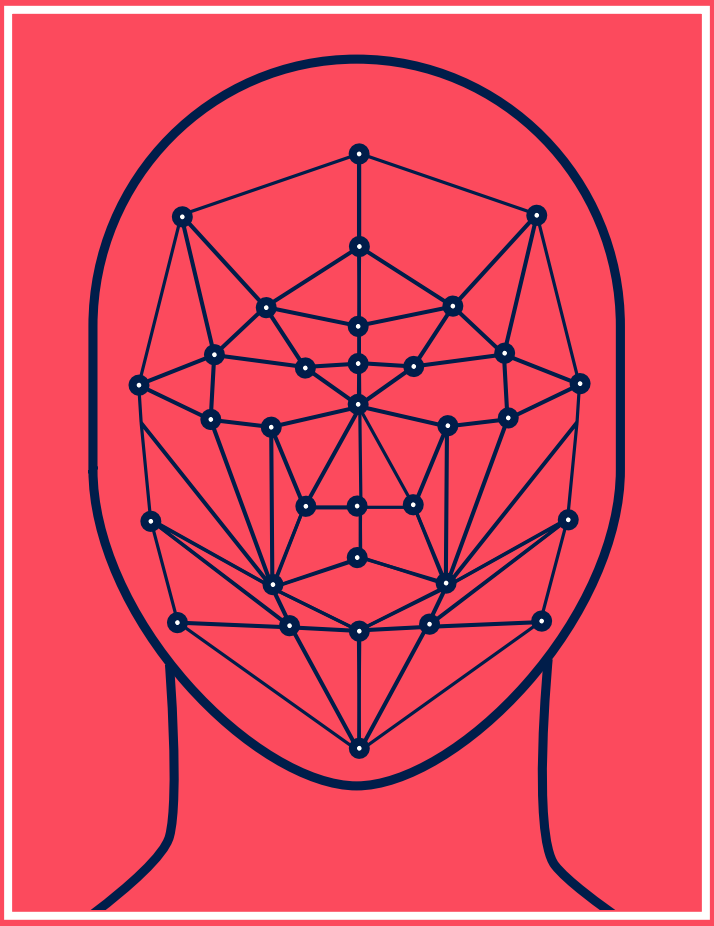
S ONE STRANE LICA:
BIOMETRIJA I DRUŠTVO



Urednici:
Ella Jakubowska, Andrej Petrovski & Danilo Krivokapić

S ONE STRANE LICA:
BIOMETRIJA I DRUŠTVO

Impresum:

Izvršni urednici

Andrej Petrovski & Danilo Krivokapić

Urednica

Ella Jakubowska

Autori

Tehnologija: Bojan Perkov

Pravo: Jelena Adamović & Duje Kozomara

Praksa: Mila Bajić & Duje Prkut

Redaktura prevoda na srpski jezik:

Milica Jovanović

Art direkcija i dizajn:

Olivia Solis Villaverde

Umetnički rad:

„Arhitektura sistema za repoznavanje lica“, Vladan Joler

Izdavač

SHARE Fondacija, 2025.

ZAHVALNOST

Zahvalni smo svojim kolegama iz SHARE Fondacije za podršku i saradnju u procesu nastanka ove knjige, kao i za sav njihov trud u borbi protiv masovnog biometrijskog nadzora u Beogradu.

Neizmerno hvala svim partnerskim organizacijama iz inicijative ReclaimYourFace.

Konačno, beskrajnu zahvalnost dugujemo svakoj pojedinoj osobi koja je doprinela inicijativi #hiljadekamera. Njihova velikodušna podrška bila nam je ključni podsticaj za rad.

Hvala vam.

SADRŽAJ

UVOD

U januaru 2019. ministar unutrašnjih poslova Srbije je na nacionalnoj televiziji izneo revolucionarni plan saradnje sa kineskim tehnološkim gigantom, kompanijom Huawei. To partnerstvo je trebalo da pretvori Beograd u prvu evropsku prestonicu koja će biti pokrivena hiljadama kamera za prepoznavanje ljudskog lica. Za nas je ministrova najava bila znak za uzbunu. Bilo je potrebno smesta preduzeti nešto kako beogradske ulice ne bi doživele nepovratnu transformaciju.

Posle pet godina istrajnog protivljenja uvođenju nadzora sa prepoznavanjem lica u naš grad – što je obuhvatilo tri ministra unutrašnjih poslova u Srbiji, dva povučena Nacrta zakona, mnoštvo sastanaka i nebrojene sate posvećene istraživanju, kampanji i javnom zagovaranju – rešili smo da napišemo knjigu. Mada imamo iskustva u kretanju nepoznatim terenom, spoznaja da se vlada hvali planovima za nadzor celokupnog stanovništva uz pomoć AI tehnologije, postavila nam je ogroman izazov. Srećom, podršku smo dobili i od naših sugrađana i od partnera iz brojnih zemalja u svetu, koji se suočavaju sa sličnim pretnjama. Bez te podrške naš posao bi bio nemoguć.

Knjiga koja je pred vama predstavlja jedno od najsveobuhvatnijih istraživanja o tome kako se biometrijski sistemi koriste širom sveta, kao i o zakonima (ili njihovom odsustvu) kojima se ta upotreba reguliše. Mada nije konačno, istraživanje nudi presek globalnih prilika u industriji biometrijskog nadzora u 2023. godini. Namenjeno je svima koji žele da bolje razumeju šta je masovni biometrijski nadzor, zašto bi trebalo da nas zabrine i šta je to što nam može pružiti nadu naspram moćnih državnih i privatnih aktera.

Centralna tema knjige je ozbiljna šteta koju ovi sistemi mogu izazvati i ekstremno nasilje koje oni omogućavaju. U središtu praksi masovnog biometrijskog nadzora naći ćemo traumatična nezakonita hapšenja, eugeniku, etničko čišćenje, nasilno odvraćanje sa granica i progon. Te prakse su vođene, s jedne strane, globalnom industrijom biometrijskog nadzora u kojoj profit ima prednost nad ljudima i našim pravima, a s druge državama koje – uprkos obilju suprotnih dokaza – i dalje veruju da ti sistemi doprinose bezbednom društvu. Iz svakog od tri poglavlja ove knjige postaje jasno da biometrijske tehnologije i način na koji se one koriste u osnovi predstavljaju političko pitanje.

Još jedan ključni nalaz istraživanja ukazuje na to koliko je teško pribaviti informacije o tome šta se zaista dešava. Od tehničkih specifikacija, preko procesa nabavke i praktične implementacije: biometrijski sistemi su obavijeni velom tajne, što dodatno utiče na neravnotežu moći između onih koji posmatraju i onih koji su posmatrani.

Sigurno ima mnogo više skrivenih zloupotreba. Autori ove knjige duguju duboku zahvalnost novinarima, pravnicima, istraživačima i grupama civilnog društva širom sveta koji se neumorno bore da razotkriju istinu. Na regulatornom frontu, desetine agencija za zaštitu podataka, kao i nezavisni nadzorni organi, poput škotskog komesara za biometriju ili posebnog kontrolnog organa njujorške policije, obavljaju posao od vitalnog značaja kako bi informisali javnost. Nažalost, svi oni hronično pate od nedostatka resursa.

Pravne prilike u svetu se brzo menjaju, čak i u završnoj fazi pisanja ove knjige. Kao rezultat teških pregovora, pokušaji da se prepoznavanje lica u javnom prostoru zabrani u pojedinim državama SAD kao i u Evropskoj uniji, naišli su na snažan otpor političara koji tvrde da ove tehnologije pomažu u borbi protiv teškog kriminala. Moratorijumi na upotrebu se proglašavaju pa ukidaju, dok regulatorni napori posustaju. Sve se to dešava uprkos činjenici da tokom našeg istraživanja nismo pronašli nijedan jedini primer iz kog se može zaključiti da su tehnologije masovnog biometrijskog nadzora sačuvale ljude ili doprinele pravdi – naprotiv, našli smo samo obilje dokaza o šteti.

***

Napomena uz izdanje na srpskom: Istraživanje je izvorno pisano na engleskom jeziku, a knjiga je objavljena krajem 2023. uoči finalne etape izrade novog zakona Evropske unije kojim se reguliše primena sistema veštačke inteligencije. Obraćali smo se prvenstveno evropskim zakonodavcima i građanskim organizacijama,[1] u nastojanju da im pružimo što jasnije informacije o novoj i nedovoljno ispitanoj tehnologiji, kao i njenoj nedovoljno promišljenoj primeni, sa potencijalno drastičnim posledicama po društvo.

Budući da se prevod knjige pojavljuje više od godinu dana kasnije, ovo je ujedno i dopunjeno izdanje koje uključuje neke najznačajnije promene na terenu do kraja 2024. Usvojen je evropski zakon o AI, dok je određenih promena na regulatornom planu bilo i u drugim zemljama i regionima koje smo obuhvatili istraživanjem. Zabeležili smo i krupnije incidente do kojih je

došlo u međuvremenu, kao i nove, drastične primere upotrebe tehnologije u ratu u Gazi.

Istraživanje je sada dostupno ne samo javnosti u Srbiji, koja se već suočava sa izazovima masovnog biometrijskog nadzora (vidi: Studija slučaja, Hiljade kamera u Beogradu), već i širom regiona u zemljama u kojima se govore srodni južnoslovenski jezici. Borba za zaštitu naših lica i tela od industrije nadzora vodi se i na Balkanu, a njen ishod zavisi od svakog od nas.

* U ovom prevodu smo odstupili od žargonske konvencije u srpskom jeziku po kojoj „lice“ u prenosnom smislu označava individualnu ličnost, pojedinca, osobu. Reč „lice“ ovde koristimo samo u njenom doslovnom značenju: prednja strana glave od čela do brade.

POJMOVNIK

Analiza glavnih komponenti (Principal Component Analysis, PCA) – Statistička tehnika koja se koristi za analizu velikih skupova podataka i izdvajanje proseka ključnih karakteristika, tj. glavnih komponenti podataka.

Biometrija — Krovni termin koji se odnosi na čitavu oblast, kao i na proces merenja karakteristika kako bi se one pretvorile u biometrijske podatke, i/ili na naknadnu obradu biometrijskih podataka ili podataka zasnovanih na biometriji.

Biometrijska identifikacija — Proces predviđanja identiteta osobe iznad određenog praga verovatnoće, putem poređenja njenih biometrijskih podataka sa podacima iz jedne ili više baza (npr. nacionalna baza podataka ličnih karata, baza podataka traženih osoba).

Biometrijske karakteristike — Fizičke i fiziološke karakteristike (lice, oko, glas) pre njihove obrade za generisanje biometrijskih ili podataka zasnovanih na biometriji.

Biometrijski nadzor — Sistem koji osmatra biometrijske karakteristike na bilo koji način koji nije pod punom kontrolom i uz pristanak osobe na koju se podaci odnose.

Biometrijski podaci — Lični podaci koji se odnose na nečije lice, telo ili druge fizičke ili fiziološke karakteristike (crte lica, držanje, način hoda itd.) koji su obično obrađeni u mašinski čitljiv format (šablon) i imaju neku vezu sa identitetom te osobe. U pojedinim jurisdikcijama, kao što je EU, podaci treba da „omoguće ili potvrde“ jedinstvenu identifikaciju osobe da bi bili biometrijski (na primer, šablon lica određene osobe) i osetljivi su samo kada se koriste za „svrhu“ jedinstvene identifikacije.

Daljinska biometrijska identifikacija (Remote Biometric Identification, RBI) — Izraz koji se obično koristi u kontekstu EU, jer je izveden iz Uredbe EU o veštačkoj inteligenciji (AI Act). Odnosi se na svaku identifikaciju na osnovu biometrijskih podataka koja se vrši na daljinu.

Detekcija lica — Tehnički metod utvrđivanja da li video ili digitalni slikovni materijal sadrži ljudska lica, koji se vrši automatizovanim sredstvima.

Eigen-lice — Vizuelna reprezentacija eigen-vektorske slike lica onako kako ga opaža ljudsko oko.

Eigen-vektor — U kompjuterskom vidu, matematički objekat koji predstavlja varijabilnost ili odstupanje između karakteristika određenog ljudskog lica i prosečne vrednosti svih lica sadržanih u skupu podataka.

Kompjuterski vid — Oblast veštačke inteligencije koja mašinama omogućava da analiziraju i razumeju informacije dobijene iz različitih vizuelnih unosa, kao što su digitalne slike ili video materijali.

Ljudi u pokretu — Pojedinci ili grupe ljudi koji migriraju iz različitih razloga, što obuhvata, ali nije ograničeno na traženje azila. Mi dajemo prednost ovom u odnosu na druge izraze poput „migranti“, koji se često koriste sa negativnim konotacijama i sugerišu da samo neke kategorije ljudi u pokretu treba da budu zaštićene. Smatramo da svi ljudi u pokretu imaju prava i zaslužuju zaštitu.

Mašinsko učenje (Machine Learning, ML) — Proces „podučavanja“ mašina da autonomno donose predviđanja ili odluke, koji se zasniva na izradi matematičkog modela iz podataka za mašinski trening.

Minorizovani — Poučeni radom Inicijative Equinox za rasnu pravdu, koristimo izraz „minorizovani“ za ljude ili zajednice koje su konstruisane kao nedominantne, posebno one gurnute na marginu društva (na primer, useljeničke i siromašne zajednice). Radije koristimo ovaj izraz nego, na primer, „ranjivi“, prepoznajući na taj način da ove zajednice nisu ranjive po sebi, već su državnim politikama i praksama stavljene u neizvestan ili ranjivi položaj.

Moratorijum — U ovom kontekstu, privremena ili vremenski ograničena zabrana ili prekid primene određenih biometrijskih tehnologija. Moratorijum može biti ograničen samo na njihovu upotrebu, a može se odnositi i na njihov razvoj i distribuciju.

Neuronske mreže — Metoda razvoja veštačke inteligencije za „podučavanje“ mašina da obrađuju informacije tako da pronađu sličnosti ili razlike između unetih podataka, na način koji je navodno sličan ljudskom mozgu.

Podaci zasnovani na biometriji — Podaci koji isprva možda ne izgledaju kao da se iz njih može identifikovati neka osoba (npr. boja kose, boja kože, emocije), a koji su obrađeni u mašinski čitljiv format. Primećujemo, međutim, da sa rastom sofisticiranosti snimanja video zapisa, mnogi od ovih podataka mogu ili će uskoro moći da jedinstveno identifikuju osobu. Čak i bez takvih kapaciteta, obrada tih podataka može biti podjednako intruzivna ili štetna. S tim u vidu, mada u ovoj knjizi koristimo izraz „podaci zasnovani na biometriji“ radi jasnoće, ne smatramo da to predstavlja solidnu ili naučnu razliku. Umesto toga, zalažemo se da podaci zasnovani na biometriji imaju istu (visoku) zaštitu kao i biometrijski podaci.

Prakse biometrijskog masovnog nadzora (Biometric Mass Surveillance, BMS) — Upotreba sistema koji snima i/ili obrađuje biometrijske karakteristike više ljudi odjednom, pri čemu bilo koja od tih osoba možda nije svesna da se to dešava. Kao takve, BMS prakse se najčešće sreću u javnim prostorima i obično su povezane sa sistemima koji mogu da identifikuju ljude – iako to nije neophodno da bi sistem bio BMS. Ova definicija se ne odnosi na primene kao što je, na primer, otključavanje privatnog telefona, sve dok su one zaista zasnovane na pristanku.

Prepoznavanje lica — Sistem/proces za identifikaciju ljudi na osnovu biometrije njihovih lica. Može se koristiti u realnom vremenu, što se često naziva prepoznavanje lica uživo (Live Facial Recognition, LFR), ili naknadno, što je poznato i kao retrospektivno prepoznavanje lica (Retrospective Facial Recognition, RFR).

Rasijalizovani — Poučeni radom Inicijative Equinox za rasnu pravdu, koristimo izraz „rasijalizovani“ kada govorimo o ljudima ili zajednicama kojima je pripisan opaženi rasni ili etnički identitet, pretežno na globalnom severu. To obuhvata zajednice crnih i braon ljudi, muslimanske zajednice, kao i Rome i Sinte.

Sekuritizacija – Posebno u kontekstu ljudi u pokretu, sekuritizacija se može posmatrati kao specifičan pristup migratornim i pograničnim javnim politikama koji je navodno fokusiran na bezbednost, a u okviru kojeg se ljudi u pokretu tretiraju kao spoljna pretnja i rizik kojim treba upravljati, umesto kao ljudska bića koja traže pomoć.

Sistem video nadzora — Povezani sistem za snimanje video zapisa, često zatvoren sistem za prenos signala (Closed Circuit Televison, CCTV).

Skupovi podataka za trening — Strukturirani podaci (uniformno pripremljeni podaci za digitalnu mašinsku obradu) koji se unose u sistem da bi se mašine obučile da obavljaju određene funkcije. Na primer, u slučaju

sistema kompjuterskog vida, skupovi podataka za trening sastoje se od više miliona digitalnih slika ljudskih lica ili različitih predmeta, u zavisnosti od tipa i namene sistema.

Tehnologija prepoznavanja lica (Facial Recognition Rechnology, FRT) — Vidi definiciju prepoznavanja lica; ovaj izraz se obično odnosi na ceo sistem, a ne na proces.

Veštačka inteligencija (Artificial Intelligence, AI) — Kapacitet mašina da opaze, analiziraju i razumeju informacije, koji se može primeniti u autonomnom obavljanju zadataka u različitim oblastima kao što su prepoznavanje govora, kompjuterski vid ili obrada prirodnog jezika.

TEHNOLOGIJA

UVOD

Počev od elementarnih tehnoloških procesa koji leže u osnovi biometrijskih tehnologija, ovo poglavlje mapira razvoj sve naprednijih sistema veštačke inteligencije. Tokom poslednje decenije, ti sistemi su transformisani od obavljanja relativno jednostavnih zadataka kao što je uočavanje objekata, u eksponencijalno sve složeniji pejzaž procesa za prepoznavanje, profilisanje, predviđanje i odlučivanje na osnovu lica, tela i ponašanja ljudi.

Ljudski um je oduvek bio ključna inspiracija za istraživanje i razvoj računarskog vida. Suštinske razlike su, međutim, nesporne. Dok su individualnost crta lica ili linija u otisku prsta idealni za algoritamsku analizu, biometrijsko prepoznavanje operiše na inherentno redukcionistički način – gde karakteristike naših lica i tela postaju mašinski čitljivi objekti.

Kasnih 1980-ih i tokom 1990-ih, kompjuterske stručnjake i istraživače mučilo je pitanje kako preneti ljudska lica u mašinski čitljive formate. Uz pomoć koncepata eigen-lice i eigen-vektor razumećemo da sistemi za prepoznavanje lica analiziraju koliko se neko konkretno ljudsko lice razlikuje od kompozitnog prosečnog lica, kako bi mogli da ih „vide“. Istovremeno, ovi koordinatni sistemi odražavaju ne samo podatke koji su u njih uneti, već i odluke onih koji su podatke unosili, a to su, u slučaju ovih ranih sistema, bili – beli muškarci.

Ljudi koji nisu bili obuhvaćeni važećim referentnim okvirom za poimanje sveta i određivanje šta je „normalno“ stoga su nužno bili isključeni i diskriminisani. Kako istraživačice poput Joy Buolamwini, Timnit Gebru i Deborah Raji već odavno ističu, takvi primeri pružaju dubinski uvid u način na koji biometrijske tehnologije kodiraju i reprodukuju ljudske predrasude i diskriminaciju. Algoritmi su, tako, ključno sredstvo moći za one koji ih stvaraju i koji propisuju pravila za obradu podataka.

Kroz proces analize glavnih komponenti (Principal Component Analysis, PCA) takođe ćemo videti kako je savremena biometrijska obrada zapravo zasnovana na grubim stereotipima, pa čak i eugeničkim teorijama koje sugerišu da se karakter neke osobe može pročitati sa njenog lica. Sistemi prepoznavanja lica koje su razvili Google i Facebook poslednjih godina, označavali su crnce kao majmune, što ukazuje koliko su ove diskriminatorne ideje duboko ukorenjene u savremenim biometrijskim sistemima.

Sve je to danas sastavni deo okolnosti u kojima države i korporacije lakše, brže i jeftinije nego ikada pre postavljaju kamere i senzore, čuvaju snimke i referentne slike i koriste algoritme za prepoznavanje lica i druge vrste analize i profilisanja. Kompanije koriste „oblak“ kako bi neslućene mogućnosti nadzora postale jednostavne kao kad instalirate aplikaciju na svoj telefon. Video visoke definicije postao je stvarnost čak i u uslovima lošeg osvetljenja, dok patenti otkrivaju tehnologije kojima je prepoznavanje ljudi moguće čak i ako im izraz lica odstupa od slike s kojom se poredi.

Javni prostori na koje se svi oslanjamo u svom životu, sve se lakše stavljaju pod stalni nadzor, što kompanije čak ističu kao glavni reklamni argument. Vidimo kako Huawei plasira svoje „pametne“ tehnologije vlasnicima nekretnina i privatnom obezbeđenju – što znači da masovni biometrijski nadzor više nije isključivi domen nacionalnih vlada. Ova decentralizacija biometrijskog nadzora odvija se u skladu sa samim tehnologijama, koje pružaju ugrađene kapacitete kamere da uoči uljeze ili promene u ponašanju mase, eliminišući potrebu za skupim kontrolnim centrima sa desetinama ekrana i zamagljujući tradicionalne granice između hardvera i softvera.

U jednom konkretnom primeru kompanije Huawei, sistem se može pohvaliti takvim mogućnostima kao što su tagovanje (obeležavanje delova snimka), automatizovana izrada spiskova ljudi koji se ponašaju „nenormalno“, praćenje putanje kretanja ljudi (funkcija koju takođe promoviše Amazon) i drugim alatima koji omogućavaju stvaranje najnaprednijeg svetskog panoptikona. Istovremeno, mnoge od tih kompanija, uključujući zloglasni Clearview AI ili PimEyes, upozoravaju svoje korisnike da ovi alati ne bi trebalo da se koriste na taj način – što zvuči licemerno, budući da je masovni nadzor u osnovi njihovog dizajna.

Takvi sistemi profilišu ponašanje ljudi i vrše razne druge vrste profilisanja – recimo, emotivno – na način koji otvara pitanje da li su se regulatori do sada suviše fokusirali na slučajeve primene u svrhu identifikacije (gde je cilj pronaći ime, referencu ili druge jedinstvene karakteristike jedne ili više osoba) a nedovoljno na zaštitu u slučajevima gde identifikacija nije cilj (na primer, kada je cilj profilisanje ljudi na osnovu boje kose, bez obzira na njihov identitet).

Ovo poglavlje takođe razotkriva suštinski problem razmera u kojima su kompanije uspele da nametnu agendu za načine na koje se tehnologije mogu koristiti. IBM je, na primer, tvrdio da je posle ubistva Džordža Flojda prestao da prodaje tehnologije za prepoznavanje lica američkoj policiji, ali ove tvrdnje nikada nisu nezavisno potvrđene. Microsoftovo odavno dato obećanje da će povući tehnologije za prepoznavanje emocija, u vreme pisanja ovog teksta još uvek nije ispunjeno.

Sama činjenica da su ove kompanije odlučile da uvedu moratorijum na vlastite proizvode i usluge nagoveštava koliko su ti sistemi opasni; istovremeno, takođe ukazuje na to koliko je važno ne dozvoliti im da donose odluke koje mogu imati tako dalekosežne reperkusije na naše građanske slobode.

Uprkos njihovom naizgled čisto tehničkom i matematičkom aspektu, jasno je da razvoj ovih sistema jeste i oduvek je bila suštinski ljudska stvar. Rasizam i drugi oblici diskriminacije predstavljaju se kao tehnička objektivnost. Sudeći po patentima i reklamnim objavama, preko kojih možemo da zavirimo u industriju biometrijskog nadzora, očigledno je da im nijedan milimetar naših lica i tela nije izvan domašaja.

TEHNOLOGIJA

DIGITIZACIJA TELA

KOMPJUTERSKI VID

KONTEKST

Da bismo razumeli kako mašine posmatraju, opažaju i razaznaju objekte i podatke – naročito ljudska lica – moramo detaljnije da pogledamo logički okvir sistema za biometrijsku obradu podataka. Kao ilustrativni sistem za ovu studiju, poslužiće nam sistem koji prepoznaje lica, što je još uvek najrasprostranjeniji i najproučavaniji oblik biometrijskog prepoznavanja u kontekstu nadzora.

Koncept kompjuterskog vida je od ključnog značaja za razumevanje mašinske obrade slika. Mašine ili sistemi trenirani za računarski vid ne samo da su u stanju da opaze i prepoznaju objekte na fotografijama i video snimcima, već su takođe trenirani da razaznaju šta je to što vide. Na primer,

mašine mogu da obrađuju određene informacije iz podataka i donose zaključke, u zavisnosti od svrhe ili potrebe za koje je sistem dizajniran. Zbog toga se sistemi kompjuterskog vida mogu primeniti u raznim prilikama, od prepoznavanja da li je neki objekat, na primer automobil, prisutan u zoni nadzora, do prepoznavanja automobila sa konkretnim registarskim tablicama.

Da bismo objasnili šta to znači u praksi, razmotrićemo uobičajene primere kompjuterskog vida:[2]

- Klasifikacija slika: sistem analizira šta je predstavljeno na slici i označava je prema određenoj kategoriji ili klasi, npr. životinja, osoba ili vozilo.
- Detekcija objekta: sistem detektuje da li je određena kategorija slike prisutna u vizuelnom unosu, kao što je video strim; npr. detektovanje da li se osoba pojavljuje u određenom prostoru.
- Praćenje objekta: ako je objekat iz definisane kategorije otkriven u vizuelnom unosu, sistem može da prati i snima njegovo kretanje i pozicije u vremenu i prostoru.
- Pronalaženje slika na osnovu sadržaja: sistem može da traži i nađe slike na osnovu njihovog sadržaja (npr. boja).

Jedan od neophodnih preduslova za razvoj sistema računarskog vida, ili bilo kog drugog sistema koji se može osposobiti za autonomno učenje (što znamo kao „mašinsko učenje"), jeste da sistem bude treniran na velikoj količini podataka. Ovi podaci služe kao ulazna vrednost za učenje, tj. za osposobljavanje sistema da razaznaje podatke koje prima i obrađuje.

Kvalitet sistema takođe treba da se testira i verifikuje na drugim skupovima podataka pre nego što bude spreman za upotrebu, kako bi se potvrdilo da je u stanju da izvršava zadatke do očekivanog nivoa tačnosti. Za treniranje sistema za prepoznavanje lica koriste se mašinski čitljivi skupovi slikovnih podataka, koji mogu da sadrže stotine hiljada, pa čak i milione digitalnih fotografija lica jednako velikog broja različitih ljudi. Fotografije u takvom setu podataka mogu biti lica stvarnih ljudi, što može da izazove značajne pravne i etičke probleme. Alternativno, fotoset se može sintetizovati, tj. digitalno generisati grafičkom obradom.

Naročito u slučaju slika stvarnih ljudi, ovi masivni skupovi podataka obično izviru iz šireg društvenog konteksta koji odražava istorijske obrasce diskriminacije. To podrazumeva odluke o tome ko će biti uključen u skupove podataka, bez obzira da li za to postoji dozvola ili ne, kao i naizgled tehničke, a zapravo duboko subjektivne odluke o tome kako funkcionišu film i blicevi kamere, čije su performanse usavršene za belu kožu.[3] Usled toga se mašine, poput onih koje se koriste za prepoznavanje lica, treniraju na često faličnim, nereprezentativnim i krajnje problematičnim podacima.

Kako objašnjavaju Vladan Joler i Matteo Pasquinelli, „pristrasnost skupa podataka se [dalje] uvodi kroz pripremu podataka za trening od strane ljudskih operatera".[4] To se posebno odnosi na osetljiv i mukotrpan proces označavanja podataka. Za skupove slika, to znači tagovanje svake slike oznakama koje je opisuju („kuća", „drvo", „vrata", „astal") što je najlakše u slučaju objekata. Međutim, kada se to radi za fotografije ljudi, svaki uvredljivi, rasistički ili na drugi način diskriminatorni izraz koji se koristi za njihovo opisivanje na kraju će se odraziti u podacima, a samim tim i u treniranom sistemu.[5]

Tako su se i Google i Facebook s pravom našli na udaru kritika zbog svojih sistema kompjuterskog vida koji crnce označavaju kao majmune.[6] Google je javno nastojao da reši ovaj problem, pri čemu je navodno rešenje bilo da spreči sistem da slici pripiše oznaku „gorila", umesto da se bavi izvornom predrasudom i diskriminacijom ugrađenom u sistem, a koju sistem samo ponavlja.[7] To dalje ukazuje na ozbiljne teškoće u rešavanju takvih problema, koji su izgleda ugrađeni u temelje dizajna sistema mašinskog učenja koje koriste Google i Facebook.

Možda najpoznatiji set slika stvarnih ljudi (uglavnom javnih ličnosti kao što su sportisti, umetnici i političari) jeste baza „Označena lica u prirodi" (Labeled Faces in the Wild, LFW) koju su kreirali istraživači sa Univerziteta Masačusets, a koja sadrži više od 13.000 fotografija prikupljenih sa javnog interneta. Ovaj skup podataka stvoren je s namerom da se prouči problem tehnologije prepoznavanja lica bez postavljenih ograničenja, kao i da se istraživačkoj zajednici pruži više uvida u proces verifikacije lica, što bi istraživačima moglo pomoći da unaprede svoja istraživanja. U kontekstu pristrasnosti skupa podataka, u disklejmeru za ovu bazu se navodi da mnoge grupe, kao što su deca, žene, ljudi stariji od 80 godina ili ljudi određenog etničkog porekla, nisu adekvatno zastupljene.[8]

Primer sintetizovanog skupa podataka je Digi-Face 1M, objavljen 2022. godine, koji sadrži više od milion fotografija povezanih sa oko 110.000 identiteta. Autori tvrde da Digi-Face 1M rešava uobičajene probleme modela treniranih na foto-setovima stvarnih ljudi, kao što su etička pitanja, greške u označavanju i pristrasnost podataka, jer su sintetičke slike kreirane iz visokokvalitetnih skenova glave dobijenih uz saglasnost malog broja ljudi.[9] Međutim, iako tehnički proces izrade ovog skupa podataka možda nije toliko problematičan kao foto-setovi stvarnih ljudi, pristrasnost onih koji sastavljaju takve setove može dovesti do podjednako diskriminatornih ishoda.

Takođe, treba napomenuti da će sistemi koji obrađuju biometrijske podatke pratiti različite korake u zavisnosti od željene funkcije sistema. Konkretno, treba razlikovati biometrijsku verifikaciju i identifikaciju. Kod verifikacije, biometrijski podaci se koriste za potvrdu identiteta osobe na osnovu njenih prethodno sačuvanih autentifikatora (tzv. poređenje 1-prema-1), obično za odobravanje pristupa određenim podacima ili uslugama. Primeri za to su otključavanje mobilnog telefona otiskom prsta ili skeniranjem lica, ili korišćenje pasoša sa biometrijskim čipom za prolazak kroz kapiju elektronske kontrole na aerodromima. S druge strane, biometrijska identifikacija se zasniva na utvrđivanju identiteta jedne ili više osoba poređenjem njihovih podataka sa bazom koja sadrži biometrijske podatke brojnih drugih pojedinaca (tzv. poređenje 1-prema-bezbroj). Te baze podataka mogu biti relativno male (npr. spisak traženih begunaca) ili mogu da obuhvate praktično čitavo stanovništvo, kao što je slučaj sa nacionalnom bazom ličnih karata. Primer biometrijske identifikacije bila bi policijska upotreba sistema za prepoznavanje lica da bi se utvrdilo da li se neka osoba, koju su CCTV kamere snimile na ulici, nalazi na listi osumnjičenih.[10]

Pre nego što podrobnije uđemo u detalje praktičnih implikacija i implementacije, objasnićemo dva ključna matematička i statistička koncepta na kojima se zasniva prepoznavanje lica kompjuterskim vidom. To su analiza glavnih komponenti (PCA) i eigen-vektori.

ULOGA ANALIZE GLAVNIH KOMPONENTI

Koncept izračunavanja proseka i statističke obrade telesnih karakteristika datira iz vremena kada se smatralo da je moguće utvrditi osobine ličnosti – na primer, ko je kriminalac, a ko „normalna“ osoba – na osnovu tipičnih fizičkih odlika, kao što je oblik lica. Tu već zalazimo u domen eugenike, što je izraz koji je skovao Francis Galton, britanski statističar, demograf i etnolog.[11]

Galtonov rad razmatra Lila Lee-Morrison u svojoj knjizi „Portreti automatskog prepoznavanja: kako mašine vide lice“. On je, naime, krajem 19. veka kreirao „kompozitne portrete“ fotografišući mnoštvo ljudskih lica na istoj fotografskoj ploči, sa određenim tačkama poređanim u odnosu na centar lica. Uz pomoć te tehnike, Galton je napravio kompozitne vizuelne predstave ljudi iz različitih društvenih grupa, na primer onih koji su učestvovali u kriminalu, imali određene bolesti ili su bili određenog etničkog porekla, kako bi klasifikovao ljude prema „tipovima“.[12] Ova gruba metoda bila je neosnovana i sa tehničkog i sa naučnog stanovišta, i nametnula je diskriminatorne stereotipe koji proizvode štetu do dana današnjeg, posebno minorizovanoj populaciji.

Danas, velike količine podataka potrebne da bi sistem mašinskog učenja mogao da obavlja svoju funkciju treba da se analiziraju na način koji je logički moguć za mašinu da opaža, obradi i razume. Digitalne slike, u zavisnosti od njihovog kvaliteta i veličine, sastoje se od piksela, najmanjeg elementa koji se može prikazati na digitalnom displeju.[13] Savremene slike visoke definicije mogu da sadrže milione piksela, što – kada se to pomnoži sa hiljadama različitih slikovnih fajlova u nekom skupu podataka – predstavlja ogroman obim podataka za obradu. Međutim, postoji metod za smanjenje složenosti podataka, poznat pod nazivom analiza glavnih komponenti (Principal Component Analysis, PCA).

Kao metod, PCA je u suštini svođenje skupa podataka na konkretne vrednosti kako bi se sačuvalo što više informacija, dok se podaci pojednostavljuju samo na bitne elemente, tako da se mogu lakše analizirati i interpretirati. Kod digitalnih slika, kako objašnjava Lee-Morrison, „PCA tretira svaku sliku lica kao tačku ili vektor na mreži u apstraktnom, visokodimenzionalnom prostoru koji omogućava visok stepen varijacije“. Cilj je da se dobije srednja vrednost iz proseka svakog piksela sadržanog u slikama lica. Imajući to na umu, karakteristike (tj. vrednosti) lica koje odstupaju od srednje vrednosti koriste se za razlikovanje slika, a samim tim i lica različitih ljudi.[14]

Istraživači Lawrence Sirovich i Michael Kirby primenili su PCA na skup od 115 lica studenata Univerziteta Braun koje su fotografisali, kako bi demonstrirali izvodljivost ove procedure. Njihovo istraživanje je objavljeno 1987. Rezultat „prosečnog lica“ predstavljao je mutnu predstavu mladog tamnokosog belca, što nije bilo iznenađujuće s obzirom na homogenost

ulaznih podataka, i biće od ključnog značaja za razumevanje kako mašina trenirana na takvim podacima opaža predstavu „ljudskog lica“.[15]

Sirovich, Kirby: Slika prosečnog lica, 1987.

Ovaj eksperiment pokazuje osnovu za pristrasnost opažanja ugrađenu u sisteme za prepoznavanje lica. Ako je mašinski sistem treniran i testiran da opaža vrlo specifičan tip oblika lica u okviru svog skupa pravila, koji znamo kao njegov „koordinatni sistem“, on će sigurno biti sklon greškama i diskriminatoran u odnosu na lica ljudi sa različitim crtama lica ili bojom kože. Kako su sistemi za prepoznavanje lica često trenirani na belim muškim licima, ljudi izvan zadatih koordinata najčešće su minorizovani i oni koji trpe najveću diskriminaciju u društvu. Na osnovu lažne tvrdnje da je nepogrešiva i superiorna u odnosu na ljude, tehnologija se često nudi kao rešenje za duboko ukorenjene društvene probleme, kao što su kriminal i bezbednosni izazovi. Ovu pogrešnu pretpostavku detaljnije ćemo razmotriti kroz studije slučaja u trećem poglavlju knjige.

Sastavni deo računarskog vida i njegove primene na prepoznavanje lica oslanja se na matematičke objekte koji takođe imaju odgovarajuće vizualizovano stanje – eigen-vektor i, posledično, eigen-lice.

EIGEN-VEKTORI I EIGEN-LICE

Kada slike lica ljudi treba predstaviti tako da mašina može da ih razume, opazi i izvede informacije iz njih, koriste se eigen-vektori kao ključni matematički element. Koncept je skovan spajanjem nemačke reči „eigen“ (što znači vlastiti, svojstven) i vektora kao matematičkog izraza, pa ovi objekti predstavljaju komponente na osnovu kojih mašina može da razaznaje mnoštvo različitih ljudskih lica.[16]

Da bi se kreirali eigen-vektori, na slike u skupu za treniranje treba da se primeni analiza glavnih komponenti (PCA). Lee-Morrison objašnjava da su rezultat toga eigen-vektori koji predstavljaju „najveći stepen mogućeg variranja slika lica“ u odnosu na prosek. Eigen-vektor je „virtualni model ’poznatih’ lica i služi kao referentna tačka za klasifikaciju nepoznatih lica“, opisuje Lee-Morrison.[17] Tako je on od suštinskog značaja za rad sistema za prepoznavanje lica i za treniranje sistema da razume i prepozna bilo koji broj različitih lica, u različitim položajima ili iz različitih uglova, kao i pod raznim spoljašnjim uslovima poput osvetljenja.

Eigen-vektori su apstraktni objekti koji omogućavaju mašinama da vide i razlikuju lica (tj. ljude), ali da bismo bolje razumeli kako oni izgledaju ljudskim bićima, pogledaćemo eigen-lice. Ljudskom oku eigen-vektor izgleda kao zamućena, neodređena pojava u obliku lica, koja ne govori mnogo o konkretnoj osobi – „što je veća varijacija eigen-vektora, eigen-lice izgleda mutnije“.[18] Ili, jednostavno rečeno, što se određena slika čini udaljenijom od „prosečnog“ lica, to će njena digitalna reprezentacija biti mutnija.

Primer seta eigen-lica[19]

Početkom 1990-ih, istraživači sa Masačusetskog instituta za tehnologiju (MIT) Matthew Turk i Alex Pentland radili su na eigen-licima kako bi istražili ovaj metod i njegove primene za prepoznavanje ljudskog lica. Objasnili su kako proces funkcioniše: „Prepoznavanje se vrši projektovanjem nove slike u podprostor koji pokrivaju eigen-lica (’prostor lica’), a zatim kroz klasifikovanje lica poređenjem njegove pozicije u prostoru lica sa pozicijama poznatih pojedinaca.“[20] U kontekstu savremenih sistema za prepoznavanje lica, Turk i Pentland su takođe predvideli da bi njihov pristup mogao da omogući prepoznavanje novih lica korišćenjem neuronskih mreža.[21] Zanimljivo je da su imali u vidu i napore u pravcu prepoznavanja roda i tumačenje izraza lica primenom metode analize eigen-lica.[22]

Iako je eigen-lice samo apstraktni konstrukt, njegov dehumanizovani izgled pokazuje nam da se brisanjem vidljivih razlika na licu identitet ljudskih bića može svesti na matematički postupak. Uz pomoć eigen-lica možemo da razumemo razliku između ljudskog i kompjuterskog vida i od suštinskog je značaja za proces prepoznavanja. Slično Galtonovim kompozitnim portretima, kada se ovi procesi primene u okruženju gde tehno-solucionistički i tehno-deterministički pogledi često utiču na aktere koji imaju ovlašćenja da odlučuju o pitanjima ljudskih prava, nužno se reprodukuju diskriminatorne prakse, posebno kada su u pitanju ljudi u ranjivom društvenom položaju (npr. ljudi u pokretu, zatvorenici).[23]

Napredak u tehnologiji biometrijske identifikacije takođe podstiče praktično eksponencijalni razvoj algoritama mašinskog učenja, koji se hrane podacima i ekstrakcijom znanja za izvršenje zadataka kao što je PCA za kreiranje eigen-vektora. Za uvid u širi kontekst, razmotrićemo neuronske mreže i njihovu primenu u kompjuterskom vidu.

NEURONSKE MREŽE

MAŠINSKO UČENJE I BIOMETRIJA

Razvoj naprednih sistema računarskog vida nije fokusiran samo na treniranje mašine za obavljanje određenog zadatka, već i za autonomno predviđanje i odlučivanje u određenim situacijama. Uloga mašinskog učenja u savremenom društvu često se predstavlja kao nekakva mistična sila koja omogućava razvoj i ekspanziju veštačke inteligencije. Realnije gledište, koje zastupaju Joler i Pasquinelli, upućuje da je mašinsko učenje samo još jedan instrument znanja, poput mnogih drugih koji su razvijeni tokom ljudske istorije. Kako oni ističu, „razumnije je posmatrati mašinsko učenje kao instrument za uvećanje znanja, koji pomaže da se sagledaju karakteristike, obrasci i korelacije u ogromnim prostorima podataka čiji je zahvat izvan ljudskog domašaja“.[24]

Mašinsko učenje zavisi od ogromnih količina podataka, kao i od algoritama koji postaju sve sofisticiraniji kako istraživanja u ovoj oblasti napreduju. U suštini, algoritmi su instrukcije koje definišu procese koje sistem treba da izvrši da bi kreirao izlaz (rezultat) iz podataka koji su mu dati, tj. ulaza (unosa). Algoritmi su stoga ključni instrument moći za one koji ih kreiraju i uspostavljaju pravila po kojima obrađuju podatke. U tom smislu, vredni vlasnički algoritmi (npr. oni koje velike tehnološke kompanije koriste za svoje proizvode kao što su platforme za društveno umrežavanje ili pretraživači) zaštićeni su kao poslovna tajna, što znatno otežava kontrolu nad njihovim radom i eventualnim štetnim efektima – kako ćemo detaljnije izložiti u završnom poglavlju o praksi.[25]

Biometrija se obično opisuje kao „merenje i analiza jedinstvenih fizičkih ili bihejvioralnih karakteristika (kao što su otisci prstiju ili glasovni obrasci), naročito kao sredstvo za proveru ličnog identiteta“.[26] Uz ogroman potencijal biometrije za analizu, statistiku, nadzor, verifikaciju identiteta i druge značajne oblasti istraživanja i razvoja, ne iznenađuje da su biometrijski podaci našli svoje mesto u mašinskom učenju. Kao što je slučaj sa mnogim drugim unosima, ljudske biološke karakteristike mogu se, barem sa tehničkog stanovišta, lako digitizovati i pripremiti u strukturirane skupove podataka za potrebe mašinskog učenja. Lica imaju karakteristične crte, otisci prstiju se sastoje od ispupčenja i udubljenja, dok se za identifikaciju mogu koristiti i tekstura irisa i šare krvnih sudova u mrežnjači.[27]

Korišćenje podataka sa tako velikom varijabilnošću, pa ipak dovoljno specifičnih da se glavne komponente skupa podataka mogu izdvojiti, omogućava sistemu da razaznaje smisao u obrascima. To čini osnovu razumevanja veza između podataka i samostalnog obavljanja naprednijih zadataka.

Na primer, možemo razlikovati klasifikaciju mašinskog učenja i predviđanje mašinskog učenja. Klasifikacija se koristi za prepoznavanje određenog objekta, dodeljivanje oznake i kategorizaciju: „Ulazni fajl (npr. snimak glave snimljen nadzornom kamerom) se unosi u model da utvrdi da li spada u njegovu statističku distribuciju ili ne. Ako je tako, dodeljuje mu se odgovarajuća izlazna oznaka.“[28] Cilj predviđanja mašinskog učenja je, međutim, da predvidi ishode ili ponašanje samo na osnovu dela dostupnih podataka, tj. „koristi se mali uzorak ulaznih podataka (prajmer) za predviđanje dela informacija koji nedostaje, opet u skladu sa statističkom distribucijom modela“.[29]

Ovi scenariji mašinskog učenja mogu se primeniti u raznim okruženjima i društvenim kontekstima, pre svega za biometrijski nadzor ili druge oblike društvene kontrole. Međutim, da bismo razumeli kako sistemi za mašinsko učenje proizvode rezultat na osnovu podataka kojima se hrane, neophodno je da razmotrimo neuronske mreže i njihov dizajn. Konvolucione neuronske mreže su posebno važne za napredne sisteme kompjuterskog vida.

RAZVOJ NEURONSKIH MREŽA

Proces mašinskog učenja koji se naziva duboko učenje, dizajniran je da omogući mašinama da prave veze između informacija kroz slojevitu strukturu međusobno veštački povezanih nodova (ili neurona). To omogućava širok spektar primene neuronskih mreža u mnogim proizvodima i uslugama sa kojima se svakodnevno susrećemo, kao što su kompjuterski vid, prepoznavanje govora, obrada prirodnog jezika ili alati za preporuke.[30]

Međutim, studija sprovedena na MIT-u pokazala je da je oprez neophodan po pitanju poređenja neuronskih mreža sa funkcijama ljudskog mozga u širem kontekstu. Analiza više od 11.000 neuronskih mreža koje su trenirane da simuliraju funkciju ključne komponente moždanog navigacionog sistema,

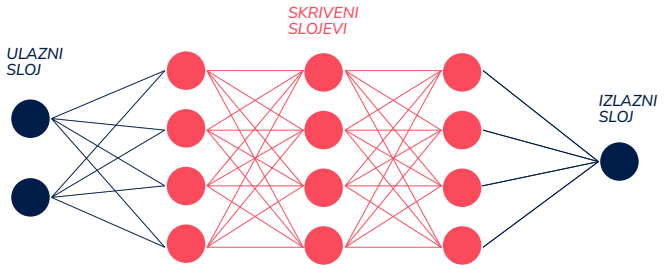
mrežnih ćelija, otkrila je da one proizvode takvu aktivnost samo kada su im data vrlo specifična ograničenja kojih nema u biološkim sistemima.[31]

Kada je reč o strukturi neuronske mreže, postoje dva opšta tipa arhitekture:[32]

» **Jednostavna arhitektura neuronske mreže**, počevši od ulaznog sloja, gde nodovi obrađuju podatke koji ulaze u sistem. Podaci zatim prelaze na skriveni sloj, u kojem nodovi analiziraju podatke iz ulaznog sloja ili drugih skrivenih slojeva, kojih neuronske mreže mogu imati mnogo. Konačno, izlazni sloj daje krajnji rezultat na osnovu obrađenih informacija u celoj mreži. Završni (izlazni) sloj može imati jedan ili više nodova, u zavisnosti od složenosti zadatka. Ako se očekuje binarni rezultat (da/ne, 1/0), onda će izlazni sloj imati samo jedan nod.

» **Arhitektura duboke neuronske mreže** strukturisana je na složeniji način i sastoji se od brojnih skrivenih slojeva sa milionima međusobno povezanih nodova. Relacije između nodova se nazivaju „težine“, a to su vrednosti koje opisuju uticaj nodova na druge nodove, tj. da li prenose podatke na dalje nodove ili ne. Ove mreže obično zahtevaju mnogo veće količine podataka za odgovarajući trening, na primer skupove podataka koji imaju više miliona slika.

Međutim, potrebno je razmotriti i drugu taksonomiju neuronskih mreža, zasnovanu na tome za kakav rad su namenjene i kako podaci teku kroz njih. Za zadatke obrade slike ili klasifikacije, najčešće korišćeni tipovi neuronskih mreža su konvolucione neuronske mreže (Convolutional Neural Networks, CNN).



Uzorak CNN arhitekture[33]

U okviru CNN-a postoje tri tipična sloja koja treba da objasnimo – konvolucioni sloj, sloj sažimanja (pooling layer) i potpuno povezani sloj.

Konvolucioni sloj je ključni deo CNN-a,[34] gde se odvija veći deo komputacije. Sastoji se od tri komponente: ulaznih podataka, filtera (ili kernela) i mape obeležja. Ulazni podaci mogu, na primer, biti slika u boji sačinjena od piksela u tri dimenzije: visina, širina i dubina u RGB-u (kombinacija vrednosti crvene, zelene i plave da bi se dobio veliki izbor različitih boja).[35]

Filter je detektor obeležja, koji se zasniva na dvodimenzionalnoj ili trodimenzionalnoj matrici sa određenim vrednostima (koje odgovaraju trima dimenzijama ulaza) i koristi se za izvođenje konvolucije – matematičke operacije za spajanje dva skupa informacija. Filter se kreće preko slike deo po deo i umnožava vrednosti piksela koje pronađe sa matricom, upisujući rezultat koji dobije u mapu obeležja. Pošto u CNN-u postoji više filtera, svaki od njih proizvodi različito obeležje. Zatim se slažu jedni na druge da bi se proizveo izlazni sloj. Proces se ponavlja za svaki konvolucijski sloj u mreži.[36]

Unutar sloja sažimanja, unos prolazi kroz sličan proces filtriranja kao u konvolucionom sloju. Razlika je, međutim, u tome što se sažimanje koristi za smanjenje ulaznih parametara za rukovanje kompresovanim informacijama.[37] Da bi se to postiglo, uz filter se primenjuje funkcija agregacije za svaki deo slike, koja može biti ili maksimalno sažimanje (za izlaz se izdvaja samo piksel sa maksimalnom vrednošću) ili prosečno sažimanje (za izlaz se izdvaja srednja vrednost piksela). Proces kreira sažete verzije filtriranih mapa obeležja koje pružaju stabilnost CNN-u, obezbeđujući pravilan rad čak i kada postoje male fluktuacije.[38] Na kraju, potpuno povezani sloj vrši konačnu klasifikaciju slike na osnovu rezultata koje dobija od prethodnih slojeva.[39]

Procesi dubokog učenja koji se neprestano odvijaju u današnjem informacionom okruženju zahtevaju ne samo posedovanje ogromne količine podataka za treniranje, već i veoma naprednu tehničku infrastrukturu na kojoj se testiraju i primenjuju neuronske mreže, kao i ljudske resurse u smislu naučno-istraživačke ekspertize. Kada je reč o neophodnim sredstvima, podrazumeva se da većinu ovih procesa kontroliše mala grupa moćnih privatnih aktera, kao što su Google[40] i Microsoft.[41]

Ovi moćni alati, koje pokreću informacije o našem svetu i o nama kao ljudskim bićima, koriste se za kompresiju informacija, odnosno kao sredstvo

za izvlačenje što više informacija i znanja u najmanjem broju koraka, koristeći najmanju količinu resursa (npr. minimizacija procesorske moći računara ili radnih sati ljudi).[42] U kontekstu policije i istrage kriminala, naporan proces ručnog pregledanja na hiljade sati snimaka sa video-nadzora – uz pomoć ekrana i tastature – koji sprovode policajci i analitičari, ne može se porediti sa kapacitetima veštačke inteligencije. Kako se navodi u jednom tekstu na sajtu Svetskog ekonomskog foruma, „mašine ne pate od monotonije ili zamora“.[43]

U postupku otkrivanja lokacije osumnjičenog za zločin ili utvrđivanja ko bi mogao da predstavlja potencijalnu pretnju po javnu bezbednost, pametni sistemi nadzora bi policijskim službenicima mogli izgledati kao savršeno sredstvo za ostvarenje maksimalne efikasnosti. Ovaj utilitaristički, resursno efikasan pristup rešavanju komplikovanih društvenih problema primenjuje mašinski tumačenu društvenu redukciju koja ne garantuje savršeno bezbedno društvo lišeno kriminala. S druge strane, čitavu zajednicu dovodi u stanje trajno smanjenog nivoa ljudskih prava.

Shodno tome, finansijski interesi programera često su usklađeni sa političkim interesima u pogledu zamišljene efikasnosti. To je dovelo do rasprostranjenog usvajanja infrastrukture za poduhvate „bezbednog/pametnog grada“ ili sličnih digitizovanih projekata javnog nadzora širom sveta. Takvi poduhvati zahtevaju javne nabavke za kupovinu, instaliranje i održavanje opreme neophodne za rad „pametnog“ nadzora. Oprema se obično sastoji od različitih uređaja, kao što su razne vrste kamera (npr. montirane na stub, na vozilo, za nošenje na telu itd.), ručni uređaji nalik pametnom telefonu, kao i jedinice za skladištenje i obradu podataka, na kojima čitav sistem radi iza kulisa.[44] Pogledajmo sada detaljnije osnovne komponente takvih sistema, neke od ključnih dobavljača i kapacitete njihovih proizvoda.

TEHNOLOGIJA

INFRASTRUKTURA I REŠENJA

KAPACITETI I POTENCIJALI PROIZVODA ZA PREPOZNAVANJE LICA

ELEMENTI I DIZAJN SISTEMA ZA PREPOZNAVANJE LICA

Prema agenciji Deloitte, očekuje se da će do 2025. globalno tržište tehnologija za prepoznavanje lica vredeti oko 8,5 milijardi američkih dolara, što je značajan porast u odnosu na 3,8 milijardi zabeleženih 2020.[45] Već je i samo mnoštvo nadzornih kamera koje su instalirali i javni i privatni subjekti u toj meri normalizovalo nadzor da mnogi ljudi danas dobrovoljno opremaju svoje domove nadzornim sistemima, verujući da će ih to zaštititi. U paradoksalnom zaokretu, to može dovesti do povećanog kršenja privatnosti i bezbednosti, kao što je pokazao nedavni zahtev ransomver napada preko

Amazonovih Ring kamera.[46] Dodatni problemi privatnosti i pristupa podacima proizlaze iz činjenice da Amazon u navodno „hitnim slučajevima" pruža američkim organima za sprovođenje zakona direktan pristup Ring kamerama bez naloga, a da većina njihovih korisnika toga nije svesna.[47]

Savremeni sistemi nadzora, posebno oni koji se koriste za nadzor javnih prostora, zahtevaju tehničku infrastrukturu koja je samo delimično vidljiva osobama koje su pod nadzorom. Uočljivi elementi obuhvataju različite vrste uličnih kamera, senzore i druge krajnje uređaje koji su instalirani ili se koriste javno, kao što su mobilni ručni terminali. Međutim, njihova vidljivost je često prigušena urbanim dizajnom ili prostom društvenom normalizacijom. Potpuno nevidljivi elementi, od kritičnog značaja za rad sistema, jesu različiti uređaji za obradu i skladištenje podataka sa naprednim analitičkim mogućnostima koji su skriveni od javnog pogleda. Ovi nevidljivi elementi dodatno učvršćuju neravnotežu moći između „posmatrača" i „posmatranih".

Dronovi su dobar primer zašto uređaji koji snimaju lica ili druge ulazne podatke izazivaju toliku zabrinutost. Kako objašnjavaju u Informacionom centru za elektronsku privatnost (Electronic Privacy Information Center, EPIC), dronovi predstavljaju pretnju po privatnost usled nekoliko faktora: u velikoj meri smanjuju troškove nadzora, olakšavaju upravljanje vazdušnim nadzorom i mogu se opremiti raznim dodacima kao što su kamere visoke rezolucije, termalni senzori ili detektori pokreta. Takođe, kada je reč o nadzoru iz vazduha, bar u SAD, zaštita privatnosti nije dovoljno regulisana.[48]

Iako se dronovi ponekad mogu videti u vazduhu, povremeno su ljudima potpuno nevidljivi, posebno ako lete na velikim visinama. Umetničko delo Trevora Paglena „Bez naziva (dron kosač)" pokazuje upravo to – dron nije ništa drugo do jedva vidljiva, sićušna tačka na fotografiji svetlog neba, koja kreće iz američke vojne baze da bi ispunila svoju misiju negde na drugom kraju sveta.[49]

Tehnička aparatura za biometrijski nadzor najviše je vidljiva u svom krajnjem sloju; na primer, CCTV kamere koje ljudi mogu da vide na otvorenom (trg, raskrsnica, okolina važne zgrade) ili u zatvorenom prostoru kao što je aerodrom ili metro stanica. Prilikom dizajniranja sistema za nadzor, međutim, potrebno je mnogo više od instaliranja kamera na određenim mestima – pažljivo planiranje, povezivanje, skladištenje i drugi pomoćni resursi su jednako važni. Obično postoji nekoliko ključnih elemenata sistema video nadzora:[50]

- **Kamere**: dostupno je mnoštvo različitih tipova na osnovu mobilnosti (tj. da li su fiksne ili prenosive), vrste izlaznih slika (npr. u boji ili crno-bele), rezolucije (standardna ili visoka definicija) ili tipa signala, koji može biti zasnovan na internet protokolu (IP) ili analogan (stariji modeli).

