja, SHARE Fondacija, 25. jun 2019. Link: https://www.sharefoundation.info/sr/zarobljeni-sluzbeni-dokumenti-sta-je-sve-informacija-od-javnog-znacaja/

[8] 2020. godine Beograd će SNIMATI 2.000 kamera (VIDEO), Mondo, 30. jul 2019. Link: https://mondo.rs/Info/Beograd/a1208322/Nebojsa-Stefanovic-o-javnim-kamerama-u-Beogradu.html

Procena uticaja ne ispunjava minimum propisanih uslova

Član 54 Zakona o zaštiti podataka o ličnosti ("Sl. glasnik RS, br. 87/2018") reguliše situacije i okolnosti u kojima su nadležni organi dužni da sprovedu prethodnu procenu uticaja na zaštitu podataka o ličnosti ukoliko određena vrsta obrade ispunjava zakonom predviđene kriterijume. MUP je u skladu sa svojom zakonskom obavezom u septembru 2019. godine pripremio dokument pod nazivom "Procena uticaja obrade na zaštitu podataka o ličnosti korišćenjem sistema video nadzora" koji je 23. septembra dostavio Povereniku za informacije od javnog značaja i zaštitu podataka o ličnosti na dalje postupanje.

Obavezni elementi ovakve procene ukoliko je vrše nadležni organi u posebne svrhe su:

1. sveobuhvatan opis predviđenih radnji obrade;
2. procena rizika za prava i slobode lica na koje se podaci odnose;
3. opis mera koje se nameravaju preduzeti u odnosu na postojanje rizika, uključujući mehanizme zaštite, kao i
4. tehničke, organizacione i kadrovske mere u cilju zaštite podatka o ličnosti i obezbeđivanja dokaza o poštovanju odredbi ovog zakona, uzimajući u obzir prava i legitimne interese lica na koje se podaci odnose i drugih lica.

Posebnu teškoću u analiziranju Procene uticaja predstavlja činjenica da njena struktura ne prati navedenu obaveznu sadržinu koji propisuje Zakon, te je teško doći do odgovora na pitanje koje od obaveznih elemenata Procena uticaja zapravo razrađuje na zadovoljavajući način. U tom smislu, početni problem predstavlja činjenica da je uvidom u Procenu uticaja teško utvrditi na koju vrstu ili vrste radnji obrade se ona uopšte odnosi.

S tim u vezi, "običan" video nadzor, to jest samo nadgledanje i snimanje određenih situacija predstavlja jednu vrstu obrade, dok je korišćenje inteligentnih sistema za prepoznavanje lica, objekata ili radnji potpuno druga vrsta obrade podataka o ličnosti u smislu propisa koji regulišu ovu oblast. Inteligentni sistemi za video nadzor prikupljaju dramatično više podataka, i po broju i po vrsti, uključujući i biometrijske podatke, čime su rizici po prava i slobode fizičkih lica nesrazmerno veći nego kada je u pitanju "običan" video nadzor. Ipak, sama Procena uticaja ne pravi ovu razliku na jasan i nedvosmislen način ni po jednom od obaveznih elemenata koje Zakon nalaže.

Procena uticaja suštinski propušta da opiše na koji način će se obrađivati podaci o ličnosti u slučaju inteligentnog video nadzora, koji su u tom slučaju mogući rizici po prava i

slobode građana, a samim tim nužno ni koje se mere preduzimaju u odnosu na postojanje takvog rizika. Stoga smatramo da MUP do ovog trenutka zapravo nije procenio uticaj inteligentnog video nadzora na zaštitu podataka o ličnosti. Na ovaj zaključak ne utiče činjenica da Procena uticaja više puta pominje i opisuje inteligentni video nadzor - s obzirom na to da se taj opis daje sa tehničkog aspekta i to samo u kontekstu predstavljanja budućih planova u okviru projekta "Sigurno društvo", što ni na koji način ne ispunjava minimum zahteva koje Zakon propisuje za prihvatljivu procenu uticaja takvih radnji obrade na zaštitu ličnih podataka.

Struktura i sadržina Procene uticaja

Obavezna minimalna sadržina procene uticaja obuhvata četiri elementa.

Sveobuhvatan opis predviđenih radnji obrade

Prvi i osnovni element Procene uticaja jeste opis predviđenih radnji obrade kojimora biti sveobuhvatan. Međutim, Zakon ne definiše ovu sveobuhvatnost, pa se treba osloniti na relevantne dokumente za tumačenje ovog pojma. U tom smislu, svakako su od najvećeg značaja smernice Radne grupe 29 u vezi sa procenom uticaja na zaštitu podataka o ličnosti.[9] Prema ovim smernicama, sveobuhvatnost predmetnog opisa podrazumeva navođenje sledećih informacija: (1) prirodu, obim, kontekst i svrhu predmetne obrade; (2) vrstu podataka o ličnosti, primaoce podataka i vremenski period čuvanja; (3) funkcionalni opis radnji obrade; (4) opis opreme i ljudstva koji obrađuju podatake.

U Proceni uticaja MUP-a se navodi da je tokom Faze 1 projekta "Video nadzor u saobraćaju" na 61 lokaciji instalirano 59 pokretnih kamera i 47 fiksnih kamera visoke rezolucije. Takođe, navedeno je da će se u ovoj fazi po planu projekta sprovoditi radnje obrade koje uključuju:

- ambijentalni, odnosno panoramni video nadzor prostora
- pregled video zapisa
  - u realnom vremenu
  - premotavanje video materijala
- analizu video zapisa[10]
  - detektovanje događaja u realnom vremenu:
    - ostavljanje i pomeranje objekata
    - napuštanje objekata
    - povećan broj ljudi na nekom prostoru
    - ulazak u definisanu zonu tokom nekog perioda vremena
    - uočavanje pogrešnog smera kretanja
    - brojanje ljudi
    - automatsko prepoznavanje registarskih brojeva tablica

[9] Smernice u vezi sa procenom uticaja na zaštitu podataka o ličnosti, Radna grupe 29, 13. oktobar 2017. Link: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

[10] Ovo obuhvata i lica koja se slučajno odnosno sticajem okolnosti zateknu na mestu događaja i na prostoru koji je pokriven video nadzorom, kako je navedeno na strani 19 Procene uticaja.

    - druge obrade
- inteligentnu pretragu video materijala prema različitim kriterijumima:
    - prostor
    - vreme
    - dešavanje na sceni
    - objekat i tip objekta (vozilo, čovek, predmet)
    - boja objekta
    - zona na sceni
    - smer kretanja
    - automatsko kreiranje video sinopsisa - sažetog prikaza video materijala. (prim. aut. prikaži mi samo snimke u kojima se pojavljuju osobe koje na sebi imaju određeno *obeležje u poslednjih 7 dana na teritoriji opštine Stari Grad*)

Dalje se navodi da je Kapitalnim projektom "Video nadzor u saobraćaju – Faza 2" predviđeno da će se u naredne tri godine postaviti kamere na više od 800 novih lokacija. U ovoj fazi takođe je planirano proširenje funkcionalnosti analitike video materijala sledećim alatima:

- automatsko prepoznavanje lica (Automatic Face Recognition, AFR),
- integracija sa GIS platformom (geografski informacioni sistem) - praćenje trajektorije vozila kao i, eventualno, uvođenje sistema za automatsko prepoznavanje registarskih tablica i detekciju saobraćajnih prekršaja motornih vozila,
- Kao i eventualno sistem za prepoznavanje registarskih tablica i detekciju saobraćajnih prekršaja.

Proširenje u drugoj fazi prati unapređenje softverskih verzija sistema i povećanje broja licenci za naprednu analitiku video signala. Takođe se planira opremanje policijskih stanica po opštinama opremom za pristup sistemu za video nadzor.

U Proceni uticaja opisan je i Sistem inteligentnog video nadzora - IVS koji se sastoji od: (a) sistema video nadzora i (b) inteligentne video analitike. Na osnovu opisa ovog sistema zaključujemo da radnje obrade obuhvataju inteligentnu video analitiku, zatim skladištenje video materijala sa kamera i rezultata same analitike, pregled snimljenog materijala, tenaprednu pretragu snimljenog materijala.

Dakle, Procena uticaja radnje obrade opisuje sa aspekta hronologije implementacije projekta "Video nadzor u saobraćaju" kroz faze. Međutim, do kraja ostaje nejasno uticaj kojih tačno radnji obrade se zapravo procenjuje. U tekstu Procene uticaja nije decidno navedeno da li ona treba da služi kao procena uticaja radnji koje su do ovog trenutka već sprovedene ili obuhvata i uticaj radnji koje su planirane u narednim fazama projekta.

Opis radnji obrade u Proceni uticaja ne sadrži ključne informacije koje su potrebne da bi se ovaj opis mogao smatrati sveobuhvatnim. Tako iz informacija koje su date ne može se razumeti koja je konkretno priroda, obim, kontekst i svrha video nadzora, koje se vrste podataka o ličnosti prikupljaju, ko su primaoci podataka, kao ni kako će u praksi funkcionisati korišćenje sistema video nadzora.