- **Veza**: kao i tipovi signala, veze sa sistemom mogu biti analogne, ali preovlađujući tip koji se koristi za savremene sisteme nadzora zasnovan je na IP-u. Drugim rečima, video izlaz se može poslati preko bežične mreže ili kablovima, u zavisnosti od slučaja upotrebe i infrastrukture.

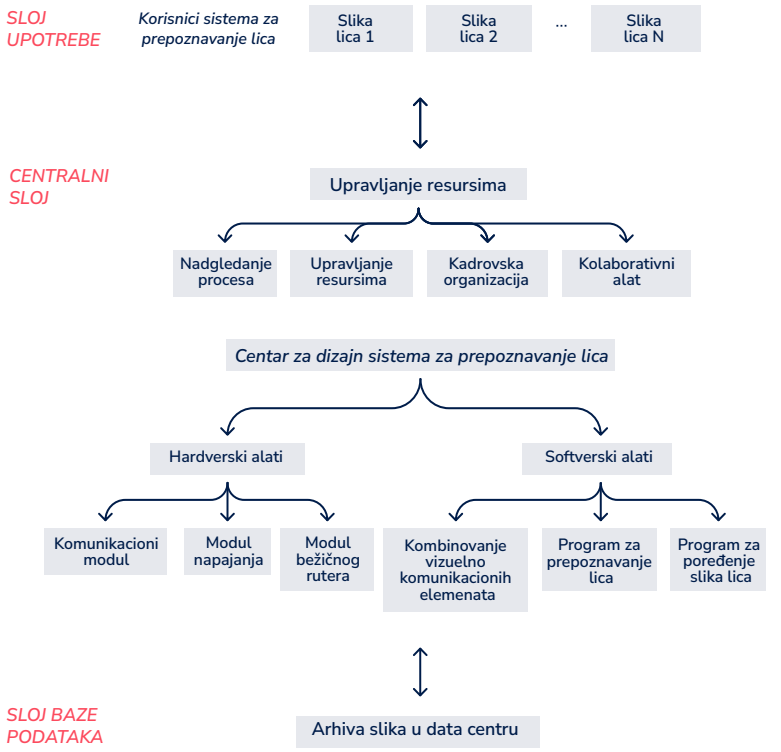
- **Video upravljanje i skladištenje**: uređaji kao što su digitalni video rekorderi (DVR), mrežni video rekorderi (NVR) ili računari/serveri sa instaliranim odgovarajućim softverom za upravljanje video zapisima (VMS) koriste se za upravljanje i skladištenje snimljenog videa. Takođe postoji nekoliko opcija za skladištenje: interno, unutar uređaja za upravljanje video zapisima, eksterne memorijske jedinice (npr. hard-diskovi), umreženo skladištenje (npr. cloud rešenja) ili ugrađena memorija na kamerama pomoću SD kartica.

- **Video analitika**: softverska rešenja koja pružaju brojne opcije za izvlačenje maksimuma informacija iz video zapisa, u rasponu od identifikacije neovlašćenog ulaska u zonu, brojanja ljudi, do prepoznavanja registarskih tablica vozila ili prepoznavanja lica.

- **Uređaji za gledanje**: video se može gledati na licu mesta direktno sa uređaja za upravljanje, daljinski sa sistema povezanog uređaj (računar, mobilni telefon) ili na video-zidu, što je tipično za najsavremenije analitičke centre, gde analitičari mogu istovremeno da gledaju video sa više stotina ili čak hiljada sigurnosnih kamera.

Međutim, ovo nije jedini način na koji se može razmišljati o komponentama sistema za prepoznavanje lica. Ispitujući dizajn sistema za prepoznavanje lica kao logički okvir, Xuhui Fu deli njegovu arhitekturu na tri sloja: sloj upotrebe, centralni sloj i sloj baze podataka. Upotrebni sloj se koristi za slanje instrukcija sistemu prema potrebama osobe koja njime upravlja, npr. za traženje podudaranja određenog lica. Uloga centralnog sloja je da izvrši proces prepoznavanja i vrati informacije korisničkom sloju, dok se sloj baze podataka koristi za prikupljanje informacija o slici lica i pružanje podataka

koji su sistemu potrebni za prepoznavanje lica.[51] Fu je ovu arhitekturu predstavio kao dijagram:



X. Fu: Dijagram arhitekture sistema za prepoznavanje lica[52]

Očigledno, presudni koraci za prepoznavanje lica se javljaju u elementima upravljanja video snimkom i analitike. CCTV sistemi iz prošlosti, sa starim analognim kamerama koje su snimale zrnast crno-beli video niske rezolucije, nisu bili zahtevni u pogledu tehničke infrastrukture i podešavanja, ali su ipak negativno uticali na ljudska prava. Sa današnjim karakteristikama sistema zasnovanih na IP-u – kamerama koje mogu da snimaju video visoke definicije čak i u uslovima lošeg osvetljenja, ogromnim resursima za skladištenje i naprednim softverom i hardverom za analitiku – kapacitet za biometrijski masovni nadzor podiže ulog na mnogo viši nivo.

Pošto su odobreni, instalirani i testirani u određenom kontekstu ili okruženju, sisteme nadzora je veoma teško ukloniti. Primer za to je upotreba prepoznavanja lica u Moskvi, koja je prošla kroz navodno eksperimentalnu fazu tokom Svetskog prvenstva u fudbalu 2018. Sličan scenario se može očekivati u Francuskoj, gde je nacionalni parlament u martu 2023. usvojio zakon koji dozvoljava upotrebu nadzora sa veštačkom inteligencijom za navodno veću javnu bezbednost tokom Olimpijskih i Paraolimpijskih igara u Parizu 2024, odobravajući eksperimente na javnim događajima uoči Igara.[53] Zakon je trebalo da važi do kraja marta 2025, ali je novi premijer Francuske Mišel Barnije u oktobru 2024. otvorio mogućnost da se eksperimentalne mere generalizuju.[54]

Fleksibilnost dizajna i raznovrsnost dostupnih proizvoda i usluga čini implementaciju pametnog sistema video nadzora relativno lakom za aktere koji poseduju finansijske, tehničke i druge resurse, kao što su državni organi.

GLAVNI PRODAVCI I PROIZVODI

Veoma unosno globalno tržište tehnologija za prepoznavanje lica podstiče stalni razvoj novih proizvoda i usluga mnoštva kompanija iz različitih delova sveta. Međutim, u aktuelnoj postavci, samo nekoliko dobavljača ove tehnologije zauzima moćne pozicije.

Istaknuto mesto drži Huawei, tehnološki gigant koji se poslednjih godina nalazi na udaru kritika zbog svojih veza sa kineskom vladom i navodnog učešća u špijunaži više država na globalnom zapadu.[55] Ova kompanija je bila jedan od glavnih aktera kineske tehnološke ekspanzije u zemljama u razvoju, posebno u Africi i Latinskoj Americi,[56] što joj je omogućilo da preuzme značajnu ulogu u geopolitičkom i diplomatskom sukobu Kine sa SAD i saveznicima.

Iz širokog spektra Huawei proizvoda, kada je u pitanju veštačka inteligencija, posebno se ističe procesor Ascend 910, lansiran 2019, koji se reklamira kao „najmoćniji AI procesor na svetu“.[57] Ovi procesori su instalirani u naprednim Huawei hardverskim proizvodima fokusiranim na veštačku inteligenciju, kao što je „Atlas 900 PoD AI cluster basic unit“, na čijoj veb stranici stoji da se koristi za „scenarija u razvoju i treniranju modela dubokog učenja“ i predstavlja se kao „idealna opcija za računarski intenzivne industrije, kao što su pametni grad, inteligentna zdravstvena zaštita, astronomska istraživanja i istraživanja nalazišta nafte“.[58]

Huawei takođe nudi „Atlas 900 AI Cluster“, složeniji proizvod koji se sastoji od više hiljada Ascend 910 procesora, a za koji se tvrdi da ima računarsku snagu ekvivalentnu snazi 500.000 desktop računara, i u stanju je da za 60 sekundi sprovede treniranje modela zasnovanog na ResNet-50.[59] ResNet-50 (Residual Network) je tip konvolucione neuronske mreže (CNN) sa 50 slojeva koju je razvila grupa istraživača 2015.[60] S obzirom na to da učinak ovog proizvoda na CNN-u kompanija Huawei predstavlja kao prednost pri kupovini, može se pretpostaviti da je proizvod pripremljen za razvoj rešenja kompjuterskog vida, kao što je prepoznavanje lica.

Ova kompanija je takođe bila ključni igrač na tržištu „bezbednog grada“, što je kombinacija navodne urbane infrastrukture javne bezbednosti i hardverskih/softverskih proizvoda sa naprednim („pametnim“) kapacitetima. Istraživači iz Centra za strateške i međunarodne studije (Center for Strategic and International Studies, CSIS) otkrili su da ponuda „bezbednog grada“ obično pokriva širok spektar proizvoda i usluga kao što su komandni centri, CCTV kamere, inteligentni video nadzor, tehnologija prepoznavanja lica i registarskih tablica vozila, i praćenje masa. Prema nalazima CSIS-a, zajednička karakteristika tržišta na kojima se obično sklapaju sporazumi sa Huawei o bezbednom gradu jeste da su to neliberalne zemlje sa srednjim prihodima u Aziji i Africi.[61] Na svojoj veb stranici, kineski tehnološki gigant takođe opisuje šta njegovi proizvodi za pametne gradove nude: „...tehnologija inteligentnog prepoznavanja ugrađena u same kamere, sa kapacitetima za prepoznavanje lica svih snimljenih i analizu specifičnog ponašanja radi prevencije kriminala u realnom vremenu.“[62]

U Beogradu, glavnom gradu Srbije, zemlje Zapadnog Balkana koja vodi pregovore o pristupanju Evropskoj uniji, pokrenut je jedan od Huawei projekata „bezbednog grada“. Jedna studija slučaja Huawei rešenja u Beogradu otkrila je „probnu vožnju“ Ministarstva unutrašnjih poslova Srbije. Međutim, stranica je skinuta sa sajta kompanije[63] ubrzo pošto je SHARE fondacija, neprofitna organizacija za digitalna prava sa sedištem u Srbiji, objavila analizu studije slučaja koja je pružila više detalja o najavljenom sistemu pametnog video nadzora u Beogradu.[64] Huawei je tvrdio da je testna mreža „uspešno verifikovala više ključnih funkcija, kao što su pronalaženje video zapisa, kompresija video zapisa, automatsko prepoznavanje registarskih tablica, analiza ponašanja, prepoznavanje lica i dijagnostika kvaliteta videa“ na zadovoljstvo službenika Ministarstva unutrašnjih poslova. U studiji slučaja se takođe pominje OceanStor, vrhunski uređaj za skladištenje sa kapacitetima skladištenja podataka iz analize video sadržaja do jedne godine.[65] Ovaj slučaj će biti detaljnije izložen u odeljku „Orvelovska nacionalna bezbednost“ u trećem poglavlju o praksama.

Još jedan azijski proizvođač tehnologije za prepoznavanje lica vredan pomena je NEC, japanski elektronski gigant koji nudi širok spektar proizvoda. Kompanija se ponosi svojom tehnologijom za prepoznavanje lica koja ubedljivo vodi na testovima dobavljača za procenu tehnoloških kapaciteta i standarda američkog Nacionalnog instituta za standarde i tehnologiju (NIST).[66]

Kompanija je u aprilu 2019. objavila svoje principe veštačke inteligencije i ljudskih prava, sa ciljem da „dodatno ojača napore NEC-a da demonstrira poštovanje privatnosti i ljudskih prava u vezi sa primenom i korišćenjem AI i biometrijskih podataka u svim preduzećima“.[67] NEC je usvojio sledeće principe: pravičnost, privatnost, transparentnost, odgovornost za objašnjenje, pravilno korišćenje, AI i razvoj talenata i dijalog sa više zainteresovanih strana.[68] S obzirom na ulogu NEC-a u razvoju i prodaji proizvoda za biometrijski nadzor, usvajanje takvih principa može biti dobar korak u pogledu korporativnog upravljanja. Mada takve politike mogu biti od pomoći za interne svrhe, one su ipak vođene i osmišljene u skladu sa komercijalnim interesima i ne mogu služiti kao zamena temeljnoj zakonskoj regulativi. To je posebno važno imajući u vidu povezanost tehnologije biometrijskog nadzora sa ozbiljnim rizicima za ljudska prava, kojima se principi NEC-a ne bave.

NEC snabdeva nekoliko država članica EU tehnologijom biometrijskog nadzora. Prema izveštaju grupe Zeleni/EFA u Evropskom parlamentu iz 2021. godine, tehnologiju biometrijskog nadzora kompanije NEC nabavile su vlasti u Rumuniji, Mađarskoj, Italiji, Portugalu i Litvaniji.[69] Van Evrope, u martu 2022. objavljeno je da je Brunej, mala južnoazijska država dobila NEC-ov proizvod za prepoznavanje lica NeoFace Watch, koji je instaliran na brunejskom međunarodnom aerodromu. To je bila besplatna donacija vlade Japana, data preko Kancelarije Ujedinjenih nacija za droge i kriminal (United Nations Office on Drugs and Crime, UNODC). O instaliranju ovih sistema za prepoznavanje lica u Bruneju prvo se razgovaralo sa japanskim ambasadorom 2019.[70] Širenje NEC proizvoda na tržišta kao što je EU donekle je predvidljivo, pošto je Japan dugogodišnji politički i vojni saveznik zemalja zapadne Evrope i severne Amerike, posebno SAD. Istovremeno, njegovo uporište u južnoj Aziji iz primera Bruneja može se tumačiti kao stvar regionalne tehnološke diplomatije.

Jedan od NEC-ovih proizvoda za prepoznavanje lica, NeoFace Watch, funkcioniše tako što „integriše tehnologiju uparivanja lica sa inputima video analitike“.[71] To je aplikacija zasnovana na vebu koja je prilagodljiva, može se integrisati u postojeća bezbednosna rešenja i ima mogućnost da obrađuje i živi i arhivirani video materijal (za prepoznavanje lica uživo i naknadno).[72] U marketinškim tekstovima kompanije takođe se navodi da se NeoFace Watch može koristiti kao fleksibilno rešenje za prepoznavanje lica na stadionima, salama i u javnom prevozu.[73]

Od nekoliko velikih američkih korporacija na tržištu biometrijskog nadzora, počećemo sa Amazonom. Njegov najpoznatiji proizvod verovatno je platforma za e-trgovinu Amazon.com, ali je tokom godina Amazon proširio svoj portfolio usluga i postao veoma uticajan provajder infrastrukture oblaka sa Amazonovim veb servisima (Amazon Web Services, AWS). Na primer, jedan od njihovih prvih data centara (zgrade u kojima se nalaze serveri i prateća oprema), otvoren 2006, na koji se značajno oslanjaju internet servisi širom sveta, nalazi se u američkoj državi Virdžinija. Kako primećuje Ingrid Burrington: „Pre nego što sam saznala da je severna Virdžinija srce interneta, znala sam je kao špijunsku zemlju – to jest, dom za plejadu obaveštajnih agencija i raznih preduzetnika u odbrambenoj industriji“, što izgleda nije slučajnost.[74] U aprilu 2023. AWS je nudio raznovrstan spektar data centara i infrastrukturnih lokacija za svoje usluge, na više od 30 geografskih regiona, koji opslužuju preko 200 zemalja i teritorija, pokrivajući praktično čitav svet.[75]

Kao raznovrsna platforma za skladištenje u oblaku, AWS nudi svojim klijentima mogućnost korišćenja Amazon Rekognition, napredne usluge kompjuterskog vida. S obzirom na činjenicu da radi na AWS-u, Amazon Rekognition se može primeniti kao veoma zgodno rešenje za prepoznavanje lica i integrisati sa postojećom infrastrukturom za nadzor (npr. CCTV sistem). U izveštaju Washington Posta iz 2019. godine opisuje se kako je lokalna policija u Oregonu počela da koristi Amazon Rekognition u svojim istragama: „Skoro preko noći, policajcima su višestruko uvećani kapaciteti za istrage, pa su mogli da pretražuju lice osumnjičenog na preko 300.000 fotografija iz okružnog zatvora snimljenih od 2001.“[76] Amazon je 2020. objavio da uvodi jednogodišnji moratorijum na policijsku upotrebu alata Rekognition, nakon afera nezakonitog hapšenja crnaca.[77] U maju 2021. kompanija je potvrdila da će produžiti policijski moratorijum za Rekognition do daljnjeg.[78] Međutim, nema javno dostupnih informacija o odlukama koje su donete kao rezultat ovog poteza, što dovodi u pitanje njegov kredibilitet.

Amazon Rekognition je u stanju da analizira slike i video za identifikaciju objekata, ljudi, teksta, scena i aktivnosti, kao i da filtrira navodno neprikladan sadržaj.[79] Postoje dva Amazon Rekognition aplikacijska programska interfejsa (API), tj. skupa pravila koji se koriste da bi se različitim aplikacijama omogućilo da međusobno komuniciraju.[80] Dva API-ja su Amazon Rekognition Image, koji se koristi za analizu slika, i Amazon Rekognition Video za video analizu.[81] To u suštini znači da svako može da razvije aplikaciju za svoje svrhe i da je integriše sa Rekognition servisom preko odgovarajućeg API-ja kako bi koristio opcije koje servis pruža.

U kontekstu tehnologije biometrijskog nadzora vredi razmotriti još jednu kompaniju sa sedištem u SAD, Microsoft. Kao stari tehnološki gigant, Microsoft je aktivno uključen u istraživanje i razvoj AI, kao i u ažuriranje svog korporativnog upravljanja. U decembru 2018, kompanija je objavila šest principa koji će voditi njen razvoj i primenu tehnologije prepoznavanja lica. To su pravičnost, transparentnost, odgovornost, nediskriminacija, obaveštenje i saglasnost, i zakoniti nadzor.[82]

Slično Amazonu, Microsoft nudi naprednu platformu za računarstvo u oblaku pod nazivom Microsoft Azure, sa više od 200 proizvoda i usluga koji se koriste za izgradnju, rad i upravljanje aplikacijama. Kompanija tvrdi da 95 odsto kompanija sa liste Fortune 500 koristi Azure i da platforma može da pokrije potrebe različitih sektora, od javne uprave, zdravstvene zaštite, maloprodaje i finansijskih usluga do proizvodnje.[83]

Jedna od usluga koje se nude u okviru ovog portfolija zove se Azure Face i „stavlja na raspolaganje AI algoritme koji otkrivaju, prepoznaju i analiziraju ljudska lica na slikama“.[84] Kao proizvod zasnovan na klaud tehnologiji, Azure Face je veoma sličan Amazon Rekognitionu u smislu povezivanja Microsoftovih klijenata s njim, preko različitih API-ja na osnovu nameravane primene proizvoda. Među opcijama koje Microsoft izdvaja na stranici sa opisom usluge Azure Face nalaze se prepoznavanje i analiza lica, verifikacija identiteta, pronalaženje sličnih lica, kao i opcija „grupe lica“ (tj. izdvajanje manje grupe sličnih lica iz skupa nepoznatih lica).[85]

Poslednjih godina, Microsoft nastoji da demonstrira oprez kada je u pitanju korišćenje proizvoda i usluga zasnovanih na veštačkoj inteligenciji, posebno onih asociranih sa visokim rizicima po ljudska prava. Na stranici sa opisom

usluge Azure Face nalazi se upozorenje da od 11. juna 2020. Microsoft ne prodaje tehnologiju za prepoznavanje lica američkim policijskim snagama i da to neće činiti sve dok se ne donese snažna regulativa zasnovana na ljudskim pravima za upotrebu takve tehnologije – mada, kao i u slučaju Amazona, nije bilo javnog objašnjenja šta to znači u praksi. Pretpostavlja se da kompanija namerava da nastavi da prodaje tehnologiju za prepoznavanje lica američkoj policiji u nekom trenutku u budućnosti.

U junu 2022. Microsoft je predstavio svoj okvir za izgradnju AI sistema na način koji kompanija smatra prihvatljivim: Standard odgovorne veštačke inteligencije. U zvaničnom saopštenju, kompanija je tvrdila da ograničava pristup uslugama prepoznavanja lica na uski skup kupaca („managed partners“), propisujući ono što smatra prihvatljivim slučajevima primene. Na primer, posebno se ističe da će Microsoft za Azure Face ukinuti kapacitete koji izvode emocionalna stanja ljudi i atribute identiteta kao što su uzrast, rod, osmeh, lice ili kosa.[86]

Još jedno Microsoftovo saopštenje u kom se detaljno opisuju planovi za odgovornu AI, takođe iz juna 2022, izričito uvodi obavezu novih klijenata da se prijave za pristup operacijama prepoznavanja lica u proizvodima Azure Face API, Computer Vision i Video Indexer. Postojećim Microsoftovim klijentima dat je rok od godinu dana (koji je istekao 30. juna 2023. godine) da se prijave za pristup i dobiju odobrenje kako bi mogli da nastave da koriste ove usluge. S druge strane, kapaciteti za detekciju lica – prepoznaju lice, ali ne pripisuju određeni identitet – ostaju dostupni.[87] Mada može izgledati da su ovo pozitivni koraci, to jednoj privatnoj kompaniji praktično daje proizvoljno ovlašćenje da otvara, odnosno sprečava pristup korišćenju kontroverzne tehnologije, uprkos njenim ogromnim posledicama po društvo.

Da bi pojasnio šta predstavlja prihvatljivu upotrebu sa dopuštenim (tj. ograničenim) pristupom, Microsoft je izložio slučajeve upotrebe Azure Face u privatnom i u javnom sektoru. Odobrena komercijalna upotreba „ograničenog pristupa“ uključuje „verifikaciju ljudskog lica za verifikaciju identiteta radi omogućavanja pristupa digitalnim ili fizičkim uslugama ili prostorima“, „identifikaciju ljudskog lica za kontrolu pristupa bez dodira“, „identifikaciju ljudskog lica za personalizaciju“ i „identifikaciju ljudskog lica za otkrivanje dupliranih ili blokiranih korisnika“.[88] Poređenja radi, holandska služba za zaštitu podataka je 2019. upozorila da bi, prema zakonu EU o zaštiti podataka, korišćenje identifikacije ljudskog lica za kontrolu pristupa za bilo

šta što je manje ozbiljno od obezbeđenja nuklearne elektrane, predstavljalo neopravdano narušavanje prava na zaštitu podataka.[89]

Kada je reč o sprovođenju zakona i krivičnom postupku, Microsoft definiše dopuštenu upotrebu uglavnom za identifikaciju, kao što su one koje se odnose na „progon ili odbranu za krivično delo osumnjičenog koji je već uhapšen, u meri u kojoj su to posebno odobrili propisno ovlašćeni državni organi u jurisdikciji u kojoj postoji pravično i nezavisno sudstvo“ ili na pomoć u procesuiranju kršenja međunarodnog prava. Dodatne navedene svrhe su reagovanje u vanrednim situacijama koje predstavljaju neposredan rizik od smrti ili teških telesnih povreda, pružanje humanitarne pomoći, identifikacija nestalih ili umrlih osoba ili žrtava kriminala.[90]

Microsoft je takođe objavio dodatna razmatranja o prihvatljivoj upotrebi servisa Azure Face, gde se napominje da politika kompanije globalno zabranjuje korišćenje tehnologije za prepoznavanje lica uživo na mobilnim kamerama, kao što su kamere koje se nose na telu ili na kontrolnoj tabli vozila, u pokušaju identifikacije ljudi – ali ne i njegove retrospektivne upotrebe, uprkos jednakom potencijalu štete. Kompanija takođe pruža uputstva klijentima o tehničkim elementima korišćenja usluge u javnim prostorima.[91]

Mada se čini da kompanije poput Microsofta i Amazona ozbiljno shvataju svoju posvećenost dužnoj pažnji i ljudskim pravima, važno je zadržati oprez u pogledu njihovih tvrdnji. Upotreba biometrijskih sistema u pružanju humanitarne pomoći, na primer, kritikuje se kao jedna od najprisilnijih i najopasnijih primena, što ljude u ionako ranjivom položaju dovodi u još veći rizik od povrede prava.[92] Upotreba za identifikaciju osumnjičenih za zločin lako može biti izgovor za legalizaciju široko rasprostranjenog nadzora, kako je već upozorio najviši regulator EU za zaštitu podataka.[93]

Postoji i šire pitanje podobnosti korporativne samoregulacije. Oslanjajući se na principe i ograničenja koje su osmislile privatne kompanije, upotreba biometrijskih tehnologija je po definiciji vezana za njihove interese – umesto da je vođena demokratskim pravima i principima. To ovim komercijalnim subjektima omogućava da određuju da li će i kako državni organi poput policije ili pravosuđa koristiti tehnologiju, što im daje ogromnu polugu moći. Takođe stvara lažan utisak da državna regulativa nije potrebna, jer su se kompanije same pozabavile svim problemima.

Za kraj ovog odeljka, Evropsku uniju predstavlja Thales Group. Sa sedištem u Francuskoj, Thales pruža proizvode i usluge za široki spektar industrija, uključujući vazduhoplovstvo, odbranu i bezbednost, digitalni identitet i bezbednost, zemaljski transport i svemir.[94] Kompanija je fokusirana na biometrijsku tehnologiju i rešenja, pokrivajući uobičajene vrste biometrije, tj. otiske prstiju, prepoznavanje lica i irisa. Kompanija tvrdi da je do aprila 2023. izvršila više od 200 implementacija u 80 zemalja.[95] U dokumentu o dizajniranju etičkog, društveno odgovornog sistema za prepoznavanje lica, Thales tvrdi da svoja rešenja dizajnira u skladu sa etičkim pravilima, a to su poverljivost i saglasnost, transparentnost, preciznost i pouzdanost, bezbednost, etičnost i zakonska usklađenost, te odgovornost.[96] I ovde važe isti problemi koje smo razmotrili u vezi sa Microsoftom i Amazonom.

Thalesova platforma za prepoznavanje lica (Facial Recognition Platform, FRP) opisana je kao napredno rešenje koje koristi „algoritam svetske klase zasnovan na dubokim neuronskim mrežama“ za detekciju, praćenje i prepoznavanje ljudskih lica. Jedna od karakteristika koje kompanija ističe jeste da se FRP može integrisati sa različitim rešenjima nezavisnih proizvođača, kao što su upravljanje granicama, video nadzor, kontrola pristupa itd. Aplikacije zasnovane na FRP takođe se mogu izgraditi korišćenjem API-ja ili razviti kao samostalni softver. FRP je pogodan za više platformi i okruženja i može se primeniti na računaru, oblaku ili mobilnom uređaju.[97] Značajno je da su mnogi slučajevi upotrebe koje Thales navodi bili predmet intenzivnog preispitivanja u Evropi, gde su grupe civilnog društva tražile zabranu korišćenja sistema za prepoznavanje lica i veštačke inteligencije, između ostalog, za identifikaciju na javnim mestima i u upravljanju granicama.[98]

Za ovaj softverski proizvod specifično je i to što sadrži nekoliko modula, od kojih je svaki prilagođen konkretnom scenariju biometrijskog nadzora. Na primer, Thales kaže da se FRP Watch može koristiti za identifikaciju pojedinaca u video strimovima uživo, koji dolaze sa stotina kamera paralelno kroz sistem za upravljanje video zapisima. FRP Search Expert je namenjen za forenzičke istrage usmerene na pronalaženje pojedinaca iz baza fotografija ili video zapisa sa naprednim funkcijama za editovanje, dok FRP Mobile omogućava kapacitete prepoznavanja lica za Android uređaje. Pored toga, na raspolaganju je i FRP Software Development Kit (SDK) koji kupci mogu koristiti za razvoj sopstvenih samostalnih aplikacija sa funkcijom prepoznavanja lica koje mogu da rade i sa fotografijama i sa video materijalom.[99]

Napredna i razuđena priroda tržišta tehnologija za prepoznavanje lica znači da će, na primer, u slučaju da jedan određeni dobavljač ili tehnološki proizvod nije dostupan organima za sprovođenje zakona, oni moći da dobiju druge slične proizvode čiji dobavljač ne odbija uslugu. Neki napredni alati, poput onih koje nudi Clearview AI, čak se reklamiraju za upotrebu kod organa za sprovođenje zakona i vladinih službi.

Opet, važno je naglasiti da pitanja zloupotrebe biometrijskog nadzora, koja u velikoj meri utiče na ljudska prava, ne mogu biti prepuštena kompanijama i pravilima i politikama koje su same postavile, posebno imajući u vidu njihove aktivnosti i planove motivisane profitom. Na primer, 2020. godine European Digital Rights (EDRi), mreža organizacija koje se zalažu za zaštitu ljudskih prava u digitalnom okruženju, pisala je izvršnom direktoru IBM-a tražeći objašnjenje za najavu kompanije da „gasi“ svoju tehnologiju za prepoznavanje lica „u opšte svrhe“ u ime „pravde i rasne jednakosti“. Međutim, IBM-ovi odgovori nisu pružili ništa suštinski značajno i čini se da su više fokusirani na odnose s javnošću, nego na pitanja ljudskih prava.[100]

KAPACITETI PROIZVODA

Pošto smo opisali elementarne koncepte tehnologije u osnovi biometrijskog nadzora, kao što su mašinsko učenje i računarski vid, možemo se fokusirati na specifične funkcije i primene ovih alata. Važno je razumeti kapacitete nekih od najčešće korišćenih alata, budući da su zloupotrebe omogućene samim dizajnom ovih tehnologija, pored pravnog i društvenog konteksta u kojem se primenjuju.

Mnogi alati koji će biti opisani u narednim odeljcima, kompanije koje ih razvijaju odavno promovišu kao alate koji ne obrađuju biometrijske podatke – da bi se javnost uverila da su sistemi usklađeni sa regulatornim ograničenjima obrade podataka koji mogu identifikovati ljude. Međutim, primeri koji slede jasno pokazuju da jedinstvena identifikacija osobe nije neophodna da bi ovi sistemi naneli ozbiljnu štetu, kao što su održavanje stereotipa i diskriminacija. Pored toga, imajući u vidu podatke koje ovi sistemi obrađuju o licima i telima ljudi, postoje solidni argumenti u prilog zahteva da takve podatke zapravo treba smatrati osetljivim biometrijskim podacima.[101]

Rasno i etničko profilisanje

Jedan od primera koji izaziva duboku zabrinutost u pogledu kapaciteta alata za prepoznavanje lica, može se opisati kao „detekcija etničke pripadnosti“, tj. funkcija za koju se tvrdi da pruža informacije o verovatnoj etničkoj pripadnosti osobe na osnovu njenog lica, kože ili drugih fizičkih ili fizioloških karakteristika.

Na primer, opciju „Ujgursko upozorenje“ mediji su otkrili u izveštaju o interoperabilnosti kompanije Huawei u vezi sa njihovom saradnjom sa Megvii, još jednim kineskim dobavljačem sistema za prepoznavanje lica. Izvorno na kineskom jeziku, dokument iz 2018. pod nazivom „Izveštaj o testu interoperabilnosti Huawei rešenja za video na oblaku i Megvii dinamičkog prepoznavanja lica“, opisuje kako se Megviijev softver za prepoznavanje lica pokazao na tehničkoj infrastrukturi kompanije Huawei.[102] Prema tom izveštaju, koji je očigledno slučajno objavljen onlajn, Megviijev alat za prepoznavanje lica i detekciju etničke pripadnosti uspešno je integrisan u servise kompanije Huawei.

Ova vrsta profilisanja predstavlja veoma ozbiljan rizik za ljudska prava rasijalizovanih i minorizovanih ljudi i zajednica, posebno u Kini, za koju postoje obimni međunarodni izveštaji o raznim kršenjima ljudskih prava nad Ujgurima, što kineska vlada dosledno poriče.[103] Kada je komentar od kompanije zatražio IPVM, onlajn medij koji izveštava o video nadzoru i sličnim bezbednosnim sistemima, Huawei je odgovorio da je opisani izveštaj bio „običan test“ i da „nije imao stvarnu primenu“. Megvii je takođe odgovorio IPVM-u da njihova rešenja „nisu dizajnirana ili prilagođena da ciljaju ili označavaju etničke grupe“.[104] Čak i da je to tačno, podjednako zabrinjava sam razvoj takvih kapaciteta.

Takođe je zanimljivo primetiti da je u ovom slučaju kombinovani sistem Huawei i Megvii koristio NVIDIA hardver, posebno njihove Tesla P4 grafičke procesorske jedinice (GPU).[105] Proizvođači hardvera – kao što je NVIDIA – stoga takođe imaju značajnu ulogu u arhitekturi naprednih sistema nadzora, koji sve više zavise od procesa dubokog učenja. Kako je navedeno u prethodnom odeljku, duboko učenje zahteva ogromne količine procesorske snage, što pokreće potražnju za čipovima visokih performansi potrebnih za vrhunske hardverske komponente kao što su grafički procesori (GPU).

Prepoznavanje emocija

Još jedna krajnje problematična mogućnost jeste navodno prepoznavanje opaženih emocionalnih stanja pojedinaca, što se obično naziva „prepoznavanje emocija“. To je veoma opasna mogućnost u kontekstu targetiranja ljudi, koji mogu biti prepoznati kao „besni“, na primer, i označeni kao štetni po društvo i društveni poredak.

Metode javnog nadzora koje se zasnivaju na mašinskom tumačenju koncepta tako osetljivog i neuhvatljivog kao što je ljudska emocija, mogu prinuditi ljude na društveno prihvatljivo ponašanje kada su u javnim prostorima. Takvo indukovano ponašanje zauzvrat dovodi do veštački „kohezivnog“ i „srećnog“ društva. Problem sa artificijelizacijom ponašanja leži u tome što svaka drugačija lična osobina ili politički ili društveni stav koji odstupa od „normalnosti“, odnosno „prosečnog“ izgleda ili ponašanja, mogu biti potisnuti i suzbijani ako se manifestuju u javnosti.

Na stranici na kojoj je predstavljen Amazon Rekognition, kompanija tvrdi da je ovaj servis u stanju da iz slika ljudskih lica tumači „emocionalne izraze (kao što su sreća, tuga ili iznenađenost) [i] demografske informacije (kao što su rod ili uzrast)“.[106] U smernicama se navodi da se za svaki atribut daje ocena pouzdanosti u procentima; na primer, sistem može da obezbedi 85% verovatnoće da je osoba „žensko“ i 90% verovatnoće da je „srećna“. Amazon, međutim, napominje da Rekognition ne bi trebalo da se koristi za donošenje ovakvih sudova.[107] To je besmislena i neiskrena mera zaštite, jer ne može sprečiti nikoga da koristi proizvod na takav način, i zapravo će to verovatno podstaći, pošto su ti alati upravo dizajnirani da prave takva predviđanja.

U objavi na blogu Amazona iz 2018. godine, u odgovoru na testiranje alata Rekognition koje je sprovela Američka unija za građanske slobode (ACLU), navodi se da je podrazumevani prag pouzdanosti za Rekognition 80%, što se smatra „dobrim za širok skup slučajeva opšte upotrebe... ali to nije pravo okruženje za slučajeve upotrebe u javnoj bezbednosti“. U blogu se takođe tvrdi da je politika Amazona da „preporuči svojim kupcima [Rekognition usluga] da ne koriste manje od 99% nivoa izvesnosti poklapanja za potrebe sprovođenja zakona“.[108] Opet, vidimo nameru korporativnog aktera da „samoreguliše“ tehnologiju koja može ozbiljno da utiče na ljudska prava, posebno u kontekstu sudskih postupaka (npr. nezakonita hapšenja, osude i slične pravne posledice). Uzimajući u obzir da su minorizovane zajednice one koje se obično suočavaju sa nezakonitim pravnim posledicama pod

uticajem tehnologije, to izaziva dodatnu sumnju u opravdanost upotrebe takvih alata.

Amazonova FaceDetail stranica pruža više informacija o mogućim „objektima“ – karakteristikama osobe koje se mogu otkriti sa određenom verovatnoćom – kao što su uzrast, emocije, osmeh, obeležja lica i da li su usta osobe otvorena, što sve može da se koristi za prikupljanje dodatnih informacija.[109] Zabrinjavajuće je i samo tretiranje ličnih osobina ljudi kao „objekata“ namenjenih programiranju, svodeći ih na puke tehničke atribute namenjene mašinskoj obradi. Kao objekte „Emocija“, Rekognition pruža sledeće vrednosti kao validne: „SREĆNO“, „TUŽNO“, „LJUTO“, „ZBUNJENO“, „ZGAĐENO“, „IZNENAĐENO“, „SMIRENO“, „NEPOZNATO“ i „STRAH“.[110]

Amazon nije jedini provajder usluga koje kategorišu ljude po spoljašnjem izgledu. Microsoftova usluga Azure Face, u vreme istraživanja za ovu knjigu, nudila je slične mogućnosti koje se „opciono mogu koristiti za analizu atributa o svakom licu korišćenjem dodatnih AI modela, kao što je poza tela ili obeležja lica kao što su položaj očiju ili nosa“.[111] Međutim, Microsoft je kasnije saopštio da do kraja juna 2023. ukida kapacitete koji navodno zaključuju emocionalna stanja i atribute ličnog identiteta kao što je rod, što je uneto i na stranicu sa objašnjenjima ovog servisa.[112]

Prepoznavanje roda

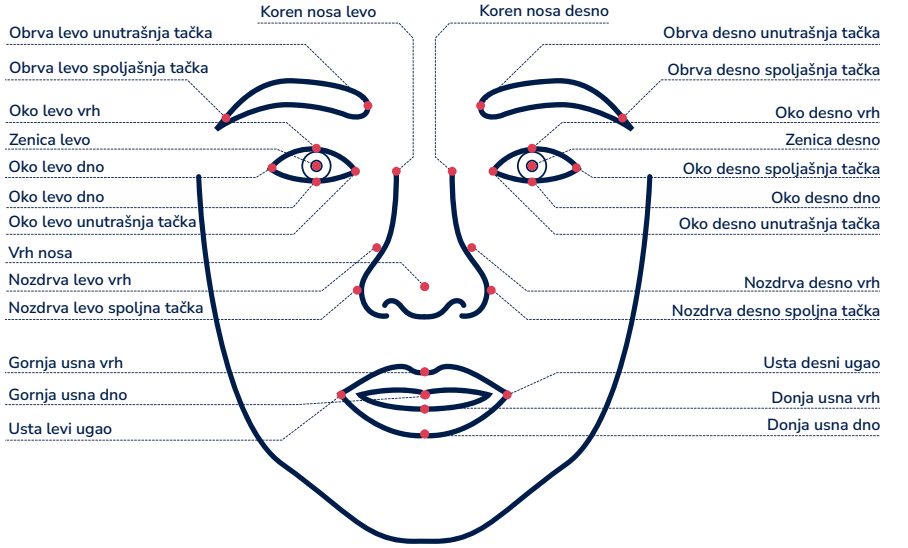
Kada je reč o prepoznavanju roda, ono funkcioniše slično kao i prepoznavanje emocija na servisima poput Amazon Rekognitiona. Na Microsoftovom servisu Azure, kapaciteti za predviđanje roda su ukinuti u skladu sa obaveštenjem kompanije da se obavezuje na to do kraja juna 2023. godine.[113] U Amazon Rekognition Gender API-ju moguće vrednosti koje aplikacija može da izvede jesu „muško“ i „žensko“.

Dakle, Amazon nudi usluge sa ciljem svrstavanja ljudi u kategorije zasnovane uglavnom na binarnim stereotipima o rodu. Osim toga, čak i kada bi kompanije ponudile širi spektar opcija rodnog identiteta, sama premisa da je rodni identitet ljudi vidljiv spolja u suprotnosti je sa idejama poštovanja ljudskog dostojanstva i samoizražavanja. Iz perspektive ljudskih prava, teško je videti bilo kakav legitiman slučaj upotrebe tehnologije za kategorizaciju ljudi na ovaj način. U širem smislu, takve tehnologije podržava duboko problematična pretpostavka da se ljudski identitet može svesti na jedinice i nule – i da je to nešto što je poželjno.

Amazon navodi da su „rodne binarne predikcije [...] najpogodnije za slučajeve gde treba analizirati zbirnu statistiku distribucije roda bez identifikacije konkretnih korisnika“ i savetuje da se rodne binarne predikcije ne koriste „za donošenje odluka koje utiču na prava pojedinca, privatnost ili pristup uslugama“.[114] Ipak, Amazonov KnownGender API, koji omogućava otkrivanje poznatog roda slavne ličnosti, funkcioniše drugačije. Vrednosti koje može da izvede jesu „muško“, „žensko“, „nebinarno“ i „neizraženo“, što poznatim ličnostima iz nekog razloga omogućava fleksibilniji rodni identitet u poređenju sa kategorijama koje se koriste za opštu populaciju.[115] Ovo ponovo ukazuje na probleme koji nastaju kada se osetljive karakteristike ljudi prinudno definišu, posebno kada to rade privatne kompanije.

Obeležja lica

Što se tiče crta lica i prepoznavanja konkretnih osoba, i Azure Face i Amazon Rekognition se oslanjaju na otkrivanje položaja obeležja na licu. To se takođe može smatrati intruzivnom tehničkom sposobnošću, s obzirom na to da svodi prepoznavanje na krajnje granularni, mikro nivo. Na primer, Azure Face ima 27 unapred definisanih obeležja lica, odnosno specifičnih tačaka na licu koje se koriste za identifikaciju osobe:



Microsoft Azure Face, predefinisana obeležja[116]

Amazon Rekognition ima 30 veoma sličnih obeležja lica čiji položaj može da detektuje kao moguće vrednosti.[117] Ova obeležja u suštini opisuju ključne elemente koji se koriste za identifikaciju ljudskog lica, kao što su oči, nos, usta, brada i obrve. Kao takva, obeležja služe za prevođenje načina na koji mašine čitaju lica, u poređenju sa načinom na koji ljudski vid razlikuje lica.

U sistemima sa kapacitetima zasnovanim na uslugama kao što su Rekognition ili Azure Face, specifični oblici i položaji obeležja na licu mogu biti izvori targetiranja i diskriminacije ljudi sa posebnim karakteristikama. To je naročito relevantno u scenarijima u kojima vlada progoni određenu grupu ili zajednicu ili se ona stereotipno povezuje sa navodnim „antisocijalnim“ ili „sumnjivim“ ponašanjem. Već smo videli da je diskriminatorna sposobnost infrastrukture biometrijskog nadzora, kao što je otkrivanje etničke pripadnosti, vrlo moguća. Primetili smo i kako represivni i rasistički režimi mogu da koriste frenologiju ili eugeniku – koje moderna nauka odbacuje – kako bi se opravdala diskriminacija ljudi na osnovu oblika njihove lobanje ili lica. Ove mogućnosti Rekognitiona i Azure Facea njihovi kupci bi mogli relativno lako da koriste za rasno ili drugo profilisanje.

Ponašanje i kontrola mase

Moguće opcije softverskih proizvoda u smislu biometrijskog nadzora, naravno, samo su jedan deo priče. Treba uzeti u obzir i hardver, odnosno fizičku infrastrukturu kao što su kamere i prateći uređaji, u koje je sve češće ugrađen softver kako bi se analize i upozorenja mogli sprovoditi direktno sa uređaja na računar onoga ko ga je instalirao. Na primeru Huawei opreme, možemo videti da su fizičke komponente, instalirane i korišćene u javnim prostorima, postale veoma moćan alat za kontrolu mase, praćenje ponašanja i nadzor različitih aktivnosti, poput saobraćaja. Tehnološki razvoj, koji gotovo eksponencijalno uvećava kapacitet za nadzor, dovodi u pitanje tradicionalne koncepcije hardvera i softvera kao različitih komponenti.

U brošuri o inteligentnom video nadzoru iz 2019, Huawei opisuje nekoliko modela kamera. Specifikacija za Huawei M1281-K, model sa oznakom „Multi-Algorithm Box Camera“, navodi da ova kamera i njen integrisani softver mogu da otkriju do 50 objekata odjednom na osnovu inteligentnih algoritama dubokog učenja za detekciju objekata – što joj omogućava da cilja pešake, motorna i nemotorna vozila. Sudeći po spisku karakteristika, čini se da je ovaj model kamere fokusiran i na nadzor saobraćaja i na nadgledanje gužve na javnim mestima. U stanju je da detektuje ne samo registarske tablice vozila, već i boje, brendove, podbrendove, godinu modela i tako dalje.[118]

Kada su u pitanju kapaciteti orijentisani na ljude, Huawei tvrdi da ovaj model može da vrši detekciju osoba i analizu ličnih atributa, što uključuje atribute lica, npr. da li osoba nosi masku, kao i predviđenih karakteristika poput roda ili uzrasta. Oblik kamere sugeriše da se može montirati i na vozila, na primer na policijska kola. Ovaj model takođe ima ono što Huawei naziva „detekcija izuzetaka“, što znači da kamera može da otkrije postojanje zvuka, iznenadno pojačanje ili utišavanje zvuka, promenu scene i gubitak fokusa. Ono što ga čini još zanimljivijim jeste analiza ponašanja i kretanja mase. Prema brošuri, analiza ponašanja uključuje detekciju brzog kretanja, napuštenih i uklonjenih objekata, detekciju ulaska u ograđenu zonu, upada, ulaska/izlaska u zonu i detekciju lutanja. Analiza mase omogućava funkcije kao što su prebrojavanje glava, detekcija dužine reda, detekcija gustine mase, detekcija okupljanja i toplotna mapa.[119] Mnoge od ovih karakteristika su iste one koje su korišćene na Olimpijskim i Paraolimpijskim igrama u Parizu 2024, a koje su detaljno ispitane u poglavlju Praksa.

Još jedan sličan model kamere sa opcijama „inteligentne“ analitike jeste kamera Huawei IPC6284-VRZ, opremljena karakteristikama kao što su detekcija objekata koji se brzo kreću, detekcija prelaza, detekcija napuštenih/uklonjenih objekata, detekcija tumaranja, upada i ljudskog lica, prepoznavanje boja i klasifikacija vozila i pešaka. Takođe je zanimljivo da Huawei ovaj model označava kao „otporan na vandalizam“. U brošuri, Huawei navodi dva dodatna modela kamera, IPC6355-VRZ i C6620-Z33, koji su u obliku kupole i stoga pogodniji za osmatranje većih prostora iz širokih uglova (trgovi, raskrsnice, parking). Oba modela obuhvataju analizu ponašanja i karakteristike detekcije izuzetaka, sa glavnom razlikom u tome što je C6620-Z33 kamera koja se može pomerati u skladu sa situacijom (pan-tilt-zoom, PTZ).[120]

Proliferacija kamera i analitike koju vidimo u savremenim CCTV sistemima zahteva dodatne uređaje i funkcionalnosti da bi mogli da vrše svoje napredne funkcije onako kako je predviđeno. Na primer, Huawei NVR800 mrežni uređaji za snimanje video zapisa dizajnirani su tako da koordinišu i proširuju AI kapacitete kamera. Prema korisničkom vodiču, NVR800 podržava analizu ponašanja (npr. detekciju pokreta, upada, prelaska označene zone, kao i audio dijagnostiku), detekciju mete i ekstrakciju strukturiranih podataka o meti, pri čemu je „meta“ verovatno osoba ili objekat, na primer vozilo, prikazana u video strimu. Uređaj takođe može da prikaže informacije kao što su „vreme pojavljivanja, učestalost i broj osoba u različitim scenarijima“. Uređaj takođe podržava opciju PTZ kontrole na

kamerama kako bi se postigao širi ugao i pokrivenost kada je to potrebno. Opcije označavanja olakšavaju preciziranje, pa čak i obeležavanje kritičnih trenutaka kada se video gleda uživo ili naknadno.[121] Dok individualne kamere mogu da izdaju upozorenja, ključna funkcija NVR800 jeste to što omogućava niz informacija o svakom upozorenju – što nadzorni potencijal svake pojedinačne „pametne“ kamere podiže do pravog panoptikona.

Kada je reč o praktičnim primerima kako se NVR800 koristi za pametni nadzor, Huawei daje scenario u kojem se CCTV sistem izgrađen pomoću ovog uređaja i Huawei kamere postavljaju da nadgledaju stambeni kvart. Sa funkcijama kao što su prepoznavanje neovlašćenih osoba, detekcija maski, upozorenja zasnovana na blok-listi, pretraga meta i otkrivanje upada, moguće je imati sveobuhvatan bezbednosni pregled ulaza i izlaza ili otvorenih prostora između zgrada. Na primer, opcija liste blokiranih funkcioniše tako da „na listu blokiranih za izdavanje upozorenja, dodaje slike osoba koje se često pojavljuju i ponašaju nenormalno na kapiji stambenog okruga“. Kada se pojavi osoba pod zabranom, aktivira se alarm. Pretraga meta omogućava snimanje svih ljudi koji ulaze ili izlaze iz zgrade i generiše putanje za određenu osobu u određenom vremenskom periodu, na osnovu slika mete, što ih čini lakim za praćenje.[122] Ovaj opis liči na scenario društvene kontrole, dok detekcija maske (da li osoba nosi masku ili ne) ostavlja utisak da je to posebno primenjivo u situacijama kao što je pandemija kovida-19.

Funkcija video analitike za praćenje kretanja, nazvana „ljudske putanje“, veoma je slična onoj koju poseduju Huawei proizvodi, a može se koristiti preko servisa Amazon Rekognition Video. Ova funkcija omogućava korisnicima da prate putanju ljudi na video snimcima i dobiju informacije o njihovim obeležjima na licu, na primer, ili o lokaciji osobe u video kadru u trenutku praćenja njihove lokacije.[123] Međutim, u objavi na sajtu AWS s kraja oktobra 2024. navodi se da će se mogućnost praćenja ljudi ukinuti do 31. oktobra 2025. godine, odnosno da novi korisnici neće moći da koriste ovu opciju od 24. oktobra 2024, dok će za postojeće biti dostupna do kraja oktobra 2025, kada je planirano njeno potpuno povlačenje iz Rekognition paketa usluga. Interesantno je da autori objave korisnicima preporučuju alternative otvorenog koda koje mogu da koriste umesto Amazon Rekognition opcije praćenja ljudi.[124] NeoFace Watch, softver kompanije NEC, ima funkciju pod nazivom „analiza toka“, za koju kažu da „anonimizovano nadgleda pojedince i izračunava njihovo vreme u redu, pružajući korisne informacije o nivoima usluga i efikasnosti operacija u celini“, što podseća na opcije analize mase koje nudi Huawei oprema, mada

je tvrdnja o anonimizaciji upitna.[125] Pored toga, funkcija „video analiza“ softvera NeoFace Watch može da obrađuje snimljeni video „brzinom boljom od realnog vremena“ što se može koristiti za „analizu ljudskih lica nakon događaja“ i „bezbednosni pregled remećenja reda velikih razmera“.[126]

Čini se da su sve ove karakteristike usmerene na javna okupljanja ili veće događaje koji uključuju bezbednosne rizike, kao što su demonstracije, marševi, sedeći protesti ili drugi oblici demokratskog neslaganja, kao i javne proslave, festivali i sportski događaji. Nekada je policija morala da angažuje brojno osoblje i druge resurse da analizira i prati takve događaje. Sa uvođenjem naprednih sistema za praćenje gužve i analizu ponašanja, policiji teoretski postaje lakše da planira, nadgleda i potencijalno reaguje na velike grupe ljudi.

U takvom okruženju, protesti i različiti oblici političkog izražavanja na ulicama, trgovima i drugim javnim prostorima pod većim su nadzorom nego ikad u istoriji. To takođe predstavlja promenu paradigme od rada policije na terenu, gde osobe koje nisu optužene ili povezane sa kriminalom neće biti dalje analizirane, ka situaciji u kojoj se identitet i ponašanje svake osobe može analizirati, zadržati i potencijalno koristiti protiv njih tokom dužeg vremenskog perioda. Činjenica da tehnologija biometrijskog nadzora nije sredstvo represivnih režima, već realnost u navodno otvorenim i liberalnim društvima, trebalo bi da nas navede da se zamislimo nad društvenim vrednostima kojima ova vrsta tehnologije daje prioritet. Države imaju legitiman cilj da čuvaju bezbednost i sprovode zakon, kao što imaju dužnost da štite slobodu i privatnost ljudi. Ali kada se jednom pređe linija masovnog nadzora pod izgovorom zaštite bezbednosti, to može biti prekretnica za svako društvo.

REŠENJA ZASNOVANA NA USLUGAMA

Pored alata koje smo opisali, a koji zahtevaju bar određeni nivo prilagođavanja postojećim sistemima, neka rešenja se pružaju kao usluga prepoznavanja lica krajnjem korisniku. Na primer, kupac pristupa specifičnoj usluzi, kao što je Clearview AI, koristi platformu koju u potpunosti kontroliše provajder, na sličan način kao kada korisnik kreira nalog na društvenoj mreži.

Clearview AI, kompanija sa sedištem u SAD koja pruža istoimenu onlajn uslugu (neku vrstu pretraživača za ljudska lica), izaziva kontroverze od samog nastanka. Zbog svojih praksi prikupljanja i obrade podataka,

Clearview AI je već bio pod istragom nekoliko regulatornih tela širom sveta. Britanska služba za zaštitu podataka, Kancelarija poverenika za informacije (Information Commissioner's Office, ICO), izrekla je kaznu od 7,5 miliona funti za Clearview AI 2022. godine,[127] dok je francuski CNIL iste godine izrekao još veću kaznu od 20 miliona evra.[128] Kompanija se žalila na odluku britanskog poverenika i sud je u oktobru 2023. poništio kaznu uz obrazloženje da Clearview AI nije pod jurisdikcijom ICO.[129] Italijanska služba Garante Privacy takođe je kompaniji izrekla kaznu od 20 miliona evra.[130] Veruje se, međutim, da Clearview AI nije reagovao ni na jednu od odluka ili kazni izrečenih u Evropi, zbog čega je u maju 2023. CNIL odredio dodatnu kaznu od 5,2 miliona evra.[131]

Još jednu visoku kaznu za Clearview AI u EU izrekao je holandski organ za zaštitu podataka o ličnosti (Autoriteit Persoonsgegevens, AP) u septembru 2024. u iznosu od 30,5 miliona evra, uz mogućnost dodatnog kažnjavanja do 5 miliona evra za nepostupanje po odluci. Direktor AP je takođe napomenuo da je upotreba Clearview AI u Holandiji nezakonita i najavio moguće kažnjavanje organizacija u toj zemlji koje su koristile usluge ove kompanije.[132]

Takođe, u zajedničkoj istrazi čiji su rezultati objavljeni početkom 2021, kancelarija poverenika za privatnost Kanade i tela za zaštitu podataka tri kanadske provincije – Alberte, Kvebeka i Britanske Kolumbije – otkrili su da je „Clearview angažovan na prikupljanju, korišćenju i otkrivanju ličnih podataka kroz razvoj i pružanje usluga svoje aplikacije za prepoznavanje lica, bez potrebne saglasnosti".[133] Međutim, verovatno najveći regulatorni udar do sada dogodio se 2022. u SAD, gde je Američka unija za građanske slobode (ACLU) pokrenula uspešan sudski spor po zakonu o privatnosti biometrijskih podataka u državi Ilinois (Biometric Information Privacy Act, BIPA) protiv Clearview AI, kako bi sprečila kompaniju da svoju bazu lica prodaje preduzećima i pojedincima bilo gde u Sjedinjenim Državama.[134]

Za Clearview AI je specifično to što je njegov alat za prepoznavanje lica zasnovan na fotografijama koje se automatski prikupljaju (skrejpuju) sa interneta, posebno sa veb lokacija na kojima ljudi objavljuju mnogo fotografija, kao što su platforme društvenih mreža. Izvršni direktor Clearview AI Hoan Ton-That izjavio je da je do marta 2023. kompanija prikupila oko 30 milijardi fotografija lica sa interneta, što zvuči zapanjujuće, jer je najverovatnije čini najvećom bazom fotografija ljudskih lica u privatnom vlasništvu koja trenutno postoji.[135] To prosečne policijske foto baze čini praktično zastarelim, posebno zato što Clearview AI svoje usluge plasira službama za sprovođenje zakona. Na stranici sa opisom kompanije, Clearview AI navodi da su razvili „revolucionarnu, veb-baziranu obaveštajnu platformu namenjenu službama za sprovođenje zakona koju će koristiti kao alat za generisanje visokokvalitetnih istražnih tragova".[136]

Reagujući na upotrebu Clearview AI servisa u švedskoj policiji – za koju se kaže da je jedna od osamnaest evropskih službi za sprovođenje zakona koja to radi, uključujući one u Španiji, Francuskoj i Srbiji[137] – švedski poverenik za zaštitu podataka, IMI, takođe je preduzeo mere.[138] Međutim, za razliku od poverenika u Italiji, Francuskoj i UK, postupak švedskog poverenika nije preduzet protiv Clearview AI, već direktno protiv policije zbog nezakonite upotrebe servisa, a kazna je iznosila 250.000 evra.

Pored brojnih kontroverzi oko Clearview AI i načina na koji kompanija koristi lične podatke praktično svakoga ko se ikada pojavio na internetu, postoji i nedostatak transparentnosti kada je u pitanju tehnički proces po kom njihov alat zapravo funkcioniše. Na osnovu javno dostupnih informacija i vlastite ekspertize, aktivistička grupa za privatnost pod nazivom None of Your Business (NOYB) pokušala je da razloži svaki korak usluge Clearview AI u žalbi podnetoj austrijskoj Upravi za zaštitu podataka:[139]

- U prvom koraku, automatski skrejper slika pretražuje sve javne veb stranice i traži bilo koju sliku koja bi mogla da sadrži ljudsko lice. Pored toga, skrejper takođe prikuplja sve metapodatke povezane sa slikama, kao što su veza (URL), naslov slike ili naslov veb stranice na kojoj je slika pronađena.
- Zatim se sve ove slike i povezani metapodaci skladište na Clearview AI serverskoj infrastrukturi i čuvaju se čak i nakon što su slike izbrisane iz originalnog izvora ili im je ograničen pristup.
- Neuronske mreže za obradu slike koriste se za izdvajanje jedinstvenih identifikacionih karakteristika svakog lica koje se pretvaraju u takozvane vektore, odnosno numeričke reprezentacije koje se sastoje od 512 tačaka.
- Vektori/identifikatori (poznatiji kao šabloni lica) čuvaju se u bazi gde se povezuju sa slikama i relevantnim metapodacima. Sledeći korak je heširanje vektora, odnosno dodela kraće vrednosti fiksne

dužine ili ključa kroz matematički proces, kako bi baza bila pretraživa, odnosno da bi se lica mogla porediti.

» Poslednji korak je podudaranje lica, koje se dešava kada korisnik/kupac Clearview AI aplouduje fotografiju osobe koju želi da identifikuje. Takva slika se analizira, ekstrahuje se vektor lica i dodeljuje heš vrednost, koja se zatim upoređuje sa hešovima u bazi podataka prethodno prikupljenih slika. Korisnik tada dobija rezultat pretrage sa svim podudarnim slikama, kao i svim drugim metapodacima povezanim sa njima.

U kontekstu servisa Clearview AI i njegovih ogromnih mogućnosti, zajedno sa regulatornim izazovima za kontrolu njegove upotrebe, takođe treba imati u vidu slične usluge pretraživanja slika lica, od kojih je jedna PimEyes. Reč je o servisu koji se predstavlja kao „obrnuta pretraga slika“ koja omogućava korisnicima da aplouduju fotografije lica i pronađu gde se slike nalaze na mreži uz pomoć tehnologije za prepoznavanje lica. Kako se objašnjava na zvaničnom sajtu, „u rezultatima prikazujemo ne samo fotografije slične onoj koju ste aploudovali za pretragu, već i slike na kojima se pojavljujete na drugoj pozadini, sa drugim ljudima, ili čak sa drugačijom frizurom“.[140]

U novembru 2022, britanska nevladina organizacija Big Brother Watch podnela je žalbu nacionalnoj službi za zaštitu podataka, tvrdeći da PimEyes nezakonito obrađuje biometrijske podatke o milionima građana Ujedinjenog Kraljevstva. Kako Big Brother Watch napominje u svojoj žalbi, pored slika, rezultati pretrage takođe pružaju njihove URL adrese i potencijalno dodatne informacije o osobi. Ove funkcije mogu dovesti ljude, posebno žene i minorizovane osobe u povećan rizik od uhođenja, uznemiravanja i nasilnih zločina. Alat se takođe poredi sa Clearview AI zbog sličnog poslovnog modela.[141] PimEyes je na žalbu odgovorio tvrdnjom da nije niti je ikada bio „alat za utvrđivanje identiteta ili detalja o bilo kojoj osobi“, dodajući da je svrha usluge „prikupljanje informacija o URL adresama koje objavljuju određene vrste slika u javnom domenu“. PimEyes dalje tvrdi da glavne „mete“ njegovog pretraživača nisu osobe, već javne veb stranice.[142]

U svom blogu, PimEyes takođe navodi da pruža samo alat, te da odgovornost za njegovu upotrebu leži na korisnicima. Platforma takođe nudi mehanizam za izuzimanje (opt-out), za šta osoba mora da podnese fotografiju, anonimizovani sken identifikacionog dokumenta i mejl adresu.[143] Apsurdno, ljudi moraju da pruže više informacija da bi sebe izuzeli iz prikupljanja podataka koje po svoj prilici nisu ni želeli. Činjenica da je odgovornost prebačena na korisnike ne umanjuje intruzivnost ovako moćnog alata.

U načelu, ogromne količine podataka sa ljudskim licem objavljenih onlajn postale su dostupne za preuzimanje zahvaljujući razvoju alata za skrejpovanje veb stranica. Čini se da nam predstoji duga borba za zaštitu naših lica od digitizacije i pretvaranja u pretražive matematičke ključeve, bez dovoljne i efikasne kontrole. Prilike za sprovođenje pravila posebno otežava globalna priroda i interneta i usluga kao što su Clearview AI i PimEyes. To je vidljivo iz odluka nekoliko EU poverenika, na primer italijanske Garante Privacy koja zahteva od Clearview AI da izbriše slike i druge podatke svih Italijana, ali se ne bavi širim strukturama i sistemima u okviru kojih ove kompanije posluju. Činjenica da alati kao što je Clearview AI postaju sve sofisticiraniji takođe je problematična iz perspektive zaštite ljudskih prava, posebno u kontekstu primene zakona. Vaše lice možda nije u bazi podataka policijskih snaga neke zemlje, ali možete se kladiti da ga Clearview AI gotovo sigurno ima negde na svojim serverima.

Ipak, izvesno je da će usvajanje Uredbe o veštačkoj inteligenciji (AI Act)[144] u Evropskoj uniji praksi dovesti do detaljnijeg preispitivanja, a možda i zabrane Clearview AI i sličnih tehnologija na teritoriji EU. Uredba kao zabranjenu propisuje upotrebu sistema veštačke inteligencije za „neselektivno skrejpovanje biometrijskih podataka sa društvenih mreža ili CCTV snimaka radi kreiranja baze podataka za prepoznavanje lica“.[145] Ova formulacija prilično odgovara načinu na koji Clearview AI sprovodi masovno prikupljanje i obradu podataka.

IZA TEHNOLOGIJE: DEKONSTRUKCIJA REŠENJA ZA PREPOZNAVANJE LICA

Mada su biometrijska rešenja za nadzor i načini na koje ona uopšte funkcionišu nedovoljno transparentni, da bi kompanije zaštitile svoje proizvode moraju ih patentirati pre svoje konkurencije. Informacije o patentima, koji su javno dostupni i pretraživi, mogu pružiti značajan uvid ne samo u mogućnosti koje sadašnji proizvodi imaju, već i u potencijale onih koji su planirani za budući razvoj. Iako su patenti izvor velike moći u društvenim odnosima posredovanim tehnologijom, iz njih se takođe može saznati nešto više o tome kako se ti odnosi moći učvršćuju.

ANALIZA PATENATA

Većina kompanija koje razvijaju hardverske i softverske proizvode stalno podnose veliki broj patenata kako bi bile konkurentne, neprestano isprobavajući nove metode. Iako patenti za mnoge tehnologije mogu da zvuče krajnje uopšteno i tehnički, kompanije se često oslanjaju na njih da zaštite svoje pravo na intelektualnu svojinu i tako očuvaju vrednost svojih unosnih proizvoda i usluga. Na primer, Amazonov patent „Prošireno prepoznavanje lica sa videa“ objašnjava kako se „infracrvena slika može koristiti za utvrđivanje trenutka kada je neka osoba u velikoj meri okrenuta ka uređaju, tako da će kadar slike snimljene u to vreme verovatno biti adekvatan za prepoznavanje lica“.[146]

Zanimljivo je videti kako se programeri i kompanije dovijaju da unaprede proces prepoznavanja lica i tako dodaju veću vrednost svojim proizvodima, posebno s obzirom na to da patenti imaju rok trajanja. Amazonov opis patenta, na primer, dalje objašnjava da je, pošto analiza informacija iz videa može biti veoma zahtevna za resurse u smislu procesorske snage i energije, poželjnije analizirati samo određene delove videa, uključujući one snimljene mobilnim uređajima. Konkretno, ovaj patent nastoji da prevaziđe izazov koji postavlja korisnik ili subjekt koji ne gleda uvek direktno u kameru, ili pojavu zamućenja slike usled kretanja.[147]

U kontekstu Ring kamera i direktnog pristupa službi za sprovođenje zakona, zanimljivo je primetiti da je Amazon patentirao tehnologiju deljenja video snimaka za upozorenja o krađi paketa. Patent nazvan „deljenje video snimaka sa audio/video zapisa i komunikacionih uređaja za sprečavanje krađe paketa“, sugeriše da korišćenje kamera na zvonu na ulaznim vratima kao što je Ring „takođe može pomoći u otkrivanju i prevenciji kriminala“.[148] Uređaj je u suštini konfigurisan da prati pakete u zoni isporuke i signalizira kada je verovatno da je došlo do krađe, tako što će poslati upozorenje najmanje jednoj službi za sprovođenje zakona. Takođe, sistem može da koristi prepoznavanje lica na snimku da utvrdi da li je osoba koja odnosi paket za to bila ovlašćena.[149]

Da bi savladao velike količine slika koje mogu da sadrže ista ili slična lica ljudi, Microsoft je obezbedio patent koji omogućava grupisanje i rangiranje slika na osnovu podataka iz prepoznavanja lica. Ovo funkcioniše tako što se prvo utvrđuju podaci za prepoznavanje lica za svako lice detektovano na svakoj slici i izdvaja identifikator lica koji jedinstveno identifikuje svako pojedinačno ljudsko lice. Sistem generiše skup deskriptora osobina lica i rangira lica na osnovu aktivnosti očiju i usta (tj. da li su otvorene ili zatvorene). To se koristi za označavanje ukupnog kvaliteta svake slike lica, kao i za stvaranje „potpisa“ lica koji na jedinstven način identifikuje osobu.[150] Proces „grupisanja“ se vrši prema ovim potpisima i rangiranju, tako da se slike iz skupa svrstavaju u jednu ili više grupa. Ove grupe se sastoje od jedne ili više slika od kojih svaka prikazuje detektovano lice koje predstavlja istu osobu kao onu koju predstavlja bilo koje drugo otkriveno lice prikazano na bilo kojoj slici u svakoj grupi.[151]

Microsoft je takođe patentirao tehnologiju za prepoznavanje lica u video sadržaju, koja se zasniva na galerijama lica generisanih iz podataka o detekciji lica u ulaznim video kadrovima. Ove galerije su označene i koriste se za prepoznavanje lica koja se pojavljuju u video snimku, a metapodaci koji povezuju lice sa kadrom se generišu i održavaju za dalju identifikaciju.[152]

Još jedna primena prepoznavanja lica za identifikaciju može se naći u Microsoftovom patentu pod nazivom „Provera identiteta zasnovana na dinamici lica“. Prema opisu, tehnika se sastoji od dve komponente. Prva komponenta uključuje poređenje novounetih podataka o ljudskom licu sa „prethodno sačuvanim strukturnim potpisom lica“ korisnika, dok

druga komponenta proverava da li se ulazni podaci o licu poklapaju sa „dinamičkim potpisom lica“. Novina ovog dinamičkog potpisa lica je da „opisuje pokretanje delova lica tokom određenog vremenskog perioda dok korisnik izvodi gest, i korelaciju različitih delova lica tokom kretanja“. Opis patenta sugeriše da ova tehnika zasnovana na pokretima lica ima za cilj da smanji rizik od pokušaja zlonamernih aktera da lažiraju izgled ovlašćenog korisnika.[153]

Da bi se bolje razumela veza između detekcije i prepoznavanja ljudskog lica, Huaweijev patent pod nazivom „Prilagodljivo isecanje slike za prepoznavanje lica“ objašnjava kako da se unapredi proces kada se slika prosleđuje sa neuronske mreže za detekciju lica („ovo je ljudsko lice“) na neuronsku mrežu za prepoznavanje lica („ovo je osoba čije je to lice“). Proces je povezan sa tzv. graničnim okvirom: područjem koje obuhvata lice. Ako lice nije tačno opisano graničnim okvirom, to će dovesti do grešaka u mreži za prepoznavanje lica.[154] Ovakav pristup pokazuje da je upotreba neuronskih mreža od ogromnog značaja za savremene sisteme za prepoznavanje lica, posebno za unapređenje njihove tačnosti i pouzdanosti, što je naravno pitanje od ekonomskog interesa za prodavce.

Patenti takođe nude uvid u to kako će kompanije poput Clearview AI strateški koristiti ove zaštite intelektualne svojine da zadrže svoju dominaciju na tržištu. U januaru 2022. Clearview AI je objavio saopštenje u kojem je najavljeno da im je odobren patent „Metode za pružanje informacija o osobi zasnovane na prepoznavanju lica“. Saopštenje ne govori mnogo o suštini tehnologije, već samo da je „ova kombinacija prikupljanja informacija sa javnog interneta sa mogućnostima prepoznavanja lica, donela Clearview AI patentnu zaštitu“.[155] Kada se pročita vrlo detaljan opis patenta, međutim, jasno je da je Clearview AI uložio značajne mere kako bi održao svoju tehnologiju.

Rezime pronalaska opisuje proces u sledećim koracima:

- primanje podataka o slici ljudskog lica prenetih sa korisničkog uređaja. Podaci o slici lica sadrže najmanje snimljenu sliku lica subjekta;
- transformisanje podataka o slici lica u podatke za prepoznavanje lica;
- poređenje sa referentnim podacima za prepoznavanje lica koji su povezani sa više sačuvanih slika lica određenih osoba, da bi se identifikovao najmanje jedan verovatni kandidat koji odgovara snimljenoj slici lica;
- nakon identifikacije kandidata koji odgovara snimljenoj slici lica, preuzimanje ličnih podataka iz baze (npr. biografija, podaci o profilu) povezanih sa kandidatom; i
- prenošenje ličnih podataka na korisnički uređaj i pokretanje korisničkog uređaja da prikaže lične podatke.[156]

U opisu patenta se navodi da su „referentni podaci za prepoznavanje lica“, tj. izvorne slike lica skrejpovane sa „interneta, profesionalnih veb sajtova, sajtova službi za sprovođenje zakona ili saobraćajnih odeljenja“. Takođe se pominje da „baza podataka sadrži mnoštvo krivičnih dosijea povezanih sa slikama lica koje se čuvaju u bazi podataka“, što se verovatno odnosi na slike uhapšenih i slične baze podataka.[157] Kada je reč o korišćenju servisa Clearview AI, patent objašnjava da se „sistemom može upravljati preko desktopa ili daljinski putem pametnog telefona, što korisnicima koji sprovode krivične istrage, provere prošlosti itd. omogućava da momentalno utvrde identitet i dobiju biografske podatke o osobama putem jedne ili više baza podataka lica sa dodatnim vezama ka društvenim medijima, konvencionalnim medijima, profesionalnim veb stranicama itd.“[158]

Patent takođe opisuje opcionu notifikaciju ukoliko je podudaranje utvrdilo „osobu od interesa“, što može značiti nestalu osobu, osobu optuženu za krivično delo ili sa krivičnim dosijeom, seksualnog prestupnika, osobu koja je pretrpela gubitak pamćenja, ili osobu za koju se može reći da „nekako predstavlja visok rizik za javnu bezbednost“.[159] U napomeni koja uistinu izaziva zebnju, opis patenta navodi da „policija može drugačije reagovati na osobu koja nije ranije hapšena i ima određeno zdravstveno stanje, nego na osobu čije je lice detektovano kao povezano sa napadom na policiju.“[160] Izgleda kao da je alat Clearview AI predodređen da još više učvrsti odnose moći usmerene protiv potlačenih grupa, na primer crnih zajednica u SAD, za koje je iscrpno dokumentovano da su mete policijske brutalnosti i lažnih optužbi o „agresivnosti“. Ističući precizno kako tehnologija ugrađuje ove diskriminatorne obrasce, jedna studija iz 2018. pokazala je da tehnologija za prepoznavanje emocija rutinski iznosi predviđanje da su crnci gnevniji od belaca čak i kada su im izrazi lica bili isti.[161]

U septembru 2022, Clearview AI je objavio da je odobren njihov drugi patent pod nazivom „Skalabilna linija za pripremu podataka za treniranje i efikasan distribuirani trener za duboke neuronske mreže u prepoznavanju lica“. Kompanija je navela da je patent odobren „zbog njegove sposobnosti da kreira visoko precizne algoritme za prepoznavanje lica bez pristrasnosti iz javno dostupnih informacija“, odnosno da je Clearview AI „u stanju da kreira skup podataka koji predstavlja svu demografiju sa svojom jedinstvenom pripremom podataka i distribuiranim algoritmima za trening“.[162]

Prema patentu, sistem izdvaja lica iz neobrađenih slika i može unapred da dodeli oznaku identiteta podskupu slika. Ove oznake identiteta mogu biti korisnička imena sa društvenih mreža ili ključne reči povezane sa upitom na pretraživaču. Jedna od bitnih karakteristika Clearview AI sistema, kako je opisano u patentu, jeste „obezbediti da slike lica koje odgovaraju oznaci identiteta zaista pripadaju identitetu (čistoća unutar identiteta) i da ne postoje druge slike istog identiteta pogrešno označenog kao drugi identitet (međuidentitetska čistoća)“.[163] Ovo „čišćenje“ skupa podataka može se postići korišćenjem modela neuronske mreže za prepoznavanje lica. Ali jedna posebno zanimljiva karakteristika jeste mogućnost augmentacije skupa podataka slike: „Visoko efikasan pristup za povećanje značajnih varijacija unutar identiteta je augmentacija slika lica na određene načine koji održavaju visoku vernost prirodnoj pojavi tog identiteta, kao što su dodaci (npr. naočare, šeširi, maske), varijacije osvetljenja i starenja“.[164] Ovo omogućava, na primer, da se proširi postojeći skup slika, pa čak i unapredi foto-baza tokom vremena kako se nove slike obrađuju i proširuju. Iako patenti pružaju izvestan uvid u to kako ove tehnologije funkcionišu i bar neki nivo transparentnosti, ključ je u izvornom kodu, koji se drži kao strogo čuvana poslovna tajna. Sve dok ne bude više zahteva za transparentnost koda, odnosno za otvoreni kod invazivnih sistema koji omogućavaju masovni biometrijski nadzor, daleko smo od poželjnog nivoa društvene svesti o opasnostima koje ove tehnologije predstavljaju za ljudska prava i slobode. Čak i ako se ispostavi da je tačna inače sumnjiva tvrdnja kompanije Clearview AI o odsustvu pristrasnosti, to ne bi naročito ublažilo nezamislive razmere kršenja prava kao posledicu njihovih servisa.

ZAKLJUČAK

Na osnovu tehničkih aspekata alata koji se koriste za (masovan) biometrijski nadzor, jasno je da pored mnogih rizika po ljudska prava i slobode, dizajn i upotreba ove tehnologije takođe doprinosi učvršćivanju sistemskih društvenih problema kao što su rasno profilisanje, targetiranje i diskriminacija. Konkretno, mnogi od ovih alata su dizajnirani da izdvoje „Drugog“, odnosno ljude koji se opažaju kao drugačiji od većinske populacije na osnovu izgleda, uverenja ili pravnog/socijalnog statusa. Čini se da je potraga za „prosekom“ ili „normalnošću“ prema fizičkom izgledu, kao što smo mogli da vidimo iz radova Francisa Galtona, samo pojačana „digitizovanim telima“ i sistemima koji su sposobni da brže i više od bilo kog ljudskog bića obrađuju ove podatke, posebno uz razvoj neuronskih mreža. Kako je sistemima mašinskog učenja neophodan beskrajan tok podataka da bi bili trenirani, razvoj skupova sve pristrasnijih podataka i dalje će podsticati probleme do kojih dovodi masovna obrada i klasifikacija biometrijskih podataka.

Ogromne mreže kamera koje pokrivaju čitave gradove i omogućavaju obradu ogromnih količina informacija o izgledu, ponašanju i kretanju ljudi, ne pružaju siguran prostor za proteste ili druge oblike građanske neposlušnosti. Čak će i prosečan građanin koji „nema šta da krije“ i koji „poštuje zakon“ postati „šetajući bar-kod“, spreman za skeniranje pod budnim okom infrastrukture biometrijskog nadzora. Politička previranja širom sveta,[165] i više od decenije globalnog opadanja slobode interneta,[166] takođe pokazuju da kada postoji prilika da se koriste tehnološka sredstva za kontrolu ili ograničavanje političkog govora, protesta i drugih oblika građanskog organizovanja, političke vlasti u autoritarnim režimima, ali i one sa navodno višim stepenom demokratije – neće mnogo oklevati da je iskoriste.

Ove ubrzane naučne i tehnološke promene očekivano su iskoristili privatni akteri sa ogromnim resursima, visokim nivoom društvenog uticaja i praktično bez javne odgovornosti, osim prema svojim akcionarima. Zbog toga je poštovanje ljudskih prava izuzetno opasno prepustiti benevolenciji, hirovima i strategijama odnosa s javnošću moćnih korporacija kao nekakvom „samoregulatornom“ postupku, kao što smo videli na primerima Microsofta i Amazona. Prepoznavanje lica i srodne tehnologije biometrijskog nadzora

su veoma unosno tržište, pa se očekuje da će kompanije koje ih prodaju samo nastaviti da ulažu u njihov razvoj, čini se bez obzira na to kako će se njihovi proizvodi zapravo koristiti.

Tehnologija je gotovo uvek korak ispred zakona koji je obuzdava, bez obzira na to koliko su današnji zakonodavci i predstavnici građana agilni u prepoznavanju njenih negativnih efekata na društvo, pa ni manjina koja razume sve te izazove. Takođe je u pitanju geopolitička pozicija i perspektiva, s obzirom da američke i kineske kompanije prednjače u odnosu na evropske u razvoju prepoznavanja lica i drugih tehnologija koje se koriste za masovni biometrijski nadzor. Dok Evropska unija počinje s primenom još jednog značajnog propisa koji ima za cilj da upravlja našim društvima u digitalnom dobu – zakona o veštačkoj inteligenciji – to neće samo po sebi obezbediti očuvanje vrednosti slobode i lične autonomije. Ako je pritisak na tehnološki vođenu „bezbednost“, javni red i „društveni sklad“ prioritet iznad svega, to bi mogla biti tačka bez povratka kada je u pitanju poštovanje slobode izražavanja i okupljanja, prava na protest, kao i privatnost na našim ulicama, trgovima, parkovima i drugim javnim prostorima.

Primena intruzivnih tehnologija, kao što to jeste prepoznavanje lica, za donošenje odluka koje mogu da izazovu ozbiljne pravne posledice po građane (pogrešna hapšenja ili krivične presude) takođe predstavlja ozbiljan rizik. Prepoznavanje lica „uživo“, odnosno identifikacija ljudi sa nadzornih snimaka obrađenih u realnom vremenu, zaslužuje veliku pažnju, ali i naknadna biometrijska identifikacija ljudi sa snimljenih video materijala nije ništa manje opasna. Slučaj gospodina H. koji je osuđen za provalu u Francuskoj samo na osnovu mašinskog prepoznavanja lica sa snimka sigurnosne kamere, pokazuje kako bi pravne posledice mogle izgledati kada ove tehnologije postanu sveprisutne. Naime, sistem za prepoznavanje lica je suzio potragu na 200 osoba kao potencijalnih osumnjičenih, a policija je izdvojila gospodina H. i optužila ga za zločin, uprkos nedostatku dodatnih dokaza koji bi potvrdili da je on počinilac.[167] Takođe, na zahtev advokata gospodina H. za uvid u informacije o tome kako je sistem došao do predikcije, sud je ocenio da pretežu prava intelektualne svojine provajdera. Ovaj primer služi kao odgovor na pitanje zašto se tehnologija ne može koristiti kao izgovor za odustajanje od pravične zakonske procedure i zašto se ne može dozvoliti da interesi privatnih kompanija pretežu nad pravom na pravično suđenje i pretpostavkom nevinosti.

PRAVO

UVOD

Pravni konteksti u kojima se odvija obrada biometrijskih podataka drastično se razlikuju širom sveta, a praktično svaka jurisdikcija ima svoju definiciju biometrijskih podataka. Zahvaljujući Opštoj uredbi o zaštiti podataka (General Data Protection Regulation, GDPR) i njenom manje poznatom policijskom pandanu, Direktivi o zaštiti podataka u službama za sprovođenje zakona (Data Protection Law Enforcement Directive, LED), Evropska unija se često smatra liderom u usvajanju zakona koji štite biometrijske podatke strogim restrikcijama, a u nekim slučajevima i zabranom njihove upotrebe. To je, međutim, još uvek daleko od savršenog, a ključne tačke kritike tiču se sprovođenja zakona i načelno uskog fokusa na slučajeve upotrebe za svrhe identifikacije. Ekvivalentni propis u Velikoj Britaniji (UK GDPR) nije uspeo da spreči mnoge štetne primene.

Tokom ovog istraživanja, naišli smo na samo dve jurisdikcije u kojima je bilo pokušaja da se konkretno regulišu razvoj, primena ili upotreba prepoznavanja lica i drugih biometrijskih sistema, a ne samo biometrijskih podataka čija obrada leži u osnovi tih sistema: to su SAD i EU. U vreme drugog izdanja ovog istraživanja, na nivou EU već su na snazi i konkretnija pravila o upotrebi biometrijskog nadzora u izuzetno značajnoj Uredbi o veštačkoj inteligenciji (AI Act), koju valja uzeti u obzir pored pravila koja predviđaju GDPR i LED, i eventualno nacionalnih pravila država članica koja moraju biti u skladu sa ovim EU propisima. Kao načelno pravilo, AI Akt predviđa zabranu svih oblika biometrijske identifikacije na daljinu iz javno dostupnih prostora uživo, sem u izuzecima koji su usko deifinisani. Na drugoj strani Atlantika, pojedine savezne države u SAD su usvojile različite nivoe zabrane upotrebe tehnologije za biometrijsku identifikaciju putem prepoznavanja lica – mada samo za određene sektore ili namene, poput policije ili obrazovanja, i često uz izuzetke. Na stolu je nekoliko predloga za zabranu na saveznom nivou, ali nijedan još nije na snazi.

Desetak američkih država koje su odlučile da u nekom obliku regulišu biometrijski nadzor, uglavnom su se ograničile na prepoznavanje lica i time posredno isključile druge vrste biometrije. Pristupi variraju od potpune zabrane, preko moratorijuma (na određeno vreme ili dok se ne donese odgovarajući zakon) do regulatornog okvira koji definiše uslove za dozvoljenu upotrebu.

U državi Vašington je dozvoljena upotreba prepoznavanja lica za pružanje mnogih javnih usluga, a spekuliše se da je takav pristup izdejstvovan iz vrha Microsofta. Zanimljivo je da Vašington zabranjuje prepoznavanje lica prema crtežu ili drugim ručno izrađenim slikama, ali dozvoljava pretragu po sličnosti. Regulativa u Koloradu je slična onoj u Vašingtonu, s tim što je Kolorado formirao i radnu grupu, za koju Vašington nije našao sredstva. Tako izgleda da nivo javne kontrole zavisi od ekonomske računice.

U nekoliko saveznih država SAD primetni su pokušaji da se umanji rizik od zloupotreba. U Virdžiniji, svako ko izvrši nedozvoljenu pretragu za prepoznavanje lica učinio je krivično delo. U Mejnu je uspostavljena obaveza da se obrišu svi dokazi koji su nezakonito prikupljeni. S druge strane, Masačusets je jedna od nekoliko država koje dozvoljavaju da se za pretrage koristi registar motornih vozila. Zahvaljujući ogromnoj količini biometrijskih podataka koje poseduje, ova naizgled obična federalna agencija tako postaje centralna tačka za pretrage za prepoznavanje lica u SAD.

Prilike u SAD govore i da je pogrešno uobičajeno uverenje da je moratorijum prvi korak ka zabrani. Mada se često pretpostavlja da je tako, Virdžinija i Vermont su pokazali da je moratorijum slab mehanizam, lako podložan ukidanju.

U Kanadi je skandal u policiji zbog saaradnje sa zloglasnom kompanijom Clearview AI služio kao katalizator za preko potrebno ažuriranje domaćih zakona o privatnosti; 2021. su, po prvi put, biometrijski podaci tretirani kao osetljivi podaci. Danas ova zemlja razmatra donošenje novog zakona, AIDA, koji će provajdere obavezati da sprovedu samoprocenu da li su njihovi sistemi veštačke inteligencije rizični ili ne. Kao i zakon u američkoj državi Virdžiniji, kanadski predlog definiše krivična dela zloupotrebe – uz predviđene novčane kazne, pa čak i zatvor. Mada kanadska AIDA zauzima pristup zasnovan na riziku, nalik evropskom zakonu o veštačkoj inteligenciji, ne sadrži nikakve zabrane, što otvara pitanje mehanizama kojima će u praksi rešavati biometrijski masovni nadzor.

Latinoameričke zemlje suočene su sa ozbiljnom kritikom zbog načina na koji tretiraju biometriju. Skoro dve trećine biometrijskih primena u ovom regionu nema pravnu osnovu, što se pripisuje opštem nedostatku doslednih i savremenih pravila o zaštiti biometrijskih podataka. Brazil je, na primer, uveo pravo na zaštitu podataka tek 2020. Međutim, u nekoliko zemalja regiona važnu ulogu su odigrali sudski sporovi: jedan argentinski sud je proglasio neustavnim sistem za prepoznavanje lica begunaca, a meksički

vrhovni sud je istu odluku doneo u slučaju nacionalnog biometrijskog registra korisnika mobilnih telefona. Argentinski sud je takođe prepoznao privatnost i zaštitu podataka kao kolektivna prava, što vredi izdvojiti jer druge jurisdikcije koje smo razmatrali u ovoj knjizi, priznaju ta prava samo u krajnje individualnom smislu.

Indija i Kina se često navode kao ekstremni primeri biometrijskog masovnog nadzora. U Indiji je zakonodavstvo uglavnom fokusirano na mogućnosti za primenu, umesto na zaštitne mere, a već ima dokaza o kršenju prava u nekoliko slučajeva primene u policiji. Takođe, ova zemlja ima najveći program biometrijske identifikacije na svetu, koji je vremenom postao nužan uslov za otvaranje bankovnog računa ili sklapanje ugovora za telefonske usluge. U Kini, policija Pekinga se hvali sa stopostotnom pokrivenošću grada nadzornim kamerama, dok dronovi u Sinđangu stižu i tamo gde kamere za video nadzor ne mogu. Možda najozloglašenija upotreba prepoznavanja lica u Kini jeste ona koja služi za masovno zatvaranje Ujgura. Poslednjih godina je usvojeno nekoliko zakona koji načelno regulišu zaštitu ličnih podataka, uz regulativu koja se posebno fokusira na upotrebu tehnologije za prepoznavanje lica. Mada se čini da se uglavnom bavi upotrebom u privatnom sektoru, novija sudska praksa u vezi sa prepoznavanjem lica priznaje prava građana na zaštitu ličnih podataka.

Drugo ključno pitanje u ovom poglavlju jeste uloga standarda tehničke tačnosti u regulisanju primene tehnologije za prepoznavanje lica. Američka država Virdžinija je propisala da sistemi moraju postići stopu od 98% stvarno pozitivnih rezultata, dok je Indija taj prag postavila na 80%. Međutim, bez uvida u to koliko lažno pozitivnih rezultata sistem generiše, ova ograničenja su praktično besmislena.

AUSTRALIJA

Koja vrsta pravnog akta reguliše obradu biometrijskih podataka?

- **Zakon o zaštiti podataka**
  Da, australijski Zakon o privatnosti (1988).
- **Propisi na lokalnom nivou**
  Da, na nivou saveznih država i samouprava.

Definicija i regulativa prepoznavanja lica

- **Podaci prikupljeni kroz prepoznavanje lica definišu se kao biometrijski podaci.**

Detalji

- **Definisani slučajevi posebne upotrebe**
  - Osetljivi podaci, uključujući biometrijske, mogu se prikupljati samo ako postoji pravni osnov za obradu ili ako prikupljanje informacija nalaže ili dozvoljava australijski zakon ili odluka suda/tribunala.
  - Služba za sprovođenje zakona može da prikuplja osetljive podatke ako postoji razumno uverenje da je prikupljanje neophodno za obavljanje, ili je u direktnoj vezi sa obavljanjem jedne ili više funkcija ili aktivnosti službe.
- **Definisane posebne vlasti**
  - Da. Australijski poverenik za informacije služi kao nadzorni organ koji daje mišljenja i smernice, i odgovoran je za rešavanje pritužbi; ima mandat da sprovodi istrage i određuje novčane kazne.

AUSTRALIJA

KONTEKST

Upotreba prepoznavanja lica i drugih vrsta biometrijske tehnologije u australijskim službama za sprovođenje zakona predmet je intenzivne debate između zagovornika ljudskih prava, s jedne, i predstavnika službi s druge strane. Još uvek ne postoji savezni zakon koji bi na sveobuhvatan način regulisao upotrebu prepoznavanja lica i drugih oblika biometrijskog nadzora. Međutim, Australija ima Zakon o privatnosti kao opšti zakon o zaštiti podataka, uključujući regulisanje upotrebe biometrijskih podataka na širem nivou. Ipak, čini se da je upotreba prepoznavanja lica u radu policije veoma prisutna u praksi.[168]

Još 2014. pokrenuta je inicijativa za stvaranje jedinstvene nacionalne baze podataka koja bi sadržala sve fotografije iz baza za pasoše i vozačke dozvole, pod nazivom Nacionalni kapaciteti za biometrijsko uparivanje lica (National Facial Biometric Matching Capability, NFBMC; skraćeno „Kapaciteti“), koja bi se koristila za različite svrhe uparivanja lica.[169] Inicijativa je formalizovana 2017. kada su čelnici svih saveznih država i teritorija potpisali međuvladin sporazum o uslugama uparivanja identiteta, koji je trebalo da postane u potpunosti operativan kada se uspostavi odgovarajući zakonodavni okvir, na saveznom i na nivou država.[170]

Baza podataka kapaciteta popunjava se određenim podacima u državama Kvinslend, Južna Australija, Zapadna Australija, Viktorija i Tasmanija, pošto su te države usvojile zakone koji omogućavaju prikupljanje podataka od različitih državnih organa.[171] Čak i kada bi sve države donele lokalne zakone koji bi omogućili prikupljanje podataka u punom obimu, kako je predviđeno međuvladinim sporazumom, razmena

podataka između država, kao i saveznih agencija, i dalje bi morala da sačeka usvajanje federalne regulative koja bi omogućila takvo deljenje podataka za svrhe prepoznavanja lica.[172]

Zakonodavni napori na saveznom nivou su propali 2019. kada je Predlog zakona o uslugama uparivanja identiteta upućen u parlament.[173] Svrha Predloga bila je da ovlasti Komonvelt (saveznu vladu) da omogući razmenu identifikacionih informacija, uključujući slike lica, između Komonvelta, država i teritorija u svrhu uparivanja identiteta.[174] Međutim, ovu verziju Predloga zakona odbacio je združeni parlamentarni komitet za obaveštajne poslove i bezbednost (Parliamentary Joint Committee on Intelligence and Security, PJCHR), koji je utvrdio da se Predlog mora preraditi tako da režim uparivanja identiteta bude utemeljen na privatnosti i transparentnosti, kao i da podleže razvijenim zaštitnim merama.[175] Prerađena verzija dosad nije dostavljena parlamentu, ali takođe nema potvrde da je vlada odustala od ovog zakona.[176] Kancelarija australijskog poverenika za informacije (Office of the Australian Information Commissioner, OAIC) biće zadužena za pripremu procene uticaja na privatnost u vezi sa Kapacitetima. Prema informacijama sa sajta Poverenika, priprema ove procene kasni usled kašnjenja sa usvajanjem Predloga zakona o uslugama uparivanja identiteta, što bi mogla biti indicija da će vlada predložiti novu verziju zakona.[177]

U decembru 2024. godine donet je savezni zakon koji reguliše usluge identiteta u onlajn transakcijama sa državnim organima.[178] Ovaj zakon je kritikovan kao preuranjen jer reguliše upotrebu tehnologije koja se zasniva na osetljvim biometrijskim podacima građana u trenutku kada sama materija zaštite podataka o ličnosti nije regulisana na zadovoljavajuć način (savezni zakon o zaštiti podataka o ličnosti donet je 1988. godine).[179]

Iako još uvek ne postoji zakonski okvir koji reguliše upotrebu prepoznavanja lica u službama za sprovođenje zakona, tehnologija se ipak koristi već neko vreme.

Prema izjavi portparola policije Novog Južnog Velsa, ova služba koristi tehnologiju prepoznavanja lica od 2004. godine za utvrđivanje i proveru identiteta osoba od interesa u istražne svrhe.[180] Ova policijska služba daje neke informacije o toj praksi na svojoj veb stranici, pozivajući se na Zakon o privatnosti i lokalni Zakon o privatnosti i ličnim podacima iz 1998, kao regulatorni okvir za svoju upotrebu prepoznavanja lica. Takođe su javno obznanili probne projekte prepoznavanja lica, koji su naišli na negodovanje stanovništva jer su nosili značajne rizike po privatnost usled nedostatka odgovarajućih pravnih mera zaštite.[181]

Policija Južne Australije takođe je iznosila informacije o upotrebi prepoznavanja lica, tvrdeći da ne postoji zakonsko ograničenje za upotrebu ove tehnologije u Južnoj Australiji za istražne svrhe.[182]

Ima naznaka da je prepoznavanje lica možda korišćeno na demonstrancijama,[183] kao i da ga je policija tokom pandemije kovida-19 koristila u probnom režimu, kao podršku merama karantina.[184] U privatnom sektoru, kamere za prepoznavanje lica koriste se u supermarketima, pod izgovorom da tehnologija služi za identifikaciju osoba od interesa koje su ranije učestvovale u incidentima,[185] ili za bolje razumevanje i unapređenje iskustva kupaca putem anketa preko tableta koji su snimali „otiske“ lica (slike snimljene kamerom na tabletu konvertovane su u algoritamske otiske lica, „faceprints“).[186] Nekoliko takvih primera detaljnije je opisano u poglavlju ove knjige posvećenom praksi.

Prepoznavanje lica takođe je izazvalo pažnju javnosti 2020, kada su Poverenik za informacije (ICO) Ujedinjenog Kraljevstva i australijski OAIC pokrenuli zajedničku istragu o rukovanju kompanije Clearview AI ličnim podacima, koncentrišući se na upotrebu biometrijskih i skrejpovanih podataka.[187] Kako ćemo dodatno objasniti u odeljku o australijskoj sudskoj praksi, ova istraga je rezultirala nalazom australijskog Poverenika da je Clearview AI prekršio nacionalne zakone o privatnosti i naredbom da prestane sa prikupljanjem slika Australijanaca, kao i da izbriše postojeće fotografije Australijanaca iz svoje baze. Takođe, u oktobru 2023. godine policijski službenici su pred Senatom dali izjavu da je u deset identifikovanih slučajeva policija neovlašćeno koristila servise PimEyes and FaceCheck u operativne svrhe, uz napomenu da preduzimaju mere da se takve sporadične i neovlašćene upotrebe ovakvih servisa više ne događaju u praksi.[188]

U svom izveštaju 2021. godine, australijski komitet za ljudska prava preporučio je zakonsku reformu kako bi se obezbedila bolja zaštita ljudskih prava i privatnosti s obzirom na razvoj i upotrebu biometrijskih tehnologija, kao i moratorijum na upotrebu biometrijskih sistema u donošenju odluka visokog rizika dok se ne usvoji odgovarajuća pravna zaštita.[189]

Akademska zajednica je pokrenula nekoliko inicijativa za izradu modela zakona u kom bi regulisanje upotrebe prepoznavanja lica bilo usklađenije sa standardima ljudskih prava.[190]

PRAVNI OKVIR

Australija je potpisnica Međunarodnog pakta o građanskim i političkim pravima (International Covenant on Civil and Political Rights, ICCPR),[191] ali ne postoji savezna povelja ili povelja o pravima (u okviru Ustava ili u drugom obliku) koja bi regulisala privatnost kao ljudsko pravo.[192]

Australijski Zakon o privatnosti usvojen je krajem 1988, da bi stupio na snagu naredne godine. Kasnije je menjan nekoliko puta,[193] dok su poslednje izmene unete 2022.[194] Zakon o privatnosti pokriva službe australijske vlade i sve organizacije sa godišnjim prometom od preko tri miliona austrijskih dolara, kao i druge organizacije pod posebnim uslovima predviđenim zakonom (npr. u zavisnosti od sektora u kojem posluju). Zakon je strukturiran tako da reguliše neka specifična pitanja, uključujući opšte obaveze relevantnih aktera i pravila za rad Poverenika. Na kraju teksta Zakona, u Prilogu 1 izloženo je 13 principa (Australijski principi privatnosti, APP). Ovi principi su veoma slični principima izloženim u članu 5 evropskog GDPR-a i pružaju pravila relevantna za svaku obradu ličnih podataka. Međutim, australijski principi su detaljniji i praktičniji od svog pandana iz GDPR-a.

Prepoznavanje lica se ne pominje posebno, niti su šabloni za prepoznavanje lica izričito navedeni u Zakonu. Međutim, uređuju se biometrijski šabloni i biometrijske informacije koje će se koristiti u svrhu automatske biometrijske verifikacije ili biometrijske identifikacije – gde se i jedno i drugo smatra vrstom osetljivih informacija. Prema tumačenju Poverenika, biometrijske informacije obuhvataju i karakteristike lica.[195]

Pravila o prikupljanju i obradi osetljivih informacija prilično su uopštena.

Prema 3. principu Zakona o privatnosti, koji reguliše prikupljanje podataka, osetljive informacije se mogu prikupljati samo ako za to postoji relevantni pravni osnov.

Nijedna državna služba ne sme da prikuplja osetljive informacije o ljudima osim ako (1) osoba ne pristane na prikupljanje informacija[196] i (2) ako su informacije razumno neophodne ili direktno povezane sa jednom ili više funkcija ili aktivnosti službe. Prema definicijama iz Zakona o privatnosti, pristanak može značiti izričiti ili implicitni pristanak.[197]

Zakon o privatnosti navodi nekoliko drugih situacija u kojima bi prikupljanje osetljivih informacija bilo dozvoljeno, čak i kada uslovi (1) i (2) nisu ispunjeni. Jedna takva situacija jeste kada je prikupljanje informacija potrebno ili odobreno australijskim zakonom ili nalogom suda/tribunala.[198] Kako je već rečeno, trenutno ne postoji nijedan drugi takav zakon koji dozvoljava ili zahteva takvu obradu.

Za organe za sprovođenje zakona važi posebno pravilo. Prikupljanje osetljivih informacija je dozvoljeno ako organ za sprovođenje ima „razumno uverenje“ da je prikupljanje takvih informacija razumno neophodno za, ili je direktno povezano sa jednom ili više funkcija ili aktivnosti organa.[199] Standard „razumnog uverenja“ je ono po čemu se organi za sprovođenje zakona razlikuju od drugih regulisanih subjekata, uključujući i druge državne službe. Međutim, tako širok izuzetak podstiče zabrinutost da bi prekomerna upotreba prepoznavanja lica i drugih vrsta biometrijskog nadzora u službama za sprovođenje zakona povećalo rizik od masovnog nadzora, uz rizike i za druga ljudska prava.[200]

Prema informacijama dostupnim na sajtu australijskog Poverenika, nisu date smernice u vezi sa prepoznavanjem lica niti sa obradom biometrijskih informacija.

PRAVNA PRAKSA

U očekivanju formalnog uvođenja Kapaciteta, nekoliko australijskih službi za sprovođenje zakona (uključujući australijsku federalnu policiju i policije Viktorije i Kvinslenda) počelo je da koristi bazu podataka Clearview AI u okviru svojih postojećih sistema za prepoznavanje lica. Vlada je prvo negirala da koristi usluge ove kompanije, ali početkom 2020. podaci o klijentima koji su procurili iz Clearview AI otkrili su da je osoblje australijske policije zapravo koristilo ovu uslugu, verovatno na neformalan način.

Kao odgovor na ovo i druga potencijalna kršenja, u julu 2020. australijski Poverenik i britanski ICO pokrenuli su zajedničku istragu o kompaniji Clearview AI.[201]

Istraga je završena naredne godine, u oktobru 2021,[202] a utvrđeno je da je Clearview AI prekršio australijski Zakon o privatnosti.[203] Prema nalazima australijskog Poverenika, kršenja su obuhvatala: (1) prikupljanje osetljivih informacija Australijanaca bez pristanka; (2) prikupljanje ličnih podataka na nepošten način; (3) nepreduzimanje razumnih koraka da se građani obaveste o prikupljanju ličnih podataka; (4) nepreduzimanje razumnih

koraka da se utvrdi da su lični podaci koji su otkriveni tačni, s obzirom na svrhu otkrivanja; i (5) nepreduzimanje koraka da se obezbedi usklađenost sa australijskim principima privatnosti primenom odgovarajućih praksi, procedura i sistema.[204]

Australijski Poverenik je naredio kompaniji Clearview AI da „prestane da prikuplja slike lica i biometrijske šablone od osoba u Australiji i da uništi postojeće slike i šablone prikupljene iz Australije".[205] Međutim, novčane kazne nisu izrečene.[206]

Kasnije te godine, u novembru 2021, Poverenik je doneo još jednu odluku kojom se utvrđuje da australijska federalna policija nije poštovala svoje obaveze u pogledu privatnosti prilikom korišćenja alata Clearview AI za prepoznavanje lica.[207] Do kršenja je došlo (1) propustom da se sprovede procena uticaja na privatnost za projekat visokog rizika u vezi sa privatnošću i (2) postupanjem u suprotnosti sa zahtevom da se preduzmu razumni koraci za sprovođenje praksi, procedura i sistema koji se odnose na funkcije ili aktivnosti subjekta, u skladu sa australijskim principom privatnosti 1.2.

Ovom odlukom Poverenik je naložio federalnoj policiji da angažuje nezavisnu procenu za reviziju i informisanje Povereника o ostalim nedostacima u praksi, procedurama, sistemima i programima obuke u federalnoj policiji, u odnosu na procene uticaja na privatnost, kao i da sprovede sve neophodne preporuke iz izveštaja, te da relevantno policijsko osoblje uputi na ažurirani program obuke o privatnosti.[208]

Nakon odluke iz 2021. godine, pojavili su se navodi u medijima da uprkos naloženim merama policija nije prestala u potpunosti da koristi Clearview AI alat.[209] Ipak, Poverenik je u avgustu 2024. saopštio da u trenutnim okolnostima neće preduzimati dalju istragu protiv ove kompanije.[210]

EVROPSKA UNIJA

KONTEKST

Među privatnim i javnim akterima u Evropskoj uniji sve je rasprostranjenija primena rešenja „pametnog nadzora“, uključujući tehnologije daljinske biometrijske identifikacije (Remote Biometric Identification, RBI)[211] koje su povezane sa praksama masovnog nadzora.[212] Dok je aktuelna primena RBI tehnologija u EU još uvek prvenstveno eksperimentalna i lokalizovana, postoji zabrinjavajući napredak u dve oblasti: prvo, tekuća izrada i nadogradnja baza biometrijskih podataka koje se koriste u građanskim i krivičnim registrima, a koje su u osnovi sistema za prepoznavanje i uživo i retrospektivno; drugo, česta testiranja sistema živog prenosa, povezanih sa daljinskim algoritmima za pretragu i prepoznavanje lica i biometrijskih informacija.

Biometrija je ključni element u politici upravljanja granicama u EU, budući da je implementirana u vize, pasoše i lične karte. Agencija odgovorna za granične i migracione sisteme EU, eu-LISA, danas upravlja informacionim sistemima koji sadrže više od 53 miliona biometrijskih podataka.[213] To su sistemi VIS, SIS I II, Eurodac, ECRIS, ETIAS i EES.[214] Eu-LISA takođe upravlja sistemom za automatizovanu identifikaciju otisaka prstiju (Automated Fingerprint Identification System, AFIS), za koji se u budućnosti očekuje da obuhvati i prepoznavanje lica.[215]

Evropska komisija je predložila ažuriranje Uredbe o automatizovanoj razmeni podataka za policijsku saradnju – predlog poznat kao „Prum II“ – sa ciljem da se unapredi mreža za razmenu podataka među državama članicama. Predloženo proširenje obuhvata slike ljudskih lica i, opciono, „policijske evidencije“. Međutim, javlja se zabrinutost u vezi sa potencijalnim

prekoračenjem i masovnim nadzorom, jer može tretirati značajan deo stanovništva kao potencijalne kriminalce i predstavljati rizik po privatnost i zaštitu podataka.[216] Pojačane policijske i nadzorne mere u predlogu pravdaju se principom slobodnog kretanja ljudi.

Zakonska pravila za sprovođenje biometrijskog nadzora na javnim površinama najpre su bila regulisana u sekundarnom zakonodavstvu Evropske unije o zaštiti podataka, uključujući Opštu uredbu o zaštiti podataka (General Data Protection Regulation, GDPR) i Direktivu o zaštiti podataka u službama za sprovođenje zakona (Data Protection Law Enforcement Directive, LED). U slučajevima upotrebe biometrijskih podataka, ovi propisi zahtevaju pažljivo razmatranje načina zaštite osnovnih prava. GDPR i LED su značajni jer načelno postavljaju visoke standarde za zaštitu ličnih podataka u EU. Ali ovi propisi ne zadiru uvek dovoljno duboko. Stručnjaci i aktivisti tvrde da su GDPR i LED nedovoljno precizno napisani, što potencijalno otvara pravne praznine, te da sadrže „izuzetke i pravila koji su naklonjeni državi, a malo ili nimalo značajnih prepreka konkretnim nadzornim tehnologijama".[217]

Uredba o veštačkoj inteligenciji (AI Act)[218] dala je važne načelne odgovore na pitanja upotrebe tehnologije za prepoznavanje lica (ili drugih vrsta daljinske biometrijske identifikacije) u javnim prostorima, i u realnom vremenu i u retroaktivnoj primeni. Rešenjima koja su prihvaćena u konačnom tektu ovog propisa prethodile su oštre debate o tome koje tehnologije i pod kojim uslovima moraju biti zabranjene, a koje izuzetno treba dozvoliti.

U oktobru 2022, Evropski parlament je usvojio neobavezujuću rezoluciju kojom se traži uvođenje moratorijuma (vremenski ograničene zabrane) na policijsku upotrebu tehnologije prepoznavanja lica na javnim mestima, prediktivni policijski rad, prakse biometrijskog masovnog nadzora i zabranu korišćenja privatnih baza podataka za prepoznavanje lica.[219] U tom kontekstu, mnoge međunarodne organizacije i institucije pozivaju na zabranu različitih praksi biometrijskog nadzora, posebno prepoznavanja lica na javno dostupnim mestima. Među njima su Ujedinjene nacije,[220] Evropski parlament,[221] Evropski odbor za zaštitu podataka (European Data Protection Board, EDPB) i Evropski supervizor za zaštitu podataka (European Data Protection Supervisor, EDPS),[222] kao i više od 170 nevladinih organizacija.[223]

Najznačajnija inicijativa civilnog društva u Evropi za zabranu upotrebe biometrijskih sistema za masovni nadzor, bila je kampanja „Reclaim Your Face".[224] Više od 260.000 ljudi podržalo je kampanju koju vodi široka koalicija organizacija civilnog društva, što je posledično uticalo i na razvoj događaja u procesu usvajanja EU zakona o veštačkoj inteligenciji.

Što se tiče odnosa država članica EU prema biometrijskim tehnologijama, vidimo različite pristupe. Italija prednjači kao prva zemlja u Evropi koja je uvela moratorijum na prepoznavanje lica u javnom prostoru.[225] Nemačka koaliciona vlada je pozvala na zabranu ovih praksi širom EU.[226] U Portugalu je predlog zakona predviđao legalizaciju nekih praksi biometrijskog masovnog nadzora – ali se od njega u međuvremenu odustalo.[227]

S druge strane, francuski zakonodavci intenzivno raspravljaju o implementaciji pravnog okvira koji bi omogućio primenu dve različite tehnologije za prepoznavanje lica, a koje navodno unapređuju bezbednost na velikim javnim događajima, s posebnim fokusom na Olimpijske i Paraolimpijske igre u Parizu 2024. Nakon snažnog protivljenja javnosti, posebno evropskih grupa civilnog društva, francuska vlada je na kraju odbila korišćenje prepoznavanja lica tokom Olimpijade u Parizu.[228]

Međutim, francuski parlament je odobrio zakon o Olimpijskim i Paraolimpijskim igrama koji omogućava automatizovano nadgledanje javnih prostora zbog „sumnjivog ponašanja". Prema odredbama zakona, živi video prenos sa dronova i na hiljade CCTV kamera moguće je analizirati, navodno da bi se identifikovale napuštene torbe i nadgledalo ponašanje u gužvi, kao i da bi se prijavilo svako „nenormalno" ponašanje.

U tekstu zakona nije definisano šta tačno znači „nenormalno" već se to prepušta budućim vladinim uredbama. Kada su pojedini poslanici zatražili primere, vlada je izbegavala direktan odgovor. Poslanička grupa Zeleni/EFA u Evropskom parlamentu nazvala je francuski zakon „prvim uvođenjem biometrijskog masovnog nadzora javnih prostora u Evropi".[229] Potez je osudio 41 poslanik Evropskog parlamenta, iz pet od sedam panevropskih političkih grupacija.[230]

Još jedan udarac zadala je nemačka koaliciona vlada koja je odustala od posvećenosti zabrani biometrijskog masovnog nadzora kada se suočila sa protivljenjem drugih država članica EU.[231]

PRAVNI OKVIR

Evropsku konvenciju o ljudskim pravima (EKLJP) potpisalo je 1950. svih 47 država članica Saveta Evrope. Konvencijom su uspostavljene jasne obaveze država da štite i poštuju ljudska prava, kao i da ustanove mehanizam za njihovo sprovođenje. Evropski sud za ljudska prava odgovoran je za tumačenje EKLJP. U smislu značenja i obima prava koja štiti, Povelja EU o osnovnim pravima pruža zaštitu ekvivalentnu Konvenciji na nivou Evropske unije. Tumači je Sud pravde EU.