Još konkretnije, ovog trenutka ne znamo: u kojim će se situacijama koristiti softver za prepoznavanje lica, na osnovu kojih i čijih biometrijskih podataka će softver uopšte moći da radi, u kojim situacijama će se prikupljati ti biometrijski podaci, da li će se podaci koje će softver za prepoznavanje lica obrađivati čuvati u video formatu ili nekom drugom formatu koji omogućava korišćenje ove tehnologije, da li će i u kojim situacijama biti moguća verifikacija rezultata napredne video analitike, u kojim rokovima se čuva video materijal, a u kom roku rezultati analize video materijala, itd.

Procena rizika za prava i slobode lica na koje se podaci odnose

Smatramo da je procena rizika po prava i slobode građana korišćenjem inteligentnog video nadzora svakako najslabiji deo Procene uticaja. Naime, na strani 19 Procene uticaja se navodi da "samo snimanje na javnom mestu od strane policije ne predstavlja povredu prava i sloboda lica jer se radi o legitimnim aktivnostima policije te se samim tim ne može govoriti o ugrožavanju privatnosti lica." Ovakva ocena MUP-a očigledno protivreči Zakonu koji nalaže da se procena uticaja sprovodi onda kada je verovatno da će određena vrsta obrade prouzrokovati visok rizik za prava i slobode fizičkih lica. Takođe je jasno da se upravo zbog mogućnosti povrede prava i sloboda lica upotrebom video nadzora širom sveta sprovode inicijative sa ciljem da se ta prava i slobode zaštite.

Kao jedini rizik Procena uticaja navodi ljudski faktor u upotrebi inteligentnog video nadzora. Iako je jasno da ovaj rizik svakako postoji, smatramo da su drugi rizici po prava i slobode građana daleko značajniji. Tako se u svetu kao glavni rizici prilikom uvođenja inteligentnog video nadzora razmatraju opasnosti po čitav niz prava i sloboda koja su

zajemčena osnovnim korpusom ljudskih prava, kao što su: pravo na privatnost, pravo na zaštitu podataka o ličnosti, pravo na slobodu okupljanja i udruživanja, pravo na miran protest, pravo na slobodu izražavanja, pravo na zaštitu od diskriminacije i druga.

Opis mera koje se nameravaju preduzeti u odnosu na postojanje rizika, uključujući mehanizme zaštite

Budući da suštinski rizici po osnovna prava i slobode lica nisu identifikovani, smatramo da ovaj element Procene uticaja nije uopšte obrađen.

Tehničke, organizacione i kadrovske mere u cilju zaštite podataka o ličnosti

Deo Procene uticaja koji se odnosi na tehničke i druge mere zaštite je svakako najdetaljniji i stoga najviše zadovoljavajući.

Upravljanje sistemom, analitika, skladištenje materijala i podataka vrše se u data centru Komandno operativnog centra (KOC) PU Beograd u ulici Bulevar despota Stefana 107. Data centar je pod video nadzorom, zaštićen merama protiv požara, poplava i "svim drugim" vidovima zaštite, a kompletan sistem video nadzora je u izolovanoj mreži MUP-a, zaštićen firewall-om, bez pristupa internetu. Sistemu pristupaju predstavnici tehničke službe Sektora za analitiku, telekomunikacione i informacione tehnologije (SATIT) čije se aktivnosti beleže (loguju), sa definisanim nivoima dozvola za svakog korisnika, isključivo sa računara koji su opredeljeni za tu namenu. Na snazi je i alarm koji bi se aktivirao na svaki pokušaj pristupa sistemu mimo procedure. Kompanija Huawei trenutno razvija sistem kriptovanja koji bi zaštitio izmenu rezultata analitike. Snimci se čuvaju u skladu sa rokovima predviđenim zakonom i bez sistemskog prenosa na spoljne medije (osim u određenim izuzetnim situacijama).

Osim u PU Beograd, monitoring centri za praćenje signala sa kamera u realnom vremenu nalaze se i u prostorijama PS Savski Venac, Stari Grad i Novi Beograd. Nije navedeno da li su i ove lokacije obezbeđene i kojim merama zaštite.

Trenutno, sistemu video nadzora se pristupa u skladu sa instrukcijama iz dva dokumenta:

1. Obavezna instrukcija o održavanju i korišćenju sistema video nadzora u Republici Srbiji.

2. Obavezna instrukcija o održavanju i korišćenju gradskih raskrsnica i saobraćajnica u Beogradu.

Sama Procena uticaja ne navodi sadržinu ovih obaveznih instrukcija, ali se u saopštenju MUP-a od 5. maja 2011. godine (kada su dokumenti usvojeni, nakon afere "Arena") navodi da su ovom instrukcijom "...detaljno i striktno regulisani prava pristupa, procedure preuzimanja snimaka iz arhive, razgraničene odgovornosti organizacionih jedinica Policijske uprave za Grad Beograd i preciziran način održavanja sistema. U skladu sa tim, u prostorijama nadležnih službi postavljeni su interni sistemi za videonadzor kojim se nadgledaju aktivnosti zaposlenih radnika i drugih prisutnih, a uvedena je obaveza instaliranja sistema za interni video nadzor na svim lokacijama budućih korisnika sistema video nadzora MUP-a. Uveden je sistem elektronske identifikacije tako da svaki korisnik može da pristupi sistemu video nadzora saobraćajnica u Beogradu isključivo korišćenjem individualne SMART kartice, pri čemu se svaki pristup i aktivnosti beleže na posebnom serveru."[11]

Uputstva u pripremi

Pored postojećih instrukcija u Proceni uticaja se navodi da je u pripremi novo Uputstvo o uslovima izgradnje, korišćenja i održavanja sistema video nadzora u MUP-u. Ovaj dokument predviđa da će SATIT voditi evidenciju o:

- svim postojećim sistemima za video nadzor koje MUP koristi (sadrži spisak mesta za kamere, lokacije, ID kamera, opis korisničkih centara sa podacima o rukovaocima i korisnicima),

- svim dodeljenim pristupnim nalozima i šiframa sa nivoima pristupa. Njih određuje načelnik Sektora ili lice koje on ovlasti.

Takođe, u toku je izrada Uputstva o jedinstvenom načinu vođenja evidencija u oblasti video akustičkog snimanja kojim se bliže uređuje način vođenja evidencija u oblasti video-akustičkog snimanja u MUP-u koje će, pored pomenutih stavki, obuhvatati:

- evidenciju materijala za obradu (tablice, tip i boja vozila ili objekta, lični opis lica, ključne reči) - može da sadrži i druge podatke koji nisu lični;

[11] MUP doneo Obaveznu instrukciju o uslovima korišćenja video nadzora u Beogradu, Vlada Republike Srbije, 5. maj 2011. Link: https://www.srbija.gov.rs/vest/152338

- evidenciju obrađenog materijala kao rezultata analitike (svi mogući podaci do kojih je došlo analizom, uključujući sliku, zvuk, lične podatke, tip vozila, JMBG, podatke o prekršaju);
- evidenciju o pristupu i korišćenju, vrstama aktivnosti, umnožavanju, broju kopija, IP adresama sa kojih je pristupano, organizacionih jedinica, službenika ili ovlašćenih lica, opis izvršenih radnji, itd;
- evidenciju odluka o izgradnji, nabavci opreme ili nadogradnji postojećeg sistema Ministarstva, ili o sporazumu o ustupanju sistema razvijenog od strane drugog organa / pravnog lica.
    - svaki korisnički centar vodi svoju evidenciju o svemu;
    - sve evidencije se vode lokalno, ručno, elektronski, u obliku tabele na obrascu br. 2 iz Uputstva;
    - neposredno nakon kopiranja na spoljne medije, korisnik je u obavezi da predmetni zapis ukloni sa memorije lokalne radne stanice ili bilo koje druge privremene memorijske lokacije.

U skladu sa ovim upustvom korisnici imaju različite nivoe pristupanja sistemu:

1. **osnovni** - praćenje video signala u realnom vremenu,
2. **srednji** - može i da pregleda snimljen materijal,
3. **viši** - može da kopira na spoljne medijume,
4. **analitičar** - može da koristi napredne alate za obradu prema zahtevima,
5. **viši analitičar** - može i da definiše zahteve i kopira materijal.

Organizacione jedinice koje ranijom odlukom nisu opredeljene kao korisnici, zahtev za pristup sistemu video nadzora sa obrazloženjem i nivoima pristupa podnose Kabinetu ministra ili Direkciji policije. Mere zaštite podataka u korisničkim centrima sprovodi i za njih odgovara rukovodilac te jedinice - mogu se ogledati u ograničavanju upotrebe sredstava za komunikaciju, snimanje, neovlašćen prenos podataka na USB-u, CD-u i sl.

Konačno, kontrolu vođenja evidencija, tačnosti, potpunosti, ispravnosti i ažurnosti podataka obezbeđuju rukovodioci organizacionih jedinica Ministarstva koji i vode tu evidenciju.

Zakonitost obrade podataka u slučaju inteligentnog video nadzora

Pravni osnov u zakonima o evidencijama i policiji

U Proceni uticaja MUP navodi da je pravni osnov za obradu podataka putem video nadzora sadržan u članovima 13 i 47 Zakona o evidencijama u oblasti unutrašnjih poslova kao i članovima 11, 52 i 245 Zakona o policiji.

Prema odredbi iz člana 13 Zakona o zaštiti podataka o ličnosti, obrada koju vrše nadležni organi u posebne svrhe je zakonita samo ako je ta obrada neophodna za obavljanje poslova nadležnih organa i ako je propisana zakonom. Takvim zakonom se određuju najmanje (1) ciljevi obrade, (2) podaci o ličnosti koji se obrađuju i (3) svrhe obrade.