Član 7 Povelje EU i član 8 EKLJP garantuju svakoj osobi pravo na poštovanje njenog privatnog i porodičnog života, doma i komunikacije. Povelja štiti individualno pravo na zaštitu podataka o ličnosti u članu 8.

Pravni okvir koji pokriva bilo koje biometrijske tehnologije može se naći u podzakonskim aktima EU koji regulišu zaštitu podataka. Principi zaštite ličnih podataka razjašnjeni su u Opštoj uredbi o zaštiti podataka,[232] koja je primenjiva u svim slučajevima obrade ličnih podataka, sa izuzecima koji obuhvataju aktivnosti sprovođenja zakona, kada se primenjuje Direktiva o zaštiti podataka u službama za sprovođenje zakona (LED).[233] Kao uredba, GDPR je direktno primenjiv u svim državama članicama EU, dok se LED mora transponovati u zakon svake države članice.

U aprilu 2024. godine, Evropski parlament usvojio je Uredbu o veštačkoj inteligenciji (EU AI Act) za stvaranje harmonizovanog pravnog okvira u vezi sa korišćenjem sistema zasnovanih na veštačkoj inteligenciji u celom bloku. Taj pravni akt daje direktne odgovore i na neka pitanja dozvoljenosti upotrebe tehnologije za prepoznavanje lica u policiji.

GDPR i LED

Dva ključna propisa u ovom kontekstu definišu biometrijske podatke na isti način, navodeći da su to „lični podaci koji su dobijeni posebnom tehničkom obradom u vezi sa fizičkim, fiziološkim ili karakteristikama ponašanja određene osobe, koji omogućavaju ili potvrđuju jedinstvenu identifikaciju te osobe, kao što su slike lica ili daktiloskopski podaci".[234] Možemo razlikovati dve kategorije informacija koje se prepoznaju kao biometrijski podaci:

- „fizičke/fiziološke karakteristike" fokusirane na telesne karakteristike kao što su analiza slike otiska prsta, prepoznavanje irisa u oku, prepoznavanje lica, prepoznavanje oblika uha i tako dalje; i
- „karakteristike ponašanja" kao što je verifikacija rukom pisanog potpisa, analiza pritiska na taster ili analiza hoda (stila hodanja).[235]

Takođe, kada se biometrijski podaci obrađuju u svrhe jedinstvene identifikacije osobe, i GDPR i LED ih svrstavaju u posebnu kategoriju ličnih podataka, koji su poznati i kao „osetljivi podaci" – a kojima je dodeljen viši nivo zaštite.[236] Važno je napomenuti da su biometrijski podaci svrstani u tu kategoriju na osnovu njihove inherentne osetljivosti, dakle, ne moraju da otkrivaju druge osetljive informacije u vezi sa konkretnom osobom (kao što su zdravstveni podaci, rasno poreklo ili seksualna orijentacija) da bi se smatrali osetljivim.

Međutim, GDPR i LED se razlikuju u pristupu obradi tih posebnih kategorija. GDPR zabranjuje ovu obradu (član 9), ali utvrđuje deset izuzetaka od zabrane, uključujući izričit pristanak osobe na koju se podaci odnose, obradu neophodnu za zaštitu vitalnih interesa osobe na koju se podaci odnose i obradu neophodnu za uspostavljanje, ostvarivanje ili odbranu pravnih zahteva. Takođe omogućava državama članicama da propišu dodatne uslove u vezi sa obradom biometrijskih podataka, naročito u cilju nametanja strožih pravila za njihovu upotrebu (član 9(4)).

Nasuprot tome, LED dozvoljava obradu posebnih kategorija „tamo gde je to strogo neophodno" (član 10), uz odgovarajuće mere zaštite, i samo u tri svrhe: kada je to dozvoljeno zakonom Unije ili države članice; da zaštiti vitalne interese osobe; ili kada se takva obrada odnosi na podatke koje je jasno učinila javnim osoba na koju se podaci odnose. Dakle, LED se razlikuje od GDPR-a po tome što ne polazi od pretpostavke zabrane.

Slučajevi automatskog donošenja odluka i profilisanja, odnosno kada automatizovani sistemi koriste lične podatke za odlučivanje ili zaključivanje, postali su uobičajena praksa u EU, pored obrade biometrijskih podataka. Na primer, agencije za zaštitu podataka u Francuskoj, Švedskoj i Bugarskoj zabranjuju upotrebu sistema za automatizovano prepoznavanje lica u školama radi provere prisustva i dozvolu pristupa.[237] GDPR i LED definišu profilisanje kao automatizovanu obradu radi procene ličnih aspekata osobe.

LED zabranjuje automatizovano donošenje odluka, osim sa ovlašćenjem zakona EU ili države članice (član 11) i uz obavezu zaštitnih mera u pogledu

prava i slobode osobe na koju se podaci odnose – sa posebnim naglaskom na pravo na ljudsku intervenciju. Član 11(3) LED-a predviđa bezuslovnu zabranu sprovođenja profilisanja koje ima diskriminatorne posledice na osobe, na osnovu njihovih osetljivih podataka (uključujući biometrijske podatke) prema zakonu EU.

Osobama na koje se podaci odnose GDPR štiti „pravo da ne budu predmet odluke zasnovane isključivo na automatizovanoj obradi", uključujući profilisanje (član 22(1)). To znači da delimično automatizovane odluke nisu obuhvaćene ovim pravom, koje se često naziva principom „čovek u petlji" (human-in-the-loop). Međutim, postoje i tri izuzetka u kojima se ovo pravo ne primenjuje: zaključivanje ugovora, kada se obrada vrši na osnovu zakona ili uz pristanak.

Istovremeno, član 22(4) zabranjuje automatsko donošenje odluka na osnovu posebnih kategorija ličnih podataka (kao što su podaci o rodu ili etničkoj pripadnosti, ili biometrijski podaci) u ovim izuzecima, osim ako osoba na koju se podaci odnose ne da svoj izričit pristanak ili je obrada neophodna iz razloga od suštinskog javnog interesa. GDPR ne zabranjuje automatsko donošenje odluka i profilisanje kao takve, već postavlja uslove za upotrebu, posebno kada je reč o podacima iz kategorije osetljivih. Uredba takođe insistira na transparentnosti u pogledu automatske obrade ličnih podataka: osoba na koju se podaci odnose mora da bude informisana o logici i posledicama takve obrade.

Dodatna kontrola je neophodna za „sistematsko nadgledanje": GDPR zahteva procenu uticaja na zaštitu podataka (DPIA) u slučaju „sistematskog nadgledanja javno dostupnih prostora u velikom obimu" (član 35(3)(c)) i utvrđuje obavezu imenovanja službenika za zaštitu podataka ako obrada „po svojoj prirodi podrazumeva redovno i sistematsko nadgledanje osoba na koje se podaci odnose u velikom obimu". To je od ključnog značaja za pitanje biometrijskog nadzora jer ova definicija podrazumeva upotrebu biometrijskih tehnologija, poput prepoznavanja lica, prilikom nadgledanja i praćenja pojedinaca u javnim prostorima. Procene uticaja takođe su potrebne u slučaju automatizovanog profilisanja (član 35(3)(a)) i kada se obrađuju podaci iz kategorije osetljivih (član 35(3)(b)).

GDPR i LED takođe predviđaju organe za zaštitu podataka, nezavisna javna tela koja nadgledaju primenu zakona. Ova tela imaju istražna i korektivna ovlašćenja, pružaju stručne savete o pitanjima zaštite podataka i rešavaju žalbe u vezi sa kršenjem GDPR-a i relevantnih nacionalnih zakona, uključujući i one u okviru LED-a.

EU AI Akt

Uredba EU o veštačkoj inteligenciji[238] postavlja različita pravila na osnovu tri kategorije rizika koje sistemi veštačke inteligencije mogu stvoriti: 1) neprihvatljiv rizik – upotreba AI sistema je zabranjena; 2) visok rizik – takav sistem veštačke inteligencije podleže dodatnim obavezama i procenama; 3) nizak ili minimalan rizik – nema dodatnih ograničenja, sa izuzetkom ograničenih zahteva za transparentnost u ograničenim slučajevima. Procena uticaja pokazuje da bi većina sistema na komercijalnom tržištu spadala u treću kategoriju.

U članu 3(41) AI Akt definiše sistem za daljinsku biometrijsku identifikaciju (Remote Biometric Identification, RBI) kao „sistem veštačke inteligencije namenjen identifikaciji fizičkih lica, bez njihovog aktivnog učešća, obično na daljinu kroz poređenje biometrijskih podataka osobe sa biometrijskim podacima sadržanim u referentnoj bazi podataka". U svojim definicijama i odredbama, AI Akt razlikuje sisteme daljinske biometrijske identifikacije „u realnom vremenu" i „naknadno".

Poslednja verzija nacrta uredbe, pre teksta koji je usvojen u toku trijaloga, klasifikovala je korišćenje RBI sistema u realnom vremenu kao zabranjene, ali uz određene izuzetke, dok je korišćenje RBI sistema za naknadnu identifikaciju svrstano u kategoriju viskorizičnih sistema.

U svojim mišljenjima o predlogu ovakvih rešenja u fazi pregovora, EDPB i EDPS, najviši organi EU za zaštitu podataka, zajedno sa brojnim organizacijama civilnog društva, izrazili su zabrinutost u pogledu načina na koji predložena uredba o veštačkoj inteligenciji reguliše biometrijsku identifikaciju u javno dostupnim prostorima. U svom zajedničkom mišljenju, EDPB i EDPS su pozvali na „opštu zabranu bilo kakve upotrebe veštačke inteligencije za automatsko prepoznavanje ljudskih karakteristika u javno dostupnim prostorima, kao što su prepoznavanje lica, hoda, otisaka prstiju, DNK, glasa, pritiska na tastere i drugih biometrijskih ili bihevioralnih signala, u bilo kom kontekstu", što je bio znatno restriktivniji pristup od onog u konačno usvojenom tekstu.[239]

Savet EU je u decembru 2022. usaglasio svoj opšti pristup (stav Saveta za buduće pregovore sa Parlamentom) kojim je izrazio još veću popustljivost

za RBI od prvobitnog nacrta. U obrazloženju, Savet je dodatno razjasnio ciljeve za koje bi se smatralo da je takva upotreba striktno neophodna u svrhe sprovođenja zakona.[240] Međutim, u maju 2023, odbori za unutrašnje tržište i građanske slobode Evropskog parlamenta, dve radne grupe nadležne za stav Parlamenta, izglasali su zabranu AI sistema koji se koriste za biometrijski nadzor, prepoznavanje emocija i prediktivni policijski rad.[241] Poslanici EP su uneli značajne izmene na listu zabranjenih upotreba AI sistema koja, prema njihovom privremenom stavu, uključuje:

- daljinske biometrijske sisteme identifikacije u „realnom vremenu“ u javno dostupnim prostorima;
- „naknadne“ (retrospektivne) daljinske biometrijske sisteme identifikacije, sa jedinim izuzetkom organa za sprovođenje zakona za krivično gonjenje teških zločina i samo nakon sudskog odobrenja;
- sisteme biometrijske kategorizacije koji koriste osetljive karakteristike (npr. rod, rasa, etnička pripadnost, status državljanstva, religija, politička orijentacija);
- prediktivne policijske sisteme (zasnovane na profilisanju, lokaciji ili prethodnom kriminalnom ponašanju);
- sisteme za prepoznavanje emocija u okviru rada službi za sprovođenje zakona i upravljanje granicama, na radnom mestu i u obrazovnim institucijama; i
- neselektivno skrejpovanje biometrijskih podataka sa društvenih mreža ili CCTV snimaka radi kreiranja baze podataka za prepoznavanje lica.

Na plenarnoj sednici u junu 2023. Evropski parlament je izglasao ove zaštitne mere i uneo ih u svoj zvaničan stav o predloženom zakonu o veštačkoj inteligenciji.[242] Posle glasanja, otvoren je trijalog između Evropskog parlamenta, Komisije i država članica za konačno usaglašavanje teksta.

Iz perspektive zabrane biometrijskog masovnog nadzora, civilno društvo je ovakav rezultat glasanja u tom trenutku nazvalo „ogromnom pobedom za osnovna prava“, uz napomenu da u predloženom tekstu zakona nema adekvatne zaštite prava migranata od diskriminatorne prakse nadzora – budući da nisu utvrđene mere koje bi se bavile upotrebom AI u nezakonitom potiskivanju migranata i diskriminatornom profilisanju na granici EU, a još uvek sadrži i druge probleme.[243] Ipak, nisu svi predlozi Evropskog parlamenta konačno usvojeni tokom trijaloga.

U konačnom tekstu uredbe o veštačkoj inteligenciji, upotreba sistema u realnom vremenu na javno dostupnim mestima u svrhu sprovođenja zakona, stavljena je načelno na listu zabranjenih AI praksi u Evropi, ali uz sledeća tri izuzetka:

- ciljana potraga za konkretnim potencijalnim žrtvama određenih zločina ili nestalim osobama;
- sprečavanje konkretne, značajne i neposredne pretnje po život ili fizičku bezbednost osoba, ili stvarne i prisutne ili stvarne i predvidljive pretnje od terorističkog napada; ili
- lociranje ili identifikacija osobe osumnjičene za krivično delo u svrhu vođenja istrage ili progona ili izvršenja krivične sankcije za određena jasno navedena dela za koja je u državi članici zaprećena kazna zatvora od najmanje četiri godine (što znači da je gornji prag za kaznu od četiri godine do kazne doživotnog zatvora, što je kriterijum osmišljen da ovaj uslov obuhvati samo relativno teška krivična dela).

Još u fazi pregovora, Evropski supervizor za zaštitu podataka, Evropski odbor za zaštitu podataka i mnoge grupe civilnog društva kritikovali su ove izuzetke kao preširoke, dok ih je mreža EDRi ocenila kao „’uputstvo’ za sprovođenje praksi biometrijskog masovnog nadzora“ umesto smislene zabrane.[244]

Prema članu 5, kada se daljinski biometrijski sistemi identifikacije u „realnom vremenu“ koriste za bilo koji od tri izuzetka, AI Akt nalaže da se u obzir uzmu „priroda situacije koja dovodi do moguće upotrebe“ i „uticaj upotrebe sistema na prava i slobode svih zainteresovanih osoba“. Svaka upotreba u okviru izuzetaka treba da bude predmet prethodnog odobrenja sudskog organa ili nezavisnog administrativnog tela države članice u kojoj će se koristiti – osim u „propisno opravdanoj hitnoj situaciji“. AI Akt propisuje i kriterijume koje organ ovlašćen za odobrenje mora da uzme u obzir prilikom odlučivanja o odobrenju. RBI sistemi koji se koriste u realnom vremenu moraju biti registrovani kod nadležnih regulatornih i nadzornih tela u državama članicama. Ova tela dostavljaju godišnje izveštaje o tim

sistemima Evropskoj komisiji, koja ima obavezu da objavi svoje izveštaje sa agregiranim podacima iz država članica.

Najzad, uredba državama članicama omogućava da utvrde detaljna pravila za korišćenje ovih sistema u okviru svojih nacionalnih zakona, o čemu moraju da obaveste Evropsku komisiju.

Upotreba „naknadnih" (retrospektivnih) daljinskih biometrijskih sistema za identifikaciju u svrhe sprovođenja zakona navedena je kao visokorizični AI sistem (Aneks III), što znači da njegovi programeri imaju niz posebnih obaveza navedenih u Poglavlju 3 predloženog zakona. Te obaveze podrazumevaju ljudski nadzor, „dovoljnu transparentnost", sisteme upravljanja kvalitetom i sprovođenje procene usaglašenosti. Što se tiče poslednje obaveze, dok drugi visokorizični sistemi veštačke inteligencije moraju da prođu kroz interne kontrole, post RBI sistemi moraju biti podvrgnuti proceni treće strane o usaglašenosti.

Takođe, u članu 26 uredbe sadržana su dodatna pravila koja se odnose upravo na korisnike post RBI sistema, uključujući i sutuacije kada za takvu upotrebu moraju da traže odobrenje sudskog organa ili nezavisnog administrativnog tela. Takođe je regulisano da takav visokorizični AI sistem za biometrijsku identifikaciju na daljinu, policija ni u kom slučaju ne sme da koristi na neciljani način, bez ikakve veze sa krivičnim delom ili postupkom, ili sa određenom pretnjom od izvršenja krivičnog dela, odnosno sa potragom za određenom nestalom osobom. Izričito je regulisano i da policija ne može doneti nikakvu odluku koja proizvodi štetne pravne posledice po čoveka samo na osnovu rezultata takvih RBI sistema. Najzad, države članice mogu predvideti strožija pravila za korišćenje ovih sistema u svojim nacionalnim propisima.

Mada je stupio na snagu 1. avgusta 2024. godine, AI Akt počinje da se primenjuje odloženo i fazno. Pravila o zabranjenim praksama se primenjuju od 2. februara 2025, a većina pravila o visokorizičnim sistemima od 2. avgusta 2026. godine.

PRAVNA PRAKSA

Obaveze iz Evropske konvencije o ljudskim pravima (EKLJP) sprovode sudije na nacionalnom nivou u državama potpisnicama, pod supervizijom Evropskog suda za ljudska prava (ESLJP) kao poslednjim pravnim sredstvom. Presude ESLJP su obavezujuće bez mogućnosti žalbe. Sud ističe da „rešava pitanja na osnovu javnih politika u zajedničkom interesu, čime [...] proširuje jurisprudenciju o ljudskim pravima širom zajednice država [Evropske] Konvencije".[245]

Nadležnost Suda pravde Evropske unije (Court of Justice of the European Union, CJEU) ograničena je na sprovođenje zakona Unije. Ipak, u svom odlučivanju CJEU uzima u obzir i Povelju EU i Evropsku konvenciju o ljudskim pravima, budući da Povelja nudi isti nivo zaštite prava koji važi u oba pravna instrumenta. Prema sudskoj praksi ESLJP i CJEU, kako ćemo ispitati u ovom odeljku, automatska analiza biometrijskih podataka predstavlja narušavanje fundamentalnog prava na privatnost i zaštitu ličnih podataka. Da bi bilo zakonito, takvo narušavanje mora da ispuni specifične zahteve u pogledu fundamentalnih prava. Prema članu 51 Povelje, svako narušavanje fundamentalnog prava mora biti neophodno, srazmerno i propisno obezbeđeno. Takođe, ne može da zadire u ono što se često naziva suštinskim jezgrom prava.[246]

Mada odluke nacionalnih tela za zaštitu podataka nemaju istu pravnu težinu kao sudske odluke, ipak mogu značajno da utiču na to kako se GDPR i LED tumače i sprovode. Kada agencija za zaštitu podataka donese odluku o određenom slučaju, ona daje smernice o tome kako zakon treba tumačiti u sličnim slučajevima u budućnosti. Ova tela takođe imaju moć da izriču kazne u visini do 4 odsto globalnog prometa kompanije.

ESLJP i CJEU

U značajnom slučaju S. i Marper protiv Ujedinjenog Kraljevstva (2008) Evropski sud za ljudska prava je presudio da uopšteno i neselektivno prikupljanje i zadržavanje biometrijskih podataka (DNK uzoraka) od osoba koje nisu osuđene za zločin, predstavlja kršenje njihovog prava na privatnost prema članu 8 Evropske konvencije o ljudskim pravima.[247] U konkretnom slučaju, vladi Ujedinjenog Kraljevstva naloženo je da revidira svoju politiku o zadržavanju uzoraka DNK, a presuda se primenjuje na sve države potpisnice EKLJP. U svojoj odluci ESLJP je takođe objasnio da takvi podaci imaju potencijal da otkriju osetljive lične podatke, kao što je etničko poreklo, što ljude može učiniti podložnim stigmatizaciji i diskriminaciji.

ESLJP je ponovio ovaj stav u slučaju Gaughran protiv Ujedinjenog Kraljevstva (2020) i po prvi put istakao da snimanje i čuvanje fotografija u pritvoru predstavlja kršenje člana 8.[248] Takav pravni razvoj može se povezati sa

tehnološkim napretkom koji je omogućio primenu ekstenzivnog mapiranja lica i prepoznavanja na takvim fotografijama.

U predmetu Uzun protiv Nemačke (2010) ESLJP je naveo da vizuelni ili audio nadzor više narušava pravo osobe na poštovanje privatnog života nego podaci o lokaciji jer „[takve vrste nadzora] otkrivaju više informacija o ponašanju, mišljenju ili osećanjima osobe".[249]

U slučaju La Quadrature du Net i drugi (C-511/18, C-512/18 i C-520/18) (2020) Sud pravde Evropske unije zaključio je da je automatska analiza saobraćaja i podataka o lokaciji bila u suprotnosti sa pravom na zaštitu ličnih podataka, garantovano članom 8 Povelje EU.[250] Na takvu obradu, dozvoljenu samo ako je narušavanje prava bilo neophodno da se odgovori na ozbiljnu pretnju nacionalnoj bezbednosti, trebalo je da se primeni koncept „stroge" proporcionalnosti. CJEU je takođe naglasio da svaka odluka o izricanju naloga za zadržavanje takvih podataka mora biti predmet delotvorne revizije od strane ili Suda ili nezavisnog administrativnog tela sa obavezujućim ovlašćenjima.

Sud je takođe ustanovio da zahtevi pružaocima elektronskih komunikacionih usluga da zadržavaju podatke o saobraćaju, propisani kroz nacionalno zakonodavstvo, ne samo da predstavljaju povredu privatnosti i zaštite ličnih podataka, već su i u sukobu sa principom slobode izražavanja iz člana 11 Povelje EU. Shodno tome, CJEU je zaključio da bi automatska analiza podataka o saobraćaju i lokaciji verovatno obeshrabrila pojedince da ostvare svoju slobodu izražavanja: „Ovakvo odvraćanje može posebno uticati na osobe čija komunikacija, prema nacionalnim pravilima, podleže obavezi profesionalne tajnosti, kao i uzbunjivača čije su radnje zaštićene Direktivom (EU) 2019/1937."

Uvođenje i upotreba biometrijskog nadzora u javnim prostorima imalo bi slične, ako ne i teže posledice. Takav nadzor eliminiše anonimnost, ograničava slobodu izražavanja i odvraća ljude od učešća u javnim aktivnostima.[251] U strahu od stalnog nadgledanja, novinari, aktivisti i politički protivnici mogu da pribegnu autocenzuri.

Agencije za zaštitu podataka

Prvu kaznu prema GDPR-u izrekla je švedska agencija za zaštitu privatnosti (Integritetsskyddsmyndigheten, IMY), u iznosu od oko 20.000 evra, a naplaćena je jednoj školi zbog korišćenja tehnologije za prepoznavanje lica da bi pratila prisustvo učenika nastavi. IMY je zaključila da je škola obrađivala osetljive biometrijske podatke bez valjanog pravnog osnova, kršeći GDPR: obrada je bila zasnovana na pristanku, što nije zakonit osnov jer je postojala jasna neravnoteža između učenika na koje se podaci odnose i škole kao rukovaoca. Škola je takođe prvo trebalo da sprovede odgovarajuću procenu uticaja, što nije uradila.[252] Francuska, poljska i britanska tela za zaštitu podataka takođe su odlučivala protiv obrade biometrijskih podataka učenika u slične svrhe, pri čemu je odluka francuskog CNIL-a potvrđena u kasnijem sudskom postupku koji je pokrenula organizacija civilnog društva La Quadrature du Net.[253]

U drugom primeru, kako je ukratko izloženo u prethodnom odeljku, IMY je utvrdila da je švedska policija nezakonito koristila aplikaciju za prepoznavanje lica kompanije Clearview AI – što je prvi put da je neka agencija za zaštitu podataka ciljala krajnjeg korisnika (policiju), a ne provajdera. IMY je zaključila da policija nije implementirala dovoljne organizacione mere, da nije sprovela procenu uticaja, te da je zaposlenima bez ovlašćenja dozvolila da koriste aplikaciju. Policija je kažnjena sa 2.500.000 švedskih kruna (oko 250.000 EUR) zbog ovog kršenja LED-a.[254]

Kao treći primer pomenućemo italijansku agenciju za zaštitu podataka – Garante Privacy – koja je odbacila pokušaj vlade da uvede prepoznavanje lica uživo (sistem poznat kao „SARI"), navodeći da bi to predstavljalo „masovni nadzor".[255] Međutim, Garante Privacy je dozvolila da se verzija ovog sistema koristi za retrospektivno prepoznavanje, što je nekoliko organizacija civilnog društva kritikovalo zbog proizvoljne tehničke razlike između dve prakse koje su podjednako štetne. Ovo su samo neki od primera brojnih odluka nacionalnih organa za zaštitu podataka širom EU koje se odnose na prepoznavanje lica ili druge vrste obrade biometrijskih podataka.[256]

Kada se uzme u obzir sudska praksa ESLJP i CJEU, kao i odluke organa za zaštitu podataka, evidentno je da EU ima načelno restriktivan pristup obradi biometrijskih podataka, vođen sa ciljem obezbeđenja osnovnih prava na zaštitu podataka, privatnost i povezanih prava na nediskriminaciju.

INDIJA

Koja vrsta pravnog akta reguliše obradu biometrijskih podataka?

Nacionalni ustav
Da. Prema sudskoj praksi, pravo na privatnost je osnovno pravo zaštićeno Ustavom.

Zakon o zaštiti podataka
Da. Zakon o zaštiti digitalnih ličnih podataka (2023).

Podzakonska akta
Da. Pravila za informacionu tehnologiju („razumne bezbednosne prakse i procedure i osetljivi lični podaci ili informacije") vlada je objavila 2011. u skladu sa Zakonom o informacionoj tehnologiji (2000).

Krivično pravo
Da. Pojedine službe za sprovođenje zakona tvrde da se oslanjaju na pravila krivičnog postupka za snimanje fotografija kada koriste tehnologiju za prepoznavanje lica.

Definicija i regulativa prepoznavanja lica

Podaci prikupljeni kroz prepoznavanje lica regulisani su kao lični podaci.

Detalji

Definisani slučajevi posebne upotrebe
- Postoji poseban pravni osnov za obradu ličnih podataka kada to rade javne vlasti, dok službe za sprovođenje zakona mogu biti potpuno izuzete od primene Zakona o zaštiti digitalnih ličnih podataka.

Definisane posebne vlasti
- Odbor koji imenuje vlada služi kao nadzorni organ.
- Odbor može da izriče novčane kazne ali ne može da daje smernice za tumačenje Zakona o zaštiti digitalnih ličnih podataka.

Definisani posebni uslovi
- Zakon o zaštiti digitalnih ličnih podataka reguliše posebne pravne osnove za obradu bilo kojih podataka od strane javnih vlasti za svrhe obavljanja svojih zadataka u interesu suvereniteta, integriteta ili bezbednosti Indije.

INDIJA

KONTEKST

Upotreba sistema za prepoznavanje lica veoma je česta u Indiji, uključujući i za potrebe sprovođenja zakona.[257] Fondacija za slobodu interneta (Internet Freedom Foundation, IFF) vodi Projekat Panoptic, koji prati i mapira različite upotrebe prepoznavanja lica u zemlji.[258] U vreme pisanja ovog teksta, popisano je 170 sistema instaliranih širom Indije. Međutim, nisu svi regioni podjednako podvrgnuti biometrijskim sistemima masovnog nadzora.

Čini se da u primeni prepoznavanja lica u javnim prostorima prednjači južna indijska država Telangana. Njen glavni grad Hajderabad ponekad se naziva „gradom sa najvećim nadzorom na svetu", sa procenjenih više od 600.000 instaliranih kamera,[259] uz „komandni i kontrolni centar".[260] Novinska agencija Associated Press obišla je ovaj centar i opisala ga kao visok toranj u kojem policijski službenici imaju pristup „24-časovnom toku podataka sa mreža CCTV kamera i mobilne telefonije za geolociranje krivičnih dela", te da koriste prepoznavanje lica za otkrivanje potencijalnih počinilaca u blizini počinjenog dela. Pored toga, službenici imaju pristup telefonskoj aplikaciji pod nazivom TSCOP sa kapacitetima skeniranja za mobilno prepoznavanje lica.[261] Prema izveštajima, aplikacija se koristi za snimanje fotografija i njihovo poređenje sa policijskom bazom;[262] za vreme pandemije kovida-19 korišćena je za otkrivanje ljudi koji ne nose maske za lice, dok uobičajeno služi za otkrivanje saobraćajnih prekršaja.[263] U vreme karantina, policija je od jednog aktiviste zahtevala da skine masku kako bi mogli da ga slikaju, bez dodatnih objašnjenja; aktivista je zbog toga tužio policiju 2022. uz podršku Fondacije za slobodu interneta, ali presuda još uvek nije doneta.[264] Mediji navode i da policija u Hajderabadu koristi prepoznavanje lica u brojne druge svrhe,

uključujući operacije kao što su postavljanje kordona i vršenje pretresa, profilisanje u vezi sa narkoticima, pa i nezakonite pretrage telefona[265] i pritvaranje ljudi koji kasno noću lutaju ulicama.[266]

Tokom 2020. i 2021. u javnost su procurili navodi da vlada planira da uvede „Program pametnog upravljanja", poznat pod nazivom Samagram. Program navodno kombinuje više skupova podataka kako bi vladi pružio sveobuhvatan „pogled od 360 stepeni" za svakog stanovnika (na primer, kada menja posao ili se venčava).[267] Još uvek nema zvaničnih informacija o programu i njegovom trenutnom statusu, kao ni kakvu tačno ulogu imaju biometrijski podaci. Na lokalnim izborima 2020. vlada države Telangana je na 10 biračkih mesta testirala prepoznavanje lica za identifikaciju birača.[268]

Još jedan indijski grad koji je zaslužio mesto na „top listi" nadzora jeste Delhi.[269] Tamošnja policija je javno obznanila kakvu ulogu tehnologija za prepoznavanje lica ima u hapšenjima. Tokom protesta 2020, kada je tadašnji predsednik SAD Donald Tramp bio u poseti Indiji, posebnu pažnju privukla su hapšenja navodnih izgrednika. Uhapšeni su pretežno bili muslimani, što je izazvalo sumnju da su hapšenja politički motivisana. Policija je demantovala ove navode. Komesar policije u Delhiju saopštio je da je tokom nereda policija izvukla i analizirala ukupno 945 video snimaka: 231 osoba je uhapšena na osnovu CCTV ili video snimaka, 137 njih je identifikovano uz pomoć tehnologije za prepoznavanje lica, dok su po rečima komesara „mnogi izgrednici identifikovani na osnovu odeće koju su nosili".[270] Prema istraživanju Fondacije za slobodu interneta, policija Delhija sva poklapanja sa preko 80 odsto sličnosti tretira kao pozitivan rezultat.[271]

Upotreba prepoznavanja lica na protestima primećena je i u severnoj državi Utar Pradeš, a prema saopštenju državne policije oni tu tehnologiju koriste samo za identifikaciju ciljanih osoba, te da ne poseduju niti čuvaju podatke o demonstrantima.[272] Na osnovu sličnih tvrdnji u kontekstu EU, koje je, kako smo ranije pomenuli, opovrgla italijanska agencija za zaštitu podataka, trebalo bi da budemo krajnje oprezni prema tvrdnjama da su ovi sistemi ciljani. Upotreba takvog sistema na protestima sama po sebi može da predstavlja biometrijski masovni nadzor, a poseban je problem to što stvara visok rizik od „efekta zebnje" po legitimna prava i slobode ljudi da protestuju.

Tehnologije za prepoznavanje lica na aerodromima takođe su prisutne u okviru probnog nacionalnog programa koji se trenutno sprovodi na dobrovoljnoj osnovi. Prema zvaničnim saopštenjima, lična karta i putna dokumenta građana čuvaju se u elektronskom novčaniku na pametnom telefonu putnika i ne postoji centralno skladištenje podataka, dok se blokčejn tehnologija koristi za bezbednost podataka, koji se brišu u roku od 24 sata od upotrebe.[273] Međutim, ovaj pilot program izazvao je zabrinutost jer bez „režima zaštite podataka i snažne reforme nadzora" ne postoje dovoljne garancije da podaci prikupljeni i obrađeni u ove svrhe neće biti zloupotrebljeni.[274]

Na saveznom nivou, Nacionalni biro za kriminalističku evidenciju (National Crime Records Bureau, NRCB) pokrenuo je 2020. proceduru za stvaranje nacionalnog automatizovanog sistema za prepoznavanje lica (Automated Facial Recognition System, AFRS).[275] U vreme kada nastaje ovaj tekst, projekat još uvek nije završen ali, prema planovima, ovakva baza navodno treba da se koristi za „brzu identifikaciju počinilaca prikupljanjem postojećih podataka iz raznih drugih databaza".[276]

Prvi veliki slučaj „curenja" podataka u vezi sa korišćenjem tehnologije za prepoznavanje lica u Indiji dogodio se u maju 2024. godine, kada su postali javno dostupni podaci preko 50.000 policijskih službenika, kao i izveštaji o upitima i „podudaranjima" prilikom korišćenja tehnologije.[277]

Kada je u pitanju privatni sektor, indijska vlada je nedavno preduzela korake da omogući bankama da za određene bankarske transakcije koriste prepoznavanje lica kao i identifikaciju prema irisu u oku.[278]

Detaljnije informacije o nacionalnom identifikacionom sistemu Aadhaar izložićemo u nastavku, u odeljku o pravnoj praksi.

PRAVNI OKVIR

Indija do 2023. nije imala sveobuhvatan pravni okvir za zaštitu ličnih podataka, kao ni relevantno telo za zaštitu podataka.[279]

Nacrt zakona o zaštiti podataka o ličnosti predstavljen je 2019. da bi bio povučen posle tri godine javnih rasprava i sporova, 81 amandmana i 12 preporuka, što je jasno pokazalo da je vladin predlog bio daleko od javnog konsenzusa.[280] Nova verzija predložena je u novembru 2022.[281] Konačno, Zakon o zaštiti digitalnih podataka o ličnosti (Digital Personal Data Protection Act, DPDPA) usvojen je početkom avgusta 2023.[282] sa manjim izmenama u odnosu na nacrt iz prethodne godine.[283]

Mada su prošle četiri godine od pripreme prvobitnog teksta DPDPA, organizacija za ljudska prava Access Now ocenila je usvajanje konačne verzije kao „ishitreno“, dok je indijski predstavnik organizacije istakao da „činjenica da je vlada progurala zakon kroz parlament za samo nedelju dana, uprkos demonstrativnim izlascima sa sednice, zahtevima za dodatne konsultacije i reformu nadzora, govori koliko je to rđava usluga za narod Indije i našu demokratiju“.[284]

Odredbama zakona nije utvrđeno kada će DPDPA stupiti na snagu. Centralna vlada ima deset meseci da odredi tačne datume stupanja na snagu različitih odredbi.[285] Po novom propisu, vlada je ovlašćena da formira Odbor za zaštitu podataka Indije. Podzakonski akt koji operacionalizuje pravila zakona stavljen je na javnu raspravu u januaru 2025. godine, međutim, on ne sadrži odredbe koje bi regulisale poseban režim za obradu biometrijskih podataka.[286]

Dok DPDPA ne stupi na snagu u potpunosti, relevantna pravila o zaštiti podataka mogu se naći u Zakonu o informacionim tehnologijama iz 2000. (Zakon o IT)[287] i Pravilima za informacionu tehnologiju (Razumne bezbednosne prakse i procedure i osetljivi lični podaci ili informacije) iz 2011. (Pravila SPDI).[288] Ova dva propisa godinama su činila srž indijskog pravnog okvira za zaštitu podataka, u očekivanju novog i modernog zakona, iako su njihova pravila ograničenog obima i ne bave se upotrebom ličnih podataka za potrebe sprovođenja zakona. Zakon o IT prvenstveno obezbeđuje pravnu potvrdu transakcija koje se obavljaju korišćenjem elektronske razmene podataka i drugih sredstava elektronske komunikacije i reguliše elektronsko podnošenje dokumenata državnim organima. Pravila SPDI izdaje vlada u skladu sa Zakonom o IT kao dodatno pojašnjenje.

DPDPA je kritikovan iz različitih razloga,[289] uključujući načelno odsustvo uslova neophodnosti i proporcionalnosti za svako ograničenje prava na privatnost – što bi ga moglo „osporiti na sudu s obzirom da jasno protivreči presudi Vrhovnog suda Indije u slučaju Puttaswamy iz 2017“.[290] (Više detalja o ovoj presudi u narednom odeljku.) Iz perspektive naše studije, čini se da najznačajniju zabrinutost izazivaju pravila o izuzecima koje zakon predviđa za vladine prakse, nadzorni organ sa niskim ovlašćenjima, kao i odsustvo pravila za podatke koji bi se mogli smatrati osetljivim, uključujući biometriju.

Naime, DPDPA ne razlikuje vrste ličnih podataka, niti daje posebnu zaštitu podacima koji bi se smatrali osetljivim u uobičajenim savremenim zakonima o zaštiti podataka. To je takođe značajno odstupanje u poređenju sa logikom u osnovi Zakona o IT-u i Pravila SPDI. Tako, na primer, Pravila SPDI definišu biometriju kao tehnologiju koja meri i analizira karakteristike ljudskog tela, kao što su otisci prstiju, mrežnjača i iris oka, obrasci glasa, obrasci lica, mere ruku i DNK za „svrhe autentifikacije“. Biometrijske informacije su definisane kao vrsta osetljivih podataka, pod uslovom da takve informacije nisu slobodno dostupne ili u javnom domenu (tj. takve javne informacije se ne bi smatrale osetljivim prema Pravilima SPDI). U okviru Pravila SPDI ne postoje odredbe koje posebno regulišu biometriju.

Pravilima SPDI utvrđeni su različiti zahtevi u pogledu obrade osetljivih informacija: (1) mora se objaviti politika privatnosti koja kao minimum mora da sadrži elemente regulisane u Pravilima SPDI; (2) prikupljanje podataka mora se vršiti na osnovu pisane saglasnosti (uključujući i elektronski) osobe na koju se podaci odnose, dok se saglasnost može povući u bilo kom trenutku; (3) osetljivi podaci se ne smeju obrađivati osim ako se prikupljaju u zakonite svrhe povezane sa funkcijom ili aktivnošću organizacije koja ih obrađuje i ako se prikupljanje smatra neophodnim za tu svrhu; (4) organizacija koja čuva osetljive podatke neće zadržati te informacije duže nego što je potrebno za svrhe za koje se informacije mogu zakonito koristiti ili se to na drugi način zahteva nekim drugim zakonom koji je u to vreme na snazi; (5) svi netačni podaci moraju biti ispravljeni ili izmenjeni, koliko je to izvodljivo; i (6) osetljivi podaci se mogu izvoziti van Indije, deliti sa trećim licima ili objavljivati samo u skladu sa Pravilima SPDI.

Iz teksta Pravila SPDI čini se evidentnim da ona nisu podesna za regulisanje upotrebe tehnologija za prepoznavanje lica u službama za sprovođenje zakona ili bilo koje druge vladine svrhe. Imati bilo kakvu saglasnost kao pravni osnov za korišćenje ove tehnologije u službama za sprovođenje zakona naprosto nije realno. Mnoge jurisdikcije su prihvatile pristup GDPR-a, ili uopšteno evropski pristup i navode saglasnost kao mogući preduslov ili pravni osnov za obradu podataka. Međutim, nemaju svi striktna pravila o kvalitetu takve saglasnosti (npr. da ona mora biti slobodno data i da se može povući u bilo kom trenutku). Takva su i Pravila SDPI, pa se može tvrditi da se saglasnost u okviru ovog pravnog režima može podrazumevati, a ne izričito dati. U svakom slučaju, teško je zamisliti scenario u kojem bi građani Indije „pristali“ na korišćenje njihovih biometrijskih podataka u svrhe koje se odnose na sprovođenje zakona.

Međutim, čini se da DPDPA ne rešava ovaj problem na zadovoljavajući način. Zakon doduše ima razrađenije odredbe za pravni osnov obrade ličnih podataka nego Pravila SPDI. I dalje se saglasnost smatra „primarnim“[291] pravnim osnovom za obradu ličnih podataka – barem kada su u pitanju „fiducijari“ privatnih podataka (izraz koji se koristi za rukovaoce). Pored saglasnosti, alternativni pravni osnov je jedna od ograničenih „legitimnih upotreba“ koje definiše DPDPA.

Te legitimne upotrebe pokrivaju različite svrhe u javnim službama, uključujući obradu „za obavljanje bilo koje funkcije države ili nekog njenog instrumenta prema bilo kom zakonu koji je u tom trenutku na snazi u Indiji ili u interesu suvereniteta i integriteta Indije ili bezbednosti države“.[292] Ova legitimna upotreba je definisana krajnje uopšteno i stoga podiže rizik da je javni organi koriste kao carte blanche za bilo kakvu obradu, što je još više zabrinjavajuće zbog pomenutog odsustva principa proporcionalnosti i neophodnosti u DPDPA.

Kada je reč o obradi biometrije od strane organa za sprovođenje zakona, još više zabrinjava činjenica da DPDPA predviđa izuzetak od primene zakona prema kojem savezna vlada može odlučiti da se nijedna od odredbi zakona ne odnosi na određene organe vlasti ili agencije, ako je to „u interesu suvereniteta i integriteta Indije, bezbednosti države, prijateljskih odnosa sa stranim državama, održavanja javnog reda ili sprečavanja podsticanja na bilo koji prepoznat prekršaj u vezi sa navedenim“.[293] Opet, ovaj izuzetak nije ograničen nikakvim zahtevima neophodnosti ili proporcionalnosti.

To praktično znači da vlada može svaku upotrebu biometrije u službama za sprovođenje zakona za bilo koju od ovih svrha, izuzeti od bilo kojih mehanizama zaštite podataka koje reguliše DPDPA. Tako postavljen izuzetak medijska udruženja nazvala su „skoro apsolutnim“,[294] dok je bivši sudija Vrhovnog suda izjavio da ovo pravilo izaziva „duboku zabrinutost“ i da „daje preširoku marginu vladi dok čini malo da zaštiti osnovno pravo ljudi na privatnost podataka“.[295]

Zabrinutost javnosti dodatno je pojačana nedostatkom efikasnih mehanizama za sprovođenje. Odbor za zaštitu podataka Indije nije nezavisan entitet, već telo koje imenuje vlada sa ograničenim ovlašćenjima (da donosi određene odluke u pojedinačnim slučajevima kao arbitražno telo). Njegova ovlašćenja ne uključuju ovlašćenje da izdaje bilo kakve smernice ili mišljenja u kontekstu tumačenja DPDPA.[296]

Kada je u pitanju indijsko zakonodavstvo koje se odnosi na korišćenje alata za prepoznavanje lica u svrhe sprovođenja zakona, treba pomenuti novi indijski zakon o krivičnom postupku (identifikaciji) (Criminal Procedure (Identification) Act, CPIA). Ovaj zakon je usvojen u aprilu 2022. i zamenio je više od stotinu godina star zakon o identifikaciji zatvorenika (1920). Čini se da CPIA ne reguliše izričito biometrijsku identifikaciju.[297] Međutim, zakonska definicija policijskih „merenja“ obuhvata fotografije, zajedno sa otiscima prstiju, otiscima dlana, otiscima stopala, skeniranjem irisa i mrežnjače, fizičkim i biološkim uzorcima i njihovom analizom, kao i atribute ponašanja, uključujući potpise i rukopis. Ova merenja su veoma slična primerima koji se obično navode u vezi sa biometrijskom obradom. Međutim, možemo samo da nagađamo da li „fotografije“ treba da uključe prepoznavanje lica ili, terminologijom CPIA, „otiske lica“. Stari zakon je definisao „merenja“ samo kroz otiske prstiju i otiske stopala. Pored tih merenja, policija je mogla da „fotografiše“ ljude pod propisanim uslovima. Iz nekog razloga, termin „fotografija“ iz starog zakona nije ažuriran u CPIA kako bi uključio formulaciju koja bi ukazivala da fotografije mogu predstavljati obradu biometrijskih podataka izvedenih iz takvih fotografija (takođe zato što druga „merenja“ iz CPIA jasno upućuju na biometrijske podatke).

U odgovorima na zahteve za pristup informacijama koje je Fond za slobodu interneta podneo 2020. i 2021. godine, policija Delhija je navela da se oslanja na odredbe tada važećeg zakona kao pravni osnov za obradu podataka prilikom korišćenja prepoznavanja lica.[298] Takav stav policije u Delhiju je pravno problematičan jer je u starom zakonu fotografisanje bilo ograničeno na osobe koje su osuđene, puštene na kauciju ili osobe koje su optužene za dela za koja je predviđena kazna strogog zatvora od jedne godine.[299] Sa novim zakonom, ovo pravno obrazloženje se i dalje nije promenilo – po CPIA, „merenja“ se mogu preduzeti samo prema ograničenom broju lica u toku krivične istrage, dakle neselektivni masovni nadzor celokupnog stanovništva u javnim prostorima nije dozvoljen.

PRAVNA PRAKSA

Najznačajniji slučaj primene biometrijskih sistema u Indiji jeste Aadhaar. Prema zvaničnom sajtu indijske Agencije za jedinstvenu identifikaciju (Unique Identification Authority of India, UIDAI),[300] Aadhaar broj predstavlja 12-cifreni nasumični broj koji UIDAI izdaje stanovnicima

Indije koji prolaze kroz proces verifikacije. Svaki stanovnik Indije može se dobrovoljno prijaviti za izdavanje Aadhaar broja, a ako je voljan da se prijavi, mora da pruži „minimalne" demografske i biometrijske podatke. Te biometrijske informacije obuhvataju otiske deset prstiju, skeniranje dva irisa i fotografiju lica. Prema istom izvoru, platforma Aadhaar za identitete jedan je od ključnih stubova „Digitalne Indije", gde svaki stanovnik zemlje dobija jedinstveni identifikator.

Ustanovljen pre više od deset godina, Aadhaar je od nacionalne identifikacione šeme prerastao u najveću nacionalnu identifikacionu bazu podataka. Opisivan je kao „najsofisticiraniji ID program na svetu";[301] u to vreme, 2017, imao je milijardu i 123 miliona upisanih korisnika, a do novembra 2022. generisano je milijardu i 352 miliona Aadhaar brojeva.[302] U početku je korišćen u vladine svrhe, ali su kasnije i privatni subjekti poput banaka i mobilnih operatora počeli da traže Aadhaar autentifikaciju za pristup svojim uslugama.[303]

Vrhovni sud Indije je 2017. godine doneo značajnu presudu kojom je privatnost u Indiji ustanovljena kao osnovno pravo, poništavajući dve prethodne odluke koje su tvrdile suprotno.[304] U to vreme se smatralo da će presuda imati neposredne implikacije i na Aadhaar, džinovski program biometrijske identifikacije. Očekivalo se da će uže veće Vrhovnog suda naredne godine odlučiti o validnosti šeme (tj. o ustavnosti „Aadhaar akta" koji je reguliše), pa se verovalo da je presuda iz 2017. korak ka poništavanju Aadhaara. Ipak, to se nije dogodilo.

Aadhaar je tokom godina bio predmet nekoliko sudskih presuda. Vrhovni sud je 2013. godine izdao privremenu naredbu u kojoj se kaže da vlada ne može uskratiti uslugu stanovniku koji ne poseduje Aadhaar.[305] Isti sud je 2015. godine odlučio da jedinstveni identifikacioni sistem Aadhaar ne može biti obavezan za građane Indije da bi koristili vladine usluge.[306] Konačno, presudom iz 2018. uže veće Vrhovnog suda od pet sudija potvrdilo je ustavnu valjanost Aadhaar šeme većinom glasova, pri čemu je jedan sudija izjavio neslaganje i istakao da je projekat „u celini neustavan".[307]

Odluka Vrhovnog suda iz 2018, međutim, nameće neka ograničenja u pogledu načina na koji se program može koristiti. Privatnim preduzećima i pojedincima više nije dozvoljeno da traže Aadhaar od građana, što znači da to ne može biti uslov za usluge kao što su otvaranje bankovnog računa, uspostavljanje veze mobilne telefonije ili upis u školu. S druge strane, vladi je dozvoljeno da Aadhaar podatke učini obaveznim za poreske svrhe i socijalne beneficije.[308]

Što je najvažnije iz perspektive upotrebe u službama za sprovođenje zakona, presuda je uticala na takozvani „izuzetak za nacionalnu bezbednost". Izuzetak je regulisan članom 33(2) Aadhaar zakona. Pre presude iz 2018. tim izuzetkom dozvoljeno je otkrivanje informacija, uključujući informacije o identitetu ili evidenciju o autentifikaciji, u interesu nacionalne bezbednosti,[309] odnosno omogućavao je istražnim službama da pristupe podacima Aadhaara bez sudskog naloga.[310] Mada sud nije dovodio u pitanje potrebu za postojanjem „izuzetka za nacionalnu bezbednost", doneo je odluku da po pitanju da li su interesi nacionalne bezbednosti prisutni u konkretnom slučaju treba da odluči: (1) službenik čiji je čin viši od združenog sekretara, što je izvršna funkcija u vladi, i (2) „u saradnji sa" pravosudnim službenikom (po mogućnosti, sa aktivnim sudijom Višeg suda). Presudom je ukinut član 33.2 Zakona u sadašnjem obliku, „sa slobodom da se donese odgovarajuća odredba" u smislu odluke, tj. koja podrazumeva učešće suda.[311]

Međutim, 2019. su usvojene izmene i dopune Aadhaar zakona i usvojen je samo uslov iz tačke (1), koji zahteva da pitanje „nacionalne bezbednosti" utvrđuje neko na poziciji sekretara (što je u vladinoj hijerarhiji više od združenog sekretara), potpuno izostavljajući učešće suda. Stoga se može pretpostaviti da će „unapređeni" član 33.2 Aadhaar zakona verovatno ponovo biti proglašen neustavnim zbog izostanka uslova iz tačke (2).

Prema saopštenju za javnost iz 2022, UIDAI je razvio sistem i mobilnu aplikaciju za autentifikaciju lica AadhaarFaceRd, kako bi omogućio Aadhaar agencijama za autentifikaciju korisnika (Authentication User Agencies, AUA) da snime lice osobe kako bi sprovele autentifikaciju,[312] što se obično odnosi na potvrdu identiteta osobe radi pristupa usluzi. Na sajtu UIDAI postoji video uputstvo o tome kako se aplikacija koristi za svrhe autentifikacije.[313]

JUŽNA AFRIKA

Koja vrsta pravnog akta reguliše obradu biometrijskih podataka?

Nacionalni ustav
Da, pravo na privatnost.

Zakon o zaštiti podataka
Da, Zakon o zaštiti ličnih informacija (2013).

Podzakonska akta
Da.

Smernice
Da.

Definicija i regulativa prepoznavanja lica

Podaci prikupljeni kroz prepoznavanje lica definišu se kao biometrijski podaci.

Detalji

Definisani slučajevi posebne upotrebe
- Upotreba osetljivih i biometrijskih podataka načelno je zabranjena, osim ako se primenjuje neki od izuzetaka.

Definisane posebne vlasti
- Regulator za informacije služi kao nadzorni organ; može da izdaje mišljenja i smernice, rešava pritužbe i vodi istrage; ne može da izriče kazne, ali može da odredi administrativnu novčanu globu.

Definisani posebni uslovi
- Prema propisanim uslovima, postoji obaveza pribavljanja prethodnog ovlašćenja za obradu od nadzornog organa.

JUŽNA AFRIKA

KONTEKST

Nema konkretnih dokaza da su javni organi u Južnoj Africi koristili tehnologiju prepoznavanja lica na opštoj populaciji. Međutim, postoji zabrinutost da bi to mogao biti slučaj, ili da bi ova tehnologija uskoro mogla da uđe u široku upotrebu.

Južnoafrička policija već petnaest godina izražava želju da počne da koristi ovu tehnologiju.[314] Javnost je zabrinuta i zbog prisustva i aktivnosti privatne kompanije Vumacam, koja je izgradila pametnu nadzornu mrežu širom zemlje za praćenje kretanja ljudi „neobičnog ponašanja". Situacija je rizična jer se od nadzora ponašanja lako može skliznuti u identifikaciju na osnovu ljudskog lica, budući da je reč o istim tehnološkim sistemima. Štaviše, iako nadzor ponašanja bez identifikacije ljudi može izgledati benigno, iz perspektive zaštite podataka i dalje je veoma osetljiv. Prikupljanje podataka o ponašanju u svojoj suštini jeste prikupljanje ličnih podataka. U kombinaciji sa drugim informacijama, takvi podaci mogu dovesti do identifikacije osobe, kao i do diskriminatornog profilisanja. U prečišćenom obliku, karakteristike ponašanja mogu dovesti do identifikacije ako se one mogu koristiti kao merljivi obrasci ljudskih aktivnosti, u kom slučaju bi se smatrali biometrijskim podacima.

Vumacam prodaje svoje usluge privatnog obezbeđenja drugim lokalnim kompanijama. Čini se da već ima monopol, koji se ne zasniva samo na navodnim kapacitetima i delotvornosti njegove tehnologije, već i na (nezvaničnoj) saradnji kompanije sa policijom. Ova pretpostavka je zasnovana na nekoliko studija slučaja u vezi sa Vumacamovim prisustvom i planovima u Južnoj Africi u poslednjih nekoliko godina.[315] Prema tim izvorima, predstavnici Vumacama su više puta poricali

da su počeli da koriste prepoznavanje lica za svoje usluge i razvoj tehnologije. Međutim, ako se pogledaju funkcije koje već koriste (npr. prepoznavanje registarskih tablica), čini se da imaju tehničku infrastrukturu i kapacitete da to omoguće.

Pored toga, ministarstvo unutrašnjih poslova Južne Afrike pokrenulo je svoj automatski biometrijski informacioni sistem (Automatic Biometric Information System, ABIS) u januaru 2016.[316] ABIS treba da služi kao jedinstven resurs za identifikaciju državljana i nedržavljana Južne Afrike za potrebe državnih institucija i entiteta u privatnom sektoru, proširujući aktuelni nacionalni sistem identifikacije, Hanis. Prema zvaničnim saopštenjima, ABIS će sadržati informacije kao što su otisak prsta, fotografija, otisak dlana, šablon lica i skenovi irisa.[317] Sistem još uvek nije u funkciji, ali na osnovu novijih izveštaja čini da je njegova implementacija neizbežna, budući da se problemi sa ugovorom koji je zaključen sa pružaocem usluga navode kao jedan od glavnih razloga za odlaganje.[318] U maju 2023. godine, parlamentarni nadzorni komitet za unutrašnje poslove saopštio je da je razočaran kašnjenjem u realizaciji projekta i problemima sa privatnim izvođačem radova na projektu, ali je u pogledu prikupljanja biometrijskih informacija izrazio podršku za „upotrebu unapređenog sistema sa inovativnim tehnološkim funkcionalnostima, kao što su prepoznavanje lica i biometrijski modaliteti dlana, što će ojačati poverenje u registar stanovništva“.[319] Prema informacijama iz ministarstva unutrašnjih poslova, mada nisu sve ABIS funkcionalnosti implementirane, sistem za prepoznavanje lica je bio operativan u septembru 2023. godine.[320]

Na svojim granicama, južnoafrička vlada primenjuje biometrijski sistem kontrole kretanja (Biometric Movement Control System, BMCS) od 2021. U maju 2023. ovaj sistem je implementiran u 34 luke i aerodroma.[321] Prema sajtu nacionalne avio kompanije, South African Airways, „ako niste državljanin Južne Afrike i ulazite preko graničnih prelaza, od vas se očekuje da date svoje otiske prstiju i fotografiju na šalteru za imigraciju“.[322] Osim sličnih praktičnih informacija, sajt ministarstva unutrašnjih poslova ne nudi nikakvo drugo objašnjenje o tome kako ovaj sistem funkcioniše.

Trend korišćenja tehnologije za prepoznavanje lica u svrhe identifikacije sve više je pristutan i u drugim javnim i privatnim sektorima, uključujući programe za dobijanje socijalne pomoći,[323] prijavu poreza[324] ili upis na univerzitet.[325]

PRAVNI OKVIR

Ustav Južne Afrike priznaje pravo na privatnost kao osnovno ljudsko pravo.[326] Prava na privatnost i zaštitu ličnih podataka bliže su regulisana Zakonom o zaštiti ličnih informacija (Protection of Personal Information Act, POPIA), koji se primenjuje od 30. juna 2021.[327] Čini se da je POPIA u velikoj meri zasnovana na pravnoj tradiciji zaštite podataka u EU. U skladu sa tim zakonom, Južna Afrika ima posebno telo za zaštitu podataka pod nazivom Regulator za informacije.[328]

Biometrija se u zakonu definiše kao „tehnika lične identifikacije koja se zasniva na fizičkoj, fiziološkoj ili bihejvioralnoj karakterizaciji, uključujući tipizaciju krvi, uzimanje otisaka prstiju, DNK analizu, skeniranje irisa i prepoznavanje glasa“. Iz nekog razloga, definicija ne pominje prepoznavanje lica (videćemo da je to takođe slučaj sa zakonom u Keniji, što možda sugeriše zajedničku istoriju definicije). Međutim, pošto lista nije konačna, nema razloga da se smatra da ova definicija isključuje prepoznavanje lica. Biometrijske informacije se smatraju „posebnim ličnim podacima“, kako je definisano u članu 26 POPIA.

Kad je reč o osetljivim ličnim podacima, POPIA u načelu zabranjuje njihovu obradu, izuzev ako je primenjiva jedna od tri kategorije izuzetaka: opšti izuzeci; ovlašćenje Regulatora za informacije primenjivo na sve osetljive lične podatke; ili, poseban izuzetak koji reguliše samo biometrijske informacije.

Nalik Opštoj uredbi o zaštiti podataka EU, POPIA predviđa pet opštih izuzetaka kada je obrada dozvoljena zato što: (1) postoji saglasnost osobe na koju se podaci odnose; (2) obrada je neophodna za uspostavljanje, ostvarivanje ili odbranu prava ili zakonske obaveze; (3) obrada je neophodna da bi se ispunila obaveza međunarodnog javnog prava; (4) obrada se vrši u istorijske, statističke ili istraživačke svrhe (podložno dodatnim uslovima); ili (5) osoba na koju se podaci odnose je informacije svesno objavila javno.[329]

Pored toga, Regulator za informacije može, na zahtev odgovorne strane,[330] da odobri obradu posebnih ličnih podataka ako je takva obrada u javnom interesu i ako su postavljene odgovarajuće mere za zaštitu podataka osobe na koju se podaci odnose. Regulator je takođe izdao uputstvo koje uređuje ovaj postupak ovlašćenja.[331]

Konačno, postoji poseban izuzetak koji reguliše samo obradu biometrijskih podataka.[332] U članu 33, POPIA predviđa da ova obrada može biti

dozvoljena ako je sprovode organi koji su po zakonu zaduženi za primenu krivičnog zakona, ili ovlašćeni službenici koji su do tih podataka došli u skladu sa zakonom. Ova dozvola za upotrebu biometrije u nekim javnim organima prilično je široka i ne reguliše nikakve specifičnosti biometrije. Jedno od mogućih tumačenja ovog pravila jeste da konkretne situacije kada se biometrijske informacije mogu obrađivati po ovom izuzetku, u principu treba dodatno regulisati odredbama koje operacionalizuju i konkretizuju ovo pravilo (putem posebnog zakona ili izmenom postojećeg). To je situacija slična pravnoj dinamici između LED-a na nivou EU i nacionalnih zakona u državama članicama, u smislu da Direktiva postavlja opšta pravila, dok bi države članice trebalo da detaljnije regulišu upotrebu biometrije u svrhe sprovođenja zakona (između ostalog, da uspostave odgovarajuće zaštitne mere za takvu obradu).

U Južnoj Africi još uvek ne postoji zakon koji bi regulisao obradu podataka putem tehnologije za prepoznavanje lica ili konkretno u službama za sprovođenje zakona, uprkos činjenici da ABIS omogućava prikupljanje podataka o licu građana.[333] S obzirom na to da službe za sprovođenje zakona u Južnoj Africi tvrde da ne koriste prepoznavanje lica u svojim istragama (niti postoje dokazi za takvu praksu), vreme će pokazati da li će se oslanjati na član 33 POPIA kao pravni osnov za takvu upotrebu.

Pravila o upotrebi biometrije u krivičnim postupcima takođe treba tumačiti u svetlu člana 6 POPIA, koji reguliše izuzeća od zakona. Prema jednom takvom izuzeću, POPIA se ne primenjuje na obradu ličnih podataka u radu javnog organa u okolnostima kao što je nacionalna bezbednost, ili kada je svrha obrade sprečavanje, otkrivanje i istraga krivičnih dela, krivično gonjenje prestupnika ili izvršenje kazne, ali samo u meri u kojoj su u zakonodavstvu uspostavljene adekvatne mere za zaštitu takvih ličnih podataka. U nedostatku zakona koji bi regulisali biometrijski nadzor u ove svrhe, izgleda da se POPIA primenjuje dok takva pravila ne budu na snazi.

U Poglavlju 6, POPIA određuje da odgovorna strana mora da dobije „prethodno odobrenje“ za određene aktivnosti obrade od Regulatora za informacije, zbog njihove specifične prirode. Odgovorno lice koje želi da obrađuje biometrijske podatke (po odgovarajućem pravnom osnovu) u principu ne mora da dobije takvo prethodno ovlašćenje za samu obradu. Međutim, ovlašćenje bi bilo potrebno ako bi se podaci preneli u inostranstvo u neadekvatnu zemlju. Postoji i uputstvo koje reguliše ovaj postupak ovlašćenja.[334]

POPIA ima pravila koja se odnose na automatizovano donošenje odluka, a koja su slična njihovim GDPR pandanima, iako se čini da su užeg obima jer se fokusiraju na donošenje odluka zasnovano na profilima stvorenim putem automatizovane obrade (član 71).

Prema tome, postoji nekoliko potencijalnih pravnih osnova za javne organe i policiju Južne Afrike, koji se mogu koristiti u budućnosti ukoliko se želi primeniti tehnologija prepoznavanja lica u praksi. Ostaje da se vidi da li će u takvom slučaju biti poštovana odgovarajuća zakonska procedura.

PRAVNA PRAKSA

Mada se nije vodio zbog tehnologije prepoznavanja lica, već masovnog video nadzora, slučaj u kojem je konačno presudio Visoki sud Južne Afrike 2020. izdvaja se po svom značaju.[335] Predmet je pokrenula kompanija Vumacam protiv Agencije za puteve iz Johanesburga (Johannesburg Road Agency, JRA) jer je suspendovala pravo prilaza koje Vumacamu omogućava da pristupi javnim putevima radi instalacije svoje opreme, antena i CCTV mreže. JRA je odluku o suspenziji obrazložila tvrdnjom da je cilj Vumacama da „nadgleda kretanje ‘nevinih ljudi’ kao i da ‘snimke’ prodaje trećim stranama“. Prema tekstu presude, JRA je u suštini tvrdila da Vumacam špijunira kretanje ljudi i time krši njihovo pravo na privatnost u skladu sa POPIA zakonom. Za rešavanje problema koji proizlaze iz takvih špijunskih aktivnosti, morao bi se uspostaviti regulatorni okvir. Takav okvir bi trebalo da se fokusira na garancije da se materijalom prikupljenim putem kamera rukuje na način koji štiti privatnost pojedinaca.[336]

Međutim, sud nije prihvatio argument JRA. Naime, domen odlučivanja Agencije uređen je relevantnim podzakonskim aktima, odnosno JRA nije nadležna da suspenduje pravo prilaza po osnovu povrede prava na privatnost. Prema rečima suda, JRA je organ uprave koji nema ovlašćenja van onih koja su mu data zakonom, a u ovom slučaju i konkretnim podzakonskim aktima.[337]

U intervjuu povodom ove pobede na sudu, izvršni direktor Vumacama je izjavio: „Naša infrastruktura je veoma korisna za javnost, bezbednosne kompanije, organe za sprovođenje zakona, pa čak i za samu JRA u utvrđivanju incidenata koji mogu da izazovu štetu ili poremećaj na putnoj infrastrukturi. Svakodnevno imamo višestruke potvrde uspešnosti, gde naše kamere i sprečavaju kriminal i pomažu u hapšenju kriminalaca.“[338]

Ovaj slučaj demonstrira ozbiljnost zabrinutosti u Južnoj Africi zbog ugrožavanja prava na privatnost u ime (obećane) bezbednosti. Taj rizik su prepoznale i javne službe kao što je JRA, iako nemaju nadležnost da ospore potencijalnu povredu privatnosti. Kada baza podataka ABIS bude uspostavljena, šanse za primenu tehnologije za prepoznavanje lica znatno će se povećati. Tek treba da se pokaže da li će se i kako sve zainteresovane strane pridržavati pravila POPIA.

KANADA

Koja vrsta pravnog akta reguliše obradu biometrijskih podataka?

Nacionalni ustav
Da, kanadska Povelja o pravima i slobodama (1982).

Zakon o zaštiti podataka
Da, Zakon o privatnosti (1985); Zakon o zaštiti ličnih informacija i elektronskom dokumentu (2000).

Podzakonska akta
Da.

Smernice
Da.

AI regulativa
Da, u razvoju.

Propisi na lokalnom nivou
Da, nivo provincija.

Definicija i regulativa prepoznavanja lica

Podaci prikupljeni kroz prepoznavanje lica definišu se kao biometrijski podaci u Kvebeku.

Podaci prikupljeni kroz prepoznavanje lica regulišu se kao osetljivi podaci.

Detalji

Definisane posebne vlasti
- Poverenik Kanade za privatnost.
- Povereništvo Kvebeka za pristup informacijama.

Definisani posebni uslovi
- Prema odredbama predloženog zakona o zaštiti privatnosti potrošača, obavezno je pružiti jasno objašnjenje upotrebe bilo kog sistema za automatizovano odlučivanje koji može značajno da utiče na pojedince.
- Prema odredbama predloženog zakona o veštačkoj inteligenciji i podacima, svako ko razvija biometrijske sisteme koji se koriste za identifikaciju i izvođenje zaključaka, obavezan je da objavi opis sistema sačinjen jezikom lako razumljivim široj javnosti.
- Kompanije su dužne da obaveste Povereništvo Kvebeka za pristup informacijama o svakoj obradi koja uključuje biometrijske informacije.

KANADA

KONTEKST

Kanadu je 2020. potresao skandal zbog biometrijskog masovnog nadzora: otkriveno je da su, zajedno sa policijama osamnaest evropskih zemalja, Kraljevska kanadska konjička policija (savezna policijska služba) i druge policijske službe Kanade bile klijenti kompanije Clearview AI sa sedištem u SAD, koja je bez saglasnosti prikupila milijarde slika kako bi napravila baze podataka za prepoznavanje lica.[339]

Istraga koju je preduzela služba kanadskog Poverenika za privatnost (Office of the Privacy Commissioner, OPC) otkrila je da je Clearview AI prekršio savezne i pokrajinske zakone o privatnosti tako što je bez dozvole skrejpovao slike sa interneta. Pokrajinske vlasti su izdale pravno obavezujuće naredbe kojima se od kompanije zahteva da prestane da nudi svoje usluge, prestane da prikuplja i koristi slike bez saglasnosti, te da izbriše prikupljene slike i biometrijske setove lica pojedinaca iz kanadskih provincija.[340] Clearview AI je u julu 2020. objavio da će povući svoju tehnologiju za prepoznavanje lica iz ponude u Kanadi.

Tadašnji kanadski Poverenik za privatnost, Daniel Therrien, iskoristio je ovaj slučaj da ukaže na nedostatke postojećih saveznih zakona o privatnosti, ističući da Zakon o zaštiti ličnih podataka i elektronskim dokumentima (Personal Information Protection and Electronic Documents Act, PIPEDA) ne daje ovlašćenja Povereniku da izdaje naredbe niti da izriče novčane kazne.[341]

Savezna policija je kasnije priznala da koristi druge alate za prepoznavanje lica koji se nude kao softver za borbu protiv trgovine ljudima i seksualne eksploatacije dece.[342] Takva upotreba tehnologija za prepoznavanje lica u policijskim snagama u Kanadi izazvala je zabrinutost

u pogledu privatnosti, odgovornosti i potrebe za jasnim i sveobuhvatnim zakonodavstvom. U zajedničkoj izjavi, federalni, pokrajinski i teritorijalni poverenici za privatnost istakli su da je za sprečavanje opšteg nadzora neophodno izričito definisati slučajeve u kojima organi za sprovođenje zakona mogu (i slučajeve u kojima ne smeju) da koriste prepoznavanje lica.[343]

Ovi događaji su pokrenuli opsežnu analizu koju je sproveo Stalni komitet Donjeg doma za pristup informacijama, privatnost i etiku (Standing Committee on Access to Information, Privacy and Ethics, ETHI). Početkom oktobra 2022, ETHI je objavio konačni izveštaj o upotrebi i uticaju tehnologije za prepoznavanje lica, naslovljen „Tehnologija za prepoznavanje lica i rastuća moć veštačke inteligencije".[344] U izveštaju se konstatuje da „aktuelni zakonodavni okvir Kanade ne reguliše adekvatno prepoznavanje lica i AI. Bez odgovarajućeg okvira, tehnologije za prepoznavanje lica i drugi alati veštačke inteligencije mogli bi da nanesu nepopravljivu štetu građanima."

Komitet je istakao potrebu za jakim zakonodavnim okvirom koji štiti prava na privatnost i građanske slobode. S obzirom na odsustvo takvog okvira, Komitet je predložio nacionalni moratorijum na upotrebu prepoznavanja lica, posebno u radu policijskih službi. U izveštaju je naglašena važnost davanja većih ovlašćenja saveznom povereniku za privatnost, uključujući izdavanje naredbi i izricanje kazni, poput onih koje propisuje Opšta uredba EU o zaštiti podataka. Takođe je ukazano na nedostatak transparentnosti kao značajno pitanje u vezi sa upotrebom prepoznavanja lica u radu organa za sprovođenje zakona. Javnost obično saznaje za upotrebu ove tehnologije putem medijskih izveštaja, procurelih dokumenata i zahteva za slobodan pristup informacijama.

Kanadska klinika za internet politike i javni interes „Samuelson-Glushko" (Canadian Internet Policy and Public Interest Clinic, CIPPIC) objavila je u septembru 2020. izveštaj o upotrebi prepoznavanja lica na granici Kanade i SAD.[345] U njemu se ističe da usvajanje sistema za prepoznavanje lica širi prakse nadzora i izvan sektora upravljanja granicama, omogućava prenamenu u odnosu na izvorni kontekst, te omogućava automatizaciju drugih alata za procenu. Odsustvo zakonske zaštite omogućava ad hoc usvajanje bez odgovornosti. U izveštaju se zaključuje da u procesu usvajanja tehnologije prepoznavanja lica nije bilo transparentnosti ni dovoljnih zaštitnih mera.

Dok je ETHI Komitet pozivao na moratorijum, kolektiv od 77 zagovornika privatnosti, ljudskih prava i građanskih sloboda, uključujući Međunarodnu grupu za monitoring građanskih sloboda, uputio je pismo ministru javne bezbednosti 2020. godine, zahtevajući potpunu zabranu upotrebe nadzornih tehnologija za prepoznavanje lica u saveznim organima za sprovođenje zakona i obaveštajnim službama.[346]

Međutim, tokom 2023. i 2024. sve više policijskih uprava javno je govorilo o načinima na koje koriste tehnologiju za prepoznavanje lica, mada ima i onih koji trvde da to neće činiti pre nego što budu usvojena odgovarajuća zakonska pravila.[347] Poverenik nadležan u Ontariu izdao je detaljne smerinice za policijske uprave koje imaju takve prakse, a koje obuhvataju sve faze od pribavljanja sistema do njegove evaluacije tokom upotrebe.[348] Policija u oblasti York se već oslanja na ove smerinice i na svom vebsajtu je, u formi čestih pitanja i odgovora, objavila informacije o tome kako koristi tehnologiju za prepoznavanje lica u svojoj praksi.[349]

PRAVNI OKVIR

Regulacija biometrije u Kanadi trenutno je rasuta u raznim propisima: od Kanadske povelje o pravima i slobodama,[350] preko sudskih presedana do drugih zakona, uključujući legislativu o privatnosti. Važeći savezni zakoni o privatnosti, Zakon o privatnosti iz 1985.[351] i Zakon o zaštiti ličnih podataka i elektronskim dokumentima (PIPEDA, 2000)[352] takođe imaju odredbe koje regulišu biometriju, iako su stare već nekoliko decenija. Stručnjaci ističu da je fragmentisano zakonodavstvo na saveznom, pokrajinskom i teritorijalnom nivou potrebno zameniti jednim krovnim zakonom koji sveobuhvatno pokriva javni, privatni, neprofitni sektor i političke partije.

Pravni okvir za regulisanje AI trenutno ne postoji. Međutim, Kanada je implementirala Direktivu o automatizovanom donošenju odluka (Automated Decision-Making, ADM Direktiva),[353] koja propisuje uslove za upotrebu automatizovanih sistema odlučivanja na nivou saveznih vlasti, prvenstveno fokusirajući se na upravljanje rizikom. U ADM Direktivi nedostaju posebne odredbe za bilo koju vrstu tehnologije biometrijskog nadzora i ona ne pokriva AI sisteme koji se koriste u sistemu krivičnog pravosuđa. Saveznoj vladi je tako omogućeno da primenjuje različite kontroverzne tehnologije bez usaglašavanja sa Direktivom.

Savezni propisi o privatnosti trenutno prolaze kroz značajnu reviziju u vidu novog zakonodavnog akta pod oznakom Predlog C-27, što je prilika da se popune neke od praznina u postojećim propisima.[354] Predlog C-27 obuhvata tri nova zakona: Zakon o zaštiti privatnosti potrošača (Consumer Privacy Protection Act, CPPA), Zakon o Tribunalu za zaštitu ličnih informacija i podataka (Personal Information and Data Protection Tribunal Act, PIDPTA) i Zakon o veštačkoj inteligenciji i podacima (Artificial Intelligence and Data Act, AIDA).

Zakon o privatnosti i PIPEDA

Kanada ima dva savezna propisa o privatnosti: Zakon o privatnosti (1985), koji reguliše upotrebu ličnih podataka na nivou saveznih vlasti, i Zakon o zaštiti ličnih podataka i elektronskim dokumentima (PIPEDA, 2000), koji se primenjuje na preduzeća. Zakon o privatnosti se odnosi na javne usluge kao što su penzije, osiguranje za nezaposlene, bezbednost granica i oporezivanje, ali se ne primenjuje na političke stranke.

PIPEDA postavlja pravila za prikupljanje, upotrebu i otkrivanje ličnih podataka u delatnosti privatnih kompanija koje se bave komercijalnim aktivnostima, ali ne važi u Alberti, Britanskoj Kolumbiji i Kvebeku, gde su na snazi slični pokrajinski zakoni.

Takođe, PIPEDA se primenjuje na kompanije koje podležu federalnoj regulativi i lične podatke njihovih zaposlenih. Pokrajinski zakoni o privatnosti postoje za vladine agencije, zdravstvene informacije, informacije vezane za zapošljavanje, a primenjuju se i sektorski zakoni.[355]

PIPEDA i Zakon o privatnosti ne definišu biometrijske podatke drugačije od drugih vrsta ličnih podataka. Poverenik za privatnost Kanade objavio je odluke u vezi sa biometrijskim podacima u više slučajeva, uključujući glasovnu autentifikaciju u kontekstu zapošljavanja i prikupljanje otisaka prstiju za polaganje testa na pravnom fakultetu.[356] U takvim slučajevima, Poverenik primenjuje standardni test za procenu prikladnosti naznačene svrhe prikupljanja ličnih podataka, postavljajući sledeća pitanja:

- da li je mera dokazivo neophodna da bi se ispunila određena potreba;
- da li će verovatno biti delotvorna za ispunjavanje potreba;
- da li je gubitak privatnosti proporcionalan stečenoj koristi; i
- da li za postizanje istog cilja postoji način manje invazivan po privatnost?

Kancelarija poverenika za privatnost Kanade je 2021. ažurirala svoje smernice kako bi razjasnila vrste ličnih podataka koji se načelno smatraju osetljivim prema PIPEDA i toj grupi dodala biometrijske podatke.[357] Prema PIPEDA, privatne kompanije moraju da štite osetljive lične podatke odgovarajućim merama i da traže izričitu saglasnost kada je verovatno da će se informacije smatrati osetljivim.

Predlog C-27: CPPA, PIDPTA & AIDA

Predlog C-27, poznat i kao Akt za implementaciju digitalne povelje iz 2022, drugi je pokušaj revizije federalnog režima privatnosti. Ovaj predlog ima za cilj uspostavljanje tri nova zakona: Zakon o zaštiti privatnosti potrošača (CPPA), Zakon o Tribunalu za zaštitu ličnih informacija i podataka (PIDPTA) i Zakon o veštačkoj inteligenciji i podacima (AIDA).

CPPA i PIDPTA su revidirane verzije iz 2020. godine, koje nisu usvojene zbog raspuštanja parlamenta za savezne izbore 2021, dok je AIDA potpuno novi zakon. Kao rezultat, Zakon o zaštiti ličnih podataka i elektronskim dokumentima (PIPEDA) će biti izmenjen i dopunjen tako da postane Zakon o elektronskim dokumentima, uklanjajući odredbe o privatnosti.

Prema predloženom tekstu CPPA, privatne kompanije bi morale da pruže jasno objašnjenje za svoju upotrebu bilo kog automatizovanog sistema odlučivanja koji bi mogao značajno da utiče na građane. To uključuje sisteme koji daju predviđanja, preporuke ili odluke o pojedincima. Na zahtev, kompanije koje koriste takve sisteme takođe moraju da pruže objašnjenje o tome kako se donose odluke, tačnije, „o vrsti ličnih podataka korišćenim za predviđanje, preporuku ili odluku, izvoru informacija i razlozima ili glavnim faktorima koji su doveli do predviđanja, preporuke ili odluke“.[358]

Privatnim kompanijama koje budu kršile odredbe CPPA, prete značajne kazne: mogu se izreći administrativne novčane kazne, u rasponu od 10 miliona kanadskih dolara ili 3 odsto bruto globalnog prihoda kompanije za opšta kršenja, pa do 25 miliona kanadskih dolara ili 5 odsto bruto globalnog prihoda kompanije za određena namerna krivična dela. Kanadski poverenik za privatnost neće direktno izricati ove kazne, već će dati preporuke Tribunalu za zaštitu ličnih informacija i podataka, koji će imati ovlašćenje

da izriče kazne. Žalbe na druge odluke Poverenika takođe se mogu uložiti Tribunalu.

Uvođenje AIDA-e predstavlja jednu od najznačajnijih promena Predloga C-27, koja ima za cilj da nametne nove obaveze upravljanja i transparentnosti preduzećima koja dizajniraju, razvijaju i koriste sisteme veštačke inteligencije. Prema tom predlogu, svako ko je odgovoran za sistem veštačke inteligencije moraće da utvrdi da li se kvalifikuje kao „sistem sa visokim uticajem". Ako je to slučaj, obavezna je primena mera za identifikaciju, procenu i ublažavanje potencijalnih rizika, kao što su šteta ili pristrasni ishodi uzrokovani radom sistema. Usklađenost sa ovim merama se takođe mora pratiti i dokumentovati.

Kategorizacija AI sistema na osnovu nivoa rizika u skladu je sa načinom na koji Evropska unija pristupa regulaciji veštačke inteligencije. Međutim, konkretna definicija sistema visokog rizika tek treba da se utvrdi kroz buduće propise. Takođe treba istaći da Uredba EU o veštačkoj inteligenciji eksplicitno zabranjuje specifične sisteme veštačke inteligencije koji se smatraju neprihvatljivo štetnim, kao što su manipulativni ili eksploatacioni sistemi i daljinska biometrijska identifikacija u realnom vremenu koju koriste organi za sprovođenje zakona – dok trenutni predlog AIDA ne uključuje zabranu AI sistema sa neprihvatljivim rizicima.

Još jedna ključna razlika je u tome što bi obim AIDA mogao biti ograničeniji u poređenju sa evropskim zakonom. Definicija AI sistema prema AIDA pokriva samo tehnološke sisteme koji obrađuju podatke autonomno ili delimično autonomno. Nasuprot tome, Uredba EU ne zahteva nužno nikakav stepen autonomije i obuhvata sisteme veštačke inteligencije razvijene korišćenjem određenih tehnika kao što su mašinsko učenje, pristupi zasnovani na logici i statistički pristupi.

Ne navodeći konačnu listu, Prateći dokument za AIDA koji je objavilo kanadsko ministarstvo za inovacije, nauku i ekonomski razvoj (Innovation, Science, and Economic Development, ISED) uključuje primere sistema koji bi mogli da se svrstaju u kategoriju visokog rizika.[359] Među njima su biometrijski sistemi koji se koriste za identifikaciju i zaključivanje, i sistemi koji se koriste za predikcije o ljudima. ISED ističe da „takvi sistemi imaju potencijal za značajan uticaj na mentalno zdravlje i autonomiju".

Prema odredbama o transparentnosti, programeri sistema sa velikim uticajem su obavezni da objave opis sistema jednostavnim jezikom na javno dostupnoj veb stranici. Ovaj opis treba da sadrži informacije o tome kako je sistem namenjen da se koristi, vrstama sadržaja koje generiše, odlukama ili predviđanjima koje donosi i uspostavljenim merama ublažavanja rizika. Pored toga, svako ko je odgovoran za sistem sa velikim uticajem mora odmah da obavesti ministra ako sistem izazove ili će verovatno izazvati materijalnu štetu.

Predloženi zakon propisuje značajne kazne za prekršaje: administrativne kazne za kršenje uslova upravljanja ili transparentnosti mogu iznositi i do 10 miliona kanadskih dolara ili 3 odsto bruto globalnih prihoda. Predlažu se i nova krivična dela u vezi sa sistemima veštačke inteligencije, sa kaznama za preduzeća do 25 miliona kanadskih dolara ili 5 odsto bruto globalnih prihoda. Pojedinci se mogu suočiti sa kaznom do 100.000 kanadskih dolara ili zatvorom za određena dela. Među njima su svesno korišćenje ličnih podataka dobijenih protivzakonito, dizajniranje ili korišćenje štetnih sistema veštačke inteligencije i namerno nanošenje značajnog ekonomskog gubitka. Predložene kazne su veće od onih u važećim propisima.

Sprovođenje AIDA-e, isključujući krivična dela, nadgledao bi novoosnovani poverenik za veštačku inteligenciju i podatke. Krivično gonjenje bi bilo u nadležnosti državnog tužilaštva Kanade, pri čemu bi ministar bio u mogućnosti da upućuje slučajeve tužilaštvu, ali ne i da učestvuje u procesu. Pored toga, spoljni stručnjaci bi pružali podršku administraciji u sprovođenju AIDA-e, nezavisni revizori bi sprovodili revizije, a savetodavni komitet bi bio imenovan za pomoć u aktivnostima sprovođenja.

Predloženi rok za usvajanje AIDA-e znači da nova pravila neće stupiti na snagu pre 2025. godine.

Kvebek

Kvebek je 2001. godine bio prva jurisdikcija u Kanadi koja je uvela zakon o uspostavljanju pravnog okvira za informacione tehnologije (QC IT Act), koji uključuje posebne odredbe za korišćenje baza biometrijskih podataka kako bi se obezbedio adekvatan nivo zaštite.[360] Nedavni amandman na QC IT Zakon, pod oznakom QC Predlog 64, nameće nove zahteve u vezi sa izveštavanjem o biometrijskim sistemima koji se koriste u svrhe identifikacije ili verifikacije. Kompanije moraju da obaveste Komisiju za pristup informacijama (Commission d'accès à l'information, CAI) o svakoj obradi koja uključuje biometrijske informacije, bez obzira da li se čuvaju

u bazi podataka, najmanje 60 dana pre nego što se baza biometrijskih podataka stavi u funkciju. CAI ima ovlašćenja da uspostavi i upravlja takvim bazama, kao i da naredi njihovo uništavanje ako nisu usklađene sa zakonom ili narušavaju privatnost. Konačno, Predlog 64 označava biometrijske informacije kao osetljive, što znači da kompanije treba da uspostave dodatne mere zaštite kada ih obrađuju.

Da bi ublažile pravne rizike povezane sa obradom biometrijskih informacija, kompanije moraju uzeti u obzir intruzivnost tehnologije, svrhu upotrebe, alternativne procese i način na koji se biometrijskim informacijama upravlja, odnosno način njihovog uništenja. Procena nivoa rizika po privatnost može pomoći u uspostavljanju smernica i sprovođenju procena uticaja na privatnost kako bi se identifikovali i ublažili rizici. Ove procene će postati obavezne od 22. septembra 2023. u skladu sa QC Predlogom 64 kada se lične informacije dele van Kvebeka, kreiraju ili pribavljaju digitalni sistemi koji uključuju privatne podatke ili kada se otkrivaju lične informacije bez saglasnosti u istraživačke svrhe.

Stručnjaci ističu da je problem sa propisima o privatnosti Kvebeka u tome što nameću obaveze samo kada se biometrija koristi za proveru identiteta, i navode da bi njihov obim trebalo proširiti i na druge svrhe.[361] Centar za medije, tehnologiju, demokratiju i politike sajber bezbednosti preporučio je usklađivanje Zakona o privatnosti i PIPEDA-e sa ADM direktivom savezne vlade.[362]

PRAVNA PRAKSA

Vrhovni sud Kanade priznao je ustavno pravo na privatnost pre nekoliko decenija, u slučaju R. v Dyment (1988).[363] U odluci se ističe da je „privatnost u srcu slobode u modernoj državi [...] Usađena u fizičku i moralnu autonomiju čoveka, privatnost je od suštinskog značaja za dobrobit pojedinca. Samo zbog toga je dostojna ustavne zaštite, ali ima i dubok značaj za javni poredak. Ograničenja koja su nametnuta vladi pri zadiranju u živote građana spadaju u suštinu demokratske države."

U predmetu R. v Spencer (2014), Vrhovni sud Kanade je presudio da pojedinci zadržavaju pravo na privatnost čak i kada su u javnom prostoru.[364] Vrhovni sud je istakao da se ljudi često ponašaju drugačije kada slute da su posmatrani, a ovaj strah od nadzora sam po sebi „uništava osećaj opuštenosti i slobode [ponašanja]" koji anonimnost pruža – sužavajući opseg autonomnih izbora dostupnih građanima.

U predmetu Wansink v Telus Communications Inc. (2007), federalni apelacioni sud je potvrdio odluku Poverenika za privatnost Kanade kojom je utvrđeno da prikupljanje i čuvanje glasovnih otisaka zaposlenih za potrebe prepoznavanja glasa prilikom daljinskog pristupa internoj računarskoj mreži kompanije, ne predstavlja narušavanje privatnosti zaposlenih.[365] Sud je našao da su svrhe prikupljanja razumne i da je Telus preduzeo odgovarajuće mere bezbednosti da zaštiti te podatke. Takođe je odlučio da se od zaposlenih mora dobiti saglasnost, uz napomenu da Telus ne može da dobije glasovne otiske bez znanja i učešća pojedinca. Sud je stao na stanovište da glasovni otisci nisu osetljivi podaci.

U predmetu IKO Industries Ltd. v. U.S.W.A. (2005) arbitar iz Ontarija utvrdio je da upotreba sistema za skeniranje otiska prsta kod poslodavca predstavlja narušavanje privatnosti zaposlenih i da se ne može opravdati.[366] IKO Industries Ltd. (poslodavac) se žalio na odluku arbitra, ali je Vrhovni sud Ontarija potvrdio odluku, navodeći da je zasnovana na balansiranju interesa poslodavca i zaposlenog. U ovom slučaju, narušavanje privatnosti nije bilo značajno, ali interes poslodavca ipak nije prevagnuo, s obzirom na okolnosti radnog mesta i dostupne alternative.

Međutim, u drugom arbitražnom slučaju odlučeno je da skeniranje otiska prsta nije narušavalo privatnost.[367] Arbitar je uzeo u obzir relevantne slučajeve biometrije rešavane po osnovu zakona o radu, a ne zakona o privatnosti, i zaključio da je skeniranje trajalo manje od jednog minuta, da nije uključivalo intimne delove tela i da je pokrilo samo pola otiska prsta, koji je odmah konvertovan u niz brojeva bez ličnih podataka.

KENIJA

KONTEKST

Prema izveštaju za 2021. koji je pripremio Institut za razvojne studije, Kenija ima dugu istoriju državnog nadzora koji je poslednjih godina delimično podstaknut borbom protiv terorizma i pranja novca, kao i merama u oblasti javnog zdravstva.[368] Čini se da želja za pojačanim nadzorom građana dobija na zamahu,[369] uz državne planove za razvoj obrade biometrijskih podataka, uključujući i onu koja koristi prepoznavanje lica.

U Keniji su u poslednjih pet godina započeta tri projekta čiji je cilj uspostavljanje nacionalne šeme za identifikaciju građana, a sva tri uključuju prikupljanje i obradu biometrijskih podataka. Ovi projekti su redom nailazili na otpor civilnog društva i stručnjaka zbog raznih rizika, uključujući bojazan od masovnog nadzora i netransparentnog korišćenja podataka.

Najpre, zakon kojim se uspostavlja Nacionalni integrisani sistem upravljanja identitetom (National Integrated Identity Management System, NIIMS), nalik projektu ABIS u Južnoj Africi i sistemu Aadhaar u Indiji, usvojen je 2019. Bilo je predviđeno da NIIMS bude „jedinstveni izvor ličnih informacija svih Kenijaca, kao i stranaca sa prebivalištem u Keniji“.[370] Svaka osoba u sistemu trebalo je da dobije lični identifikacioni broj pod nazivom „Huduma Namba“. Prilikom pristupanja državnim i privatnim uslugama, broj bi bio neophodan za identifikaciju, zajedno sa biometrijskim šablonima poput otisaka prstiju, kao i slika lica, ušnih školjki i irisa.[371]

Međutim, nova kenijska vlada i predsednik izabrani 2022. godine, napustili su ovaj projekat. U januaru 2023. predsednik Vilijam Ruto najavio je plan za novu šemu digitalne identifikacije u roku od 12 meseci, navodeći da se vlada neće baviti izdavanjem ličnih karata,

već identifikacijom Kenijaca.[372] U maju iste godine, vladini zvaničnici su objavili novi rok za implementaciju u martu 2024. napominjući da je glavna svrha identifikacionog programa „omogućiti optimalan pristup državnim uslugama".[373] Na sastanku proširenog skupa panafričkog pokreta ID4Africa, održanom u maju 2023, zvaničnici su najavili da će u program biti uključene i karakteristike za biometrijsku identifikaciju. Prema tim planovima, vlada će unaprediti trenutno postojeći automatizovani sistem identifikacije otisaka prstiju (nazvan „AFIS") kako bi uključio prepoznavanje irisa i lica, što bi rezultiralo kreiranjem „automatizovanog biometrijskog sistema identifikacije".[374] Takođe, ova šema elektronske identifikacije treba da omogući autentifikaciju na vebu preko čipa i QR koda, dok bi čitav program bio povezan sa novim nacionalnim identifikacionim brojem ili Jedinstvenim ličnim identifikatorom (Unique Personal Identifier, UPI).[375] Takođe se navodi da su ovi planovi motivisani „bezbednosnim pretnjama"[376] i rizicima „krađe identiteta", protiv čega bi trebalo da se bori „konsolidacijom i digitalizacijom postojećih baza podataka" kojima rukuje vlada.[377] Ima, dakle, razloga za zabrinutost zbog rizika od „neprimetnih funkcija" u ovom projektu, jer vlada može da proglasi nove svrhe za upotrebu tako sveobuhvatnog sistema identifikacije tokom njegove implementacije, pa i u kasnijoj fazi kada se svi podaci prikupe i baze podataka povežu. Ova zabrinutost izvire i iz činjenice da se predsednik Ruto pre izbora „snažno protivio uvođenju Huduma Namba",[378] a sada kad se dizajnira nova identifikaciona šema, nema objašnjenja o tome kako će se ona razlikovati od NIIMS-a.

Nepoverenje u funkcionisanje novog sitema nastavilo se i tokom trećeg pokušaja implementacije eID projekta nazvanog „Maisha Namba". Ovaj projekat takođe ima za cilj da se u okviru jedinstvene šeme elektronske identifikcije na centralizovan način prikupljaju i obrađuju biometrijski podaci. Opravdanost prikupljanja takvih podataka nadležni organi, navodno, procenju putem pripreme odgovarajućih procena uticaja na zaštitu podataka. Međutim, takva dokumenta još uvek nisu javno dostupna.[379] Glavne zamerke koje stručnjaci upućuju projektu ostaju kao i za njegove prethodnike, a tiču se sumnji u neovlašćeno korišćenje i deljenje podataka iz jedne jedistvene baze među različitim državnim organima.[380] Naležni sudovi su donosili više privremenih mera kojima su zaustavljali dalju implementaciju Maisha Namba projekta, dok civilno društvo tvrdi da je projekat neustavan.[381]

Što se tiče upotrebe biometrijskih podataka u radu policije, još 2018. godine je objavljeno da su kenijske policijske snage lansirale prepoznavanje lica na gradskoj CCTV mreži, u okviru paketa za upravljanje kritičnim incidentima (Critical Incident Management Suite, CIMS) koji nadgleda Uprava za krivične istrage.[382] Ova primena prepoznavanja lica obuhvatala je instalaciju hiljada kamera duž glavnih puteva i autoputeva,[383] fokusiranih na ulice i aerodrome u Najrobiju i Mombasi.[384]

Pored unapređenja bezbednosti i smanjenja kriminala, među motivima za uvođenje biometrije navodi se i sprečavanje prevara. Prema javno dostupnim informacijama, u sudskom predmetu povodom neophodnosti instaliranja opreme za biometrijsku registraciju i verifikaciju pacijenata i podnošenje e-zahteva za plaćanje, 850 bolnica je 2021. godine tužilo Nacionalni fond za bolničko osiguranje Kenije (National Hospital Insurance Fund, NHIF).[385] NHIF je tvrdio da biometrijska registracija ima za cilj rešavanje prevara, kao i ubrzavanje naplate potraživanja u zdravstvu. Ukoliko se ovaj projekat sprovede, od bolnica će se očekivati da verifikuju identitet pacijenata skeniranjem otiska prsta, umesto da od pacijenata traže ličnu kartu na uvid.[386] Nema dostupnih informacija o ishodu ovog spora.

Jedan slučaj od šireg značaja koji se tiče prepoznavanja lica u privatnom sektoru uključuje telekomunikacionu kompaniju Safaricom, koja je od svojih korisnika tražila da se ponovo registruju uz pomoć ove tehnologije. Naime, Uprava za komunikacije Kenije je zahtevala od operatora mobilnih usluga da ponovo registruju svoje korisnike, kao meru za suzbijanje kriminala.[387] Safaricom je smatrao da to znači da mogu da primene registraciju sa prepoznavanjem lica kao bezbednosnu funkciju. Međutim, međunarodna organizacija za ljudska prava Access Now reagovala je javnim pismom u kojem je istakla da je takvo prikupljanje podataka u suprotnosti sa kenijskim zakonom i zatražila brisanje podataka.[388]

PRAVNI OKVIR

Član 31 Povelje o pravima, koja je ugrađena u kenijski Ustav, štiti pravo na privatnost, što obuhvata pravo da se informacije koje se odnose na nečiju porodicu ili privatne poslove ne traže niti otkrivaju bez potrebe.[389]

Zakon o zaštiti podataka stupio je na snagu 25. novembra 2019.[390] Ubrzo potom, različita nadležna tela sačinila su nekoliko podzakonskih akata, odnosno pravilnika za regulisanje konkretnih pitanja.[391] Organ za superviziju pod nazivom Poverenik za zaštitu podataka, imenovan je 16. novembra

2020.[392] Poverenik je do sada bio aktivan u davanju smernica o pojedinim pitanjima, od kojih nijedno nije u direktnoj vezi sa obradom biometrijskih podataka.[393] Pravni pejzaž je u velikoj meri oblikovan po uzoru na tradiciju i strukturu zaštite podataka u EU.[394]

Slično Južnoj Africi, kenijski zakon o zaštiti podataka uređuje izuzetke, odnosno situacije kada je obrada ličnih podataka izuzeta od odredbi. Jedna od njih je ista kao u GDPR-u: zakon se ne primenjuje na obradu ličnih podataka kada to radi osoba u okviru čisto privatnih, odnosno aktivnosti u domaćinstvu. Druga dva izuzetka su specifična za Keniju: (1) ako je obrada neophodna za nacionalnu bezbednost ili javni interes; ili (2) da se obelodanjivanje traži prema bilo kom pisanom zakonu ili na osnovu naloga suda. Oba izuzetka su relevantna za obradu biometrijskih podataka u službama za sprovođenje zakona, ali ostaje pitanje koji su zakoni primenjivi u ovim situacijama. Takva obrada bi, dakle, morala da bude regulisana nekim drugim odredbama u kenijskom pravnom sistemu. Štaviše, zakon o zaštiti podataka izričito reguliše da čak i kada su izuzeci primenjivi, nijedan rukovalac ili obrađivač ne može biti izuzet od poštovanja principa zaštite podataka koji se odnose na zakonitu obradu, minimizovanje prikupljanja, kvalitet podataka i primenu bezbednosnih mera za zaštitu ličnih podataka.

Zakon definiše biometrijske podatke kao lične podatke koji su rezultat specifične tehničke obrade zasnovane na fizičkoj, fiziološkoj ili karakterizaciji ponašanja, uključujući analizu krvne grupe, uzimanje otisaka prstiju, DNK analizu, geometriju ušne školjke, skeniranje mrežnjače oka i prepoznavanje glasa. Kao u slučaju južnoafričke POPIA, prepoznavanje lica se ne pominje izričito, ali bi trebalo da se podrazumeva definicijom jer predstavlja fizičku karakterizaciju. Biometrijski podaci su takođe pokriveni definicijom osetljivih ličnih podataka.

Zakon određuje da se moraju registrovati samo posebne vrste aktivnosti obrade. Poverenik ima mandat da propiše prag obavezne registracije, dok zakon o zaštiti podataka ukazuje da u tu svrhu Poverenik mora da razmotri da li se obrađuju osetljivi lični podaci. Prema Pravilniku o zaštiti podataka (registracija rukovalaca i obrađivača podataka) iz 2021, prag registracije se prvenstveno utvrđuje na osnovu godišnjeg prometa rukovaoca i obrađivača.[395] Međutim, postoji lista aktivnosti obrade čija je registracija obavezna bez obzira na promet a to se, između ostalog, odnosi na „sprečavanje kriminala i krivično gonjenje prestupnika (uključujući upotrebu bezbednosnih CCTV sistema)“ kao i na „preduzeća koja obrađuju genetske podatke“.[396] Međutim, osim DNK, biometrijski podaci se ne pominju posebno.

U skladu sa zakonom, u slučajevima kada se osnovne aktivnosti rukovaoca ili obrađivača podataka sastoje od obrade osetljivih ličnih podataka, obavezno je imenovanje službenika za zaštitu podataka. Odredbe koje regulišu položaj i dužnosti službenika za zaštitu podataka vrlo su slične onima u GDPR-u. Ne postoje javno dostupne informacije o tome da li su relevantni rukovaoci imenovali službenike koji nadgledaju obradu biometrijskih podataka.

Osetljivi lični podaci mogu se obrađivati samo ako postoji poseban pravni osnov regulisan članom 45 Zakona o zaštiti podataka, uz poštovanje principa obrade. I ovde je logika veoma slična GDPR-u. Takođe, Poverenik može da propiše dodatni osnov po kom se takvi osetljivi podaci mogu obrađivati. Nijedan od pravnih osnova ne reguliše posebno obradu biometrijskih podataka, tako da se i dalje primenjuje opšti režim za osetljive podatke.[397]

Prenos osetljivih podataka van Kenije dozvoljen je po dobijanju saglasnosti osobe na koju se podaci odnose i Poverenikove potvrde odgovarajućih zaštitnih mera, prema članu 49 Zakona.[398]

Zakonska pravila o automatizovanom odlučivanju vrlo su slična GDPR-u, dok su u nekim aspektima čak i detaljnija od onih iz člana 22. Prema članu 35 kenijskog zakona, osoba na koju se podaci odnose mora biti obaveštena da se odluka o njoj donosi isključivo putem automatizovane obrade. Subjekt podataka tada može zatražiti od rukovaoca ili obrađivača da (1) preispita odluku, ili (2) donese novu odluku koja nije zasnovana samo na automatizovanoj obradi. Štaviše, nakon prijema takvog zahteva, rukovalac ili obrađivač moraju da obaveste osobu na koju se podaci odnose o koracima preduzetim da odgovore na zahtev i ishodu tih aktivnosti, pisanim obaveštenjem.

Neka pravila o obradi biometrijskih i drugih osetljivih podataka mogu se naći u odgovarajućim pravilnicima koji su do sada doneti. Opšti pravilnik o zaštiti podataka iz 2021. propisuje da se podaci, pod uslovom da su ispunjeni uslovi propisani zakonom,[399] mogu prikupljati kroz „biometrijsku tehnologiju, uključujući prepoznavanje glasa ili lica“.[400] Prema članu 49(1) (c) istog pravilnika, u slučaju obrade biometrijskih podataka obavezna je izrada procene uticaja.

Poverenik je objavio niz smernica, uključujući i smernice za pripremu procene uticaja. Nijedna od do sada objavljenih smernica ne bavi se konkretnim pitanjima koja se odnose na biometrijske podatke ili prepoznavanje lica.[401]

Čini se da Kenija danas ima moderan i robustan pravni okvir za obradu ličnih podataka i različite pravne instrumente za rešavanje povišenog

rizika koji proizlazi iz obrade osetljivih podataka, uključujući biometriju. Zabrinjava, međutim, to što za biometrijske podatke nema posebne zaštite fokusirane na njihovo prikupljanje i korišćenje. Budući da su ova pravila nedavno stupila na snagu, ostaje da se vidi da li će biti u stanju da se pozabave relativno raširenom upotrebom biometrijskih sistema.

Jedna presuda Višeg suda Kenije u sporu oko programa Huduma Namba i spremnost Poverenika da izrekne visoke kazne, ohrabrujući su koraci za vladavinu prava, kako ćemo pokazati u narednom odeljku.

PRAVNA PRAKSA

Visoki sud Kenije doneo je dve važne odluke u vezi sa NIIMS-om.

Vlada je, naime, 2019. planirala da uspostavi integrisani identitetski sistem. Prema zakonima donetim u tu svrhu, i državljani Kenije i stranci su obavezni da daju osetljive lične podatke kako bi dobili jedinstveni matični broj, poznat kao Huduma Namba. Inicijativa je od samog početka naišla na snažno protivljenje, iz različitih razloga, uključujući rizike po privatnost.[402]

Visoki sud je 30. januara 2020. odlučio po predstavci tri podnosioca, proglasivši da je prikupljanje DNK i GPS koordinata u svrhu identifikacije prema NIIMS-u, „intruzivno i nepotrebno".[403] Mada prikupljanje drugih biometrijskih podataka nije bilo isključeno po sličnim osnovama, opšti zaključak je glasio da je pravni okvir o poslovanju NIIMS-a „neadekvatan i da predstavlja rizik po bezbednost podataka koji će se prikupljati u okviru sistema".[404] U takvim okolnostima, sud je odlučio da vlada može da nastavi sa implementacijom NIIMS-a samo pod uslovom da postoji odgovarajući i sveobuhvatan regulatorni okvir za njegovu primenu, u skladu sa važećim ustavnim garancijama.[405]

Naredne godine, u odluci donetoj 14. oktobra 2021, kao odgovor na zahtev za obustavu primene Huduma Namba kartice u odsustvu procene uticaja, Visoki sud je zaključio da se Zakon o zaštiti podataka retroaktivno primenjuje na NIIMS.[406] U svom obrazloženju, sud je naveo da „pošto je država odlučila da stavi kola ispred konja [tj. implementira tehnologiju pre donošenja zakona koji je reguliše], mora da se pomiri sa činjenicom da sada postoje propisi u odnosu na koje se njeni postupci moraju odmeravati, bez obzira na to kada su preduzeti, sve dok te radnje utiču na prava građana u skladu sa članom 31 Ustava".[407] Tom presudom Visoki sud je poništio odluku vlade da primeni Huduma Namba kartice, mada privremeno, pošto je naloženo da se sprovede procena uticaja pre nastavka procesa implementacije.[408]

Nakon ove presude, vlada Kenije je tvrdila da je naučila lekciju,[409] dok je u maju 2023. devet grupa za ljudska i digitalna prava izdalo saopštenje za javnost u kojem naglašava potrebu za transparentnošću, učešćem javnosti i poštovanjem zakonskih pravila (uključujući obezbeđivanje odgovarajuće pravne osnove i pripremu odgovarajućih procena uticaja) kao preduslove za primenu nove ID šeme.[410]

Ipak, i novi Maisha Namba projekat naišao je na kritike civilnog društva zbog manjka transparentnosi oko njegove implementacije čim je iniciran u septembru 2023. godine, uz bojazan da će iste greške biti ponovljene.[411] Kao dokaz da lekcije nisu naučene, Visoki sud je u decembru 2023. godine suspendovao dalju implementaciju projekta zbog toga što nije bila pripremljena procena uticaja na zaštitu podataka.[412] Privremena mera zabrane dalje implementacije je ukunuta u februaru 2024. godine, dok je slučaj u meritumu nastavljen pred Ustavnim sudom.[413] Još jedna privremena mera zabrane implementacije je doneta u julu 2024. godine u Visokom sudu, uz obrazloženje da bi mogla nastati nanadoknadiva šteta po građane ukoliko bi Ustavni sud doneo negativnu odluku o čitavom projektu.[414] Međutim, i ova mera je ukunuta zbog toga što je procenjeno da prethodna zabrana nije bila u najboljem javnom interesu.[415]

Prema javno dostupnim informacijama, u vreme pisanja ovog izveštaja nema drugih sudskih odluka u vezi sa upotrebom prepoznavanja lica, uključujući bezbednosne upotrebe u policiji i drugim vladinim službama.

Od značaja je pomenuti prvu kaznu za kršenje Zakona o zaštiti podataka koju je u decembru 2022. izrekao Poverenik.[416] Kažnjena je kompanija koja je narušila privatnost podnosioca žalbe jer je bez pristanka koristila njihovu fotografiju na svom nalogu na Instagramu, kao i naknadnim kršenjem zakonskih obaveza, uključujući odsustvo saradnje sa Poverenikom. Za ovaj prekršaj, kompanija je kažnjena sa 5.000.000 kenijskih šilinga (oko 36.000 evra), što je najviša moguća kazna propisana zakonom. Odluka podleže žalbi, ali ukazuje na spremnost Poverenika da izriče stroge novčane kazne u nastojanjima da obezbedi primenu zakona.

KINA

Koja vrsta pravnog akta reguliše obradu biometrijskih podataka?

Zakon o zaštiti podataka
Da; Zakon o zaštiti ličnih informacija (2021).

Podzakonska akta
Da.

Smernice
Da.

Poseban zakon o biometrijskim podacima
Da, na nivou podzakonskog akta.

Regulativa za službe za sprovođenje zakona
Da, u zakonima o nacionalnoj bezbednosti i borbi protiv terorizma.

Krivični propisi
Da, zakoni o nacionalnoj bezbednosti i borbi protiv terorizma.

Definicija i regulativa prepoznavanja lica

Podaci prikupljeni kroz prepoznavanje lica regulisani su kao osetljivi podaci.

Detalji

Definisani slučajevi posebne upotrebe
· Zakon o zaštiti ličnih informacija reguliše upotrebu videa snimljenih kamerama u javnom prostoru.

Definisane posebne vlasti
· Uprava Kine za sajberspejs služi kao nadzorni organ sa ovlašćenjem da sprovodi istrage, određuje novčane kazne, kao i da donosi mišljenja i smernice.

Definisani posebni uslovi
· Zakonom o zaštiti ličnih informacija uspostavljena su pravila o ograničenju svrhe, a prepoznaje se i koncept pravnog osnova za obradu.
· Obaveze transparentnosti konkretno su propisane Zakonom o zaštiti ličnih informacija.
· Prema propisanim uslovima, mora se pripremiti procena uticaja.

KINA

KONTEKST

Masovni nadzor u Narodnoj Republici Kini jedna je od najsofisticiranijih mreža sistema za nadgledanje koju centralna vlada koristi nad svojim građanima. Savremena kineska šema nadzora pokrenuta je 2003. stvaranjem projekta „Zlatni štit“ koji je prvenstveno bio fokusiran na cenzuru interneta.[417]

Posle tog projekta, Kina je pokrenula još dva programa nadzora: Bezbedni gradovi (2003), koji se fokusira na upozorenja o katastrofama, upravljanje saobraćajem i javnu bezbednost, i SkyNet (2005), program za prepoznavanje lica. Prema nekim izveštajima, „SkyNet može da skenira čitavu kinesku populaciju u jednoj sekundi sa 99,8 odsto preciznosti“ (navodno, ove brojeve su izneli kineski državni mediji).[418] Međutim, te tvrdnje treba uzeti sa rezervom budući da nema nezavisne potvrde – dok s obzirom na veličinu stanovništva Kine, takav nivo tačnosti zapravo podrazumeva mnogo miliona grešaka.

Međutim, jasno je da se u Kini značajna sredstva ulažu u nadzor, čiji budžet daleko premašuje budžet drugih opštinskih službi, sa procenjenih 176 miliona nadzornih kamera u funkciji do 2017.[419]

Biometrijski nadzor se uglavnom koristi u urbanim sredinama u Kini. Do 2010, samo u Pekingu je bilo postavljeno 800.000 kamera za nadzor, dok se gradska policija 2015. hvalila da je grad potpuno pokriven.[420] U maju 2018. softver za prepoznavanje lica je izdao upozorenje službi za obezbeđenje koncerta da je jedan od 60.000 posetilaca osumnjičeni begunac, što je rezultiralo hapšenjem 31-godišnjeg muškarca u roku od nekoliko minuta.[421] Na pojedinim raskrsnicama u

Šangaju, za pešake koji se kreću van pešačkog prelaza, osim 20 juana, kazna podrazumeva i prikazivanje njihove slike na obližnjem ekranu radi javnog sramoćenja.[422]

Razmere upotrebe tehnologija za prepoznavanje lica u Kini su značajne; kineska policija je navodno primenila prepoznavanje lica u službenim naočarima početkom 2018. godine, a pekinška kompanija LLVision Technology Co. prodaje osnovne verzije zemljama u Africi i Evropi.[423] U gradu Hangdžou navodno je moguće kupiti obrok u KFC-u koristeći sistem „Plati osmehom" gde su lica kupaca povezana s njihovim Alipay nalozima; u Jinčuanu se možete ukrcati u autobus sa pozitivnom identifikacijom lica.[424]

Ove prakse se prvenstveno sprovode preko vlade, mada ima navoda o korporativnom nadzoru u vezi sa kineskom vladom. Softverske kompanije Megvii i Neurosoft učestvuju u prikupljanju podataka iz preko dvadeset sektora kineske vlade i na desetine miliona izvora video snimaka, i mogu da otkriju i identifikuju neke osnovne lične podatke.[425] Iako poriče optužbe, kako je objašnjeno u poglavlju o tehnologiji, postoje indicije da je Megvii sarađivala sa kompanijom Huawei na razvoju „ujgurskog alarma" koji može da automatizuje detekciju ujgurskih lica u video nadzoru.[426]

Značajne kontroverze oko prepoznavanja lica u Kini odvijaju se usred kampanje „Snažan udar protiv nasilnog terorizma", koju sprovodi kineska vlada u provinciji Sinđijang.[427] Na policijskim punktovima od Ujgura se često prikuplja DNK, skeniraju im se oči i instalira špijunski softver na njihove telefone radi praćenja onlajn aktivnosti.[428] Ove mere su nesrazmeran odgovor na nekoliko terorističkih napada u Pekingu 2013-2014, što je kulminiralo zatvaranjem oko milion Ujgura u različite kampove, sabirne centre i zatvore širom Sinđijanga.[429] Dešavanja u ovoj pokrajini predstavljaju važnu studiju slučaja, jer pokazuju kako veći kapacitet biometrijskog nadzora može povećati otvorenu represiju. Skoro svaki stanovnik regiona je dostavio svoje biometrijske podatke vlastima na nekom od više hiljada kontrolnih punktova za skeniranje lica i telefona na granicama jurisdikcije.[430] To se dešava u vreme zabrinjavajuće repatrijacije Ujgura iz drugih zemalja, dok je od početka kampanje protiv nasilnog terorizma više od 1.300 Ujgura pritvoreno, deportovano ili izručeno.[431]

Pored toga, bezbednosne službe u Sinđijangu su čak „počele da raspoređuju jata malih dronova za nadzor kako bi se pokrila područja na kojima nema CCTV mreže".[432]

Kina koristi različite tehnike nadzora, preko kamera ili interneta, kako bi stalno nadgledala svoje građane.[433] Proizvod kompanije Huawei, Safe City, koristi monitoring društvenih medija i prepoznavanje lica i registarskih tablica za potrebe „bezbednosti" u kineskim gradovima. Pod administracijom generalnog sekretara Komunističke partije Kine Si Đinpinga, nadzor postaje rasprostranjen i sofisticiran.[434]

Softver „Bezbedan grad" je do 2019. godine primenjen u 73 grada u 52 zemlje, uključujući Nemačku, Francusku, Pakistan, Španiju i Srbiju.[435] Vlasti u Srbiji su 2019. počele da instaliraju planiranih 8.000 kamera, kada je centar Beograda prekriven kamerama sa kapacitetima za prepoznavanje lica, kako ćemo detaljnije izložiti u trećem poglavlju.[436] Dakle, možemo videti da se kineski razvoj biometrije ne odvija u vakuumu.