Snimanje na javnim mestima, kao vrsta radnje koja podrazumeva obradu određenih podataka o ličnosti, načelno je regulisano u članu 52 Zakona o policiji ("Sl. glasnik RS", br. 6/2016, 24/2018 i 87/2018), prema čijem stavu 1 policija vrši nadzor i snimanje javnog mesta, radi obavljanja policijskih poslova, korišćenjem opreme za video akustičke snimke i fotografisanje u skladu sa propisom o evidencijama i obradi podataka u oblasti unutrašnjih poslova.

Dakle, policijska radnja "snimanja na javnim mestima", može se sprovoditi samo u granicama koje su regulisane u Zakonu o evidencijama i obradi podataka u oblasti unutrašnjih poslova ("Sl. glasnik RS", br. 24/2018). Međutim, sam Zakon o evidencijama, u prvom redu, eksplicitno ne reguliše takvo snimanje na javnim mestima, niti uopšte prepoznaje pojam "javnog mesta". Već ova okolnost ozbiljno dovodi u pitanje postojanje pravnog osnova za radnje iz člana 52 Zakona o policiji (dok se Zakon o evidencijama ne dopuni odgovarajućim novim odredbama o evidencijama koje se tiču snimanja na javnim mestima).

U tom smislu je važno osvrnuti se i na odredbe oba zakona koje regulišu rokove čuvanja podataka prikupljenih opremom za video nadzor, pri čemu posebnu zabunu unose različita pravila koja su sadržana u članu 52 stav 7 Zakona o policiji, odnosno članu 47 stav 3 Zakona o evidencijama. Naime, prema odredbi iz Zakona o policiji, podaci prikupljeni korišćenjem opreme za video akustičke snimke i fotografisanje koji se ne mogu koristiti u postupku, **uništavaju se u roku od godinu dana** (pri čemu ostaje nejasno o kom postupku se radi). S druge strane, član 47 stav 3 Zakona o evidencijama predviđa 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 spoljnih poslova.

Stoga ostaje otvoreno pitanje da li se evidencija iz člana 47 Zakona o evidencijama uopšte odnosi na evidenciju iz člana 52 Zakona o policiji. Ako to nije slučaj, opet se moramo vratiti na pitanje u kom članu Zakona o evidencijama je onda regulisana evidencija na koju referiše član 52 stav 1 Zakona o policiji.

Dalje, sam Zakon o policiji nema definiciju pojma video nadzora, već je ona sadržana u Zakonu o evidencijama. Prema tom propisu, definicija sistema video-akustičkog snimanja (video nadzor) glasi: "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".

Dakle, prema samoj definiciji iz Zakona o evidencijama, na koji u svom članu 52, stav 1 referiše Zakon o policiji, sistem video nadzora obuhvata samo "nadgledanje" i "snimanje", a ne i sisteme prepoznavanja bilo kojih objekata, lica ili radnji. Laički rečeno, u pitanju je "običan" video nadzor, nasuprot inteligentnom video nadzoru koji se u Proceni uticaja pominje. U tom smislu, važno je istaći da "sistem inteligentnog video nadzora" nigde nije definisan u merodavnim propisima Republike Srbije.

Ni Zakon o policiji ni Zakon o evidencijama u svojim odredbama ne definišu pojam video nadzora koji bi mogao da vrši bilo koje druge radnje obrade podataka o ličnosti sem radnji nadgledanja, snimanja i prenosa signala, ukoliko su određeni lični podaci sadržani u situaciji koja je predmet nadgledanja, snimanja i prenosa signala.

Da nije u pitanju slučajan propust u definisanju pojma video nadzora, zaključujemo iz toga što Zakon o evidencijama u svom članu 13, stavu 1, eksplicitno koristi dodatne pojmove opreme "za prepoznavanje i identifikaciju lica", kao i opreme "za prepoznavanje registarskih tablica", pored pojma "opreme za video-akustičko snimanje i fotografisanje", u skladu sa definicijom video nadzora (koja doduše ne pominje fotografisanje kao posebnu radnju, što je samo po sebi takođe zbunjujuće).

Predmetna odredba člana 13 stav 1 glasi: "Ministarstvo, u cilju izvršavanja poslova iz svog delokruga prikuplja i obrađuje **video i audio zapise** korišćenjem opreme za video-

akustičko snimanje i fotografisanje, prepoznavanje i identifikaciju lica, automatsko očitavanje isprava i za prepoznavanje registarskih tablica".

Međutim, definicije ovih dodatnih vrsta opreme za prepoznavanje i identifikaciju, koje su očigledno drugačije od eksplicitno definisanog video nadzora, nisu date. Stoga ostaje nejasno šta se podrazumeva pod opremom za prepoznavanje i identifikaciju lica ili registarskih tablica. To takođe znači da nema jasnih odgovora na pitanja koje tačno podatke o ličnosti ta oprema može i mora da prikuplja da bi mogla da pravilno radi, kao i na koji način se vrše prepoznavanje i identifikacija. Ono što znamo na osnovu formulacije iz člana 13 stav 1 je da se predmetnom opremom mogu prikupljati samo video i audio zapisi, tj. kada se radi o podacima o ličnosti oni se mogu prikupljati ovom opremom isključivo u formi audio i/ili video zapisa. Iz navedenog bi se moglo zaključiti da su, prema odredbama Zakona o policiji i Zakona i evidencijama, dozvoljene samo radnje prepoznavanja i identifikacije koji su zasnovani na "običnim" audio i video zapisima.

U vezi sa ovim novim vrstama opreme koje ne spadaju u video nadzor, važno je istaći i to da ih Zakon o policiji uopšte ne pominje, već u članu 52 jasno navodi da se na javnim mestima može vršiti snimanje samo putem "opreme za video akustičke snimke i fotografisanje" (u stavu 4 ovog člana navedeno da se mogu koristiti i prevozna i druga sredstva sa ili bez spoljnih obeležja Policije, sa uređajima za snimanje, kao i uređaje za snimanje i prepoznavanje registarskih tablica, ali ove radnje se očigledno ne odnose na radnje koje su predmet Procene uticaja u okviru projekta "Sigurno društvo").

Posledica nedostatka jasnih definicija ovih krucijalnih pojmova je u tome da je zapravo teško ili nemoguće odrediti da postoji pravni osnov da se na javnim mestima prikupljaju bilo koji podaci o ličnosti sem onih koji su dobijeni nadgledanjem ili snimanjem putem definisanog video nadzora u obliku video ili audio zapisa.

Ni u Zakonu o policiji, ni u Zakonu o evidencijama **ne postoji pravni osnov da se putem video nadzora na javnim mestima prikupljaju i dalje obrađuju bilo kakvi biometrijski podac**i. Naime, prema članu 13 Zakona o zaštiti podataka o ličnosti, da bi takav pravni osnov postojao, bilo bi neophodno da bude eksplicitno navedeno koji se biometrijski podaci o ličnosti prikupljaju putem video nazora (pored ciljeva i svrha obrade), što nijedan od navedenih relevantnih zakona trenutno ne reguliše.

S tim u vezi, takođe je važno naglasiti da je u članu 13 stav 2 Zakona o evidencijama navedeno da se video i audio zapisi koji su prikupljeni u skladu sa prvim stavom ovog

člana mogu koristiti za sledeće svrhe: praćenja javnih skupova, povećanja bezbednosti saobraćaja, ljudi i imovine, granične kontrole, koja obuhvata vršenje provera na graničnim prelazima i nadzor državne granice van graničnih prelaza, kao i u svrhu prepoznavanja, identifikacije i pronalaska izvršilaca krivičnih dela i nestalih lica na osnovu biometrijskih podataka o licu, obezbeđenja dokaza za podnošenje prekršajnih i krivičnih prijava, vršenja poslova unutrašnje kontrole, praćenja zakonitosti i unapređenja rada Ministarstva, pokretanja i vođenja disciplinskih postupaka.

Međutim, iako ova odredba previđa da se za svrhe prepoznavanja, identifikacije i pronalaska izvršilaca krivičnih dela i nestalih lica moraju obrađivati neki lični i biometrijski podaci, nigde u propisima nije regulisano koji su tačno lični i biometrijski podaci u pitanju, čiji su to biometrijski podaci tj. kojih tačno lica, te na koji način, kojom opremom i u kom trenutku su ti podaci prikupljeni.

Sličan zaključak možemo izvući i uvidom u član 47, stav 1 Zakona o evidencijama, u kome je navedeno da se u Evidencijama u oblasti video-akustičkog snimanja obrađuju sledeći podaci prikupljeni upotrebom opreme za video-akustičko snimanje i fotografisanje: fotografije i audio i video zapisi lica, vozila, događaja, prostora, **lični i biometrijski podaci o licima**, registarske oznake vozila, datum događaja, vreme događaja, informacije o lokaciji, JMBG, identifikacioni brojevi događaja, podaci o vlasnicima vozila, podaci o vozilima i podaci o učinjenim prekršajima.

Opet, nigde u odredbama Zakona o evidencijama ili Zakona o policiji nije regulisano na koji način se prikupljaju lični i biometrijski podaci koji se mogu naći u ovim evidencijama (niti koji su to tačno podaci), osim što se iz navedenog može zaključiti da ne mogu biti prikupljeni opremom za eksplicitno definisani video nadzor, kao ni opremom za prepoznavanje i identifikaciju lica koja nije ni definisana, jer se ovom opremom u skladu sa članom 13 Zakona o evidencijama prikupljaju **samo audio i video zapisi**.

Očigledno da je u regulisanju ovako važnih pitanja koja direktno utiču na privatnost građana i na zaštitu njihovih podataka o ličnosti previše pravne nesigurnosti, previše otvorenih pitanja i nedefinisanih i nedosledno korišćenih pojmova - što takođe navodi na zaključak o nepostojanju validnog pravnog osnova za prikupljanje podataka o ličnosti u okviru projekta “Sigurno društvo”.

Najzad, član 13 Zakona o zaštiti podataka o ličnosti sadrži i drugi kriterijum za zakonitost obrade koju vrše organi u posebne svrhe - a to je **postojanje neophodnosti** predmetne

obrade za obavljanje poslova nadležnih organa. Procena uticaja ne sadrži objašnjenje zbog čega bi sistem video nadzora iz projekta "Sigurno društvo" bio neophodan za navedenu svrhu, odnosno šta su razlozi zbog kojih se ista svrha ne bi mogla postići sredstvima i načinima koji bi bili manje intruzivni po privatnosti svih građana. Stoga nikako ne možemo znati ni prihvatiti da je obrada podataka o ličnosti koja je predviđena navedenim projektom zaista neophodna u smislu člana 13 Zakona o zaštiti podataka o ličnosti.

Principi zaštite podataka o ličnosti

Dozvoljenost uvođenja sistema inteligentnog video nadzora nad javnim površinama od strane Ministarstva unutrašnjih poslova, mora se ceniti u odnosu na važeći pravni okvir Republike Srbije u oblasti zaštite podataka o ličnosti i unutrašnjih poslova, ali i na međunarodne standarde i prakse u ovim oblastima.

U duhu člana 8 Evropske konvencije za zaštitu ljudskih prava i osnovnih sloboda, obrada podataka o ličnosti korišćenjem video nadzora u javnim prostoru nesumnjivo predstavlja vid mešanja države u privatnost građana, te ova mera mora ispuniti kumulativne uslove navedene stavom 2 člana 8.[12] Pre svega, mera treba da bude u skladu sa zakonom. Dalje, potrebno je da se pokaže da mera služi jednom od navedenih legitimnih ciljeva: interesima nacionalne sigurnosti, javnoj bezbednosti, ekonomskoj dobrobiti, sprečavanju nereda ili sprečavanju kriminala, zaštiti zdravlja i morala ili zaštiti prava i sloboda drugih. U slučaju upotrebe video nadzora od strane MUP-a, nesumnjivo je da data mera može biti u svrsi nekih od navedenih interesa, pre svih javne bezbednosti, sprečavanja nereda ili sprečavanja kriminala. Konačno, mera treba da bude "neophodna u demokratskom društvu". Prema tumačenju Evropskog suda za ljudska prava u predmetu *Dudgeon v. United Kingdom*, to znači da mora da postoji "nužna društvena potreba za mešanjem".

Procena uticaja, kao ni pravni okvir na kome se sistem pametnog video nadzora MUP-a zasniva, propustila je da obrazloži ovaj element – Procena ne navodi ni jedan izvor niti konkretan podatak koji ukazuje da u našem društvu postoji neophodna potreba za

[12] Član 8 Evropske konvencije za zaštitu ljudskih prava i osnovnih sloboda garantuje pravo na poštovanje privatnog i porodičnog života, kako sledi: Svako ima pravo na poštovanje svog privatnog i porodičnog života, doma i prepiske.Javne vlasti neće se mešati u vršenje ovog prava sem ako to nije u skladu sa zakonom i neophodno u demokratskom društvu u interesu nacionalne bezbednosti, javne bezbednosti ili ekonomske dobrobiti zemlje, radi sprečavanja nereda ili kriminala, zaštite zdravlja ili morala, ili radi zaštite prava i sloboda drugih.

uvođenjem jednog invanzivnog sistema nadzora poput ovog (na primer, da li je stopa kriminaliteta u Srbiji u porastu, koja su to najučestalija izvršena krivična dela i prekršaji, koje su njihove društvene posledice, te da li se, i u kojoj meri, njihovo nastupanje može sprečiti primenom video nadzora). Umesto tog obrazloženja, Procena uticaja daje niz uopštenih zaključaka, poput toga da se Ministarstvo "opredelilo za uvođenje novih tehničkih rešenja i sistema koji prate najnovije tendencije u razvoju tehnologije kako bi se povećala bezbednost građana i doprinelo efikasnijoj borbi protiv kriminala, kao i drugih pojavnih oblika ugrožavanja društva, po ugledu na moge zemlje koje koriste tzv. inteligentne sisteme video nadzora, a koji se primenjuju širom sveta."[13]

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.

Iskustva uporedne prakse ukazuju da, u pogledu primene načela obrade podataka o ličnosti, mera pametnog video nadzora ne samo da nije izuzetak u odnosu na druge radnje obrade podataka, već da se njena neophodnost mora ceniti sa dodatnom pažnjom. Prema Smernicama o obradi ličnih podataka putem video opreme, koje je jula 2019. godine usvojio Evropski odbor za zaštitu podataka, upotreba biometrijskih podataka, a posebno prepoznavanje lica, podrazumeva povećane rizike za prava subjekata podataka. Smernice dalje navode da je od presudnog značaja "da se pri pribegavanju takvim tehnologijama poštuju principi zakonitosti, neophodnosti, proporcionalnosti i minimalizacije podataka kako je utvrđeno u GDPR-u. Iako se upotreba ovih tehnologija može shvatiti kao naročito efikasna, rukovaoci pre svega treba da procene uticaj na osnovna prava i slobode lica i razmotre manje invanzivna sredstva za postizanje svojih legitimnih svrha obrade."[14]

Dozvoljenost video nadzora (kao i bilo koje druge radnje obrade podataka) ceni se u odnosu na poštovanje načela obrade podataka koja, propisuje i naš Zakon o zaštiti podataka oličnosti kao opšta načela za sve radnje obrade. Konkretno, član 5 Zakona

[13] Strana 16 Procene uticaja

[14] Smernice 3/2019 o obradi ličnih podataka putem video opreme, Evropski odbor za zaštitu podataka, str. 15, 10. jul 2019, Link: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf

propisuje da se podaci o ličnosti moraju obrađivati: (1) zakonito, pošteno i transparentno u odnosu na lice na koje se podaci odnose; (2) da se moraju prikupljati u svrhe koje su konkretno određene, izričite, opravdane i zakonite i dalje se ne mogu obrađivati na način koji nije u skladu sa tim svrhama; (3) da podaci moraju biti primereni, bitni i ograničeni na ono što je neophodno u odnosu na svrhu obrade; (4) moraju biti tačni i, ako je to neophodno, ažurirani; (5) da se moraju čuvati u obliku koji omogućava identifikaciju lica samo u roku koji je neophodan za ostvarivanje svrhe obrade; (6) da se moraju obrađivati na način koji obezbeđuje odgovarajuću zaštitu podataka o ličnosti, uključujući zaštitu od neovlašćene ili nezakonite obrade, kao i od slučajnog gubitka, uništenja ili oštećenja primenom odgovarajućih tehničkih, organizacionih i kadrovskih mera, te da; (7) rukovalac mora biti u mogućnosti da predoči primenu navedenih principa (odgovornost rukovaoca). Za obradu podataka suprotno načelima obrade, Zakon predviđa i kaznu u iznosu od 50.000 do 2.000.000 RSD za rukovaoca, odnosno obrađivača. Važno je ukazati da se načela obrade moraju poštovati tokom čitavog trajanja obrade podataka, dakle od njihovog prikupljanja, preko daljeg korišćenja i čuvanja/arhiviranja.

Zakonita je ona obrada podataka koja se vrši u skladu sa Zakonom o zaštiti podataka o ličnosti, odnosno drugim zakonom kojim se uređuje obrada podataka. Zakonitost obrade podrazumeva i da rukovalac ima široko razumevanje pravila zaštite podataka, a pre svega svojih obaveza povodom zaštite podataka o ličnosti. Dakle, da bi obrada podataka bila zakonita, nije dovoljno da postoji pravni osnov za obradu podataka, već da su ispoštovana i druga pravila predviđena Zakonom i sektorskim propisima. Kako je navedeno u Proceni uticaja, MUP Srbije pravni osnov za obradu podataka putem mere pametnog video nadzora crpi iz Zakona o evidencijama i obradi podataka u oblasti unutrašnjih poslova i Zakona o policiji. Međutim, to što rukovalac tvrdi da ima pravni osnov da obrađuje podatke lica, ne znači i da je ta obrada dozvoljena u pogledu, na primer, obima podataka koji se obrađuje, ili se pak, ista svrha obrade mogla postići manje invanzivnim radnjama obrade podataka. U skladu sa načelom minimizacije podataka, obim podataka koja se prikuplja radi obrade mora biti primeren i ograničen samo na one podatke koji su neophodni za svrhu koja se želi postići prikupljanjem podataka. S tim u vezi, postavlja se pitanje, da li bi se svrha "ostvarivanja bezbednosne zaštite života, prava i sloboda građana, zaštita imovine, kao i podrška vladavini prava"[15] mogla ostvariti video nadzorom koji ne obuhvata sistem prepoznavanja lica, ili manjim brojem kamera na mestima za koja postoje dokazi za povećanim rizikom za bezbednost lica i imovine, itd.