Ideološki i politički imperativi partijske države oslonjeni su na kineski pravni sistem, sa zakonima i uredbama koji regulišu izradu i upotrebu tehnologija nadzora u privatnim i državnim firmama.[437] Umesto razvoja klime povoljne za zaštitu ostvarivanja prava građana, kineski regulatorni sistem primorava preduzeća da služe kao „nadzorni agenti države".[438] To je bar jednim delom zato što je pravni okvir u Kini za tehnologije nadzora zasnovan na preterano uopštenoj definiciji nacionalne bezbednosti, što služi kao opravdanje za širok spektar praksi nadzora.[439]

PRAVNI OKVIR

Pregled propisa za zaštitu podataka

Zakoni koji regulišu prava privatnosti i pitanja zaštite podataka pojavljuju se u Kini u poslednjih nekoliko godina i, bar na papiru, čini se da su u skladu sa savremenim okvirima zaštite podataka, a pisani su pravnim stilom pod jasnim uticajem prava Evropske unije (rečju, GDPR-a i prethodne Direktive za zaštitu podataka iz 1995).

Za razliku od evropske pravne tradicije, privatnost nije ustavom zaštićeno ljudsko pravo u Kini.[440] Prvi zakon koji reguliše privatnost kao zaštićeno pravo jeste Građanski zakonik,[441] koji je stupio na snagu 1. januara 2021. Prava na privatnost i zaštitu ličnih informacija klasifikovana su kao „prava ličnosti", a u slučaju povrede Građanski zakonik predviđa pravne lekove (iz perspektive deliktnog regulisanja).[442]

Od novembra 2021. Kina takođe ima Zakon o zaštiti ličnih informacija (Personal Information Protection Law, PIPL), koji je usvojen u avgustu 2021. i stupio je na snagu 1. novembra iste godine.[443] PIPL je prvi zakon koji reguliše pitanja zaštite ličnih podataka na sveobuhvatan način. Samo nekoliko godina ranije, kineska legislativa je dobila prvu pravnu definiciju ličnih podataka koja je sadržana u Zakonu o sajber bezbednosti iz 2016.[444] Još jedan važan propis usvojen je 2021. i bavi se pitanjima bezbednosti podataka.[445] Ova tri zakona zajedno regulišu opšti režim zaštite podataka o ličnosti u Kini.

U Kini je na snazi i niz zakona koji regulišu pitanja nacionalne bezbednosti i stoga bi mogli biti relevantni za pravni režim koji se odnosi na masovni biometrijski nadzor. To su Zakon o nacionalnoj bezbednosti iz 2015,[446] Zakon o borbi protiv terorizma iz 2015[447] i Zakon o nacionalnoj obaveštajnoj službi iz 2017. godine.[448] Kao oslonac u vladinim aktivnostima na očuvanju nacionalne bezbednosti, ovi zakoni regulišu opšte zahteve za to kako privatna preduzeća moraju da sarađuju i podržavaju vladine potrebe u sprovođenju zakona i tehnologiji.[449]

Ova regulativa je od septembra 2024. godine dodatno zaokružena propisima o upravljanju bezbednošću mrežnih podataka (Network Data Security Management Regulations), koju je doneo Državni savet. Ova pravila stupila su na snagu 1. januara 2025. Ne regulišu pitanja u vezi sa korišćenjem tehnologije za prepoznavanje lica direktno, već se bave pitanjima digitalne bezbednosti u kontekstu obrade podataka o ličnosti.[450]

U avgustu 2023. godine kineska administracija za sajber prostor je objavila Smernice za upotrebu tehnologije za prepoznavanje lica u privatnom sektoru, koje su još uvek u fazi nacrta. Međutim, one se svakako ne odnose na prakse organa bezbednosti za upotrebu ove tehnologije.[451]

Određena pitanja u vezi sa zaštitom podataka sadržana su i u sektorskim zakonima (kao i podzakonskim aktima) koji regulišu obradu podataka o ličnosti iz ugla svog osnovnog predmeta regulisanja. Takav je slučaj, na primer, sa Krivičnim zakonom, Zakonom o elektronskoj trgovini, Zakonom o ličnoj karti za rezidente, Zakonom o zaštiti prava i interesa potrošača i Zakonom o turizmu.[452]

Na lokalnom nivou postoje incijative da se pooštre pravila za korišćenje prepoznavanja lica ukoliko postoje manje intruzivne mere. U nekim gradovima je to bio slučaj sa zabranom korišćenja ove tehnologije u hotelima radi prijave boravka, između ostalog, zbog pritiska stranih gostiju koji su do skoro bili primorani da se čekiraju u hotelima koristeći svoje biometrijske podatke.[453]

Dodatno, Vrhovni narodni sud i Vrhovno narodno tužilaštvo izdaju tumačenja zakona, od kojih bi neka mogla biti relevantna za obradu biometrije. Među njima se izdvajaju odredbe Vrhovnog narodnog suda „o nekoliko pitanja koja se odnose na primenu prava u građanskim predmetima koji uključuju obradu ličnih informacija korišćenjem tehnologije prepoznavanja lica“.[454]

Nadležni državni organi takođe izdaju nacionalne standarde koji obično nisu obavezni, ali ih „preduzeća načelno smatraju uputstvom za dobru praksu“,[455] dok se standardi „Tehnologija informacione bezbednosti – Specifikacija bezbednosti ličnih informacija“[456] i „Tehnologija informacione bezbednosti – zahtevi za bezbednost podataka za prepoznavanje lica“[457] konkretno bave tehnologijom za prepoznavanje lica.

Neki od zakona regulišu veoma slične ili čak iste teme, budući da su doneti u vreme kada su određenim specifičnim propisima doneta nova sistemska pravila, sadržana uglavnom u Građanskom zakoniku i PIPL-u. Sledstveno tome, kineski pravni režim zaštite podataka je složen, pravila o istoj stvari se preklapaju, a razlike pravnog režima za javne i privatne aktere nisu uvek do kraja jasne.

Odredbe relevantne za biometrijski nadzor

Građanski zakonik

Celo jedno poglavlje Građanskog zakonika (poglavlje VI) posvećeno je pravu na privatnost i zaštitu ličnih podataka. Definicija ličnih podataka iz člana 1034 izričito obuhvata biometrijske informacije, ali bez definicije takvih podataka, dok biometrija nije uključena u kategoriju osetljivih podataka. Građanski zakonik sadrži nekoliko opštih pravila (od kojih su neka prilično slična GDPR-u) u vezi sa obradom ličnih podataka, kao što su:

- **Načela obrade (član 1035)** – obrada mora biti „u skladu sa principima zakonitosti, opravdanosti i u granicama neophodnosti, i ne sme se preterano obrađivati“.
- **Uslovi za obradu (član 1035)** – obrada je dozvoljena pod sledećim uslovima: (1) osoba je dala saglasnost za obradu svojih

podataka ili je obrada na drugi način dozvoljena zakonom ili administrativnim propisom (dakle, podzakonski akti, koji su niži od zakona, mogu pružiti pravni osnov za obradu ličnih podataka); (2) transparentnost je obezbeđena; (3) svrha, metod i obim obrade su jasno naznačeni; i (4) obrada ne krši nikakva pravna pravila.

» **Prava građana (član 1037)** – regulisano je nekoliko vrsta prava, uključujući pravo na kopiju, pravo na ispravku i pravo na brisanje, ali veoma uopšteno.

» **Otkrivanje i bezbednost podataka (član 1038)** – postoje opšta pravila koja ograničavaju deljenje podataka, kao i opšte odredbe koje regulišu mere bezbednosti kako bi se sprečilo „curenje, neovlašćeno menjanje ili gubitak podataka" (uključujući obavezu obaveštavanja nadležnih regulatornih organa i osobe na koje to utiče).

Građanski zakonik takođe ima odredbu (član 1036) koja reguliše kada „akter" koji obrađuje lične podatke ne snosi nikakvu građansku odgovornost za takvu obradu. Dve takve situacije su kada postoji saglasnost i kada su podaci već javni (što je slično pravilu „očigledno je objavljeno" iz člana 9 GPDR-a). Međutim, treća situacija je veoma široko definisana i uključuje slučajeve kada „akter razumno čini druge radnje da bi zaštitio javni interes ili zakonita prava i interese osobe". Javni interes nije definisan u Građanskom zakoniku i može se samo nagađati kakav interes državni projekat nadzora može da pokriva. Kao što je uvek slučaj sa ovako široko definisanim pravilima, ili čak pravnim standardima, sudska praksa bi trebalo da pruži neka pojašnjenja i smernice.

Konačno, Građanski zakonik sadrži opšta pravila koja na poverljivost obavezuju državu, javne organe i javne funkcionere, ali ne reguliše sankcije za kršenje ovih pravila.

Sve u svemu, pravila iz Građanskog zakonika pružaju određena prava građanima, koja se mogu primeniti u skladu sa drugim domaćim zakonima, ali ne daju smernice u pogledu obaveza države u kontekstu projekata masovnog nadzora – osim principa, čija relevantnost ostaje da se proveri u praksi.

Zakon o zašiti ličnih informacija

PIPL je u velikoj meri inspirisan tekstom i strukturom GDPR-a (između ostalog, u pogledu pravne osnove za obradu, obaveza obaveštavanja i transparentnosti, kvaliteta saglasnosti, prava građana, mera bezbednosti, prekograničnih transfera itd.). Za razliku od GDPR-a, kao i propisa u Keniji i Južnoj Africi, na primer, PIPL ne izuzima nijedno državno telo od primene odredbi. Međutim, ima posebno poglavlje od pet članova koje reguliše obradu ličnih podataka u radu državnih organa.

Prema tim odredbama, državni organi moraju da obrađuju informacije u skladu sa važećim sektorskim zakonima, ali ne smeju „preći obim i granice neophodne za obavljanje svojih zakonskih obaveza" (član 34). Kako ćemo pokazati u nastavku, to je jedan od nekoliko opštih principa koji mogu pravno uticati na projekte masovnog biometrijskog nadzora u Kini, dok su relevantna i konkretna zakonska ograničenja, dužnosti i restrikcije retki u zakonodavstvu koje se razmatra za ovu knjigu. Prema ovom poglavlju PIPL-a, državni organi takođe moraju da ispunjavaju svoje obaveze transparentnosti i čuvaju podatke u Republici Kini (sa nekim ograničenim izuzecima).

U načelu, PIPL zauzima pristup sličan GDPR-u kada je u pitanju obrada biometrijskih podataka koji su regulisani u okviru šire kategorije „osetljivih ličnih podataka". Međutim, jedna odredba posebno reguliše upotrebu tehnologije za prepoznavanje lica u javnim prostorima (iako ne koristi izraz „prepoznavanje lica" u ovom konkretnom članu).

Član 26 PIPL-a glasi: „Oprema za prikupljanje slika i ličnu identifikaciju na javnim mestima postavlja se samo kada je to neophodno radi održavanja javne bezbednosti i postavlja se u skladu sa odgovarajućim odredbama države i sa istaknutom napomenom. Prikupljene lične slike i informacije o identifikaciji mogu se koristiti samo u svrhu održavanja javne bezbednosti i, osim ako se pribavi poseban pristanak pojedinaca, neće se koristiti u bilo koju drugu svrhu."

Najpre, ova odredba ne reguliše obradu podataka koja uključuje prepoznavanje lica, već se fokusira na instalaciju opreme i prikupljanje. Takođe, ne govori o obradi slika ili video zapisa koji nisu prikupljeni u javnim prostorima. U pogledu prikupljanja slika u javnim prostorima, odredba sadrži trostruko pravilo: (1) jedina dozvoljena svrha za postavljanje identifikacione opreme i prikupljanje slika je „održavanje javne bezbednosti" (koju PIPL ne definiše) i nijedna druga svrha nije dozvoljena, osim uskog

izuzetka kada se dobije saglasnost (prema članu 14 PIPL-a, saglasnost mora biti „dobrovoljna, izričita i potpuno informisana“); (2) mora postojati transparentnost u smislu da treba da postoje „napomene“ kojima se javnost obaveštava o prikupljanju slika i mogućnosti identifikacije (zahtev za obaveštavanje je naglašen u ovom članu, pored opšteg načela iz člana 7 o „otvorenosti i transparentnosti“); (3) svi ostali državni zakoni moraju biti poštovani prilikom instalacije opreme i prikupljanja podataka. Iako to nije eksplicitno navedeno u ovoj odredbi, na osnovu formulacije možemo spekulisati da samo država može da instalira opremu za prepoznavanje lica u javnim prostorima. To ona može učiniti samo u cilju „održavanja javne bezbednosti“, što je jedinstvena, ali dovoljno široka svrha da obuhvati sve vrste državnih inicijativa. Tako široka svrha se može tumačiti da pokrije gotovo sve namere javnih organa, bez garancija da ti organi vlasti neće preterano koristiti ili čak zloupotrebiti tehnologiju. U praksi, to bi moglo poslužiti kao prolaz za različite državne projekte masovnog nadzora.

U članu 24 PIPL takođe prepoznaje pojam automatizovanog odlučivanja i reguliše pravila transparentnosti i pravičnosti kada postoji ova vrsta obrade. Slično GDPR-u, član 24 reguliše situaciju kada se ova obrada koristi za donošenje odluke koja može imati značajan uticaj na prava i interese pojedinca. Kada je to slučaj, pojedinac ima pravo da zahteva pojašnjenje, kao i pravo da odbije odluku koja je doneta samo putem automatizovanog odlučivanja.

Osetljive lične podatke PIPL definiše nešto drugačije nego GDPR. Naime, postoji otvorena definicija prema kojoj se radi o „informacijama koje ako procure ili se nezakonito upotrebe mogu lako dovesti do povrede ličnog dostojanstva osobe ili ugroziti njenu ličnu bezbednost ili imovinu, uključujući informacije kao što su na primer biometrijske [...]“ (član 28). Mada je biometrija izričito navedena kao prva vrsta takvih informacija, PIPL ne daje posebnu definiciju biometrijskih podataka (kao ni Građanski zakonik).

U poređenju sa Građanskim zakonikom, PIPL se ne bavi detaljno regulisanjem obrade osetljivih informacija. Prema odredbama PIPL-a, primenjuju se sledeća pravila:

- Svaka obrada osetljivih informacija je dozvoljena „samo kada postoji određena svrha i kada je to neophodno, u okolnostima pod kojima se preduzimaju stroge mere zaštite“ (član 28).
- Prema opštem režimu, obrada osetljivih informacija mora biti zasnovana na saglasnosti, a posebna pravila o transparentnosti uključuju obavezu davanja informacija o uticaju koje ona ima na prava i interese pojedinca (članovi 29 i 30).
- Subjekti koji obrađuju podatke o maloletnicima mlađim od 14 godina, moraju izraditi posebna pravila, ali nema dodatnih uputstava o tome šta ta posebna pravila treba da regulišu (član 31).
- Drugi zakoni i uredbe mogu regulisati obradu posebnih ličnih podataka, u kom slučaju te odredbe imaju prednost u odnosu na odredbe koje predviđa PIPL – verovatno u skladu sa opštim ograničenjem iz člana 28.

Takođe, prema članu 55 PIPL-a, u slučaju obrade osetljivih ličnih podataka ili automatizovanog odlučivanja, moraju se pripremiti „izveštaj o proceni uticaja na zaštitu ličnih informacija“ i „evidencija o obradi“. Mada je minimalni sadržaj ovog izveštaja regulisan u članu 56, ne postoji pravilo da takav izveštaj mora da pregleda ili odobri neki nezavisni organ (što je standardno pravilo u zakonodavstvu EU odakle je ovaj institut preuzet).

Osim principa načelnog ograničenja svrhe, neophodnosti i bezbednosti, PIPL ne donosi druga pravila koja bi izričito ograničila masovnu državnu obradu biometrijskih informacija, u skladu sa važećim zakonima.

Drugi propisi

Kineski zakon o borbi protiv terorizma u određenoj meri reguliše ovlašćenja države za nadzor. Tako, na primer, prema članu 27 ovog zakona, lokalne samouprave na svim nivoima imaju obavezu da „organizuju i nadgledaju relevantne građevinske jedinice prilikom raspoređivanja i postavljanja video-informacionih sistema javne bezbednosti [za] sprečavanje terorističkih napada, na ključnim mestima glavnih puteva, saobraćajnih čvorišta i javnih površina grada po potrebi“. Takođe, u skladu sa članom 32, nadležni organi moraju da uspostave video-informacioni sistem javne bezbednosti i da održavaju njegovo redovno funkcionisanje. Video snimci ili slike prikupljeni putem takvih sistema moraju se čuvati najmanje 90 dana. Zakon o borbi protiv terorizma ne navodi da se ova video oprema ne može koristiti u bilo koju drugu svrhu osim za antiterorističke aktivnosti, iako bi se takvo pravilo

indirektno moglo izvesti iz principa ograničenja svrhe predviđenog članom 28 PIPL-a.

Zakon o sajber bezbednosti i Zakon o bezbednosti podataka nemaju ništa konkretno da kažu o obradi biometrije ili upotrebi tehnologije za prepoznavanje lica. Kao što mu naziv govori, Zakon o sajber bezbednosti se odnosi na „izgradnju, funkcije, održavanje i korišćenje mreža, kao i na nadgledanje i administraciju sajber bezbednosti na teritoriji Narodne Republike Kine".[458] Takođe, budući da je usvojen 2016. godine, ovaj propis sadrži mnoge uslove za zaštitu podataka koji su 2021. ponovo navedeni u Građanskom zakoniku.[459] Zakon o bezbednosti podataka, s druge strane, „primarno se fokusira na zaštitu ukupne nacionalne bezbednosti podataka",[460] odnosno primenjuje se na obradu svih, ne samo ličnih podataka i sadrži „metodologije i pravila za upravljanje i zaštitu podataka visokog nivoa"[461] za sve privatne ili javne aktere koji obrađuju podatke.

U skladu sa Zakonom o sajber bezbednosti, nadležni organi su u martu 2020. izdali standard pod nazivom „Tehnologija informacione bezbednosti – Specifikacija bezbednosti ličnih informacija". Ovim standardom regulisani su određeni bezbednosni zahtevi koji su posebno namenjeni za biometrijske podatke i prepoznavanje lica. Rečnik ove specifikacije ukazuje da je prvenstveno usmerena na komercijalne aktivnosti, odnosno da je to kontekst u kome je dokument napisan. Član 1 kaže da se primenjuje na „aktivnosti obrade koje sprovode sve vrste organizacija", ali da je „mogu koristiti i nadležni organi". Stoga, sama specifikacija bezbednosti ličnih informacija nema za cilj da reguliše upotrebu prepoznavanja lica u javnim organima, mada su „ohrabreni" da je uzmu u obzir prilikom primene takve tehnologije.[462]

Takođe bi vredelo napomenuti da je specifikacija bezbednosti ličnih informacija izdata godinu dana pre donošenja PIPL-a i reguliše neka pitanja koja su kasnije obuhvaćena tim propisom (npr. zahtevi za saglasnost i transparentnost). U slučaju bilo kakvih neslaganja ili nedoumica o tome kako treba tumačiti određena pravila, odredbe PIPL-a treba da budu pretežna u skladu sa opštim principom tumačenja „lex posterior derogat legi priori" (kasnije donet zakon ukida onaj koji je donet ranije).

Jedno pitanje koje PIPL ne reguliše, ali je detaljno obrađeno u specifikaciji bezbednosti ličnih informacija, jeste zadržavanje biometrijskih podataka. Prema članu 6.3, rukovaocima u principu nije dozvoljeno da čuvaju „izvorne lične biometrijske informacije (kao što su uzorci i slike)", uz neke ograničene izuzetke koji uključuju skladištenje na „terminalu koji prikuplja takve informacije" do završetka funkcija identifikacije i autentifikacije, nakon čega izvorni podaci moraju biti obrisani.

Drugi standard posvećen prepoznavanju lica jeste „Tehnologija informacione bezbednosti – zahtevi za bezbednost podataka za prepoznavanje lica" (Standard za prepoznavanje lica) usvojen u aprilu 2022. ali je samo nacrt za konsultacije iz 2021. javno dostupan.[463] Za razliku od specifikacije bezbednosti ličnih informacija, ovaj standard ne pravi eksplicitnu razliku između javnih i privatnih rukovalaca. Međutim, u svom članu 3.5 (u kom se definiše rukovalac) konkretno referiše na definiciju „organizacije" iz specifikacije bezbednosti ličnih informacija kako bi odredio entitete na koje se primenjuje. Iz tog razloga, čini se da je ovaj standard (slično specifikaciji bezbednosti ličnih informacija) usmeren na aktivnosti obrade u privatnim kompanijama, a ne na prakse prepoznavanja lica u državnim organima.

Standard za prepoznavanje lica, između ostalog, reguliše: (1) obavezu saglasnosti koju rukovaoci moraju da obezbede ako nameravaju da koriste prepoznavanje lica u svrhe identifikacije i verifikacije; (2) pravila u vezi sa deljenjem, prenosom i otkrivanjem podataka za prepoznavanje lica; (3) obaveze brisanja takvih podataka; i (4) obaveze rukovaoca o transparentnosti i bezbednosti. Ovaj standard izričito zabranjuje „procene ili predikcije radnog učinka, ekonomskog statusa, zdravstvenog statusa, preferencija ili interesovanja subjekata podataka" (član 5).

Pored ovih standarda, privatne kompanije koje koriste prepoznavanje lica takođe moraju da postupaju u skladu sa dokumentom naslovljenim „Odredbe Vrhovnog narodnog suda o nekoliko pitanja koja se odnose na primenu prava u građanskim predmetima koji uključuju obradu ličnih informacija korišćenjem tehnologije prepoznavanja lica" (Sudsko tumačenje), koji je Vrhovni narodni sud izdao u julu 2021. Ovde sud sumira praksu u predmetima iz privatnog sektora i pruža smernice o nekoliko pitanja iz perspektive građanskog prava, kao što su uslovi za valjanu saglasnost i proceduralna pitanja u predmetima koji se odnose na delikte (npr. teret dokazivanja, solidarna odgovornost, uslovi za sudske zabrane i naknada štete).[464]

Sudsko tumačenje izdato je pre stupanja na snagu PIPL-a i ne uzima u obzir njegove odredbe, već se zasniva samo na tumačenju Građanskog zakonika. Mada se ne bavi direktno upotrebom prepoznavanja lica u radu javnih organa, Sudsko tumačenje pominje upotrebu u javnim prostorima.

Naime, prema Sudskom tumačenju, upotreba tehnologije za prepoznavanje lica je zabranjena na javnim mestima poput hotela, tržnih centara, banaka, aerodroma, sportskih stadiona i mesta za zabavu (verovatno, između ostalog, jer se iz praktičnih razloga takva upotreba ne može zasnivati na saglasnosti). Ova zabrana bi se mogla tumačiti tako da se svako prikupljanje podataka za prepoznavanje lica u javnim prostorima može zasnivati samo na važećim zakonima koji regulišu takvu obradu – što bi bilo u skladu sa odredbama PIPL-a koji je usvojen mesec dana kasnije.

Nadležni nacionalni organ

Prema odredbama PIPL-a, kineska administracija za sajber prostor je organ zadužen za primenu zakona, sa mandatom da izdaje standarde i smernice o nekoliko pitanja, uključujući prepoznavanje lica i veštačku inteligenciju. Međutim, prema dostupnim informacijama, ne postoje smernice kada je u pitanju prikupljanje i obrada biometrijskih podataka od strane države u privatne svrhe, ili korišćenje alata za nadzor u javnim prostorima.

PRAVNA PRAKSA

Do sada je doneto nekoliko presuda koje se konkretno bave upotrebom tehnologije za prepoznavanje lica od strane privatnih subjekata, ali nijedna presuda u slučajevima koji bi uključivali državne organe.

Prvi te vrste bio je slučaj koji je pokrenuo jedan profesor prava tužbom protiv safari parka u gradu Hangdžou.[465] Podnosilac tužbe je 2019. kupio godišnju propusnicu za park. U to vreme, kao metoda verifikacije za ulazak korišćeni su otisci prstiju (zanimljivo, podnosilac nije problematizovao činjenicu da su otisci prstiju takođe biometrijski podaci), koje je podnosilac dostavio parku uz svoju fotografiju. Kasnije te godine, park je prešao na verifikaciju putem prepoznavanja lica. Kada je od podnosioca tužbe zatraženo da se registruje za ovu vrstu verifikacije, on je odbio i podneo tužbu za povredu ugovora.[466] Prvostepeni sud je 2020. godine doneo odluku u korist podnosioca tužbe iz razloga što podnosilac nije dao saglasnost (niti je to morao) za prepoznavanje lica. U skladu s tim, sud je naložio parku da izbriše fotografiju podnosioca, ali nije odlučio da je park obavezan da obriše i ostale podatke podnosioca.[467] Podnosilac tužbe je uložio žalbu, takođe u nadi da će sud doneti načelnu odluku, uključujući smernice primenjive na slične slučajeve upotrebe prepoznavanja lica, umesto po meritumu konkretnog slučaja.[468]

Drugostepena odluka doneta je u aprilu 2022. godine i ponovo je bila samo delimično u korist podnosioca. Ovde je sud potvrdio prvostepenu odluku, ali i odlučio o brisanju podataka o otiscima prstiju – jer oni više nisu bili ni za šta potrebni (dok je njihovo prvobitno prikupljanje bilo opravdano, jer se zasnivalo na saglasnosti).[469] Sud nije, međutim, imao ništa da kaže o tome da li je parku u načelu dozvoljeno da čuva biometrijske podatke svojih korisnika, ili je „pravilo da su otisak prsta i prepoznavanje lica jedini način da se uđe u park ipak nevažeće“.[470] Možda bi ove presude bile drugačije da su donete nakon što je PIPL stupio na snagu.

Slična odluka doneta je u slučaju stambenog kompleksa koji je koristio prepoznavanje lica kao jedino sredstvo verifikacije prilikom ulaska. Jedan od stanara je podneo tužbu, a sud je „naložio kompaniji za upravljanje imovinom da izbriše podatke za prepoznavanje lica, obezbedi alternativne metode pristupa i plati nadoknadu“.[471] Takva odluka zasnovana je, između ostalog, na pravilima i smernicama Vrhovnog narodnog suda u Sudskom tumačenju koje se posebno bavi takvim situacijama.[472] Naime, Sudsko tumačenje jasno stavlja do znanja da preduzeće koje upravlja imovinom ne može insistirati da se prepoznavanje lica koristi kao isključivi metod identifikacije vlasnika imovine kada ulaze ili izlaze iz svojih stanova.[473]

Poslednjih godina u mnogim afričkim zemljama pokreću se raznovrsne inicijative i projekti koji se odnose na pametne gradove ili reforme nacionalnih sistema identifikacije, a koji podrazumevaju široku upotrebu tehnologija koje obrađuju biometrijske podatke.[474] Spekuliše se da Kina ostvaruje značajan uticaj u pogledu tehnologije u osnovi tih projekata, budući da vlade nekih zemalja na jugu Afrike kupuju tehnologiju za prepoznavanje lica od kineskih kompanija.[475] S druge strane, u smislu zakona i propisa, čini se da su afričke zemlje sklone da slede pravnu tradiciju EU, stavljajući u prvi plan osetljivost biometrijskih podataka i potrebu da se reguliše njihova upotreba.[476]

LATINSKA AMERIKA

Koja vrsta pravnog akta reguliše obradu biometrijskih podataka?

- **Nacionalni ustav**
  Da.
- **Zakon o zaštiti podataka**
  Da. U mnogim zemljama na snazi je zakon o zaštiti podataka, uglavnom pod uticajem EU regulative.
- **Smernice**
  Da.
- **AI regulativa**
  Da, Brazil je 2022. objavio nacrt zakona.
- **Propisi na lokalnom nivou**
  Da. Buenos Ajres je ozakonio prepoznavanje lica izmenama postojeće regulative o bezbednosnim sistemima.

Definicija i regulativa prepoznavanja lica

- **Prepoznavanje lica je izričito definisano u Brazilu.**
- **U brojnim zemljama, podaci prikupljeni kroz prepoznavanje lica definisani su kao biometrijski podaci.**

Detalji

- **Definisani slučajevi posebne upotrebe**
  - Biometrijski podaci moraju se prikupljati od svakoga ko ulazi u Argentinu za svrhe zaštite bezbednosti.
  - U Brazilu postoje zakoni koji regulišu upotrebu tehnologije za prepoznavanje lica na stadionima i u sistemu međugradskog saobraćaja.
  - Predlog zakona u Kolumbiji omogućava Nacionalnom registru građana da koristi različitu biometriju za identifikaciju i autentifikaciju.
- **Definisani posebni uslovi**
  - Očekuje se da će konačna verzija brazilskog zakona o AI definisati posebne uslove za obradu biometrije.

LATINSKA AMERIKA

KONTEKST

Mnoge zemlje Latinske Amerike uvele su biometrijske tehnologije za nadzor, koje javni zvaničnici obično predstavljaju kao tehnološki napredak u borbi protiv kriminala i unapređenje javne bezbednosti.[477] Tehnologije se primenjuju bez odgovarajućeg pravnog osnova, procene uticaja na ljudska prava ili transparentnosti, a koriste se za svrhe koje prevazilaze javnu bezbednost, pa čak i za špijuniranje političkih protivnika.[478] Odsustvo posebnih regulativa za njihovu upotrebu, kao i pravnog leka, izaziva zabrinutost zbog kršenja privatnosti i drugih ljudskih prava. Ove tehnologije se takođe u velikoj meri oslanjaju na policijske baze podataka koje mogu da pogoršaju posledice diskriminatornih metoda po kojima su stvorene, dok standardi za korišćenje podataka nisu dobro definisani.[479]

Mada su zemlje regiona usvojile demokratske procedure, autoritarna politička kultura i dalje opstojava, na šta ukazuje žestoka državna represija nad demonstrantima u zemljama kao što su Venecuela, Ekvador i Čile.[480] Primena sistema za prepoznavanje lica i drugih biometrijskih tehnologija u ovom kontekstu dodatno povećavaju rizike i izazivaju zabrinutost.

Dok nekoliko latinoameričkih zemalja imaju u znatnoj meri slične pristupe usvajanju tehnologija biometrijskog nadzora, Argentina i Brazil se izdvajaju po razmerama upotrebe i stoga su u fokusu ovog odeljka. Uvođenje federalnog sistema biometrijske identifikacije za bezbednost (Sistema Federal de Identificación Biométrica para la Seguridad, SIBIOS) u Argentini je 2011. godine označilo prekretnicu koja bi mogla

da omogući biometrijski masovni nadzor.[481] U okviru SIBIOS-a, svaki građanin i svako ko ulazi u zemlju, mora da dostavi biometrijske podatke uključujući otiske prstiju, otiske dlanova i fotografije lica. Krajnji korisnici SIBIOS-a, policajci i službenici granične kontrole, nisu u obavezi da pribave nalog ili sudsko ovlašćenje za pristup biometrijskoj bazi podataka. Odsustvo zakonodavne debate i konsultacija sa nevladinim akterima u vezi sa implementacijom, drže ovaj sistem van domašaja javnosti. To je uslovilo nisku pažnju građana za rizike povezane sa obimnim prikupljanjem ličnih podataka od strane države.[482]

U poslednjoj deceniji, upotreba biometrijskih tehnologija ubrzano se širi u Argentini, a one se koriste ne samo za navodne svrhe javne bezbednosti i kontrole imigracije, već i za verifikaciju identiteta u oblastima kao što su socijalno osiguranje, bankarstvo, naplata poreza, obrazovanje, izbori i sport.[483] Buenos Ajres, glavni grad Argentine, koristi prepoznavanje lica uživo na gradskim železničkim stanicama, sa kamerama postavljenim i unutar stanica i na uličnim prilazima. Sistem, predstavljen kao sredstvo za lociranje ljudi iz nacionalne baze begunaca, korišćen je između 2019. i 2022. godine.[484] Prijavljeni su brojni lažno pozitivni slučajevi, što ukazuje na činjenicu da je tehnologija manjkava, sklona greškama i da može dovesti do ozbiljnih kršenja osnovnih prava.[485] Tehnologija je privremeno suspendovana, a gradski sud je upotrebu kasnije ocenio kao neustavnu.[486]

Biometrijske tehnologije, uključujući prepoznavanje lica, široko se koriste u brazilskom javnom i privatnom sektoru. Česte su implementacije sistema za identifikaciju na osnovu ljudskog lica u javnim prostorima i na javnim događajima pod izgovorom visoke stope nasilja i kriminala.[487] Biometrijska verifikacija se takođe koristi za otkrivanje prevara u javnim uslugama, pa čak i za kontrolu prisustva u obrazovnim institucijama.[488] Takođe su zabeleženi slučajevi prepoznavanja roda, uzrasta i emocija u marketinške svrhe, mada su neki od tih projekata kasnije osporeni na sudu.[489]

Nacionalni sistem identifikacije građana (Identificação Civil Nacional, ICN) u Brazilu treba da prikupi biometrijske podatke čitavog biračkog tela do 2026.[490] Sistem podrazumeva centralizovanu bazu u kojoj se ukrštaju različite postojeće vladine baze podataka, uključujući birački biometrijski registar. Od juna 2022. godine, 130 miliona korisnika je biometrijski registrovano za glasanje, što čini značajan deo stanovništva. Stručnjaci ističu zabrinutost zbog rizika povezanih sa ICN sistemom, grupisanih u dve kategorije: rizici koji se odnose na informacionu arhitekturu sistema i aranžmane upravljanja, uključujući potencijalne zloupotrebe ličnih podataka, i rizici od isključenja građana usled korišćenja centralne baze za autentifikaciju korisnika na državnoj gov.br platformi.[491]

Kada je reč o upotrebi biometrijskih tehnologija na granicama, grupe civilnog društva u Latinskoj Americi zatražile su raskid sporazuma o saradnji koji su sa Sjedinjenim Državama sklopili Meksiko, Gvatemala, Honduras i Salvador, a koji omogućavaju prekogranični prenos biometrijskih i drugih vrsta ličnih podataka ljudi u pokretu.[492] Ovi sporazumi o deljenju podataka izazvali su ozbiljnu zabrinutost zbog zadiranja u privatnost, diskriminacije i proizvoljnog odlučivanja. Organizacije civilnog društva koje se zalažu za raskid sporazuma, takođe su apelovale na usvajanje mera za zaštitu privatnosti i podataka ljudi u pokretu, kao što su zabrana obrade bez lokalnih zakona o zaštiti podataka, sprečavanje profilisanja i prediktivne analize i ograničavanje pristupa podacima. Takođe se traže posebne mere za zaštitu dece, uvođenje obaveze pribavljanja informisane saglasnosti i poštovanje prava na pristup, ispravku, brisanje i prigovor.

Predlažu se različiti pristupi za rešavanje rizika povezanih sa tehnologijom prepoznavanja lica u regionu. Jedni se zalažu za moratorijum dok se ne uspostave odgovarajuće zaštitne mere, dok drugi pozivaju na sveobuhvatnu zabranu korišćenja u javnim prostorima u svrhe sprovođenja zakona.[493] Nekoliko organizacija civilnog društva takođe traži regulatorne mere zaštite, uključujući pravne lekove za kršenje privatnosti, veću odgovornost i transparentnost tehnoloških kompanija ali i državnih organa.[494]

Od 2022. godine, kampanja civilnog društva #SaiDaMinhaCara („Skloni mi se s lica“) podstakla je 50 državnih i lokalnih zakonodavaca u Brazilu da formulišu predloge za zabranu korišćenja prepoznavanja lica u javnim prostorima.[495] Kao povod za zabrinutost posebno su naglasili pristrasne ishode, nezakonita hapšenja i jačanje rasne diskriminacije. Ova inicijativa ističe rizike od masovnog nadzora i eroziju privatnosti u javnim prostorima. Predvode je organizacije specijalizovane za tehnologiju, bezbednost i ljudska prava, koje sarađuju sa parlamentarcima kako bi izdejstvovali zakonska ograničenja.

PRAVNI OKVIR

Brojne latinoameričke zemlje, kao što su Čile,[496] Urugvaj,[497] Meksiko,[498] Kostarika,[499] Peru, Brazil, Panama i Ekvador usvojile su zakone o zaštiti podataka, često pod uticajem GDPR modela Evropske unije. Međutim, pojedine zemlje regiona, poput Venecuele i Bolivije, još uvek nemaju zakone o zaštiti podataka.[500]

Značajan izazov u vezi sa regulacijom biometrijskih tehnologija širom Latinske Amerike predstavlja to što veliki broj zemalja koje imaju posebne zakone za zaštitu podataka, nije te zakone ažuriralo na adekvatan način kako bi odgovorili na izazove savremenih digitalnih tehnologija. Nekim od tih zemalja nedostaju posebni propisi koji se odnose na korišćenje biometrijskih podataka. Na primer, u izveštaju koji mapira 38 inicijativa za korišćenje prepoznavanja lica u Latinskoj Americi, preko 60 odsto njih nije imalo konkretne pravne osnove za implementaciju tehnologije koja je već bila uvedena.[501] U pojedinim slučajevima, kao osnova za upotrebu uzimana su široka tumačenja postojećih propisa ili analogije sa drugim tehnologijama.

Tek u nekolicini slučajeva propisi se izričito odnose na prepoznavanje lica ili druge tehnologije biometrijske identifikacije. Među primerima su brazilska regulativa koja omogućava prikupljanje biometrijskih podataka za vozačke dozvole,[502] propisi koji regulišu sveobuhvatni sistem javnog video nadzora u Buenos Ajresu[503] i zakon u Kolumbiji koji nacionalnom civilnom registru dozvoljava da koristi različite biometrijske podatke za identifikaciju i autentifikaciju.[504]

ARGENTINA

Ustav Argentine pruža snažnu zaštitu privatnosti (članovi 18 i 19),[505] a ova zemlja je ratifikovala i međunarodne sporazume o ljudskim pravima. Solidan, ali zastareo režim zaštite podataka prisutan je u članu 43 Ustava kao i u Zakonu o zaštiti podataka o ličnosti,[506] koji je usvojen 2000. Evropska komisija je uvrstila Argentinu među zemlje koje obezbeđuju adekvatan nivo zaštite podataka. Međutim, postojeća nacionalna regulativa pokazala se nedovoljnom u zaštiti građana od državnog nadzora, pošto vlada koristi zakonske izuzetke za pokretanje programa nadzora iz širokog spektra razloga, uključujući funkcionisanje države, unapređenje usluga i javnu bezbednost.

Primena tehnologije za prepoznavanje lica u Buenos Ajresu, na primer, u početku nije imala odgovarajući pravni okvir i zasnivala se na odluci gradske vlade, umesto na zakonu. Međutim, u oktobru 2020. godine, gradska skupština je ozakonila upotrebu izmenama postojećeg propisa o bezbednosnim sistemima.[507] Organizacije civilnog društva su se oštro protivile amandmanu, tvrdeći da nije sprovedena odgovarajuća procena uticaja na ljudska prava, posebno u pogledu prava na privatnost.[508] Specijalni izvestilac UN-a za pravo na privatnost takođe je izrazio zabrinutost u vezi sa primenom prepoznavanja lica u Buenos Ajresu, posebno zbog nedostatka procene uticaja na privatnost i adekvatnih zaštitnih mera.[509]

Zastareli argentinski zakon o zaštiti podataka, usvojen 2000. godine, takođe je sporna tačka u pogledu primene prepoznavanja lica. Grupe civilnog društva zahtevaju ažuriranje zakona kako bi se obezbedile jasne smernice i zaštita u prikupljanju osetljivih ličnih podataka putem novih tehnologija.[510]

Dva meseca posle javnih konsultacija održanih u septembru 2022, argentinska agencija u čijoj je nadležnosti i zaštita podataka (La Agencia de Acceso a la Información Pública, AAIP) objavila je nacrt za ažuriranje Zakona o zaštiti podataka o ličnosti.[511] Nacrtom amandmana predviđene su nove definicije, uključujući „biometrijske podatke“ koji se smatraju osetljivim samo ako mogu otkriti dodatne informacije, te čija upotreba može potencijalno dovesti do diskriminacije subjekta podataka. Smernice za biometriju koje je objavila AAIP daje primere takvih osetljivih podataka, uključujući etničko poreklo i zdravstvene informacije.[512] Međutim, ovaj dodatni uslov za zaštitu biometrijskih podataka smanjuje nivo zaštite subjekata podataka u poređenju sa sličnim propisima u svetu koji regulišu upotrebu biometrijskih podataka, kao što je GDPR.

Takođe, u poređenju sa GDPR-om, uslov u argentinskom Zakonu za saglasnost za obradu osetljivih podataka ne pruža dovoljno jaku zaštitu za osobe na koje se podaci odnose. S obzirom na povećane rizike obrade osetljivih podataka, stručnjaci ističu da treba zahtevati izričitu saglasnost.[513]

U julu 2024. godine, vlada je osnovala posebno telo sa zadatkom da se bavi pitanjima upotrebe veštačke inteligencije za potrebe prevencije kriminala i sprovođenja istraga.[514] Ideja je da se u Argentini koriste alati za „prediktivni policijski rad“, kao što je to slučaj u Ujedinjenim Arapskim Emiratima. Inicijativa je dočekana kritikama zbog istorije zlouopotreba i povrede prava građana Argentine koje su do sada zabeležene. Štaviše, najavljene upotrebe novih tehnologija sve su opsežnije i invazivnije jer ne podrazumevaju

korišćenje veštačke inteligencije samo za rasvetljavanje postojećih zločina, već i alate za predviđanje budućih aktivnosti koje bi policija trebalo da sprečava.[515]

BRAZIL

Postojeći pravni okvir za zaštitu prava na privatnost u Brazilu obuhvata zaštitu privatnosti kao osnovnog prava unetu u savezni Ustav,[516] te priznavanje međunarodnih konvencija o ljudskim pravima. Ova zemlja takođe ima poseban zakon, Okvir građanskih prava za internet (Marco Civil da Internet), koji štiti privatnost u onlajn kontekstu.[517] Pored toga, na saveznom nivou donet je Zakon o zaštiti podataka (Lei Geral de Proteção de Dados Pessoais, LGPD), koji je stupio na snagu u septembru 2020. LGPD nastoji da objedini preko 40 različitih propisa koji su prethodno regulisali upotrebu ličnih podataka u Brazilu, te da uspostavi moderne standarde zaštite podataka.[518] U oktobru 2021, brazilski Senat je jednoglasno odobrio predloženi amandman na Ustav kojim je zaštita ličnih podataka priznata kao osnovno pravo.[519]

Dok se LGPD smatra jednim od najprogresivnijih zakona o zaštiti podataka u čitavom regionu Latinske Amerike, u njemu nema konkretne definicije biometrijskih podataka, što ostavlja pravne praznine i mogućnost za zloupotrebe. Zakon izričito navodi izuzetke za aktivnosti koje se odnose na javnu bezbednost, državnu odbranu, državnu bezbednost i istragu i gonjenje krivičnih dela. To znači da upotreba prepoznavanja lica u radu službi javne bezbednosti ne spada u domen zaštite LGPD-a. U toku su napori da se reguliše zaštita podataka u radu organa za sprovođenje zakona, gde eksperti predlažu model krivične verzije LGPD koja bi utvrdila principe zaštite podataka i obaveze organa za sprovođenje zakona.[520] Međutim, neizvesno je kada će taj posao biti dovršen.

U kontekstu privatnih kompanija koje učestvuju u implementaciji sistema za prepoznavanje lica, kao što je na primer slučaj sa privatnim koncesionarom javnog prevoza u Sao Paulu, primenjuju se odredbe LGPD-a, Okvira građanskih prava za internet i Zakona o zaštiti potrošača.

Od značaja za upotrebu tehologija za prepoznavanje lica u radu policije, tu su i propisi koji indirektno regulišu ovu oblast: savezna uredba br. 10.046/2019, koja sadrži smernice za razmenu podataka između organa javne uprave i reguliše objedinjavanje baza podataka uključujući baze koje sadrže biometrijske podatke (što je pristup kritikovan zbog neusklađenosti sa LGPD-om) i pravilnik br. 793/2019 Ministarstva pravde i javne bezbednosti koji se direktno tiče upotrebe tehnologije za prepoznavanje lica u svrhe javne bezbednosti, jer dozvoljava primenu sredstava iz fonda za nacionalnu bezbednost radi kupovine ovakvih tehnologija bez regulisanja bilo kakvih mera zaštite.[521]

Pojedine savezne države imaju svoje propise koji se direktno bave tehnologijama za prepoznavanje lica. Na primer, tri države imaju posebne zakone koji regulišu upotrebu tehnologije prepoznavanja lica na stadionima: Seara,[522] Minas Žerais[523] i Alagoas.[524] Takođe, Rio de Žaneiro ima zakon fokusiran na primenu tehnologije za prepoznavanje lica u međumesnom transportnom sistemu.[525] Međutim, ovi zakoni ne sadrže dovoljne zaštitne mere za primenu tehnologije.

Brazilska prestonica ima zakon koji reguliše upotrebu prepoznavanja lica u svrhe javne bezbednosti, ali je nedovoljan u pogledu zaštite sajber bezbednosti i prava građana na koje se podaci odnose.[526] Takođe dozvoljava upotrebu tehnologije u krivičnim istragama. Ministarstvo pravde i javne bezbednosti izdalo je direktivu kojom se promoviše implementacija sistema za prepoznavanje lica i drugih tehnologija za nadzor.

U decembru 2022. godine, komitet brazilskog Senata predstavio je nacrt zakona o veštačkoj inteligenciji.[527] Predloženim tekstom sistemi veštačke inteligencije kategorizuju se na osnovu rizika: biometrijski sistemi identifikacije su klasifikovani kao visokorizični AI sistemi. Nadležni organ ima zadatak da kreira i održava javno dostupne baze podataka visokorizičnih AI sistema, zajedno sa sprovedenim procenama rizika koje dostavljaju dobavljači i krajnji korisnici.

Predlogom su zabranjene upotrebe sistema klasifikovanih u kategoriju „prekomernog“ rizika, u kojoj se nalaze prepoznavanje lica i drugi biometrijski sistemi identifikacije u svrhe javne bezbednosti – osim ako to nije dozvoljeno zakonom ili sudskim ovlašćenjem u slučajevima zločina u toku ili potrage za nestalima ili žrtvama zločina. Tako definisana osnova otvara prostor za veoma široka tumačenja i mogućnost za pravdanje praktično neprekidne upotrebe.

S druge strane, predloženi tekst garantuje različita prava građana, uključujući obrazloženje odluka, mogućnost osporavanja i ljudsko učešće u procesu

odlučivanja. Predlog takođe ističe pravo na nediskriminaciju i na ispravljanje utvrđenih pristrasnosti.

Javna rasprava o predloženom tekstu ovog propisa slična je onoj koja se vodila u Evrpskoj uniji pre usvajanja AI Akta. Oranizacije civilnog društva koje istražuju kako se tehnologija za prepoznavanje lica dosad koristila u Brazilu, zahtevaju zabranu njene upotrebe u radu policije, jer se pokazalo koliko problema izaziva u praksi.[528]

PRAVNA PRAKSA

U istorijskoj presudi iz maja 2020. godine, brazilski Vrhovni sud proglasio je pravo na zaštitu podataka kao nezavisno i osnovno pravo po brazilskom ustavu.[529] Sud je suspendovao izvršnu naredbu predsednika kojom se od telekomunikacionih kompanija zahtevalo da dele lične podatke preko 200 miliona ljudi sa Brazilskim institutom za geografiju i statistiku (Instituto Brasileiro de Geografia e Estatística, IBGE) za potrebe popisnog istraživanja. Presuda je označila značajan korak ka priznavanju zaštite ličnih podataka kao zasebnog prava u odnosu na pravo na privatnost, slično rešenju u Povelji o osnovnim pravima Evropske unije.

Građanski sud u Sao Paulu presudio je u maju 2021. da je upotrebom tehnologije za prepoznavanje lica na jednoj liniji metroa prekršeno pravo ljudi na privatnost i slobodu informacija.[530] Operator metroa, ViaQuatro, uveo je interaktivna vrata vagona koja su prikazivala personalizovane reklame zasnovane na tehnologiji prepoznavanja emocija. Organizacija za prava potrošača podnela je tužbu tražeći odštetu i nalog za zabranu upotrebe tehnologije. Sud je smatrao da je za korišćenje softvera za detekciju ili prepoznavanje lica potrebna saglasnost korisnika i naložio je operatoru metroa da obustavi upotrebu. Sud je naglasio značaj zaštite podataka i prava na privatnost prema LGPD. Takođe je dosudio odštetu za kolektivnu štetu, ali je odbacio zahtev za naknadu u vezi sa neekonomskom štetom koju su putnici pretrpeli pojedinačno, navodeći da bi to dupliralo odštetu koja je već dodeljena za kolektivnu štetu.[531]

U značajnom procesu u Argentini, prvostepeni sud iz Buenos Ajresa proglasio je neustavnim sistem za prepoznavanje lica begunaca (Sistema de Reconocimiento Facial de Prófugos, SRFP) koji je koristila lokalna vlast.[532] Presudom je uspostavljen presedan za zaštitu privatnosti i osnovnih prava u kontekstu javnog nadzora za potrebe sprovođenja zakona. Najpre, presudom su privatnost, intima i zaštita podataka priznata i kao kolektivna, a ne isključivo individualna prava. Drugo, sud je utvrdio da organizacije civilnog društva mogu da podnesu tužbu zbog povrede ovih kolektivnih prava. Konačno, sudija je takođe zaključio da je „amparo“ (ustavni lek) odgovarajuća mera za rešavanje štete koju je sistem prouzrokovao. Odluka je ukazala na kršenje privatnosti i zloupotrebu ovlašćenja operatora sistema.

Za SRFP je korišćen softver za prepoznavanje lica instaliran u nadzorne kamere – kapacitet koji smo u tehničkom poglavlju knjige istakli kao sve češći – koji poredi slike sa bazom podataka begunaca. Organizacije civilnog društva ukazale su na rizike po privatnost i druga ljudska prava. Sud je utvrdio da SRFP nije imao odgovarajuću kontrolu, da je rezultirao nezakonitim pritvaranjem i da se oslanjao na nepouzdanu bazu podataka. Sudija je takođe istakao zloupotrebu sistema i odsustvo odgovornosti. Sistem je zabranjen dok se ne uspostave mehanizmi kontrole. Odlukom, dakle, nije proglašen neustavnim zakon kojim je uspostavljen SRFP, već su navedeni uslovi za njegovu buduću primenu.

U aprilu 2022. Vrhovni sud Meksika je presudio da je plan za uspostavljanje nacionalnog registra korisnika mobilnih telefona sa biometrijskim podacima neustavan.[533] Ova državna inicijativa pokrenuta je u okviru borbe protiv kriminala, jer bi navodno kriminalcima bilo teže da ostanu anonimni kad kupuju mobilni telefon. Sud je uočio potencijalna kršenja ljudskih prava i bezbednosne rizike povezane sa prikupljanjem osetljivih biometrijskih podataka, uključujući otiske prstiju ili biometriju očiju od oko 120 miliona korisnika usluga mobilne telefonije. Presudom je zaštićena privatnost građana i postavljen kriterijum zaštite ličnih podataka u odnosu na tehnološki napredak.

SJEDINJENE DRŽAVE

KONTEKST

Za razliku od drugih vrsta biometrijskog nadzora, tehnologija za prepoznavanje lica (facial recognition technology, FRT) veoma je prisutna u Sjedinjenim Državama i posvećeni su joj brojni projekti monitoringa[534] i izveštavanja[535] upravo zbog raširenosti njene upotrebe.

Međutim, regulativa takvih tehnologija u SAD zasad predstavlja nasumični skup propisa koji se bave različitim aspektima tehnologije na nivou države ili drugim lokalnim nivoima, uključujući opštine. Zakoni se međusobno veoma razlikuju u pogledu onoga što regulišu: neki su usmereni na komercijalnu upotrebu, drugi na upotrebu u službama za sprovođenje zakona ili čak upotrebu u konkretnim prostorima kao što su škole[536] i radna mesta[537] ili na izuzetke u borbi protiv seksualnog zlostavljanja dece i trgovine ljudima.[538]

Ne postoji zakon na saveznom nivou koji reguliše upotrebu FRT-a. Taj jaz je prepoznat i pokrenuto je nekoliko inicijativa i predloga o tome kako bi Kongres trebalo da pristupi ovom pitanju, ali za sada bez ishoda.[539]

Moratorijum koji bi službama za sprovođenje zakona u SAD praktično zabranio upotrebu prepoznavanja lica na određeni vremenski period, predložen je u nekoliko navrata,[540] poslednji put 2023. godine u obliku predloga zakona o moratorijumu na prepoznavanje lica i biometrijske tehnologije.[541] Prema tom predlogu, zabrana upotrebe FRT-a federalnim organima može biti ukinuta samo aktom Kongresa. Zakon bi regulisao i druge upotrebe biometrijskih podataka, kao što su

SJEDINJENE DRŽAVE

Koja vrsta pravnog akta reguliše obradu biometrijskih podataka?

Poseban zakon o biometrijskim podacima
Da.

Regulativa u službama za sprovođenje zakona
U načelu, ne. Neki aspekti ovlašćenja službi za sprovođenje zakona regulisani su posebnim zakonom o biometrijskim podacima.

Krivično pravo
U načelu, ne. Neki aspekti krivičnog prava regulisani su posebnim zakonom o biometrijskim podacima.

Regulativa na lokalnom nivou
Da; na nivou saveznih država i samouprava.

Definicija i regulativa prepoznavanja lica

Prepoznavanje lica je izričito definisano u mnogim saveznim državama.

Detalji

Definisani slučajevi posebne upotrebe
-Većina zakona reguliše upotrebu tehnologije za prepoznavanje lica u službama za sprovođenje zakona ili, opštije, u organima javne vlasti.
- Većina zakona izričito propisuje kada je upotreba tehnologije za prepoznavanje lica dozvoljena i/ili nije dozvoljena (neki zakoni sadrže listu takvih slučajeva).
- Neki zakoni se konkretno bave upotrebom tehnologije za prepoznavanje lica u realnom vremenu i propisuju kada je ona dozvoljena.
- Neki zakoni propisuju upotrebu prepoznavanja lica u kontekstu krivičnog prava, ograničavajući vrste dela koja se mogu istraživati upotrebom tehnologije za prepoznavanje lica.
- Neki zakoni regulišu konkretne upotrebe kao što su potraga za nestalim ili preminulim osobama.

Definisane posebne vlasti
- Različita relevantna tela imaju različita ovlašćenja, koja pretežno obuhvataju ili ex ante ili ex post kontrolu.
- Nijedno relevantno telo nema ovlašćenje da zaustavi upotrebu ili izrekne novčanu kaznu za nezakonitu upotrebu.

Definisani posebni uslovi
- Najčešći uslovi za upotrebu tehnologije za prepoznavanje lica uključuju obaveze testiranja i obuke zaposlenih, kao i obaveze obaveštavanja relevantnih vlasti i transparentnosti.
- Neki zakoni nalažu neophodnost učešća ljudi u verifikaciji rezultata pretrage.

prepoznavanje glasa i hoda. Usvajanje tog zakona, međutim, ne bi sprečilo države i lokalne vlasti da donose sopstvene propise koji strože regulišu upotrebu prepoznavanja lica i drugih biometrijskih tehnologija.[542]

Jedan od predloga za uspostavljanje ograničenja, umesto potpune zabrane FRT-a pojavio se 2022. godine u vidu nacrta zakona o prepoznavanju lica.[543] Ovim predlogom trebalo je utvrditi regulatorni režim za upotrebu FRT-a u državnim i saveznim službama za sprovođenje zakona, kako u slučajevima rizika usled lošeg rada FRT-a, tako i u slučajevima kada tehnologija radi kako je predviđeno, ali službama za sprovođenje zakona omogućava upotrebe koje bi neprihvatljivo uticale na ljudska prava.[544] Predloženi zakon bi sprečio službenike za sprovođenje zakona da koriste softver za prepoznavanje lica na načine koji bi mogli da predstavljaju masovni nadzor, uključujući korišćenje tehnologije preko kontrolne table u vozilu ili kamera za uniforme, kao i na javnim demonstracijama.[545]

Na osnovu iskustava na nivou država, bilo je predloga elemenata upotrebe FRT-a koje treba regulisati na saveznom nivou, poput implementacije (1) zahteva za sudski nalog na osnovu osnovane sumnje; (2) uslova ozbiljnog krivičnog dela; (3) transparentnosti upotrebe; (4) zaštitnih mehanizama tako da FRT ne može biti jedina osnova za hapšenje; (5) zabrane neciljanog skeniranja gde sistem identifikuje sve pojedince na video snimku; i (6) standarda za testiranje i tačnost.[546]

PRAVNI OKVIR

Pregled pravnog pejzaža u SAD

Prema taksonomiji različitih pristupa regulisanju FRT-a u SAD koju je predložio Institut AI Now, postoje tri opšte zakonodavne opcije: (1) potpuna zabrana; (2) moratorijum koji se može podeliti na dva tipa: vremenski ograničeni moratorijum, koji pauzira upotrebu FRT-a na određeno vreme, i moratorijum po direktivi, koji upotrebu pauzira dok se ne postave zakonodavne mere koje će zameniti moratorijum; i (3) zakoni koji uspostavljaju parametre.[547]

Potpune zabrane i moratorijumi na državnu ili privatnu upotrebu, ili i jedno i drugo, uglavnom su uvodile gradske vlasti,[548] ili su predlagani na državnom i drugim lokalnim nivoima.[549] Pojedine države su uvele moratorijume koji su kasnije zamenjeni regulativom, kao što je bio slučaj u Virdžiniji 2022. godine[550] i Vermontu 2021. (gde je potpuna zabrana donekle bila ublažena striktno ograničenim izuzecima), što ćemo detaljnije opisati u ovom odeljku.[551] U Kaliforniji, na primer, moratorijum iz 2019. naprosto je istekao bez usvajanja relevantnog zakona, iako su neki predlozi bili na stolu.[552] Slična je situacija i u Nju Orleansu, gde je moratorijum ukinut posle dve godine.[553] Pretpostavljalo se da je povod za ovu promenu pristupa bio porast nasilnih zločina[554] i veći pritisak lobista za industriju.[555]

Regulisanje upotrebe prepoznavanja lica i drugih biometrijskih sistema u komercijalne i privatne svrhe, predvodila je država Ilinois koja je 2008. usvojila Zakon o privatnosti biometrijskih informacija (Biometric Information Privacy Act, BIPA).[556] Ovaj propis reguliše prikupljanje biometrijskih podataka i ograničava privatne kompanije da prikupljaju takve podatke bez saglasnosti. Takođe uspostavlja pravo na akciju (pravo, u ovom slučaju za pojedinca, da podnese tužbu protiv nekoga na sudu) i pravo na naknadu štete od kompanija koje krše odredbe. Teksas je 2009. godine doneo sličan zakon, s tim što nije predviđeno pravo pojedinaca da tuže, odnosno tužbe za kršenje zakona može da podnese samo država.[557] Slični propisi doneti su u državi Vašington i gradovima Portlandu i Njujorku.[558]

Kada je reč o specifičnostima zakonskih odredbi koje regulišu prepoznavanje lica – kao i druge oblike biometrijskog nadzora – za potrebe sprovođenja zakona, u SAD se javlja nekoliko pristupa koji se preklapaju. Sveobuhvatni pregled usvojenih zakona i dostupnih zakonskih predloga na saveznom, državnim i drugim lokalnim nivoima, koji je objavio Centar za međunarodne i strateške studije, identifikuje niz opcija u bavljenju različitim fazama razvoja i implementacije sistema.[559]

Neki američki zakoni regulišu fazu pre implementacije tehnologije, propisujući obavezu ovlašćenja i/ili kontrole nad državnom primenom sistema za prepoznavanje lica. Na primer, u pojedinim državama uspostavljena je obaveza da se traži dozvola od zakonodavnog tela pre nego što službe za sprovođenje zakona mogu da kupe i instaliraju sisteme za prepoznavanje lica (recimo, u Vašingtonu i Koloradu putem obaveznog obaveštenja o nameri). U drugim državama propisani su obavezni koraci pre nego što službe za sprovođenje zakona mogu da koriste tehnologiju u svakom konkretnom slučaju, kao što su: (1) uspostavljanje kontrole kroz ovlašćenje malog broja organizacija za upotrebu prepoznavanja lica (u Masačusetsu i Juti, policija mora da podnese pisane zahteve ovlašćenim državnim službama, koje potom odlučuju da li će izvršiti pretragu sistema

u njihovo ime); i (2) nametanje pravosudne kontrole obavezivanjem službe za sprovođenje zakona da pribavi nalog ili sudsku naredbu pre upotrebe sistema za prepoznavanje lica (Vašington, Kolorado i Masačusets).

Okolnosti pod kojima se FRT može ili ne sme koristiti značajno variraju. Neki zakoni propisuju listu slučajeva u kojima je upotreba FRT-a dozvoljena, čime se sve druge situacije isključuju iz dozvoljene upotrebe (to je slučaj u Vermontu), i obično obuhvataju upotrebu u vezi sa krivičnim delima i istragom, ponekad ograničenu samo na određena dela (kao u Juti), ili posebno za potragu za nestalim ili umrlim osobama (Vašington, Kolorado, Mejn, Virdžinija, Juta i Masačusets). Drugi zakoni izričito zabranjuju određene upotrebe, kao što su pretrage na osnovu vere, rase, roda, političke pripadnosti ili bilo koje druge lične karakteristike zaštićene zakonom (Vašington i Kolorado); i/ili korišćenje pozitivnih podudaranja za utvrđivanje osnovane sumnje tokom krivične istrage, u nedostatku drugih dokaza (Vašington, Kolorado, Mejn, Virdžinija i Alabama); ili izradu zapisnika koji opisuje ostvarivanje prava pojedinca zagarantovanih Prvim amandmanom – koji štiti slobodu govora, štampe, okupljanja i pravo na prigovor vlastima – iako će se tačan smisao ove zabrane vremenom tek pokazati (Vašington i Kolorado).[560]

Zahtevi za transparentnost takođe imaju različite oblike. Neki zakoni nalažu da se već u postupku nabavke utvrde neke obaveze u odnosu na tehnologiju koja se kupuje (u Vašingtonu i Koloradu se mora pripremiti izveštaj o odgovornosti pre razvoja, nabavke ili upotrebe sistema ili servisa za prepoznavanje lica). Drugi zakoni regulišu da javnost – tj. ljudi na koje upotreba utiče – mora biti na odgovarajući način obaveštena pre nego što se tehnologija primeni (Juta), ili da se okrivljenima mora dati obaveštenje ako je prepoznavanje lica korišćeno kao pomoć u istrazi (Vašington i Kolorado). Mnoge države su takođe propisale zahtev da se, posle primene tehnologije za prepoznavanje lica, detalji i rezultati te upotrebe učine dostupnim javnosti u vidu različitih izveštaja (čiji je sadržaj takođe regulisan).

Zahtevi o testiranju tehnologije mogu uključivati (1) obavezu testiranja tehnologije u radnim uslovima pre nego što se ona upotrebi i (2) tekuće testiranje kako bi se proverile razlike u performansama i omogućilo ublažavanje bilo kakvih nepoštenih razlika u performansama među različitim podgrupama stanovništva (Vašington i Kolorado). Takođe, (3) da bi se ublažio rizik od grešaka i pogrešne identifikacije, neki zakoni zahtevaju ljudsku intervenciju za potvrdu pozitivnog podudaranja u određenim situacijama (Vašington, Kolorado i Juta). Neki zakoni takođe regulišu (4) obaveze obuke za ljude koji neposredno rukuju tehnologijom (Vašington, Kolorado, Juta, Virdžinija i Kentaki).

Konačno, pojedini zakoni izričito razlikuju stalni nadzor ili nadzor u realnom vremenu (Vašington, Kolorado i Virdžinija) i tretiraju ga restriktivnije od naknadnog retrospektivnog nadzora (na primer, analiza CCTV izvora), dok je u mnogim državama samo ova druga vrsta dozvoljena.

Postoje i drugi načini za kategorizaciju različitih zakonodavnih pristupa. Univerzitet u Pensilvaniji razlikuje zakone koji (1) ograničavaju okolnosti u kojima se prepoznavanje lica može koristiti; (2) procenjuju tehnologiju u odnosu na unapred definisane principe ili smernice za odgovarajuću upotrebu; (3) propisuju učešće javnosti i odobrenje kao preduslov za primenu tehnologije; i (4) predviđaju uslove koji kombinuju sve navedene aspekte.[561]

U narednim odeljcima razmotrićemo zakonske odredbe koje regulišu tehnologiju prepoznavanja lica širom SAD, kako je to bio slučaj u vreme pisanja ovog istraživanja, uz opis zakona u pojedinim državama.

Pregled propisa na nivou država

Odredbe koje regulišu upotrebu FRT-a u radu službi za sprovođenje zakona mogu se klasifikovati na osnovu nekoliko kriterijuma, uključujući njihovu rasprostranjenost (od najčešćih do pomalo „egzotičnih“) ili konkretnu fazu upotrebe FRT-a koju regulišu. Rezime koji sledi nije konačna lista zakonskih rešenja koja su trenutno prisutna u SAD, uzimajući u obzir ova dva kriterijuma.

Pravni režim samo za službe za sprovođenje zakona ili i za druge državne vlasti

U pojedinim državama postoje propisi sa odredbama o prepoznavanju lica konkretno namenjenim službama za sprovođenje zakona. To su Virdžinija, Alabama, Masačusets, Vermont, Kentaki i Merilend. Druge države imaju pravila koja regulišu kako se FRT može ili ne sme koristiti i u radu drugih državnih organa.

U Vašingtonu i Koloradu zakon se primenjuje na državne i lokalne vladine službe. U Mejnu se primenjuje na državnu, okružnu ili opštinsku vladu ili na odeljenje, agenciju ili pododeljenje, ili bilo koji drugi entitet koji je zakonom

identifikovan kao javni organ, što uključuje i organe za sprovođenje zakona i njihove zaposlene ili imenovane službenike. U Juti je zakon usmeren na državne organe, dok je lista tih subjekata precizirana u tekstu zakona.

Pravni režimi u kojima važi opšta zabrana podložna izuzecima, koji omogućavaju posebne slučajeve upotrebe ili izričito zabranjuju neke upotrebe

Zakoni u SAD se razlikuju u pogledu načina na koji u načelu pristupaju regulaciji FRT-a. Većina polazi od opšte zabrane upotrebe FRT-a, da bi zatim propisala neke izuzetke. Drugi ne navode izričitu zabranu, ali regulišu okolnosti ili situacije kada se tehnologija može koristiti.

Moglo bi se reći da je ova razlika samo varijacija u formulaciji i da je krajnji rezultat isti – upotreba FRT-a je legalna samo u prisustvu izuzetka, situacije ili okolnosti navedenih u zakonu.

Međutim, takođe se može tvrditi da to nije samo semantičko pitanje, već da izabrani pristup može imati neke pravne posledice. Jedno od opštih pravila ili smernica koje advokati koriste da bi tumačili zakon kaže da izuzetke treba tumačiti usko ili, prema latinskom kredu, expressio unius esclusio alterius. Primena ovog interpretativnog alata mogla bi efikasno da suzi dozvoljene slučajeve upotrebe za prepoznavanje lica u državama koje su zauzele pristup sa izuzecima. S druge strane, postoji uputstvo za tumačenje prema kojem se odredba po analogiji može primeniti na situaciju sličnoj onoj koja je navedena u konkretnoj zakonskoj odredbi, ali nije izričito pomenuta. Ovo pravilo, na latinskom ejusdem generis („od iste vrste“), može se koristiti za proširenje scenarija u kojima se primenjuju dozvoljene upotrebe, odnosno može proširiti primenu FRT-a u državama koje su zauzele drugi pristup.

Merilend, Vermont, Alabama, Juta i Mejn su zauzeli prvi pristup, dok se Masačusets opredelio za drugi.

U pojedinim državama na snazi su odredbe koje izričito zabranjuju određene upotrebe FRT-a, tako da nikakvi interpretativni alati ne mogu poslužiti njihovoj legalizaciji. Takve odredbe se nalaze u zakonima Merilenda, Vašingtona, Kolorada, Virdžinije i Jute.1

Nadzor u realnom vremenu

Nekim zakonima izričito je regulisana upotreba alata za prepoznavanje lica u realnom vremenu ili drugi slični scenariji. Ta pravila se direktno odnose na masovni biometrijski nadzor upotrebom alata za prepoznavanje lica. Države koje imaju neka zakonska pravila o tome, uglavnom zabranjuju nadzor u realnom vremenu ili skoro u realnom vremenu ili ga izuzetno dozvoljavaju pod nekim vrlo ograničenim uslovima.

Zakon Kolorada definiše „tekući nadzor“ kao kontinualnu upotrebu servisa za prepoznavanje lica za potrebe službe da u realnom vremenu prati fizička kretanja određene osobe kroz jedno ili više javnih mesta. Međutim, ova definicija ne obuhvata prepoznavanje ili pokušaj prepoznavanja osobe ako nema pokušaja da se zatim prati njeno kretanje tokom vremena nakon što je osoba prepoznata. „Neprekidno praćenje“ se definiše kao korišćenje FRT-a za potrebe službe da bi pratila kretanje osobe na neprekinutoj osnovi bez identifikacije ili verifikacije identiteta. Praćenje postaje neprekidno u sledećim okolnostima: (1) šablon lica koji omogućava praćenje održava se duže od četrdeset osam sati nakon prvog upisa tog šablona; ili (2) podaci koje je kreirao servis za prepoznavanje lica povezani su sa drugim podacima tako da se osoba koja se prati identifikuje ili se može identifikovati.

Zakon potom predviđa da služba za sprovođenje zakona neće koristiti uslugu prepoznavanja lica da bi vršila tekući nadzor, sprovela identifikaciju u realnom vremenu ili u skoro realnom vremenu, ili da bi započela neprekidno praćenje, osim ako: (1) služba pribavi nalog kojim se takva upotreba odobrava; (2) takva upotreba je neophodna za razvoj istražnih tragova; (3) služba je utvrdila osnovan razlog za takvu upotrebu; ili (4) služba je dobila sudski nalog kojim se odobrava korišćenje usluge isključivo u svrhu lociranja ili identifikacije nestale osobe ili identifikacije preminule osobe.

Zakon u državi Vašington ima istu definiciju „neprekidnog praćenja“ i sličnu definiciju „tekućeg nadzora“, uz jedan dodatak. Naime, precizira se da tekući nadzor podrazumeva korišćenje FRT-a u realnom vremenu, ali i kroz primenu usluge prepoznavanja lica na istorijske zapise. Regulisanje situacija u kojima se dozvoljava tekući nadzor, identifikacija u realnom vremenu ili u skoro realnom vremenu, ili neprekidno praćenje, takođe se donekle razlikuje od propisa u Koloradu, a obuhvaćene su situacije kada (1) postoji nalog kojim se odobrava korišćenje usluge za te svrhe; (2) postoje hitne okolnosti; ili (3) postoji sudski nalog kojim se odobrava korišćenje usluge isključivo u svrhu lociranja ili identifikacije nestale osobe ili identifikacije preminule osobe.

Prema zakonima u Virdžiniji, službi za sprovođenje zakona nije dozvoljeno da koristi FRT za praćenje kretanja identifikovane osobe u javnom prostoru

u realnom vremenu, ili da kreira bazu podataka slika koristeći živi video prenos za primenu FRT-a.

U zakonu koji je na snazi u Merilendu, identifikacija „uživo“ ili „u realnom vremenu“ na osnovu snimaka ili fotografija opisana je u članu kojim se uspostavlja potpuna zabrana uporebe FRT tehnogije u okviru krivične istrage.

Evaluacija tehnologije pre upotrebe

I Vašington i Kolorado regulišu proceduru koju treba preduzeti pre nego što se bilo koja usluga prepoznavanja lica stavi u upotrebu, i to dvojako: (1) obaveštenje o nameri mora biti podneto nadležnom organu, a zatim (2) mora biti pripremljen i javno objavljen izveštaj o odgovornosti. Sadržaj izveštaja o odgovornosti detaljno je regulisan u obe države i on uključuje, između ostalog, tehničke specifikacije, politiku upravljanja, proceduru testiranja, stopu lažnih podudaranja i opis uticaja upotrebe prepoznavanja lica na građanska prava i slobode. Pre nego što se izveštaj o odgovornosti usvoji, mora biti dostupan za javnu raspravu.

U Virdžiniji, zakon propisuje da svaka tehnologija prepoznavanja lica koja je u upotrebi mora da koristi algoritme koji su pokazali (1) rezultat tačnosti od najmanje 98% tačno pozitivnih rezultata u jednom ili više skupova podataka i (2) minimalne varijacije u performansama u demografskim kategorijama koje su povezane sa rasom, bojom kože, etničkim poreklom ili rodom. Taj test vrši Nacionalni institut za standarde i tehnologiju kao deo testa dobavljača tehnologije za prepoznavanje lica, pre nabavke. Pored toga, svaka lokalna služba za sprovođenje zakona mora da izradi politiku korišćenja tehnologije za prepoznavanje lica pre nego što je upotrebi u istrazi određenog krivičnog dela ili u situaciji koja utiče na dobrobit građana, ili da umesto toga usvoji Model politike državne policije za primenu tehnologije za prepoznavanje lica (ako se služba odluči da piše sopstvenu politiku, ona mora da zadovolji ili premaši standarde postavljene u državnom modelu). Služba svoju politiku mora da učini javno dostupnom i da je ažurira jednom godišnje.

U poređenju sa pravilima evropskog GDPR-a, čini se da ove odredbe slede logiku zahteva za pripremu procene uticaja pre primene tehnologije koja može dovesti do rizika po prava i slobode ljudi.

Transparentnost posle upotrebe tehnologije

U fazi nakon što je upotreba tehnologije počela, nekoliko zakona traži nivo transparentnosti koji bi omogućio javnu odgovornost. Takve odredbe o transparentnosti uglavnom se mogu naći u vidu zahteva da izveštaji sadrže neke statističke informacije. Stoga se to donekle razlikuje od režima sličnih GDPR-u, gde se transparentnost prvenstveno postiže kroz politike privatnosti i slična dokumenta (koji treba da sadrže informacije propisane članovima 12 i 13 GDPR-a).

U Vašingtonu i Koloradu odgovarajuću evidenciju moraju da vode organi koji su koristili tehnologiju, ali i sudije koje su izdavale ili produžavale izdate naloge za korišćenje tehnologije, ili uskratile odobrenje za upotrebu. I jedni i drugi su dužni da dostave godišnje izveštaje, čiji je sadržaj regulisan zakonom.

U Virdžiniji, svaka služba koja koristi tehnologiju za prepoznavanje lica mora javno da objavi i godišnje ažurira izveštaj kako bi pružila javnosti informacije o korišćenju FRT-a. Minimalni sadržaj izveštaja je regulisan zakonom. Služba takođe mora javno objavljivati i godišnje ažurirati svoju politiku u vezi sa korišćenjem tehnologije za prepoznavanje lica.

U Juti, državni organi su obavezani da na zahtev objave statističke informacije u vezi izvršenih poređenja za prepoznavanje lica. Takve statističke informacije mogu uključivati (1) različite vrste krivičnih dela za koje je državni organ primio zahtev za obradu; (2) koliko je zahteva za obradu državni organ primio za svaku vrstu krivičnog dela; i (3) broj verovatnih podudaranja koje je državni organ dao kao odgovor na svaki zahtev. Državni organ takođe mora da pripremi privremene godišnje izveštaje nadležnom vladinom odboru. Pored statističkih informacija iz tačaka (1) do (3), izveštaj mora da sadrži i izvor slike iz kojeg je odeljenje izvelo svako podudaranje. Zakon izričito reguliše da u odgovoru na zahtev za objavljivanje statističkih informacija ili u pripremi odgovarajućeg izveštaja, državni organ ne može otkriti detalje u vezi sa istragom koja je u toku.

Zakon u Mejnu uređuje obavezu agencija koje vrše pretrage da vode evidenciju svih zahteva za pretragu sistema za nadzor koje primaju. Anonimizovani logovi – koji sadrže datum zahteva za pretragu, ime službenika ili funkcionera koji je podneo zahtev i naziv odeljenja za koje službenik ili funkcioner radi, baze podataka koje su pretražene, zakonski prekršaj koji se istražuje, kao i rasu i pol osobe pod istragom – predstavljaju

javnu evidenciju u smislu državnih propisa koji regulišu slobodu pristupa informacijama od javnog značaja.

U skladu sa zakonom u Masačusetsu, propisan je način na koji su službe obavezne da dokumentuju svaku izvršenu pretragu za prepoznavanje lica i da tu dokumentaciju tromesečno dostavljaju izvršnoj kancelariji za javnu bezbednost. Ova kancelarija ima obavezu da na svom sajtu godišnje objavljuje dokumentaciju dobijenu od organa za sprovođenje zakona, kao i dodatne podatke za prethodnu kalendarsku godinu sa ukupnim brojevima iz cele države (kako zakon detaljno propisuje).

U Merilendu, godišnji izveštaji koje agencije za sprovođenje zakona moraju da pripreme i objave mininalno sadrže sledeće elemente: (1) naziv FRT sistema i baza koje se koriste za pretraživanje, (2) broj pretraga u svakom od sistema i tip krivičnog dela ili incidenta, (3) broj mogućih pozitivnih rezultata koji su doveli do dalje istrage i to sa informacijama o rasi, uzrastu i polu osoba za koje je utvrđeno moguće podudaranje – po sistemu i po bazi, (4) slučajevi povrede podataka i neautorizovanih pristupa.

Tekuće testiranje

Nekoliko država ima pravila o uslovima koje tehnologija mora da ispunjava ne samo pre nego što se tehnologija kupi ili stavi u funkciju, već i tokom njenog životnog ciklusa. Ove odredbe nisu toliko uobičajene van SAD.

Zakoni Vašingtona i Kolorada imaju najrazrađenija pravila o tome kako se tehnologija mora testirati za tačnost i kontrolu pristrasnosti. Pre primene FRT-a za odlučivanje koje proizvodi pravno dejstvo na pojedince ili ima slična značajna dejstva, takva usluga mora biti testirana u operativnim uslovima. Štaviše, služba mora da zahteva od provajdera usluga da učini dostupnim interfejs za programiranje aplikacije ili druge tehničke mogućnosti da omogući legitimne, nezavisne i razumne testove tačnosti i nepravednih razlika u performansama između različitih podpopulacija (takve podpopulacije su definisane vizuelno uočljivim karakteristikama kao što je boja kože, rod, uzrast itd.). Ako nezavisno testiranje utvrdi materijalno nepošten učinak, dobavljač mora da razvije i primeni plan za ublažavanje utvrđenih odstupanja.

Virdžinija propisuje obavezu godišnjeg testiranja kako bi se potvrdilo da su uslovi za primenu tehnologije i dalje zadovoljeni, odnosno u skladu sa zakonom, dok svi odobreni dobavljači moraju jednom godišnje da dostave nezavisnu procenu i referentne vrednosti koje daje Nacionalni institut za standarde i tehnologiju, kako bi potvrdili kontinuirano poštovanje zakonskih obaveza.

Obuka osoblja

Još jedan tip pravnog zahteva specifičan za SAD, opet, usmeren je na potvrdu da se tehnologija koristi na zakonit način. Ne samo da tehnologija mora da zadovolji unapred definisane uslove i da se redovno testira, već i ljudi koji rade sa tom tehnologijom moraju da znaju kako da je pravilno koriste.

Obuka službenika ili zaposlenih koji će koristiti FRT u praksi detaljno je regulisana zakonima Merilenda, Vašingtona i Kolorada, uključujući i predviđene obaveze. Minimalna obuka treba da pokrije (1) mogućnosti i ograničenja FRT-a; (2) procedure za tumačenje i delovanje na osnovu rezultata FRT-a; i, u meri koja je primenjiva na kontekst upotrebe, (3) značajno ljudsko učešće u preispitivanju odluka koje proizvode pravno dejstvo u vezi sa pojedincima ili slična značajna dejstva.

Drugi zakoni ne ulaze toliko u detalje. Po zakonu koji je na snazi u Virdžiniji, državna policija mora da razvije i objavi Model politike državne policije za primenu tehnologije prepoznavanja lica. Ovaj model politike mora, između ostalog, da obuhvati obavezu obuke koja se odvija preko službe, te da razradi prirodu i učestalost specijalizovane obuke potrebne da bi neko dobio ovlašćenje za korišćenje FRT-a.

Slično, zakon u Kentakiju propisuje da model politike izrađuje imenovana radna grupa, a takvom politikom biće konkretizovane procedure i procesi obuke kako bi svo osoblje koje koristi FRT ili pristupa relevantnim podacima, steklo znanja i veštine da obezbedi usklađenost sa politikom.

Izrada interne politike je obaveza i prema propisima Merilenda, ali bez dodatnog regulisanja njenog sadržaja.

Osnovana sumnja u krivičnoj istrazi

Ovaj zahtev treba tumačiti u skladu sa odredbama krivičnog prava SAD. Međutim, pošto je prepoznavanje lica u kontekstu rada službi za sprovođenje zakona u velikoj meri direktno povezano sa istragama i krivičnim postupcima, slične zakonske odredbe se mogu naći i u drugim pravnim sistemima. Na primer, u Indiji, policija u Delhiju se oslanjala na indijski krivični zakon kao pravnu osnovu za upotrebu FRT-a (iako zakon ne propisuje nikakva

pravila o značaju dokaza koji se odnose na prepoznavanje lica u krivičnim postupcima).

Nekoliko američkih država reguliše zabranu upotrebe pozitivnih poklapanja iz FRT-a za utvrđivanje osnovane sumnje u krivičnoj istrazi, uz neke lokalne razlike. U Alabami, zakon dodaje pravilo da državna ili lokalna služba za sprovođenje zakona ne sme da koristi rezultate poklapanja kao osnov za hapšenje.

Zakoni Merilenda, Alabame, Vašingtona i Kolorada regulišu da se rezultati prepoznavanja lica mogu koristiti zajedno sa drugim informacijama i dokazima koje je službenik za sprovođenje zakona zakonito pribavio za utvrđivanje osnovane sumnje u krivičnoj istrazi (u Alabami i za hapšenje).

Prema zakonu u Virdžiniji, podudaranje izvedeno preko FRT-a neće biti uključeno u izjavu pod zakletvom radi utvrđivanja osnovane sumnje za izdavanje naloga za pretres ili za hapšenje, ali će biti prihvatljivo kao oslobađajući dokaz.

Prema zakonu u Mejnu, podaci o ljudskom licu izvedeni iz nadzora ne mogu da služe, bez drugih dokaza, kao razuman osnov za hapšenje, pretres ili zaplenu.

Ograničeni obim krivičnih i drugih dela

Upotreba FRT-a u službama za provođenje zakona uglavnom je usmerena na istragu krivičnih dela. Dok većina američkih država ne pravi razliku između dela u smislu dozvoljene upotrebe, neke su ograničile upotrebu alata za prepoznavanje lica na ozbiljnija krivična dela.

Zakon Mejna sadrži definiciju teškog zločina i ograničava dozvoljenu svrhu upotrebe prepoznavanja lica za istragu takvih dela kada postoji razumna osnova da se veruje da ih je počinila neidentifikovana osoba na određenoj slici. Težak zločin se definiše kao svako krivično delo za koje je propisana kazna zatvora od jedne ili više godina kao i neka posebna krivična dela – ako se zakon Mejna primenjuje na pravnu kvalifikaciju. Ako su primenjivi krivični zakoni druge jurisdikcije, težak zločin se definiše kao krivično delo koje podrazumeva upotrebu vatrenog ili drugog opasnog oružja ili je kažnjivo zatvorom od jedne ili više godina.

Zakon u Juti ograničava upotrebu na istrage krivičnog dela ili nasilnog zločina ili, uopštenije, pretnji po ljudski život. Zakon u Merilendu sadrži konkretan spisak od 12 dela, koja po pravilu uključuju nasilnu komponentu ili ugroženost života.

Poredeći sa prilikama u drugim jurisdikcijama u svetu, prvi i drugi nacrt odredbi koje regulišu upotrebu FRT u policiji Srbije, obuhvatali su sva krivična dela koja se gone po službenoj dužnosti, dok postupak po privatnoj tužbi nije bio pokriven. Međutim, ova druga kategorija uključuje vrlo malo krivičnih dela, kao što su ona protiv dostojanstva i prava intelektualne svojine, ili dela kao što su lakše telesne povrede i sitne krađe.

Identifikacija preminule i/ili nestale osobe

Zakoni u Vašingtonu i Koloradu imaju istu odredbu na ovu temu – služba za sprovođenje zakona može da koristi uslugu prepoznavanja lica ako dobije sudski nalog kojim se odobrava korišćenje usluge isključivo u svrhu lociranja ili identifikacije nestale osobe ili identifikacije preminule osobe.

Definicija „ovlašćene upotrebe“ FRT-a u zakonu Virdžinije obuhvata identifikaciju preminule ili nestale osobe. Slično tome, zakon u Mejnu dozvoljava državnim organima upotrebu FRT-a ako je svrha pomoć u identifikaciji osobe koja je umrla ili se veruje da je umrla, kao i nestale osobe, dok u Merilendu to ovlašćenje imaju agencije za sprovođenje zakona.

Dve američke države su isključile identifikaciju nestale osobe kao dozvoljenu upotrebu. U Juti, upotreba FRT-a je dozvoljena u svrhu identifikacije preminule ili onesposobljene osobe ili osobe koja je u opasnosti a ne može da potvrdi svoj identitet službi za sprovođenje zakona. Zakon u Masačusetsu propisuje da služba za sprovođenje zakona može da koristi FRT bez sudskog naloga kako bi identifikovala preminulu osobu.

Obaveza ljudske intervencije

Dok neki zakoni uzimaju u obzir da ljudi mogu da pogreše, pa stoga zahtevaju da službenici koji koriste tehnologiju u praksi moraju da prođu odgovarajuću obuku, drugi zakoni imaju u vidu da i tehnologija pravi greške.

Zakoni u Vašingtonu i Koloradu regulišu situacije kada ljudi moraju da verifikuju pozitivno podudaranje koje je izveo sistem za prepoznavanje lica. Prema zakonima u obe ove države, služba koja koristi FRT za donošenje odluka koje proizvode pravno dejstvo u vezi sa pojedincima, ili slična značajna dejstva na pojedince, dužna je da se postara da takve odluke budu predmet smislenog ljudskog pregleda. „Smisleni ljudski pregled“ se definiše

kao pregled ili kontrola koju vrši jedan ili više obučenih ljudi sa ovlašćenjem da izmene odluku koja se preispituje.

Prema zakonu u Juti i Merilendu, ako sistem za prepoznavanje lica izvede moguće podudaranje, ovlašćeni zaposleni mora da izvrši nezavisnu vizuelnu proveru takvog podudaranja. Zakon precizira dalju proceduru u zavisnosti od toga da li je provera pokazala da je poklapanje samo moguće ili je verovatno. Verovatno podudaranje mora proći kroz drugi krug ljudske provere, a takvo drugo mišljenje treba da pruži drugi obučeni zaposleni ili nadležni supervizor. Na taj način, konačnu odluku o tome da li podudaranje treba da se tretira kao verovatno uvek donosi čovek.

Ovlašćenje za pretragu

Pojedine države su usvojile pravilo prema kojem policajci ne mogu imati direktan pristup FRT sistemu radi vršenja poređenja, već se za to moraju obratiti drugom organu. To je neka vrsta zaštite od neovlašćene upotrebe ili zloupotrebe tehnologije u policiji.

U Mejnu, zahtevi za pretragu nadzornih sistema za prepoznavanje lica šalju se Birou za motorna vozila, osim u nekim uskim i specifičnim situacijama.

Po važećim propisima u Masačusetsu, svaka služba za sprovođenje zakona koja obavlja ili zahteva FRT pretragu, to može učiniti samo putem pisanog zahteva koji se podnosi registru motornih vozila, državnoj policiji ili ogranku FBI.

U Juti, služba za sprovođenje zakona treba da podnese zahtev za pretragu baze za prepoznavanje lica vladinom organu koji upravlja odgovarajućom bazom ili odeljenju za javnu bezbednost, ako to odeljenje ima pristup ili vodi takvu bazu podataka.

Kazne za kršenje zakona

Neke države propisuju kazne za službenike ili druge zaposlene koji koriste tehnologiju kršeći zakon. Ovakav pristup se verovatno može povezati sa opštim pravnim režimom u tim državama, gde primena odredbe ima određene rezultate u praksi u sličnim scenarijima. Mada izgleda kao moćno pravno sredstvo za odvraćanje od postupanja suprotno zakonskim obavezama i dužnostima, malo je verovatno da će se poštovati u pravnim sistemima (kao u nekim zemljama civilnog prava) koji načelno ne koriste ovaj pristup odgovornosti javnih službenika.

Zakon Virdžinije nameće takvu kaznu za bilo kog operatera zaposlenog u lokalnoj službi za sprovođenje zakona koji (1) prekrši politiku službe za korišćenje FRT-a ili (2) izvrši pretragu iz razloga mimo ovlašćene upotrebe. Takav operater je kriv za prekršaj i od njega se traži da se podvrgne obuci o politikama službe za ovlašćenu upotrebu tehnologije, pre nego što bude vraćen u rad na FRT sistemu. Lokalna služba za sprovođenje zakona će prekinuti radni odnos svakog operatera FRT-a koji prekrši klauzulu (1) ili (2) po drugi put. Drugi ili naredni prekršaj smatraće se težim prekršajem.

Prema zakonu koji reguliše upotrebu prepoznavanja lica u Mejnu, javni službenik ili funkcioner koji u vršenju službene dužnosti prekrši odredbu zakona može biti podvrgnut disciplinskim merama, uključujući prekvalifikaciju, suspenziju ili otkaz, u skladu sa odredbama o pravičnom postupku i primenjivim kolektivnim ugovorom.

Prema zakonu Merilenda, moguće je u parničnom postupku ostvarivati prava zbog kršenja pravila o upotrebi FRT tehnologije iz tog zakona (civil action).

Moratorijum do usvajanja relevantne regulative

Vermont i Kentaki su doneli zakone kojima je praktično proglašen moratorijum na upotrebu FRT-a u službama za sprovođenje zakona, sve dok se ne donesu relevantna zakonska pravila za takvu upotrebu.

U Vermontu pravila mora da donese Generalna skupština Vermonta.

U Kentakiju je osnovana radna grupa za tehnologiju prepoznavanja lica sa mandatom da kreira politiku koja precizira pravila za upotrebu FRT-a u službama za sprovođenje zakona. Kao rok za izradu takve politike bio je predviđen 1. januar 2024.

Izuzetak za krivičnu istragu seksualne eksploatacije dece

Zakon Vermonta za sada zabranjuje svaku upotrebu prepoznavanja lica, ali predviđa jedan izuzetak: svrhe sprovođenja zakona tokom krivične istrage o seksualnoj eksploataciji dece.

	VAŠINGTON	KOLORADO	VIRDŽINIJA	MEJN	JUTA	MASAČUSETS	ALABAMA	VERMONT	KENTAKI	MERILEND
Pravni režim samo za službe za sprovođenje zakona			✓			✓	✓	✓	✓	✓
Pravni režimi u kojima važi opšta zabrana upotrebe FRT podložna izuzecima				✓	✓		✓	✓		✓
Pravni režimi koji omogućavaju						✓				✓
Izričita zabrana određenih upotreba FRT	✓	✓	✓		✓					✓
Regulisanje nadzora u realnom	✓	✓	✓							✓
Evaluacija tehnologije pre upotrebe	✓	✓	✓							
Transparentnost nakon	✓	✓	✓	✓	✓	✓				✓
Tekuće testiranje	✓	✓	✓							
Obuka osoblja	✓	✓	✓						✓	✓
Zabrana utvrđivanja osnovane	✓	✓	✓	✓			✓			✓
Ograničeni obim krivičnih dela				✓	✓					✓
Identifikacija preminule osobe	✓	✓	✓	✓	✓	✓				✓
Potraga za nestalom osobom	✓	✓	✓	✓						✓
Obaveza ljudske intervencije	✓	✓			✓					
Ovlašćenje za pretragu				✓	✓	✓				✓
Kazne za kršenje zakona			✓	✓						
Moratorijum do usvajanja relevantne regulative								✓	✓	
Izuzetak za krivičnu istragu seksualne eksploatacije dece								✓		

Država Vašington

U martu 2020, Vašington je usvojio sveobuhvatan zakon koji reguliše upotrebu tehnologije za prepoznavanje lica kod svih vladinih subjekata, državnih i lokalnih, uključujući i organe za sprovođenje zakona (sa datumom stupanja na snagu 1. jula 2021.).[562] Pojedini komentatori su zakon opisali kao pokušaj da se pronađe kompromis između potpune zabrane FRT-a i njegove neselektivne upotrebe.[563] Cilj zakonodavca bio je dvostruk: stvoriti pravni okvir u kom se FRT može upotrebljavati za pretpostavljenu korist društva, a da se istovremeno društvo zaštiti od upotreba koje ugrožavaju demokratske slobode a prava građana izlažu riziku.[564]

Američka unija za građanske slobode (American Civil Liberties Union, ACLU) izrazila je zabrinutost zbog preslabih zaštitnih mera predviđenih zakonom, te zbog nedostatka „smislenih mehanizama odgovornosti ili sprovođenja“. Zakon je takođe kritikovan jer dozvoljava upotrebu FRT-a prilikom donošenja odluka u vezi sa finansijskim uslugama i uslugama zajma, stanovanjem, osiguranjem, obrazovanjem, krivičnim postupkom, zapošljavanjem, zdravstvenom zaštitom i osnovnim potrepštinama, ukoliko takve odluke prolaze kroz labavo definisani „smisleni ljudski pregled“.[565]

Pošto je zakon sponzorisao senator koji je u to vreme radio kao viši programski menadžer u Microsoftu, spekulisalo se o neprimerenom uticaju ove korporacije na zakonodavni proces.[566]

Zakon reguliše različite aspekte primene FRT-a, uključujući obaveze pre primene tehnologije, kao i neke mehanizme transparentnosti i odgovornosti. Na osnovu teksta zakona ova pravila se mogu sažeti na sledeći način:[567]

» **Obaveštenje o namerama i izveštaji o odgovornosti** — Predlog zakona propisuje obavezu svake službe koja planira da koristi FRT, da podnese obaveštenje o nameri odgovarajućim zakonodavnim vlastima pre primene tehnologije. Služba takođe mora da izradi javni „izveštaj o odgovornosti“ koji pruža detalje o nizu tačaka navedenih u zakonu (služba može da počne da radi na izveštaju o odgovornosti nakon što zakonodavnim vlastima podnese obaveštenje o nameri). Pre implementacije sistema za prepoznavanje lica, izveštaj će biti otvoren za javnu reviziju i komentare, a mora se ažurirati po potrebi.

» **Ljudski pregled i testiranje** — Agencije koje koriste FRT za donošenje odluka koje proizvode pravno dejstvo na pojedince, moraju testirati sistem u operativnim uslovima, a takođe su u obavezi da te odluke podvrgnu „smislenom" ljudskom pregledu, mada je ovaj izraz loše definisan, što otvara pitanja o stvarnoj smislenosti tog pregleda.

» **Neslaganja u performansama** — Da bi se omogućilo nezavisno testiranje tačnosti, kao i da se obezbedi da nema „nepoštenih" razlika u performansama u različitim podpopulacijama, agencije moraju da obavežu provajdera usluga da učini dostupnim interfejs za programiranje aplikacije (application programming interface, API). Ako nezavisno testiranje otkrije nepravedne razlike u učinku između podpopulacija, provajder mora da napravi i sprovede plan za ispravku. Međutim, kako je detaljno izloženo u poglavlju Praksa, ovako uzan fokus na tehničku pristrasnost može prikriti širu štetu, posebno na društvenom nivou, kao što je sistemski rasizam. To je posebno slučaj ovde, gde je korišćenje nadzora i dalje dozvoljeno, uprkos sistemskim rizicima koje predstavljaju po prava, uključujući privatnost, jednakost i nediskriminaciju.

» **Obuka** — Zaposleni koji rade sa FRT-om moraju da prolaze redovne obuke. Minimalni zahtevi za obuku su propisani zakonom.

» **Vođenje evidencije** — Svaka agencija koja koristi FRT mora da vodi evidenciju koja je dovoljna da olakša javno izveštavanje i reviziju usklađenosti.

» **Krivično pravo i pravosuđe** — Službe su dužne da proaktivno obaveste okrivljenog pre suđenja kada je u postupku korišćeno prepoznavanje lica. Pored njih, i sudije koje su izdavale, produžavale ili odbijale naloge za upotrebu FRT-a, moraju dostaviti godišnje izveštaje sa propisanim minumom informacija.

» **Upotreba za nadzor, uključujući identifikaciju u realnom vremenu i neprekidno praćenje** — Agencijama je dozvoljeno da koriste FRT za tekući nadzor, identifikaciju u realnom vremenu ili u skoro realnom vremenu i neprekidno praćenje (definisano zakonom kao praćenje kretanja bez identifikacije) samo u tri scenarija: (1) na osnovu naloga; (2) ako postoje hitne okolnosti; ili (3) sa sudskom naredbom za isključivu svrhu lociranja ili identifikacije nestale ili preminule osobe.

» **Zabrane** — Zakon izričito zabranjuje nekoliko upotreba, kao što je (1) primena prepoznavanja lica na osnovu verskih ili političkih stavova, roda, rodnog identiteta, stvarne ili pretpostavljene rase, etničke pripadnosti, državljanstva, starosti ili invaliditeta (dok zakon to eksplicitno reguliše ova zabrana ne omogućava profilisanje uključujući, ali ne ograničavajući se na prediktivne alate za sprovođenje zakona). FRT se takođe ne može koristiti (2) za identifikaciju osobe na osnovu crteža ili druge ručno izrađene slike (mada se ne bavi posebno upotrebom slika sličnih osoba, kao što je to bio slučaj sa fotografijom glumca Woodyja Harrelsona koju je njujorška policija koristila u potrazi za osumnjičenim za koga su verovali da liči na glumca); (3) za izradu evidencije koja opisuje događaje kada je osoba koristila svoja prava iz Prvog amandmana; ili (4) kao jedinu osnovu za utvrđivanje osnovane sumnje u krivičnoj istrazi. Međutim, rezultati pretrage sistema za prepoznavanje lica mogu se koristiti zajedno sa drugim informacijama i dokazima koje je službenik za sprovođenje zakona zakonito pribavio da bi se utvrdila osnovana sumnja u krivičnoj istrazi.

» **Izuzeci** — Zakon se ne odnosi na upotrebu sistema za prepoznavanje lica u radu službe nadležne za izdavanje vozačkih dozvola, niti na situacije u kojima učestvuje neka savezna agencija.

» **Bez radne grupe** — Predlog zakona je predviđao uspostavljanje radne grupe koja će analizirati i davati preporuke po nekoliko pitanja koja proizlaze iz upotrebe FRT-a, ali je guverner stavio veto na ovu odredbu jer nije imala budžetsku alokaciju.

Država Kolorado

U Koloradu je na snazi vrlo detaljan zakon o prepoznavanju lica koji reguliše upotrebu tehnologije u radu službi za sprovođenje zakona, ali i drugih službi lokalne vlasti. Zakon je usvojen u maju 2022, a stupio je na snagu u avgustu iste godine.[568]

Struktura je veoma slična zakonu usvojenom u Vašingtonu. Mada su pravila gotovo ista, postoje razlike u pojedinim pravilima kao i u formulaciji odredbi. Sličnosti su sledeće:[569]

- postoji obaveza pripreme i podnošenja obaveštenja o nameri i izveštaja o odgovornosti;
- mora da postoji smislen ljudski pregled i testiranje u slučaju svake odluke koja može proizvesti pravno ili slično značajno dejstvo na pojedince;
- da bi ublažili odstupanja u performansama, provajderi usluga moraju staviti na raspolaganje tehničku mogućnost za sprovođenje testova tačnosti;
- mora biti organizovana obuka ljudi koji koriste FRT;
- agencija koja primenjuje tehnologiju mora voditi evidenciju dovoljnu da olakša javnu kontrolu;
- gencija koja koristi FRT mora okrivljenom pre suđenja otkriti da je koristila pretragu za prepoznavanje lica; i
- i agencije koje koriste FRT i sudije koje su upotrebu odobravale ili odbijale, moraju podneti propisane informacije o svom učešću u upotrebi FRT-a.

Međutim, u nekim tačkama se zakon u Koloradu razlikuje od onog u Vašingtonu:

- Sadržaj izveštaja o odgovornosti je nešto drugačiji, budući da zakon u Koloradu ne propisuje da izveštaj sadrži informacije o tome kako pružalac usluga i agencija nameravaju da ispune obaveze obaveštavanja u slučaju bezbednosnog incidenta. Zakon u Koloradu takođe reguliše ograničene situacije kada agencija ne mora da priprema izveštaj (uglavnom kada je upotreba prepoznavanja lica u komercijalne, a ne u vladine svrhe).
- Tekući nadzor, uključujući identifikaciju u realnom vremenu ili u skoro realnom vremenu i neprekidno praćenje, dozvoljeni su pod nešto drugačijim uslovima nego u Vašingtonu, odnosno samo ako (1) postoji nalog; (2) postoji potreba da se razviju tragovi u istrazi; (3) služba je utvrdila osnovanu sumnju za takvu upotrebu; ili (4) služba je pribavila sudsku naredbu kojom se odobrava upotreba isključivo za svrhe lociranja ili identifikacije nestale osobe ili identifikacije preminule osobe.
- Zakon ne reguliše niti pominje prediktivne alate u sprovođenju zakona (iako bi zabrana prediktivnog rada policije mogla biti implicirana tumačenjem zakona), niti reguliše da se prepoznavanje lica ne može koristiti za identifikaciju pojedinca na osnovu crteža ili druge ručno proizvedene slike.
- Izuzeci od zakona su nešto drugačiji. Zakon u Koloradu ne pominje izuzetak organa nadležnih za izdavanje vozačkih dozvola. Međutim, reguliše nekoliko situacija u kojima se zakon ne primenjuje: (1) kada agencija koristi sistem za prepoznavanje lica u vezi sa sistemom kontrole fizičkog pristupa kako bi odobrila ili uskratila pristup obezbeđenoj oblasti (što obično znači biometrijsku verifikaciju); ili (2) kada državna agencija koristi sistem za prepoznavanje lica isključivo u istraživačke svrhe, sve dok upotreba ne rezultira niti utiče na bilo koju odluku koja proizvodi pravno dejstvo ili slično značajno dejstvo u vezi sa pojedincima; ili (3) na kompaniju koja pruža komunalne usluge.
- Zakon u Koloradu posvećuje ceo odeljak upotrebi prepoznavanja lica u školama. Opšte pravilo je da školama nije dozvoljeno da sklapaju ugovor sa bilo kojim dobavljačem za kupovinu usluga prepoznavanja lica. Postoje dva izuzetka: (1) ako je ugovor sa dobavljačem potpisan pre nego što je zakon stupio na snagu, izuzetak se primenjuje samo tokom važenja ugovora; (2) ako ugovor reguliše široko dostupan potrošački proizvod, uključujući tablet ili pametni telefon, koji omogućava analizu crta lica kako bi se korisnicima olakšalo upravljanje adresarom ili galerijom slika ili video snimaka za ličnu ili kućnu upotrebu.
- Zakon u Koloradu uspostavlja i reguliše članstvo, dužnosti i obaveze radne grupe zadužene za procenu upotrebe FRT-a u državnim službama, sa mandatom da ispita i izveštava o razmerama tekuće upotrebe, kao i da daje preporuke za buduću upotrebu, na način regulisan zakonom.

Komonvelt Virdžinija

U dvofaznom zakonodavnom procesu, Virdžinija je usvojila razrađen zakon koji reguliše upotrebu prepoznavanja lica u svim agencijama za sprovođenje zakona, uključujući policijska odeljenja na univerzitetskim kampusima i državnu policiju. Najpre, u aprilu 2021. godine, usvojen je zakon kojim se uspostavlja de facto zabrana upotrebe FRT-a u organima za sprovođenje zakona.[570] Zabrana se prvenstveno sastojala od zabrane upotrebe ili kupovine tehnologije bez prethodnog zakonodavnog odobrenja – u toj fazi, država nije imala nikakav relevantan propis.[571] Međutim, nakon dodatne debate, taj zakon je ubrzo zamenjen novim skupom pravila u aprilu 2022.[572] koji regulišu uslove pod kojima bi upotreba FRT-a bila dozvoljena.[573] ACLU i mediji ocenili su da su nova pravila preširoka i ostavljaju mnoga neregulisana pitanja.[574]

Novim pravilima definisano je najpre četrnaest „ovlašćenih upotreba" FRT-a.[575] Nekoliko slučajeva upotrebe tiče se situacija kada bi tehnologija „pomogla u identifikaciji osobe", uključujući osumnjičene, žrtve određenih zločina, svedoke krivičnog dela, nestale ili preminule osobe, ili osobe koje su onesposobljene za samoidentifikaciju, kao i osobe za koje se razumno veruje da predstavljaju opasnost za sebe ili druge. Drugi slučajevi obuhvataju neposrednu pretnju po javnu bezbednost, značajnu pretnju po život ili pretnju nacionalnoj bezbednosti, uključujući dela terorizma, ili kada je potrebno da se utvrdi da li je osoba nezakonito dobila vozačku dozvolu, finansijski instrument, ili drugi službeni oblik identifikacije. Ovaj popis slučajeva dozvoljene upotrebe daleko je širi od izuzetaka navedenih u zakonu EU o veštačkoj inteligenciji, koji su kontrolna tela EU za zaštitu podataka kritikovala kao dovoljno široke da omoguće opštu upotrebu.

Takođe, zakon u Virdžiniji propisuje evaluaciju tehnologije pre upotrebe, sa ocenom tačnosti od najmanje 98% tačno pozitivnih rezultata (stvarnih podudaranja) u svim demografskim grupama. Ovu ocenu daje Nacionalni institut za standarde i tehnologiju u okviru testa dobavljača tehnologije za prepoznavanje lica.

Ovaj zahtev možda zvuči preterano, međutim u stvarnosti svaki sistem nadzora koji se koristi na masovnom nivou – bilo da se radi o testiranju na kovid-19, profilisanju putnika u aviosaobraćaju ili identifikaciji ljudi putem biometrije – čak i sa 98% tačno pozitivnih rezultata i dalje zapravo ima veliki broj grešaka. Fenomen u statistici koji se naziva zanemarivanje osnovne stope (eng. base rate neglect) čini određeni broj grešaka neizbežnim. Štaviše, bez pratećih stopa lažno pozitivnih (ljudi koji su bili označeni, a nije trebalo da budu) i lažno negativnih rezultata (ljudi koji nisu bili označeni, ali je trebalo da budu), prava pozitivna stopa predstavlja samo jedan deo slagalice. Kompleksna matematika biometrijskih poklapanja detaljnije se ispituje u poglavlju Praksa u vezi sa upotrebom FRT-a u londonskoj Metropoliten policiji.

Zakon Virdžinije predviđa i obaveze transparentnosti, na primer da agencije za sprovođenje zakona moraju da vode evidencije u vezi sa korišćenjem FRT-a, a takođe su dužne i da objave godišnji izveštaj. Prema zakonu, svako podudaranje izvedeno kroz FRT neće se koristiti u izjavi pod zakletvom za utvrđivanje osnovane sumnje za odobrenje naloga za pretres ili hapšenje. Regulisana su i kaznena pravila: svaki operater FRT-a koji prekrši politiku službe ili odeljenja za korišćenje tehnologije za prepoznavanje lica, ili izvrši pretragu iz bilo kog razloga osim onih za koje je ovlašćen po zakonu, kriv je za odgovarajući prekršaj.

Zakon reguliše i nekoliko slučajeva u kojima je zabranjena upotreba tehnologije. Zabrana obuhvata (1) korišćenje FRT-a za praćenje kretanja identifikovane osobe u javnom prostoru u realnom vremenu; (2) kreiranje baze slika uz pomoć živog video prenosa za svrhe upotrebe FRT-a; ili (3) unos slike za poređenje u komercijalnu bazu provajdera FRT usluga, osim u skladu sa ovlašćenom upotrebom.

Konačno, zakon predviđa da se pre stavljanja sistema za prepoznavanje lica u upotrebu, mora razviti politika koja će regulisati upotrebu u istrazi, obaveze obuke, kao i određene protokole upotrebe. Državna policija objavila je model politike koja daje smernice agencijama za sprovođenje zakona za dalju upotrebu FRT-a. Policijske uprave mogu da preuzmu ovaj model ili da razviju sopstvene politike sa strožim smernicama.[576]

Država Mejn

Zakon koji reguliše nadzor, uključujući tehnologije za analizu karakteristika lica kao što je iris oka, usvojen je u julu 2021.[577] U to vreme je opisivan kao „najjači državni zakon o prepoznavanju lica u SAD", posebno u odnosu na prethodnike, što se u to vreme uglavnom odnosilo na državu Vašington.[578] Prema definiciji iz zakona, nadzor ljudskog lica označava „automatizovani ili poluautomatizovani proces koji pomaže u identifikaciji ili verifikaciji identiteta pojedinca, ili u prikupljanju informacija o pojedincu, zasnovan na fizičkim karakteristikama lica konkretnog pojedinca".

Ova definicija pokriva širok spektar slučajeva upotrebe uključujući identifikaciju i bilo koji oblik kategorizacije ili profilisanja osobe na osnovu njenih fizičkih karakteristika. Stoga je verovatno šira od definicije u GDPR-u, koja pokriva samo podatke koji su prošli specifičnu tehničku obradu i mogu omogućiti identifikaciju ili potvrditi identitet osobe. Međutim, mada sugeriše da bi druge crte lica poput irisa u oku, ili predviđanje emocija na osnovu izraza lica, mogli biti obuhvaćeni definicijom „fizičkih karakteristika lica osobe“, izgleda da druga telesna ili bihevioralna biometrija nije pokrivena.