[15] Strana 17 Procene uticaja

Pravičnost obrade podataka podrazumeva da rukovaoci uvek uzimaju u obzir kontekst, interese lica čije podatke obrađuju i njihova očekivanja u pogledu privatnosti u datim okolnostima, a posebno da ne smeju iskorišćavati svoju svoju nesrazmerno jaču poziciju u odnosu na lice čije podatke obrađuju (na primer, u odnosu organa vlasti i građana).[16] U tom smislu, poštovanje principa pravičnosti obrade u slučajevima obrade podataka od strane organa sile se mora uzeti u obzir sa posebnom pažnjom, jer su predmet radnji obrade ne samo lica koja su mogući osumnjičeni ili okrivljeni za krivična dela ili prekršaje, već svi građani koji se mogu zateći na lokacijama pokrivenim kamerama, a koji imaju određeni stepen očekivanja u pogledu privatnosti.

Još jedan problem u pogledu poštovanja načela obrade podataka kome se u evropskom i domaćem novom režimu zaštite podataka daje primat, jeste transparentnost obrade podataka. Za razliku od Policijske direktive EU koja ne predviđa načelo transparentnosti u slučajevima obrade podataka koju vrše nadležni organi u posebne svrhe, naš Zakon ne pravi ovu vrstu izuzetka, te je transparentnost (uz izuzetke predviđene za ostvarenje prava lica) obaveza za sve rukovaoce podacima. Transparentnost podrazumeva da lice na koje se podaci odnose mora biti obavešteno o svim aspektima obrade pre otpočinjanja obrade podataka, te da se tokom obrade u svakom momentu može obratiti rukovaocu tražeći informacije o tome da li obrađuje njegove/njene podatke, u koje svrhe, po kom pravnom osnovu, da li ih ustupa nekom trećem licu, itd.

S tim u vezi, ukazujemo na nedavnu presudu Visokog suda Engleske i Velsa, kojom je potvrđena neophodnost ili srazmernost upotrebe pametnog video nadzrora za ostvarenje zakonskih ovlašćenja policije. Sud je ovakvu odluku doneo nakon što je utvrdio da su u ovom konkretnom slučaju ispunjeni uslovi da je navedena tehnologija upotrebljena na otvoren i transparentan način, i uz značajno učešće javnosti. Dalje, navodi sud, ova tehnologija korišćena je u ograničenom vremenskom periodu, za konkretne svrhe, a pre same upotrebe to je i javno objavljeno (na primer, na društvenim mrežama).[17] Činjenica da građani do danas nisu obavešteni o aspektima mere pametnog video nadzora, a da ni udruženja građana nisu dobila informacije o lokacijama kamera i planovima MUP-a u

[16] Videti: Vodič kroz Zakon o zaštiti podataka o ličnosti i GDPR – Tumačenje novog pravnog okvira, Misija OEBS-a u Srbiji i SHARE Fondacija, str. 33, 2019. Link: https://www.sharefoundation.info/Documents/vodic_zzpl_gdpr_share_2019.pdf

[17] Videti više na: High Court Dismisses Challenge to Police Use of Facial Recognition Technology, Hunton Privacy Blog, 9. septembar 2019. Link: https://www.huntonprivacyblog.com/2019/09/09/high-court-dismisses-challenge-to-police-use-of-facial-recognition-technology/

povodom ovog projekta, ukazuje da je došlo do ozbiljne povrede načela transparentnosti obrade podataka.

Takođe ističemo da se, prema uporednim iskustvima zemalja EU, poseban režim obrade ne primenjuje na sve aktivnosti nadležnih organa, već samo kada oni preduzimaju aktivnosti u svrhe sprečavanja, istrage i otkrivanja krivičnih dela, gonjenja učinilaca krivičnih dela ili izvršenja krivičnih sankcija, uključujući sprečavanje i zaštitu od pretnji javnoj i nacionalnoj bezbednosti. Tako bi, dakle, lice koje je snimljeno kamerama MUP-a moglo da ostvaruje svoja prava prema opštem režimu zaštite podataka o ličnosti, dok bi se poseban režim (onaj preuzet iz Policijske direktive) mogao primenjivati samo ukoliko bi se zaista i sprovodile aktivnosti sprečavanja, istrage ili otkrivanja konkretnih krivičnih dela, gonjenja učinilaca krivičnih dela ili izvršenja krivičnih sankcija, uključujući sprečavanje i zaštitu od pretnji javnoj i nacionalnoj bezbednosti.

Uticaj video nadzora na bezbednost u javnom prostoru

Video nadzor u javnom prostoru je sistem optičke kontrole mesta putem kamera koje postavlja organ javne vlasti. Javna mesta su prostori (ulice, trgovi, parkinzi, škole) u kojima bi ljudi trebalo da imaju najveću slobodu kretanja bez potrebe da objašnjavaju svoje prisustvo. Danas je video nadzor popularno sredstvo za povećanje bezbednosti i smanjenje kriminala. Najviše se koristi u Evropi, Severnoj Americi i Kini.

U Velikoj Britaniji je za manje od dve decenije drastično povećan broj kamera – od 100 instaliranih kamera 1990. godine do preko četiri miliona u prvoj deceniji 20. veka.[18] Skoro polovina policijskih službi Sjedinjenih Američkih Država svakodnevno koristi video nadzor, dok je značajno povećan broj postavljenih kamera u mestima sa preko 250,000 stanovnika.[19] Osam od deset gradova sa najvećim brojem instaliranih kamera nalaze se u Kini,[20] u kojoj se kamere koriste i za ocenjivanje ponašanja građana.[21]

Nepoznat je tačan broj instaliranih kamera u javnom prostoru Srbije, ali se postavljanje novih kamera u Beogradu intenzivno najavljuje od februara 2017. godine kada je potpisan sporazum o strateškom partnerstvu u sistemima javne bezbednosti između Ministarstva unutrašnjih poslova Srbije i kineske kompanije Huawei. Trenutno je u skladu sa ovim sporazumom u glavnom gradu instalirano 106 kamera na 61 lokaciji, a u planu je da do kraja 2020. godine gradske ulice pokriva više hiljada kamera na 800 lokacija.

Visoki zvaničnici Ministarstva unutrašnjih poslova su u prethodne dve godine iznosili različite argumente u korist instaliranja kamera za video nadzor kineske kompanije Huawei. Tako je ministar unutrašnjih poslova istakao da će kamere omogućiti da policija bolje kontroliše saobraćaj i "borbu protiv organizovanog i svih drugih vidova kriminala".[22]

---

[18] Armitage, R. (2002). To CCTV or not to CCTV? A review of current research into the effectiveness of CCTV systems in reducing crime. Narco, Crime and Social Policy Section, 8; Farrington, D. P., Bennett, T. H., & Welsh, B. C. (2007). The Cambridge evaluation of the effects of CCTV on crime.

[19] Reaves, B. A. (2015). Local police departments, 2013: Equipment and technology. Washington, DC: U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics.

[20] The world's most-surveilled cities, Comparitech, 15. avgust 2019. Link: https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/

[21] How the West Got China's Social Credit System Wrong, Wired, 29. jul 2019. Link: https://www.wired.com/story/china-social-credit-score-system/

[22] 2020. godine Beograd će SNIMATI 2.000 kamera (VIDEO), Mondo, 30. jul 2019. Link: https://mondo.rs/Info/Beograd/a1208322/Nebojsa-Stefanovic-o-javnim-kamerama-u-Beogradu.html

Navedeno je i da se postavljenjem kamera šalje "jasna i snažna poruka da borba protiv narko-dilera neće stati".[23]

Jedan od glavnih argumenta ministra unutrašnjih poslova za Huawei kamere je da video nadzor "u velikoj meri smanjuje stopu kriminala – od razbojništva i džeparenja do teških krivičnih dela".[24] Direktor policije je zaokružio argumentaciju izjavom da kamere "čine čuda" i da će u značajnoj meri olakšati rad policije.[25] Istovremeno su visoki zvaničnici MUP-a ubeđivali građane da ne brinu da će njihova privatnost biti ugrožena.

Dodatno, u Proceni uticaja se na strani 16, bez navođenja izvora, ističe da britanski krimonolozi smatraju da sistemi video nadzora mogu značajno doprineti prevenciji kriminala. Nasuprot tome, na strani 31 se navodi da su rezultati malobrojnih istraživanja u ovoj oblasti poprilično neusaglašeni i međusobno neuporedivi.

Zbog ovakvih iskaza osnovano je upitati se u kojoj meri video nadzor utiče na bezbednost građana. U prethodnih četrdeset godina sprovedeno je više desetina istraživanja o delotvornosti video nadzora u kontroli kriminala. Takva istraživanja su najčešće realizovana u Velikoj Britaniji, Sjedinjenim Američkim Državama, Kanadi, Južnoj Koreji, Švedskoj, Norveškoj, Španiji, Poljskoj i Australiji. Najveći broj istraživanja je testirao efekat video nadzora na stepen kriminaliteta upoređujući periode pre i posle instaliranja kamera.

Jedno od prvih istraživanja uticaja video nadzora na smanjenje kriminala je sprovedeno u Velikoj Britaniji 2002. godine. Posmatrajući stepen kriminaliteta na 22 lokacije, istraživači su otrili da kamere značajno utiču na smanjenje obijanja i krađe automobila, ali da nemaju uticaja na nasilna krivična dela.[26] Sedam godina kasnije istraživanje je ponovljeno na 44 lokacije i utvrđeno je da kamere smanjuju za više od 50 odsto kriminalitet na parkinzima,

[23] MINISTAR U ZAJEČARU Stefanović: Ne stajemo u borbi protiv organizovanog kriminala, Alo, 28. april 2019. Link: https://www.alo.rs/vesti/drustvo/stefanovic-ne-stajemo-u-borbi-protiv-organizovanog-kriminala/161614/vest

[24] MUP nabavlja Huawei kamere i softvere, N1, 11. septembar 2017. Link: http://rs.n1info.com/Vesti/a317159/Stefanovic-Huawei-kamere-i-softveri.html

[25] Šta će i koga snimati 1.000 novih kamera po gradskim ulicama, RTS, 9. februar 2019. Link: http://www.rts.rs/page/stories/sr/story/125/drustvo/3415215/sta-ce-i-koga-snimati-1000-novih-kamera-po-gradskim-ulicama.html

[26] Welsh, B. C., & Farrington, D. P. (2002). Crime prevention effects of closed-circuit television: A systematic review (No. 252). London, England: Home Office Research.

ali da se stanje nije značajno promenilo u centru grada, socijalnim zgradama u zaštićenim oblastima i javnom prevozu.[27]

Nešto drugačiji rezultati su dobijeni u studiji koja je objavljena pre dve godine. Otkriveno da je video nadzor smanjuje za četvrtinu kriminalitet na ulicama i stanicama metroa, ali da ne postiže značajne efekte na parkiralištima i prigradskim stanicama metroa. Dodatno, primećeno je da nadzorne kamere mogu da smanje nasilničko ponašanje na fudbalskim stadionima, kao i u krađama u supermarketima i tržnim centrima. Ogromna novina u odnosu na prvobitno istraživanje je da video nadzor samostalno bez spoljnih faktora, kao što je dodatni policijski rad kroz patrole, ne može drastično da utiče na smanjenje kriminala.[28]

Ove godine objavljen je najsveobuhvatniji presek istraživanja o uticaju video nadzora na kriminalitet i bezbednost. Analizirano je 76 različitih procena uticaja kamera na smanjenje kriminala u tačno definisanim javnim prostorima u kojima se najčešće prijavljuju nasilni zločini i imovinski kriminal, a naročito obijanje i krađa automobila. Mnogo manje je prijavljenih slučajeva ometanja javnog reda i mira, kao i kriminala u vezi sa drogom. U preseku istraživanja je ukazano da je video nadzor najviše uticao na smanjenje imovinskog kriminala i droge, dok nasilni zločini nisu značajno smanjeni. Kamere najviše utiču na smanjenje kriminala na parkinzima, dok efekti nisu tako dobri u ostalim prostorima kao što su centri grada, socijalna naselja, stambena područja i javni prevoz.[29]

Upoređivanjem izjava visokih zvaničnika MUP-a sa rezultatima istraživanja, moguće je zaključiti da direktor policije uopšte nije govorio istinu kada je rekao da video nadzor čini čuda, dok je ministar unutrašnjih poslova delimično bio u pravu.

Video nadzor utiče na bezbednost u saobraćaju ako se kombinuje sa visokim kaznama za prekršaje u saobraćaju, kao i za razbojništva i džeparenja. Ipak, nije utvrđeno da kamere utiču na smanjenje organizovanog kriminala, kao i na teška krivična dela koja su povezana

[27] Welsh, B. C., & Farrington, D. P. (2009). Public area CCTV and crime prevention: An updated systematic review and meta-analysis. Justice Quarterly, 26, 716–745.
[28] Alexandrie, G. (2017). Surveillance cameras and crime: A review of randomized and natural experiments. Journal of Scandinavian Studies in Criminology and Crime Prevention, 18, 210–222.
[29] Piza, E. L., Welsh, B. C., Farrington, D. P., Thomas, A. L.. CCTV Surveillance for crime prevention: A 40-year systematic review with meta-analysis. Criminology & Public Policy. 2019; 18: 135– 159.

sa nasiljem. Video nadzor može da smanji ilegalnu prodaju narkotika ako je kamera postavljena visoko tako da pruža policajcu širi pregled ulice nego kada je na ulici.[30]

Efikasnost video nadzora u velikoj meri zavisi od sposobnosti policijskog službenika ili operatera da prati dešavanja na monitoru i ukršta sa drugim podacima koje policija ima. Na uspešnost video nadzora u prevenciji kriminala utiče i kvalitet i jasnoća procedura za upotrebu celog sistema nadzora, pogotovo ako i kada se koristi softver za prepoznavanje lica koji često pravi greške – daje lažne pozitivne rezultate i sadrži rasne i rodne predrasude.

Problem oko nadzornih kamera ima veliki potencijal za zloupotrebu. Materijal koji se skuplja putem video nadzora može da bude osnova za ucene, naročito kada se ukršta sa drugim podacima koje policija poseduje. Na primer, visoki službenik policije u SAD je uhvaćen kada je na osnovu snimaka sa kamera i baze registracionih brojeva automobila identifikovao ljude koji su se našli ispred kontroverznog kluba i kasnije ih ucenjivao.[31]

Postoje i primeri gde su policajci koristili video nadzor i policijske baze podataka kako bi pomogli sebi ili svojim prijateljima da uhode žene, saznaju gde su bile određenog dana ili prete učesnicima u saobraćaju zbog prekršaja.[32] Neizostavno, tu je i vojearizam. U Srbiji je 2011. godine na internet procurio snimak sa policijskih kamera u kome dvoje ljudi vodi ljubav na automobilu kod Beogradske arene.[33] Takođe, nedavno objavljena studija upozorava da softver za prepoznavanje lica može da pojača predrasude, što omogućava da pojedine grupe ljudi postanu meta zaustavljanja policije češće nego druge grupe.[34]

[30] Piza, E. L., Caplan, J. M., & Kennedy, L. W. (2014a). Is the punishment more certain? An analysis of CCTV detections and enforcement. Justice Quarterly, 31, 1015–1043.
[31] Chief's Friend Accused of Extortion, Washington Post, 26. novembar 1997. Link: https://www.washingtonpost.com/wp-srv/local/longterm/library/dc/dcpolice/stories/stowe25.htm
[32] Testimony by ACLU's Barry Steinhardt on Surveillance System before DC City Council, ACLU, 12. decembar 2002. Link: https://www.aclu.org/other/testimony-aclus-barry-steinhardt-surveillance-system-dc-city-council
[33] Seks kod Beogradske arene na kameri MUPa! (VIDEO+FOTO), Samo provereno, 5. mart 2011. Link: http://www.samoprovereno.com/2011/03/seks-kod-beogradske-arene-na-kameri.html
[34] Data Analytics and Algorithmic Bias in Policing, Royal United Services Institute, 16. septembar 2019. Link: https://rusi.org/publication/briefing-papers/data-analytics-and-algorithmic-bias-policing

Inicijative protiv pametnog nadzora

Rizici po prava i slobode građana usled korišćenja inteligentnog video nadzora su brojni i ozbiljni, dok sa druge strane pozitivni efekti korišćenja ove tehnologije nisu zadovoljavajući. Stoga širom sveta postoje inicijative za zabranu ili strogo regulisanje ove vrste tehnologije.

Sjedinjene Američke Države

Slobodno tržište, manjak regulacije novih tehnologija, kao i blizina velikih tehnoloških razvojnih centara, omogućilo je da različiti oblici praćenja i invanzivnog kršenja privatnosti godinama budu stvarnost građana SAD. Brzopleta implementacija veštačke inteligencije u gotovo svakoj industriji, pokrenulo je sve otvorenije diskusije o etičnosti algoritamskog donošenja odluka i diskriminatornim težnjama ugrađenim u nova tehnološka rešenja, među koje spada i video nadzor. Štaviše, prepoznavanje lica koristi se u nadzoru u više od polovine američkih država; na aerodromima, u radnjama, i od strane policijskih službi. Širenje tehnologije sve više zaokuplja i pažnju građana: ovo je tema o kojoj političari i javne ličnosti sve češće govore - troje stranačkih kandidata za predsednika skrenuli su pažnju na probleme pametnog praćenja tokom aktuelne kampanje: senator Sanders je pozvao na potpunu zabranu prepoznavanja lica u elektronskom nadzoru, dok senatorka Voren i senatorka Haris zahtevaju regulaciju nadzora u krivičnom pravosuđu. Zanimljivo je da političari sa obe strane partijske podele iskazuju protivljenje neregulisanom širenju pametnog nadzora, što nije čest slučaj u atmosferi velikih razdora koji garantuje *status quo* u drugim oblastima. Senatori dve glavne partije su početkom godine zajedno podneli predlog zakona, koji bi ograničio mogućnost kompanija da dele podatke sakupljene prepoznavanjem lica, te zabranio ovu tehnologiju u celosti bez prethodne dozvole subjekata.[35] Rasprave se vode širom zemlje, na svim nivoima vlasti i institucija, a propisi protiv invanzivnog nadzora prepoznavanjem lica postali su stvarnost na nivou gradova, opština i državnih jedinica. Zbog ovoga, SAD predstavljaju bitan uzor za inicijative protiv invanzivnih tehnologija nadzora.

Značajan talas protesta dolazi iz tehnološki najrazvijenijih gradova i država SAD, među zaposlenima u tehnološkoj industriji: ljudi koji dobro poznaju nedostatke i predrasude

[35] Business Groups Push Back Against Proposed Facial-Recognition Bans, The Wall Street Journal, 30. oktobar 2019. Link: https://www.wsj.com/articles/business-groups-push-back-against-proposed-facial-recognition-bans-11572427801

utkane u veštačku inteligenciju; uticaj struke na donosioce zakona je izražen, što se može videti i na javno dostupnim slušanjima članova Senata i opštinskih veća sa ekspertima iz oblasti tehnologije. Država Masačusets u procesu je diskusije i izglasavanja moratorijuma na kupovinu i korišćenje tehnologije prepoznavanja lica u nadzoru od strane vlasti i institucija na nivou te države.[36] Političari imaju visoku podršku birača: čak 79% u Masačusetsu podržava moratorijum, a 91% smatra da vlada ne bi trebalo da koristi praćenje lica u nadzoru bez regulative.[37]

Država Kalifornija je tokom 2019. izborila nekoliko pomaka na polju regulacije. Početkom oktobra 2019, guverner ove države je potpisao zakon kojim se zabranjuje instaliranje i korišćenje prepoznavanja lica na kamerama koje policajci nose na uniformama.[38] Ovaj propis važi tri godine, ne bi li dao aktivistima, zakonodavcima i tehnološkim kompanijama vremena da osiguraju mere zaštite privatnih lica. Prepoznavanje lica u nadzoru je tokom ove godine zabranjeno u četiri američka grada: u San Francisku,[39] Berkliju,[40] Ouklendu[41] (država Kalifornija) i Somervilu[42] (država Masačusets). Sve zabrane se odnose na korišćenje tehnologije od strane vlade i lokalnih institucija, uključujući i policiju; dodatno, regulativa usvojena u Ouklendu, štiti uzbunjivače koji istupe sa informacijama o kupovini, finansiranju i korišćenju nadzora protivno regulativi.

Lokalne uredbe, kao i diskusije koje se trenutno vode, postoje u petnaest država; među njima su uredbe o obaveznoj javnoj raspravi pre kupovine i instaliranja tehnologije

[36] Massachusetts is ready to press pause on face surveillance, ACLU Massachusetts, 22. oktobar 2019. Link: https://www.aclum.org/en/news/massachusetts-ready-press-pause-face-surveillance
[37] Massachusetts voters strongly support pausing use of unregulated face recognition technology, ACLU Massachusetts, 18. jun 2019. Link: https://www.aclum.org/en/news/massachusetts-voters-strongly-support-pausing-use-unregulated-face-recognition-technology
[38] Victory! California Governor Signs A.B. 1215, EFF, 9. oktobar 2019. Link: https://www.eff.org/deeplinks/2019/10/victory-california-governor-signs-ab-1215
[39] San Francisco Bans Facial Recognition Technology, The New York Times, 14. maj 2019. Link: https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html
[40] Berkeley bans facial recognition, The Mercury News, 16. oktobar 2019. Link: https://www.mercurynews.com/2019/10/16/berkeley-bans-facial-recognition/
[41] Odluka Gradskog veća Ouklenda. Link: http://www2.oaklandnet.com/oakca1/groups/cityadministrator/documents/standard/oak070617.pdf
[42] Somerville City Council passes facial recognition ban, The Boston Globe, 27. jun 2019. Link: https://www.bostonglobe.com/metro/2019/06/27/somerville-city-council-passes-facial-recognition-ban/SfaqQ7mG3DGulXonBHSCYK/story.html

nadzora od strane policije u Sijetlu;[43] u državi Teksas uredba o informisanom pristanku zabranjuje korišćenje prepoznavanja lica kroz nadzor bez prethodnog obaveštenja i saglasnosti subjekta nadzora;[44] skupština države Nju Hempšir izglasala je u aprilu 2019. godine zakon o zaštiti potrošača koji zabranjuje firmama da čuvaju, koriste i otkrivaju biometrijske podatke potrošača.[45]

Zanimljivo je i da vidimo prve primere kompanija koje su samostalno odlučile da ne šire nepouzdanu tehnologiju i pre nego što ih vlade regulišu. Odbor za etiku kompanije *Axon*, koja snabdeva opremom većinu policijskih biroa u Sjedinjenim Državama, doneo je odluku da neće koristiti *face matching* tehnologiju, zbog "ozbiljnih etičkih problema".[46] Izvršni direktor Majkrosofta Satja Nadela[47] i predsednik ove kompanije Bred Smit izjavili su da je pravno regulisanje prepoznavanja lica neophodno, kako se implementiranje tehnologije ne bi pretvorilo u "trku do dna".[48] Devet industrijskih grupa, među njima i Privredna komora, Asocijacija direktora aerodroma Sjedinjenih Država, kao i Asocijacija bezbednosne industrije, u oktobru ove godine uputile su pismo na adrese članova Kongresa upozoravajući da potpuno ukidanje tehnologije ne bi pomoglo njenom daljem razvoju, te da treba težiti ka zakonskom regulisanju, a ne zabrani.[49]

[43] West Coast Jurisdictions Advance Community Oversight of Police Surveillance, EFF, 7. avgust 2017. Link: https://www.eff.org/deeplinks/2017/08/west-coast-jurisdictions-advance-community-oversight-police-surveillance

[44] Business and Commerce Code, Chapter 503. Link: https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm

[45] Privacy concerns over 'biometric information' like facial recognition fuel debate, Concord Monitor, 30. april 2019. Link: https://www.concordmonitor.com/biometric-privacy-nh-bill-law-state-house-legislators-senate-25222448

[46] AI Ethics Board Report, Axon, 27. jun 2019. Link: https://www.axon.com/company/news/ai-ethics-board-report

[47] Microsoft's CEO says that facial recognition technology can be 'terrible' and detrimental to society, even as Amazon sells it to law enforcement, Business Insider, 17. januar 2019. Link: https://www.businessinsider.com/microsoft-satya-nadella-calls-facial-recognition-uses-terrible-2019-1?r=US&IR=T

[48] Facial recognition: It's time for action, Microsoft, 6. decembar 2019. Link: https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/

[49] Business Groups Push Back Against Proposed Facial-Recognition Bans, The Wall Street Journal, 30. oktobar 2019. Link: https://www.wsj.com/articles/business-groups-push-back-against-proposed-facial-recognition-bans-11572427801

Osim državnih institucija i velikih kompanija, i industrija zabave pokrenula je inicijativu kojoj se pridružilo četrdeset najvećih muzičkih festivala obećanjem da neće dozvoliti korišćenje prepoznavanja lica u nadzoru na svojim koncertima.[50]

Evropska unija

U avgustu 2019. godine procureo je plan Evropske komisije da građanima i građankama Evropske unije da eksplicitna prava kao subjektima nadzora i da ograniči korišćenje prepoznavanja lica u nadzoru.[51] Ovo će biti još jedan dodatni akt uz GDPR koji štiti biometrijske podatke građanstva, a čini deo opširnijeg zakonodavnog okvira za regulisanje rizika pri implementaciji veštačke inteligencije. Predlog zakona očekuje se 2020. godine. Poređenja radi, predlog GDPR-a objavljen je 2012. godine, a stupio je na snagu šest godina kasnije - procedura je duga, tako da se usvajanje regulacije nadzora na nivou Unije ne očekuje u skorije vreme.

Do tada će države članice svaka za sebe da odlučuje kako da se odnosi prema ovome, i da se oslanja na GDPR kada to može. Francuska Komisija za zaštitu podataka je krajem oktobra upozorila da je testiranje tehnologije prepoznavanja lica u školama na jugu Francuske nezakonito,[52] ali ova preporuka nije zakonski obavezujuća. Ovo je objavljeno par meseci nakon što je Komisija za zaštitu podataka Švedske kaznila opštinu na severu zemlje kada je dozvolila lokalnoj školi da testira prepoznavanje lica za praćenje prisustvovanja časovima,[53] što krši nekoliko članova GDPR-a. Ipak, ista institucija je dozvolila policiji da koristi prepoznavanje lica u svojim aktivnostima.[54]

Velika Britanija je visoko na listi zemalja po broju kamera po glavi stanovnika. Dok Bregzit skreće pažnju javnosti i poličara sa mnogih drugih bitnih pitanja, pojedinci i grupe uspevaju da i u nepovoljnim uslovima unaprede diskusiju o zabrani tehnologije

[50] Ban Facial Recognition at Live Shows. Link: https://www.banfacialrecognition.com/festivals/
[51] EU plans strict limits for facial recognition technology, The Irish Times, 22. avgust 2019. Link: https://www.irishtimes.com/business/technology/eu-plans-strict-limits-for-facial-recognition-technology-1.3993782
[52] French privacy watchdog says facial recognition trial in high schools is illegal, Politico, 29. oktobar 2019. Link: https://www.politico.eu/article/french-privacy-watchdog-says-facial-recognition-trial-in-high-schools-is-illegal-privacy/
[53] Sanktionsavgift för ansiktsigenkänning i skola, Datainspektionen, 21. avgust 2019. Link: https://www.datainspektionen.se/nyheter/sanktionsavgift-for-ansiktsigenkanning-i-skola/
[54] Polisen får använda ansiktsigenkänning för att utreda brott, Datainspektionen, 24. oktobar 2019. Link: https://www.datainspektionen.se/nyheter/polisen-far-anvanda-ansiktsigenkanning-for-att-utreda-brott/

prepoznavanja lica i sakupljanja drugih biometrijskih podataka. Iako je i ranijih godina postojala spoznaja o obuhvatnosti CCTV nadzora na ulicama, deluje da je tek uvođenje veštačke inteligencije u nadzor, odnosno tehnologije prepoznavanja lica, pokrenulo lavinu aktivizma i građanske akcije. Ovo govori u prilog činjenici da se radi o nepouzdanoj tehnologiji koja, na talasu širenja mogućnosti veštačke inteligencije i njene komercijalizacije, velikom brzinom invanzivno zauzima javni prostor i krši osnovne postulate zaštite građanske privatnosti. Sredinom 2018. godine, privatno lice u Velsu je uz pomoć *crowdfunding* kampanje pokrenulo pravni postupak protiv upotrebe prepoznavanja lica od strane policije u Kardifu; sud je upotrebu tehnologije ipak ocenio legalnom, na šta je podneta žalba i čeka se nastavak procesa.[55] *Big Brother Watch* je zajedno sa članovima Parlamenta i organizacijama za zaštitu ljudskih prava, pozvala na zabranu korišćenja tehnologije u policiji, navodeći visoke stope nepravilnosti pri identifikovanju lica.[56] U septembru ove godine, firma nadležna za razvoj prestižne *King's Cross* zone u centralnom Londonu, našla se pod paljbom oštre kritike kada je obelodanjeno da je između 2016. i 2018. instalirala kamere sa softverom za prepoznavanje lica. Usled pritiska javnosti, firma se obavezala da neće koristiti prepoznavanje lica u budućem razvoju *King's Cross* zone. Najveća pravna pobeda za građane Britanije do sada, došla je poslednjeg dana oktobra 2019. godine; tada je parlamentu podnet predlog zakona kojim se uspostavlja moratorijum na tehnologiju praćenja lica, a svako upravljanje, instaliranje, poručivanje opreme sposobne na analiziranje biometrije prolaznika na javnom prostoru smatra se krivičnim delom.[57]

Ministarstvo unutrašnjih poslova Nemačke je 2017. godine pokrenulo pilot projekat testiranja prepoznavanja lica na jednoj od najprometnijih železničkih stanica u zemlji; u zamenu za Amazon vaučer od 25 evra, oko tri stotine učesnika eksperimenta podelilo je svoje podatke, uključujući i biometrijsku fotografiju. Ni Ministarstvo, niti Železnice Nemačke, nisu podelili detalje o projektu sa javnošću, što je dodatno ojačalo negodovanje građana. Pravni stručnjaci ocenjuju da bi implementacija prepoznavanja lica u sprovođenju reda i zakona bila protivna pravu na privatnost nemačkih građana. Po

[55] Police use of facial recognition is legal, Cardiff high court rules, The Guardian, 4. septembar 2019. Link: https://www.theguardian.com/technology/2019/sep/04/police-use-of-facial-recognition-is-legal-cardiff-high-court-rules

[56] MPs and rights groups call for "urgent stop" to facial recognition surveillance, Big Brother Watch, 18. septembar 2019. https://bigbrotherwatch.org.uk/all-media/mps-and-rights-groups-call-for-urgent-stop-to-facial-recognition-surveillance/

[57] Automated Facial Recognition Technology (Moratorium and Review) Bill [HL], UK Parliament. Link: https://publications.parliament.uk/pa/bills/lbill/2019-2020/0047/20047.pdf

zaključenju prve faze testa, Ministarstvo je objavilo da su se rezultati pokazali slabim, a industrijski predstavnici su predložili da je ovo zbog senzibilnosti nemačkih građana po pitanju privatnosti;[58] takvo objašnjenje je nedovoljno i zanemaruje nedostatke tehnologije.

Ostala iskustva

Iako kineski korisnici važe za najopuštenije kada je privatnost u pitanju, istina je da je teško znati šta građani Kine zaista misle i da li pružaju otpor nadzoru kako onlajn tako i oflajn, zbog visokih zidina kojima je Komunistička partija ogradila svoju zemlju.[59] Postoje navodi o povećanom broju onlajn diskusija, sajtova i aplikacija uz pomoć kojih korisnici mogu da zaobiđu internet nadzor, što sugeriše na moguće postojanje slojeva građanstva koji bi se usprotivili pametnom nadzoru na ulicama. Ovome u prilog ide i prva tužba koju je podnelo privatno lice protiv jedne organizacije zbog upotrebe tehnologije prepoznavanja lica, o kojoj se čulo van Kine, početkom novembra. Profesor prava na Žedžijang Univerzitetu, tužio je jedan safari park zbog obaveznog prikupljanja biometrijskih podataka lica od svih posetilaca i tražio povraćaj novca na osnovu zloupotrebe njegovih podataka.[60]

Da savest o nadzoru i te kako postoji u delovima Azije, pokazao je odgovor građana Hong Konga, koji mesecima protestuju. Građani su organizovano demontirali pametne kamere na ulicama;[61] nakon što je vlast zabranila prekrivanje lica maskama,[62] pojavio se niz saveta za zaštitu od prepoznavanja lica, uz pomoć duge kose, šminke, naočara. Takođe, tokom

[58] Big Brother in Berlin, Politico, 13. septembar 2018. Link: https://www.politico.eu/article/berlin-big-brother-state-surveillance-facial-recognition-technology/
[59] How people in China are trying to evade Beijing's digital surveillance, Quartz, 6. avgust 2019. Link: https://qz.com/1659328/chinese-people-are-pushing-back-on-beijings-digital-surveillance/
[60] China wildlife park sued for forcing visitors to submit to facial recognition scan, The Guardian, 4. novembar 2019. Link: https://www.theguardian.com/world/2019/nov/04/china-wildlife-park-sued-for-forcing-visitors-to-submit-to-facial-recognition-scan
[61] Hong Kong: anti-surveillance protesters tear down 'smart' lamp-post – video, The Guardian, 26. avgust 2019. Link: https://www.theguardian.com/world/video/2019/aug/26/hong-kong-anti-surveillance-protesters-tear-down-smart-lamp-post-video
[62] Hong Kong: anti-surveillance protesters tear down 'smart' lamp-post – video, The Guardian, 26. avgust 2019. Link: https://www.theguardian.com/world/video/2019/aug/26/hong-kong-anti-surveillance-protesters-tear-down-smart-lamp-post-video

protestne šetnje, građani su laserskim zracima blokirali kamere,[63] što je simbolično shvaćeno kao odgovor kineskim vlastima i firmama koje masovno prodaju veštačku inteligenciju za javni nadzor.

Australija u poslednjih nekoliko godina gradi nacionalnu bazu podataka koja će omogućiti vladi, bankama i telekomunikacionim službama da koriste veštačku inteligenciju za identifikovanje korisnika na osnovu fotografija iz pasoša, viza i vozačkih dozvola. Međutim, parlamentarni komitet za obaveštajne poslove i bezbednost vratili su na doradu zakone koji bi bazu podataka ozakonili.[64] Komitet je ocenio da bi zakoni u sadašnjem stanju omogućili masovni nadzor građana, a da nova verzija predloga zakona mora biti izgrađena oko "privatnosti, transparentnosti i podložna jakim merama zaštite".

Među supranacionalnim organizacijama, Ujedinjene nacije istupile su sa pozivom na zabranu prodaje tehnologije za nadzor. Specijalni izvestilac za slobodu mišljenja i izražavanja, Dejvid Kej, objavio je izveštaj sredinom ove godine, u kome proziva i vlade i kompanije kao odgovorne za širenje nadzora bez kontrole i pozvao države članice UN da zaštite demokratiju ograničavanjem širenja pametnog nadzora.[65]

Najveći međunarodni poziv za moratorijum na tehnologije prepoznavanja lica potpisalo je osamdeset i devet organizacija iz trideset i četiri zemlje, a među potpisnicima je i SHARE Fondacija.[66]

[63] Hong Kong protesters use lasers to avoid facial recognition cameras and blind police, The Independent, 1. avgust 2019. Link: https://www.independent.co.uk/news/world/asia/hong-kong-protests-lasers-facial-recognition-ai-china-police-a9033046.html

[64] Coalition-led security and intelligence committee rejects Government surveillance bill, ABC News, 24. oktobar 2019. Link: https://www.abc.net.au/news/2019-10-24/parliamentary-security-committee-rejects-identity-matching-bill/11634742

[65] Moratorium call on surveillance technology to end 'free-for-all' abuses: UN expert, UN, 25. jun 2019. Link: https://news.un.org/en/story/2019/06/1041231

[66] Declaration: A Moratorium on Facial Recognition Technology for Mass Surveillance, The Public Voice, oktobar 2019. Link: https://thepublicvoice.org/ban-facial-recognition/