Zakon reguliše upotrebu prepoznavanja lica ne samo u službama za sprovođenje zakona, već i u bilo kojoj državnoj ili lokalnoj vlasti. Osnovno pravilo i polazna odredba zakona jeste da nijedan javni funkcioner ni telo ne mogu da pribave, zadrže, poseduju, pristupe, zahtevaju ili koriste sistem FRT ili informacije koje iz njega proističu, niti da sklapaju ugovore u tom smislu, niti da bilo kojoj trećoj strani izdaju dozvolu za bilo koju od navedenih radnji – uz nekoliko izričito regulisanih izuzetaka.

Jedna grupa izuzetaka od ove osnovne zabrane predviđena je za svrhe (1) istrage teškog zločina (kako je definisano u samom zakonu), kada postoji osnovana sumnja da je neidentifikovana osoba na slici počinila teško krivično delo; (2) pomoći u identifikaciji preminule osobe; ili (3) pomaganja u identifikaciji nestale ili ugrožene osobe. Tako u ovim slučajevima državni organi mogu koristiti FRT bez sudskog naloga. Ovi izuzeci su donekle slični izuzecima koji su predviđeni evropskim zakonom o veštačkoj inteligenciji, kao i u povučenom predlogu zakona o unutrašnjim poslovima Srbije (čije su odredbe bile sročene po uzoru na evropski predlog o AI), o kojima ima više reči u drugim poglavljima ove knjige, mada EU zakona ipak zahteva sudsko odobrenje.

Dodatno, kada se FRT koristi u ove svrhe, javne službe ne mogu same da vrše pretrage za prepoznavanje lica, već moraju da zahtevaju pretragu od nadležne institucije, kao što je Biro za motorna vozila, FBI ili državna agencija koja izdaje službene akreditive. To podleže daljim pravilima o tome kako i pod kojim uslovima se takve pretrage mogu vršiti. Zakon takođe reguliše da državna policija i uprava za motorna vozila vode logove (sa elementima regulisanim zakonom) koji prate sve primljene i izvršene zahteve za pretragu sistema za nadzor. Dok pretraga sistema u državnoj ili saveznoj agenciji bar implicira da su referentne baze sastavljene po osnovanoj sumnji ili kriminalnoj aktivnosti (mada to možda nije slučaj u praksi), činjenica da Biro za motorna vozila može da preduzme pretragu znači da će se svaki vlasnik vozačke dozvole naći u redu za prepoznavanje. Pretrage vršene na takvim osnovama bile su na meti kritika u drugim zemljama, kao što je slučaj sa predloženim režimom prekogranične razmene podataka EU, Uredbom Prum II, koji je osporila organizacija civilnog društva Statewatch.[579]

Zakon predviđa još jednu grupu izuzetaka od opšte zabrane prepoznavanja lica. To uključuje različite konkretne situacije kao što su nabavka, održavanje ili korišćenje sistema za prepoznavanje lica u okviru Biroa za motorna vozila u skladu sa pravilima koja regulišu vozačke dozvole, ili u svrhu prevencije ili istrage prevara; upotreba tehnologije koja analizira iris oka u regionalnom ili okružnom zatvoru; kao i za autentifikaciju korisnika (npr. otključavanje ličnog uređaja). Zakon takođe potvrđuje da se sledeći slučajevi upotrebe ne smatraju zabranjenom upotrebom: upotreba društvenih medija ili komunikacionog softvera ili aplikacija za komunikaciju sa javnošću, sve dok takva upotreba ne uključuje afirmativnu upotrebu prepoznavanja lica; kao i upotreba softvera za automatsko redigovanje teksta, sve dok takav softver nije u stanju da vrši prepoznavanje lica.

Odredba koja reguliše dozvoljenu upotrebu omogućava vladinim agencijama da koriste dokaze koji su dobijeni FRT pretragom i koji se odnose na istragu određenog krivičnog dela. Formulacija ove odredbe je toliko široka da se postavlja pitanje njenih granica u praksi. Čini se da se može tumačiti tako da obuhvata različite scenarije koji bi praktično zaobišli načelnu zabranu na kojoj se zasniva ceo zakon.

Po zakonu, podaci iz nadzora ljudskog lica, bez drugih dokaza, ne mogu da čine osnovanu sumnju za hapšenje, pretres ili zaplenu.

Konačno, zakon propisuje nekoliko pravila u slučaju povrede. U skladu s tim, podaci iz nadzora ljudskog lica prikupljeni ili izvedeni u suprotnosti sa zakonom moraju se smatrati nezakonito pribavljenim i, osim ako je drugačije propisano zakonom, moraju se izbrisati po otkrivanju; takođe, predstavljaće neprihvatljiv dokaz u svakom postupku pred državnim organima. Građanin koji je oštećen ovakvim kršenjem zakona, može podneti tužbu sudu protiv javnog organa koji je izvršio povredu. Službenik ili funkcioner koji u vršenju službene dužnosti krši zakon, može biti podvrgnut disciplinskom postupku.

Država Juta

Juta je u martu 2021. godine usvojila zakon o FRT-u kojim se reguliše upotreba prepoznavanja lica u svim državnim organima.[580] Cilj je bio regulisanje upotrebe – umesto zabrane – budući da je tehnologija već bila u upotrebi u Juti, pa je čak i naišla na izvesnu podršku građana.[581]

Slično pravilima u Mejnu, služba za sprovođenje zakona ne može sama da vrši pretragu, već treba da podnese zahtev nadležnom državnom organu (u ovom slučaju, vladinom telu koje upravlja bazom slika, ili službi za javnu bezbednost, ako ta služba vodi ili ima pristup takvoj bazi). Zakonom je propisano da obučeni i ovlašćeni službenici mogu da podnose zahteve za pretragu samo ako je ona predviđena za svrhu uređenu zakonom; ako zahtev sadrži identifikacioni broj predmeta; kao i, kada se radi o zahtevu u cilju istrage krivičnog dela, da se u njemu precizira delo i činjenični narativ, kako bi se potvrdilo da postoji realna verovatnoća da je osoba koja je predmet zahteva povezana sa delom koje je predmet istrage.

Prema slovu zakona, služba može da podnese zahtev za poređenje u sistemu za prepoznavanje lica samo u svrhe (1) istraživanja krivičnog dela, nasilnog zločina ili pretnje po ljudski život; ili (2) identifikacije osobe koja je preminula, onesposobljena ili je u opasnosti i na drugi način nije u mogućnosti da službi za sprovođenje zakona potvrdi svoj identitet.

Kada obučeni službenik dobije zahtev od nadležnog odeljenja, pretraga se mora izvršiti u skladu sa procedurom koju zakon detaljno propisuje. U skladu sa tim odredbama, ako sistem za prepoznavanje lica pokazuje moguće podudaranje, zaposleni mora da izvrši nezavisno vizuelno poređenje kako bi utvrdio da li je podudaranje moguće ili verovatno. Ako zaposleni utvrdi da postoji verovatnoća podudaranja, potrebno je da zatraži mišljenje od drugog zaposlenog ili pretpostavljenog. Ako se slažu da je podudaranje verovatno, dostaviće rezultat službi za sprovođenje zakona koja je zahtevala pretragu, i to putem šifrovane komunikacije. Dakle, propisana obaveza je da se na zahtev za pretragu dostavljaju samo oni rezultati za koje se u dva kruga provere potvrdi da predstavljaju verovatno podudaranje. Međutim, ako se dva nivoa provere međusobno ne slažu o verovatnoći podudaranja, službi koja je poslala zahtev odgovoriće se da pretraga nije dala rezultate.

Prilikom podnošenja predmeta tužilaštvu, služba za sprovođenje zakona je dužna da dostavi informaciju da li je tokom istrage korišćen sistem za prepoznavanje lica, pa ako jeste, dostaviće i opis upotrebe.

Bilo koji državni organ, uključujući agencije za sprovođenje zakona, mora unapred da obavesti javnost o svojim praksama upotrebe FRT-a, u skladu sa pravilima propisanim zakonom. Pored toga, državni organ je dužan da na zahtev objavi statističke informacije o izvršenim poređenjima za prepoznavanje lica. Takođe je u obavezi da pripremi godišnje privremene izveštaje za nadležni vladin komitet (isključujući detalje u vezi sa istragom koja je u toku).

Zakon izričito propisuje da državni organ ne sme da koristi sistem za prepoznavanje lica za prekršaje iz oblasti civilnih migracija, što Jutu čini jedinom američkom državom čiji propisi za FRT izričito prepoznaju specifičnu štetu minorizovanim zajednicama.

Komonvelt Masačusets

Zakon ove države reguliše neka pitanja u vezi sa upotrebom prepoznavanja lica u službama za sprovođenje zakona, ali u ograničenom obimu. Pravila su doneta tokom reforme policije 2020. i postala su pravno važeća u julu 2021.[582] Iako je prvobitno planirano usvajanje obuhvatnih pravila po tom pitanju, političke reakcije[583] su uslovile da se važeće odredbe odnose samo na upotrebu prepoznavanja lica za pretragu slika i identifikaciju osobe u databazi.[584]

Prema članu 220 Poglavlja 6 Opštih zakona, službe za sprovođenje zakona moraju da dobiju sudski nalog pre nego što pokrenu pretragu za prepoznavanje lica, osim u dve situacije: kada traže preminulu osobu, ili kada organ opravdano veruje da hitan slučaj povlači značajan rizik od štete po pojedinca ili grupu ljudi. Zakon propisuje da nalog mora da izda sud ili pravosudni organ ovlašćen za izdavanje naloga u krivičnim predmetima, na osnovu konkretnih i artikulisanih činjenica i razumnih zaključaka iz njih, a koji pružaju osnovano uverenje da će tražene informacije biti relevantne i materijalne za tekuću krivičnu istragu ili za ublažavanje značajnog rizika od štete po bilo kojeg pojedinca ili grupe ljudi.

Kada se ovi uslovi ispune, služba ne može sama da izvrši pretragu, već je sprovodi neko iz državne policije, ogranka FBI ili Registra motornih vozila.

Zakonom je propisana transparentnost. Služba mora da dokumentuje svaku obavljenu pretragu za prepoznavanje lica i da tromesečno dostavlja dokumentaciju izvršnoj kancelariji za javnu bezbednost. Takođe su regulisani i minimalni elementi izveštavanja. Izvršna kancelarija je u obavezi

da svake godine na svojoj internet stranici objavi dokumentaciju dobijenu od službi za sprovođenje zakona, sa propisanim sadržajem.

Konačno, zakon ima nekoliko odredbi koje preciziraju pod kojim okolnostima bi upotreba alata za prepoznavanje lica bila dozvoljena. Tako agencija za sprovođenje zakona može da koristi FRT isključivo u svrhu autentifikacije korisnika na njihovim uređajima. Štaviše, agencija može da koristi automatizovani softver za redigovanje videa ili slika ako takav softver nema mogućnost da izvrši prepoznavanje lica, i može da primi dokaze vezane za istragu krivičnog dela izvedene iz sistema za prepoznavanje lica ako nisu bili svesno pribavljeni kršenjem zakona javnog službenika ili funkcionera.

Ovakav pravni okvir kritikovala je Američka unija za građanske slobode (ACLU) koja nastoji da obezbedi zaštitu prava u zakonodavstvu.[585] ACLU tvrdi da važeći zakon ne pruža dovoljno zaštite za građane i njihova prava, posebno iz perspektive rasne pravde, privatnosti, zakonitog procesa i građanskih sloboda.[586] Unija je 2021. godine pokrenula kampanju za izmene zakona u pravcu sveobuhvatnije regulative nadzora ljudskog lica.[587]

Konačno, tokom policijske reforme, osnovana je specijalna komisija[588] sa zadatkom da analizira tehnologiju prepoznavanja lica i daje preporuke za buduća pravila u vezi sa njenom upotrebom.[589] Komisija je u martu 2022. izdala izveštaj sa 13 preporuka. Među njima, preporuka da softver za prepoznavanje lica treba da se koristi samo uz sudski nalog zasnovan na osnovanoj sumnji da je osoba počinila krivično delo, čini se najvećim odstupanjem od važećeg zakona (sa nekim ograničenim i strogo regulisanim izuzecima). Preporuke takođe sadrže zabranu upotrebe prepoznavanja lica za nadzor uživo ili praćenje, kao i za „prepoznavanje emocija". Izveštaj Komisije pokrenuo je širu diskusiju oko upozorenja da bi predložena pravila sprečila policiju da koristi tehnologiju na smislen i koristan način, dok ne otklanjaju rizike po privatnost.[590]

Država Alabama

Zakon koji reguliše prepoznavanje lica u Alabami usvojen je u aprilu 2022. i stupio je na snagu u julu iste godine.[591]

Predloženi tekst zakona u početku je imao tri komponente:[592] (1) da se agencijama za sprovođenje zakona zabrani da koriste podudaranje u prepoznavanju lica kao jedini element osnovane sumnje ili za hapšenje; (2) da im se zabrani upotreba veštačke inteligencije ili usluga prepoznavanja lica[593] za tekući nadzor, osim u određenim okolnostima; i (3) da se zabrani upotreba veštačke inteligencije ili usluga prepoznavanja lica kao sredstva za identifikaciju osobe na osnovu drugih slika (da je usvojena u ovom obliku, čini se da bi bilo teško protumačiti šta tačno znači ova zabrana).[594]

Međutim, posle izmena, usvojeni tekst reguliše samo prvu komponentu. Prema zakonu, državna ili lokalna agencija za sprovođenje zakona ne sme da koristi rezultate podudaranja iz FRT kao jedini element za utvrđivanje osnovane sumnje u krivičnoj istrazi ili za hapšenje, a da se u navedene svrhe rezultati podudaranja mogu koristiti samo u vezi sa drugim zakonito dobijenim informacijama i dokazima.

Nema dostupnih informacija o obrazloženju izmena prvobitnog predloga, niti zašto je usvojena odredba tako ograničenog obima. Nagađa se da je regulaciju podstakla potreba da se reši ključna zabrinutost javnosti u vezi sa mogućnošću pogrešne identifikacije.[595] To bi moglo biti u vezi sa izveštajima medija da je, pre nego što je zakon predložen, policija Alabame koristila usluge prepoznavanje lica da identifikuje osumnjičene za nerede, uz učešće već zloglasne kompanije Clearview AI.[596]

Država Vermont

U oktobru 2020. godine, Vermont je usvojio zakon koji u potpunosti zabranjuje upotrebu tehnologija za prepoznavanje lica u organima za sprovođenje zakona, odnosno uspostavlja moratorijum na njihovu upotrebu do dalje pravne procedure.[597] Prema zakonu, službenici organa za sprovođenje zakona ne smeju da koriste tehnologiju prepoznavanja lica ili informacije dobijene korišćenjem tehnologije prepoznavanja lica – sve dok za to ne dobiju ovlašćenje Generalne skupštine Vermonta.[598]

Međutim, stroga zabrana je revidirana 2021. na inicijativu državnog tužioca, koji je zatražio izuzetak za upotrebu prepoznavanja lica u policijskoj istrazi seksualnog zlostavljanja dece.[599] Izuzetak je omogućen propisom kojim je Generalna skupština ove države odobrila upotrebu FRT-a u službama za sprovođenje zakona tokom krivične istrage seksualnog iskorišćavanja dece. Ova tehnologija se može koristiti samo kada policija poseduje sliku osobe za koju veruju da je žrtva, potencijalna žrtva ili identifikovan osumnjičeni u istrazi, a pretraga je isključivo ograničena na lociranje slika, uključujući video zapise, na elektronskim uređajima koje su organi za sprovođenje zakona zakonito zaplenili u vezi sa konkretnom istragom.[600] I pored toga, zabrana policijske upotrebe tehnologija za prepoznavanje lica, posebno u

svrhe masovnog nadzora, koja je na snazi u Vermontu, daleko je restriktivnija nego u bilo kojoj drugoj američkoj državi.

Prema informacijama dostupnim na sajtu vlade Vermonta, očekuje se uspostavljanje radne grupe za tehnologiju prepoznavanja lica,[601] u skladu sa zakonom, koja će imati mandat da analizira rizike i mogućnosti u pogledu upotrebe FRT-a u agencijama za sprovođenje zakona, kao i da daje preporuke za potencijalna buduća zakonska ovlašćenja, u duhu važećih pravila.

Komonvelt Kentaki

Propis koji uređuje prepoznavanje lica usvojen je u aprilu 2022.[602] Ovaj zakon ne postavlja direktno primenjiva pravila o upotrebi tehnologija za prepoznavanje lica, već reguliše proces izrade standarda i obaveza u službama za sprovođenje zakona na nivou cele države.[603]

Zakonom je predviđeno formiranje radne grupe za tehnologiju prepoznavanja lica, uređeno je njeno članstvo, kao i dužnosti i nadležnost. Primarni zadatak grupe bio je da izradi i učini javno dostupnim model politike za korišćenje prepoznavanja lica u agencijama za sprovođenje zakona, najkasnije do 1. januara 2024.

Sadržaj modela politike je detaljno regulisan i obuhvata, između ostalog: (1) specifikaciju dozvoljenih upotreba FRT-a u skladu sa zakonom (uključujući utvrđivanje osnovane sumnje za hapšenje na osnovu rezultata pretrage, kao i zabranu korišćenja tehnologije za identifikaciju građana koji učestvuju u ustavom zaštićenim aktivnostima u javnim prostorima), kao i obaveze zaposlenih u agencijama za sprovođenje zakona koji su ovlašćeni da koriste FRT; (2) obavezu službe za sprovođenje zakona da dokumentuje slučajeve u kojima se koristi FRT; (3) procedure za potvrdu inicijalnih rezultata prepoznavanja lica, koju daje sekundarni analitičar; (4) politike integriteta i zadržavanja podataka, kao i mere bezbednosti podataka, procedure i procese obuke; (5) minimalni standard tačnosti za podudaranje lica u svim demografskim grupama kako bi se obezbedilo odsustvo diskriminacije; i (6) mehanizam za izradu izveštaja o prethodnoj upotrebi FRT-a koji se može koristiti za reviziju i verifikaciju.

Internom politikom takođe treba da se uspostavi proces koji obavezuje službe da poredi javno dostupne ili zakonito stečene slike sa bazom javno dostupnih ili zakonito stečenih slika. Jedan neobičan zahtev propisan zakonom glasi da politika treba da konkretizuje proces vezan za privatnost osoba kroz isključivanje, redigovanje, zamagljivanje ili na drugi način prikrivanje golotinje ili seksualnog ponašanja osobe koju je moguće identifikovati.

Služba za sprovođenje zakona koja koristi FRT mora imati uspostavljene interne politike pre upotrebe tehnologije i dužna je da dostavi integralni primerak svoje politike ili svaku reviziju politike Kabinetu za pravosuđe i javnu bezbednost u roku od trideset dana od usvajanja ili revizije.

Zakon nije bio tema značajne javne diskusije, sudeći po dostupnim informacijama, možda zato što će se pravila tek definisati kada se objavi model politika. U vreme pisanja ovog teksta, to još uvek nije bio slučaj.

Država Merilend

Zakonska pravila koja regulišu upotrebu tehnologije za prepoznavanje lice u državi Merilend stupila su na snagu 1. oktobra 2024. godine,[604] iako je policija već koristila tehnologiju bar deset godina.[605] Zakon pripada kategoriji zakona koji regulišu upotrebu tehnologije u službama za sprovođenje zakona, i nalazi se u delu krivičnog zakona koji reguliše krivični postupak.

Pravilima je predviđena obaveza policije da izradi detaljan model politike za upotrebu tehnologije na koju bi se oslanjale sve policijske službe, a koji bi bio u skladu sa minimalnim pravilima iz samog zakona i koji je već javno dostupan.[606]

Zakon i sam detaljno reguliše kako se tehnologija za prepoznavanje lica koristi u okviru krivičnog postupka. Tako se navodi da rezultati dobijeni ovom tehnologijom mogu da se koriste kao dokaz u vezi sa krivičnim postupkom samo u svrhu utvrđivanja verovatnog uzroka ili pozitivne identifikacije (1) u vezi sa izdavanjem sudskog naloga ili (2) na pripremnom ročištu. Takvi rezultati ne mogu se koristiti kao jedini osnov za utvrđivanje osnovane sumnje, već je to moguće samo ako su rezultati potkrepljeni dodatnim, nezavisno dobijenim dokazima.

Dalje, prema odredbama zakona, tehnologiju za prepoznavanje lica je moguće koristiti u istragama samo za određena krivična dela koja zakon taksativno nabraja, te za identifikaciju preminulih i nestalih lica (uz par dodatnih specifičnih izuzetaka). Dozvoljena upotreba tokom krivične istrage i u ostalim navedenim slučajevima regulisana je kao izuzetak od opšte zabrane da se tehnologija upotrebljava van granica zakona.

Dodatno, zakon eksplicitno navodi da je zabranjena upotreba tehnologije u sledećim slučajevima: (1) da bi se identifikovala lica koja upražnjavaju svoja prava garanovana Ustavom i zakonima, (2) da bi se analizirale skice ili crteži, (3) da bi se svedok upoznao sa licem osumnjičenog pre nego što svedok ima priliku da osumnjičenog identifikuje uživo ili iz skupa fotografija; (4) radi sprovođenja identifikacije uživo i u realnom vremenu. Takođe je regulisano da se tehnologija ne sme koristiti za identifikaciju pojedinca isključivo na osnovu (1) ličnog interesa policijskih službenika ili ciljeva službe za sprovođenje zakona; (2) političkih uverenja pojedinca; (3) učešća pojedinca u zakonitim aktivnostima; ili (4) rase, verskih uverenja, seksualne orijentacije, roda, invaliditeta, nacionalnog porekla ili statusa beskućnika.

Zakon takođe reguliše sa kojim bazama fotografija se može vršiti poređenje radi identifikacije (registar vozačkih dozvola i ličnih karata, postojeće policijske evidencije i drugi regulisani izuzeci). Takođe propisuje da je rezultat poređenja neophodno da potvrdi obučeni službenik.

Što se tiče pravila iz domena transparentnosti, postoji obaveza u skladu sa pravilima o pristupu informacijama od javnog značaja da se obelodani da li je tehnologija prepoznavanja lica korišćena u istrazi, uz naziv svakog korišćenog sistema za prepoznavanje lica, opis i naziv baza podataka koje su pretraživane, te rezultata svakog od sistema i svake baze koji su dalje korišćeni u istragama.

Zakon sadrži i odredbe o (1) reviziji ugovora koji su zaključeni radi upotrebe FRT tehnologije sa ciljem utvrđivanja da li su oni implementirani u skladu sa zakonom, (2) obaveznim treninzima službenika koji koriste FRT tehnologiju, (3) obaveznom usvajanju internih politika koje regulišu upravljanje podacima (eng. data management policy), (4) pripremi i objavljivanju godišnjih detaljnih izveštaja o upotrebi tehnologije u praksi.

Najzad, zakon reguliše pravo pojedinaca da pokrenu sudski spor u slučaju povrede njihovih prava kršenjem pravila iz zakona.

PRAVNA PRAKSA

Budući da se zakoni koji uređuju razvoj, implementaciju ili upotrebu prepoznavanja lica u agencijama za sprovođenje zakona u SAD javljaju tek u novije vreme, još uvek nema sudskih odluka u vezi sa njihovom primenom koje bi pomogle u tumačenju zakonskih odredbi, pa čak i njihove ustavnosti.

Međutim, bilo je nekoliko slučajeva pogrešne identifikacije kroz prepoznavanje lica koji su završili na sudu. Čovek po imenu Robert Williams tužio je 2021. policijsku upravu grada Detroita zbog nezakonitog hapšenja i zatvaranja na osnovu pogrešnog podudaranja u njihovom sistemu za prepoznavanje lica. Presuda u ovom slučaju još nije doneta.[607] To nije jedini put da je hapšenje izvršeno u ovakvim okolnostima,[608] ali još uvek čekamo da vidimo kakva će sudska praksa proizaći iz ovakvih situacija, na državnom i saveznom nivou.[609]

Kada je reč o upotrebi prepoznavanja lica u saveznim agencijama, jedan značajan slučaj koji je pokrenuo ACLU 2019. još uvek nije rešen. Organizacija je, naime, tužila saveznu vladu da bi dobila informacije o praksama nadzora ljudskih lica, uključujući upotrebu tehnologije prepoznavanja lica u radu FBI-a i Uprave za suzbijanje narkotika (Drug Enforcement Administration, DEA). U januaru 2019, ACLU je prvi put podneo zahtev za dostavljanje javne evidencije, i mada su i FBI i DEA potvrdili prijem zahteva, nijedna služba nije dostavila tražene informacije. U tužbi se tvrdi da bi „dokumenti informisali javnost o tome kako vlada trenutno koristi tehnologiju za nadzor ljudskog lica i kakvi zaštitni mehanizmi postoje, ako postoje, za zaštitu osnovnih ustavnih prava“.[610]

Sudska praksa u pogledu komercijalne upotrebe mnogo je razvijenija od kada su se zakoni koji regulišu takvu upotrebu (npr. BIPA u Ilinoisu i teksaški CUBI) prvi put pojavili pre više od jedne decenije.

U skladu sa pravilima koje propisuje BIPA, kompanija Clearview AI je pristala na novi set ograničenja u sudskom poravnanju pred državnim sudom Ilinoisa u martu 2022. Prema nagodbi, Clearview AI ne sme da omogući pristup svojoj bazi za prepoznavanje lica bilo kom vladinom organu na državnom ili lokalnom nivou u Ilinoisu, uključujući službe za sprovođenje zakona, u periodu od pet godina (što znači da kompanija za to vreme ne može da koristi izuzetak koji BIPA predviđa za privatne izvođače po ugovorima sa javnim vlastima). Ograničenja su još stroža kada su u pitanju privatni subjekti i postavljaju zabranu kompaniji Clearview AI da odobrava plaćeni ili besplatan pristup svojoj bazi svim privatnim subjektima širom SAD (ne samo u Ilinoisu), podložno uskim izuzecima sadržanim u BIPA.[611]

Komercijalni slučajevi za različita kršenja privatnosti putem upotrebe FRT-a uglavnom se na kraju rešavaju nagodbom.[612] Među njima se izdvaja nagodba od 50 miliona dolara sa kompanijom Meta (Fejsbuk) 2021. godine,

opet prema BIPA pravilima.[613] Sličan slučaj u Teksasu, zbog kršenja odredbi CUBI, pokrenula je teksaška vlada protiv Mete početkom 2022. Proces je još uvek u toku.[614]

TikTok je 2021. bio strana u nagodbi zbog kršenja BIPA od 92 miliona dolara, a u vezi sa praksama popularne platforme u kojima se koristi prepoznavanje lica.[615] Snap, matična kompanija aplikacije Snapchat, pristala je na nagodbu od 35 miliona dolara 2022. zbog upotrebe prepoznavanja lica u okviru funkcija aplikacije Sočiva i Filteri,[616] dok je otprilike u isto vreme Google pristao na nagodbu od čitavih 100 miliona dolara u slučaju pokrenutom na osnovu navoda da Google Photos prikuplja podatke o geometriji lica za utvrđivanje sličnosti i varijacija među ljudima, te da nudi funkciju grupisanja slika sličnih lica, kršeći odredbe BIPA.[617]

UJEDINJENI ARAPSKI EMIRATI

KONTEKST

Upotreba tehnologije za prepoznavanje lica široko je rasprostranjena u Ujedinjenim Arapskim Emiratima (UAE). Koristi se i u javnom i u privatnom sektoru u različite svrhe, a takav trend ima značajnu podršku vlade.

Iz tehničkog ugla, zagovornici i dobavljači biometrijskih tehnologija su primetili da su UAE sa svojim raznolikim stanovništvom i više od 200 različitih nacionalnosti u Abu Dabiju i Dubaiju, idealni za testiranje novih tehnologija za prepoznavanje lica.[618] Podstaknuti tom činjenicom, ali i drugim razlozima, svoje usluge i proizvode na tržištu UAE nude mnoge tehnološke kompanije, posebno kineske.[619]

Jedan od strateških ciljeva vlade UAE jeste da postane globalni lider u tehnologijama veštačke inteligencije.[620] Sastavni deo ove strategije jeste i izgradnja pametnih gradova, uključujući upotrebu tehnologija za prepoznavanje lica na načine koji liče na biometrijski masovni nadzor. Jedan od slučajeva upotrebe pomenutih u strategiji jeste „primena prepoznavanja lica za potrebe praćenja umora vozača".[621]

Vladine službe su 2018. razvile i primenile aplikaciju „UAE Pass".[622] Na zvaničnom sajtu navodi se da je to „prvo nacionalno rešenje za digitalni identitet i potpis" koje korisnicima omogućava da se uz pomoć svog pametnog telefona identifikuju pred državnim i privatnim pružaocima usluga, odnosno da pristupe onlajn uslugama. Aplikacija ima dodatne karakteristike koje je razlikuju od, na primer, Aadhaara u Indiji i ABIS-a u Južnoj Africi, pa su građanima dostupni alati za digitalno potpisivanje i overu dokumenata i transakcija, dostavljanje zahteva za zvanične dokumente

u digitalnom obliku, kao i da koriste usluge partnera platforme UAE Pass.[623] Aplikacija koristi prepoznavanje lica za registraciju i autentifikaciju korisnika, kreiranjem „identifikacionog dokumenta ljudskog lica".[624] Prema rečima javnih zvaničnika, korišćenje tehnologije prepoznavanja lica u procesu registracije predstavlja „ključni korak ka implementaciji novih tehnologija zasnovanih na veštačkoj inteligenciji, kako bi se uspostavo digitalni stil života u UAE".[625] U međuvremenu, UAE Pass je povezana i sa nacionalnom ličnom kartom, Emirates ID.[626]

Tehnologije za prepoznavanje lica široko su rasprostranjene i u službama za sprovođenje zakona, uključujući nadzor uživo 24/7. Bilo je navoda i da policija Dubaija planira da u svoj proces donošenja odluka uvede prediktivne policijske alate koji bi se zasnivali na biometrijskim podacima.[627]

Kako se navodi na portalu vlade UAE, Ministarstvo unutrašnjih poslova implementiralo je sistem za prepoznavanje lica kako bi „zaštitilo" državne granice, kritičnu infrastrukturu i vrednu imovinu. Sistem koristi „osetljive kamere" (nema objašnjenja šta su osetljive kamere) za snimanje lica ljudi. Kamere mogu da skeniraju i slikaju ljude koji se nalaze i blizu i daleko od njih i mogu da detektuju da li se kreću ili miruju.[628]

Policija Dubaija pokrenula je 2018. godine program veštačke inteligencije za nadzor, „Oyoon". Prema informacijama koje su tada objavljene na Facebook stranici policije, cilj projekta je „stvaranje integrisanog bezbednosnog sistema koji u saradnji sa strateškim partnerima koristi savremene sofisticirane tehnologije i funkcije veštačke inteligencije za sprečavanje kriminala, smanjenje broja smrtnih ishoda u saobraćajnim nezgodama, sprečavanje negativnih incidenata u stambenim, poslovnim i sredinama od vitalnog značaja, kao i za spremnost da se na incidente reaguje i pre nego su prijavljeni komandnoj jedinici".[629]

Policija je već 2019. tvrdila da je program pomogao u hapšenju 319 osumnjičenih u prvoj godini njegovog korišćenja. Prema tim izveštajima, oko 5.000 bezbednosnih kamera širom Dubaija u okviru mreže Oyoon prenosilo je žive slike kršenja bezbednosti u Centralni komandni centar, dok su u fokusu nadzora bila tri sektora – turizam, saobraćaj i objekti od čvrstih materijala. Na drugom kraju sistema, policija digitalno prati osumnjičene samo učitavanjem njihovih slika u bazu podataka.[630] Prema izveštajima iz 2022, preko 300.000 kamera je bilo povezano sa Oyoon mrežom.[631]

Takođe, 2020. je najavljeno da će novi sistem za prepoznavanje lica biti uveden na metro stanicama u Dubaiju. Dodatne karakteristike sistema uključuju „pametne kacige" i „pametne naočare". Naime, prema rečima zvaničnika, pametne naočare pod nazivom Rokid T1 i pametni šlemovi, oprema korišćena tokom pandemije kovida-19 za skeniranje temperature putnika, imaće „napredniju" tehnologiju poput prepoznavanja lica, za koju policija navodi da će je koristiti za identifikaciju traženih lica.[632]

Kada je reč o praksi u Abu Dabiju, tamošnja policija je u martu 2020. opremila svoja patrolna vozila sistemom za prepoznavanje lica uživo. Server centralnog operativnog odeljenja policije povezan je sa pametnim uređajem u automobilu, a softver može momentalno da izvede poređenje slike sa policijskom kontrolnom listom. Kada dođe do uparivanja, policija dobija znak da preduzme akciju.[633]

Ekstenzivna upotreba prepoznavanja lica u UAE može se posmatrati kao posebno problematična iz perspektive ljudskih prava. Prema pojedinim izvorima, Emirati imaju jednu od najviših stopa političkih zatvorenika po glavi stanovnika u svetu.[634] Uz ostale programe veštačke inteligencije i masovnog nadzora, sistem za prepoznavanje lica omogućava vladi dodatni alat za represiju, opravdan razlozima bezbednosti, delotvornosti i pogodnosti.[635]

PRAVNI OKVIR

Ustav UAE reguliše opšte pravo na privatnost. Privatnost doma jemči se članom 36, dok je članom 31 zagarantovana sloboda komunikacije poštom, telegrafom ili drugim sredstvima komunikacije, kao i njena tajnost, u skladu sa zakonom.[636]

Emirati su 20. septembra 2021. godine usvojili svoj prvi savezni zakon koji reguliše zaštitu ličnih podataka, Zakon o zaštiti podataka o ličnosti.[637] Stupio je na snagu 2. januara 2022, a počeće da se primenjuje šest meseci po donošenju povezanih izvršnih propisa.[638] Ovi izvršni propisi bi trebalo da urede niz praktičnih i operativnih detalja iz Zakona, ali još uvek nisu doneti (uprkos činjenici da je to trebalo da se desi u roku od šest meseci od donošenja Zakona, koji je istekao u martu 2022.). Kancelarija za podatke UAE, koja će biti osnovana posebnim zakonom, delovaće kao savezni regulator za podatke u UAE.[639]

Nema javno dostupnih objašnjenja za kašnjenje u donošenju izvršnih propisa i uspostavljanju Kancelarije za podatke UAE.

U Ujedinjenim Arapskim Emiratima postoji nekoliko „slobodnih zona“, odnosno posebnih ekonomskih zona. Tri od njih – Globalno tržište Abu Dabija (Abu Dhabi Global Market, ADGM), Grad zdravstvene zaštite Dubai (Dubai Healthcare City, DHCC) i Međunarodni finansijski centar Dubaija (Dubai International Financial Centre, DIFC) – usvojili su sopstvene propise o privatnosti podataka, koji se primenjuju na kompanije koje posluju u okviru njihove nadležnosti.[640]

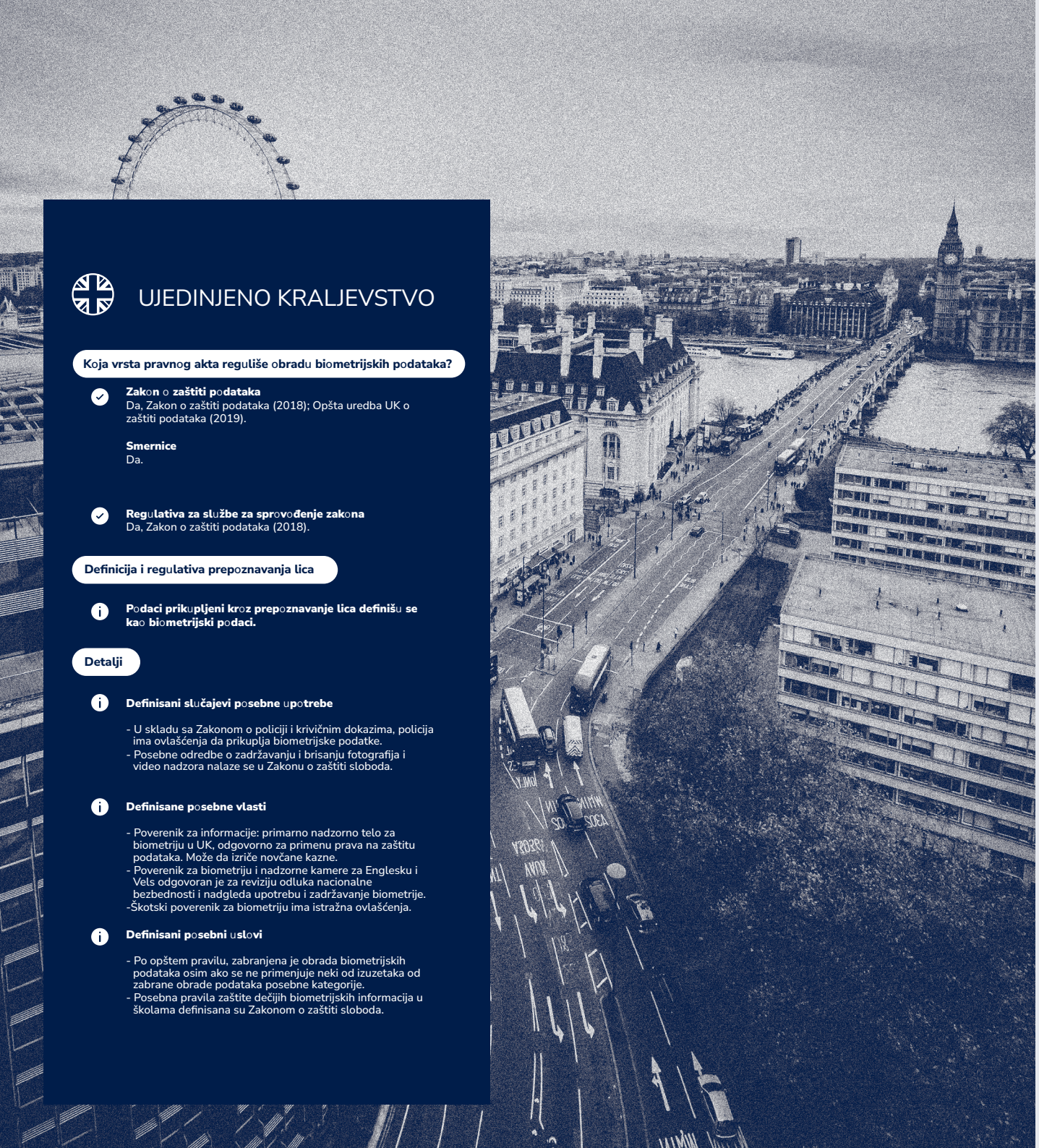
U pogledu regulative prepoznavanja lica, Zakon o zaštiti podataka o ličnosti sadrži definiciju biometrijskih podataka u kojoj se izričito pominju slike ljudskih lica. Obrada biometrijskih podataka nije detaljno regulisana, ali spada u širu definiciju osetljivih podataka (tako da je to, u suštini, regulatorni pristup u GDPR stilu, kao u Keniji).

Postoje dve osnovne grupe obaveza u vezi sa obradom svih osetljivih podataka: (1) službenik za zaštitu podataka mora biti imenovan kada obrada uključuje sistematsku i sveobuhvatnu procenu osetljivih ličnih podataka, uključujući profilisanje i automatizovanu obradu, ili obradu velike količine takvih podataka;[641] i (2) procena uticaja na zaštitu podataka mora biti pripremljena pre obrade za koju se koristi bilo koja od savremenih tehnologija koja bi predstavljala visok rizik po privatnost i poverljivost ličnih podataka, ako se obrađuje velika količina osetljivih podataka.[642] Nijedna javno dostupna informacija ne ukazuje na to da je ikad vršena procena uticaja radi upotrebe biometrije prilikom obrade u bilo koje svrhe sprovođenja zakona, niti da je imenovan službenik za zaštitu podataka.

Te zakonske obaveze su, dakle, prilično slične onima koje postavlja GDPR. Međutim, nisu propisani posebni uslovi ni posebna pravna osnova za dozvoljenu obradu osetljivih podataka, kako to zahteva GDPR članu 9 po posebnom režimu koji se primenjuje na takve podatke. Takođe, Zakon u Emiratima nema pravila tipa direktive EU za službe za sprovođenje zakona (LED) koja bi regulisala detalje obrade biometrijskih, ili bilo kojih drugih osetljivih podataka u svrhe sprovođenja zakona. Dakle, za sada se čini da se upotreba prepoznavanja lica u službama za sprovođenje zakona odvija u svojevrsnom pravnom vakuumu sa stanovišta regulative zaštite podataka, kao u Indiji i Australiji. Ostaje da se vidi da li će izvršni propisi promeniti ovu situaciju.

PRAVNA PRAKSA

Još uvek ne postoji značajna sudska praksa u vezi sa upotrebom prepoznavanja lica ili drugih biometrijskih sistema u UAE, bilo u javnom ili privatnom sektoru.



UJEDINJENO KRALJEVSTVO

Koja vrsta pravnog akta reguliše obradu biometrijskih podataka?

Zakon o zaštiti podataka
Da, Zakon o zaštiti podataka (2018); Opšta uredba UK o zaštiti podataka (2019).

Smernice
Da.

Regulativa za službe za sprovođenje zakona
Da, Zakon o zaštiti podataka (2018).

Definicija i regulativa prepoznavanja lica

Podaci prikupljeni kroz prepoznavanje lica definišu se kao biometrijski podaci.

Detalji

Definisani slučajevi posebne upotrebe

- U skladu sa Zakonom o policiji i krivičnim dokazima, policija ima ovlašćenja da prikuplja biometrijske podatke.
- Posebne odredbe o zadržavanju i brisanju fotografija i video nadzora nalaze se u Zakonu o zaštiti sloboda.

Definisane posebne vlasti

- Poverenik za informacije: primarno nadzorno telo za biometriju u UK, odgovorno za primenu prava na zaštitu podataka. Može da izriče novčane kazne.
- Poverenik za biometriju i nadzorne kamere za Englesku i Vels odgovoran je za reviziju odluka nacionalne bezbednosti i nadgleda upotrebu i zadržavanje biometrije.
- Škotski poverenik za biometriju ima istražna ovlašćenja.

Definisani posebni uslovi

- Po opštem pravilu, zabranjena je obrada biometrijskih podataka osim ako se ne primenjuje neki od izuzetaka od zabrane obrade podataka posebne kategorije.
- Posebna pravila zaštite dečijih biometrijskih informacija u školama definisana su Zakonom o zaštiti sloboda.

UJEDINJENO KRALJEVSTVO

KONTEKST

Jedan uzorak DNK uzet 1998. od čoveka optuženog za provalu u Londonu, nezakonito je zadržan i kasnije korišćen za njegovu identifikaciju u mnogo težem slučaju – u kojem je osuđen za silovanje i napad.[643] To je bio neposredan povod da se 2001. promeni zakon kako bi se omogućilo prikupljanje i zadržavanje biometrijskih podataka skoro na neodređeno vreme.[644] Tako je Ujedinjeno Kraljevstvo izgradilo najveću svetsku bazu DNK podataka, uključujući podatke ljudi koji nikad nisu bili optuženi ni osuđeni za zločine, pa čak i podatke dece.

Tek nakon odluke u značajnom predmetu pred Evropskim sudom za ljudska prava S. i Marper protiv Ujedinjenog Kraljevstva (2008), Zakonom o zaštiti sloboda iz 2012. ograničeni su obim i zadržavanje biometrijskih podataka. Novim zakonom uspostavljene su uloge javnih tela – poverenika za biometriju, čiji je osnovni zadatak revizija zadržavanja i korišćenja DNK uzoraka, i poverenika za nadzorne kamere u Engleskoj i Velsu, koji nadgleda poštovanje Kodeksa prakse nadzornih kamera. Predlog zakona o zaštiti podataka i digitalnim informacijama koji treba da revidira režim zaštite podataka u zemlji nakon Bregzita, predviđa ukidanje ovih supervizora. Stručnjaci su izrazili zabrinutost zbog takvog razvoja koji vodi u slabljenje kontrole, narušavanje poverenja javnosti i zanemarivanje širih posledica nadzora. Kritičari konstatuju da bi ukidanje ovih funkcija dodatno opteretilo ionako preopterećen i nedovoljno opremljen sistem javne kontrole nadzora.[645]

Jedan od najkontroverznijih slučajeva upotrebe biometrijske tehnologije u Velikoj Britaniji svakako je prepoznavanje lica uživo (live facial recognition, LFR) u radu policije, što je posebno privuklo pažnju javnosti nakon što je londonska policija primenila tehnologiju na karnevalu u Noting Hilu 2017,[646] a policija Južnog Velsa testirala u periodu 2017-2018. U odlukama iz 2019. i 2020, Apelacioni sud je utvrdio da je pravni okvir za primenu LFR-a nedovoljan da obezbedi poštovanje ljudskih prava.

Nakon tragedije u kojoj je sedamnaestogodišnjak ubio troje dece u Sautportu u avgustu 2024. godine, premijer je najavio još intenzivniju upotrebu tehnologije za prepoznavanje lica zajedno sa drugim alatima koji bi trebalo da pomognu za svrhe prediktivnog policijskog rada.[647] Kao alat za predviđanje zločina, prema navodima medija, britanska policija takođe ima praksu pravljenja spiskova osoba za koje postoji rizik da će izvršiti krivično delo a koje mogu biti predmet potrage na osnovu svojih biometrijskih podataka[648] dok, prema istraživanju organizacije Liberty, 14 lokalnih policijkih uprava već koristi ili je najavilo korišćenje algoritama za prediktivne svrhe radi sprečavanja zločina pre nego što se dogode.[649]

Primeri upotrebe tehnologije za prepoznavanje lica do oktobra 2023. godine u radu policije Ujedinjenog Kraljevstva objavljen je na blogu Home Office. Na istom mestu se, između ostalog, navodi da policija ima prava da koristi ovu tehnologiju na osnovu svojih opštih policijskih nadležnosti i da je u tome ograničena poštovanjem propisa koji regulišu zaštitu podataka o ličnosti, jednakosti i ljudskih prava.[650]

S druge strane, britanski regulator za zaštitu podataka izrazio je zabrinutost zbog tehničke pristrasnosti i problematične efikasnosti i statističke tačnosti LFR sistema, kao i nepoštovanja odredbi o zaštiti podataka.[651] U avgustu 2021, preko 30 organizacija za ljudska prava objavilo je otvoreno pismo pozivajući Vladu UK da u potpunosti zabrani upotrebu LFR-a u javnom prostoru.[652]

Upotreba LFR-a do sada je u velikoj meri izmicala zakonodavnoj kontroli u britanskom parlamentu, dok su policijske snage donosile samostalne odluke o primeni i zaštitnim merama. Uprkos novim smernicama i preporukama za kriterijume proporcionalnosti i neophodnosti, procene uticaja na privatnost i određene zaštite prava na privatnost pojedinaca, implementirane posle 2018, ove preporuke su se pokazale kao nedelotvorne, a problemi zbog policijske upotrebe LFR nisu otklonjeni.[653]

Nezavisna analiza britanske legislative, koju je naručio Institut Ada Lovelace, a kojom je rukovodio Matthew Ryder QC, iznela je upozorenje da je trenutni pravni režim Ujedinjenog Kraljevstva „fragmentiran i zbunjujući“ i da ne ide u korak sa razvojem biometrije.[654] U analizi se zaključuje da su zemlji hitno potrebni novi zakoni koji bi regulisali upotrebu biometrijskih tehnologija, a vlada se poziva da pokrene legislativnu inicijativu. Takođe se preporučuje suspenzija LFR-a na javnim mestima do uvođenja relevantnih propisa. Više nevladinih organizacija je u avgustu 2024. uputilo otvoreno pismo premijeru u kom se skreće pažnja na rizike koji proizlaze iz postojećeg pravnog vakuma i grešaka prilikom upotrebe tehnologije koje dovode do diskriminacije, hapšenja nevinih građana i ozbiljnih pretnji po demokratiju.[655]

PRAVNI OKVIR

Upravljanje biometrijskim podacima u Ujedinjenom Kraljevstvu trenutno je regulisano nizom zakona koji se međusobno preklapaju, a bave se zaštitom podataka, ljudskim pravima, diskriminacijom i pitanjima krivičnog pravosuđa. Ne postoji jedinstven sveobuhvatni pravni okvir za upravljanje biometrijskim podacima, a izvori prava koji su se razvili kao odgovor na opštije probleme, regulišu biometrijske podatke ad hoc.

Zakon o ljudskim pravima (1998)

Mnoga prava zaštićena Evropskom konvencijom o ljudskim pravima u domaće zakonodavstvo Ujedinjenog Kraljevstva implementirana su propisom iz 1998. (Human Rights Act, HRA).[656] To je relevantan pravni instrument za regulisanje biometrijskih podataka u UK, budući da u članu 8 štiti pravo na privatnost. Prema Odeljku 6 HRA, organi javne vlasti su u obavezi da poštuju pravo pojedinca na privatnost. Međutim, Zakon ne obavezuje privatne kompanije da poštuju ljudska prava, što otvara pravnu prazninu u regulisanju upotrebe biometrijskih podataka u privatnom sektoru.

UK GDPR i DPA (2018)

Opšta uredba Ujedinjenog Kraljevstva o zaštiti podataka (UK GDPR)[657] i Zakon o zaštiti podataka iz 2018. (Data Protection Act, DPA)[658] pružaju pravni okvir za zaštitu ličnih podataka, uključujući biometrijske podatke. Pored opštih odredbi, DPA implementira evropsku Direktivu za zaštitu podataka u službama za sprovođenje zakona (LED) u zakon UK, a

primenjuje se na sve slučajeve obrade podataka koji uključuju aktivnosti na sprovođenju zakona. U oba ova zakona, definicija biometrijskih podataka je ista kao u GDPR-u i kaže da su to „podaci o ličnosti dobijeni posebnom tehničkom obradom u vezi s fizičkim osobinama, fiziološkim osobinama ili karakteristikama ponašanja pojedinca koja omogućavaju ili potvrđuju jedinstvenu identifikaciju tog pojedinca, kao što su fotografije lica ili daktiloskopski podaci".

Međutim, primetno je da biometrijski podaci imaju drugačiju definiciju za potrebe policije i krivičnog pravosuđa u Škotskoj, zemlji u Ujedinjenom Kraljevstvu koja je preuzela ovlašćenja od Engleske i Velsa.[659] Ova šira definicija obuhvata izvorni materijal (pre njegove specifične tehničke obrade), sa ciljem zaštite materijala kao što su otisci prstiju ili slike lica, a ne samo iz njih izvedene biometrijske šablone. To bi se moglo ceniti kao pozitivna primena presude ESPLJ u slučaju Gaughran protiv Ujedinjenog Kraljevstva, jer prepoznaje osetljivost izvornih fotografija iz kojih su izvedeni biometrijski podaci. To je takođe značajno u pogledu kapaciteta tehnologija nadzora, koji eksponencijalno rastu i omogućavaju lakšu i bržu identifikaciju i praćenje osobe čak i na osnovu podataka slabijeg kvaliteta.

UK GDPR zabranjuje obradu podataka posebne kategorije, uključujući biometrijske podatke, osim u određenim ograničenim okolnostima. DPA dopunjava i prilagođava uslove za rukovanje podacima posebne kategorije postavljene u GDPR UK, dozvoljavajući obradu u svrhe zapošljavanja, socijalnog osiguranja, zdravstvene zaštite, javnog zdravlja, arhiviranja, istraživanja i statistike, u vezi sa krivičnim presudama ili krivičnim delima, ili kada postoji značajan javni interes, sve dok su ispunjeni uslovi popisani u prvom aneksu Zakona. Uočljivo je da DPA zauzima permisivan pristup, nudeći čak 23 potencijalna uslova za „značajan javni interes" koji omogućavaju obradu podataka posebne kategorije. Za razliku od Zakona o ljudskim pravima iz 1998, koji se odnosi samo na javne organe, Odeljak 2 DPA primenjuje se na organizacije iz javnog i privatnog sektora i na pojedince kada obrađuju podatke u ove svrhe.

Odeljak 3 DPA predviđa obradu ličnih podataka kod nadležnih organa u svrhe sprovođenja krivičnog zakona, uključujući obradu biometrijskih podataka radi jedinstvene identifikacije pojedinca. Ova vrsta obrade biometrijskih podataka je zakonita samo ako je dobijena saglasnost od subjekta podataka ili ako je „strogo neophodna" i ispunjava bar jedan od uslova iz aneksa 8 DPA.

Odeljak 4 DPA tiče se obrade podataka od strane obaveštajnih službi Ujedinjenog Kraljevstva, definisanih kao MI5, MI6 i GCHQ. Upotreba biometrijskih podataka za identifikaciju pojedinaca kategorisana je kao osetljiva obrada i može se obaviti samo ako su ispunjeni određeni uslovi iz aneksa 9 i 10.

Kancelarija poverenika za informacije (Information Commissioner's Office, ICO) je primarni supervizorski organ za biometriju u UK, odgovoran za primenu zaštite podataka i prava na slobodan pristup informacijama od javnog značaja. ICO je do sada objavila dva mišljenja o tehnologiji za prepoznavanje lica, fokusirajući se na upotrebu u radu organa za sprovođenje zakona,[660] kao i na upotrebu biometrijske tehnologije za identifikaciju i kategorizaciju na javnim mestima.[661]

PACE i antiteroristički zakoni

Policija i drugi organi za sprovođenje zakona u Ujedinjenom Kraljevstvu imaju posebna ovlašćenja da prikupljaju i čuvaju biometrijske podatke za svrhe krivičnog procesa i borbe protiv terorizma. Ova ovlašćenja su propisana različitim zakonima, uključujući Zakon o policiji i krivičnim dokazima iz 1984. (Police and Criminal Evidence Act, PACE),[662] Zakon o terorizmu iz 2000. godine,[663] Zakon o borbi protiv terorizma iz 2008. godine, Zakon o merama za sprečavanje i istragu terorizma iz 2011. i Zakon o protivterorizmu i bezbednosti granica iz 2019.

Prema PACE, policija ima ovlašćenje da uzima otiske prstiju, „intimne i neintimne" (DNK) uzorke i fotografije osumnjičenih koji su podvrgnuti krivičnoj istrazi. Odeljak 63D propisuje da se otisci prstiju i DNK profili dobijeni iz DNK uzoraka unište ako se čini da su uzeti protivzakonito, ili na osnovu nezakonitog hapšenja ili hapšenja zasnovanog na pogrešnoj identifikaciji.

Zakon o terorizmu iz 2000. daje policiji ovlašćenje da zaustavlja, ispituje i zadržava pojedince u lukama ili pograničnim oblastima kako bi utvrdila da li su umešani u teroristička dela, kao i da prikuplja biometrijske podatke u određenim okolnostima. U aneksu 8 navedene su okolnosti pod kojima se mogu uzeti otisci prstiju i neintimni DNK uzorci, uključujući i bez saglasnosti po odobrenju starešine. Aneks 8 utvrđuje opšti period zadržavanja od najviše 6 meseci, osim ako odluka o nacionalnoj bezbednosti ne dozvoli njihovo zadržavanje na duži period. Slične odredbe za čuvanje

biometrijskih podataka pojavljuju se i u drugim zakonima koji se odnose na mere protiv terorizma.

PoFA

Zakon o zaštiti sloboda iz 2012. (Protection of Freedoms Act, PoFA)[664] usvojen je delimično kao reakcija na odluku Evropskog suda za ljudska prava u slučaju S. i Marper, kojom je utvrđeno da prikupljanje i zadržavanje biometrijskih podataka u Velikoj Britaniji krši član 8 EKLJP. PoFA reguliše obradu biometrijskih podataka od strane javnih i privatnih aktera i uključuje odredbe za zadržavanje i brisanje DNK, otisaka prstiju, fotografija i snimaka sa video nadzora. PoFA je takođe unela odredbe o zadržavanju i brisanju biometrijskih podataka u Zakon o policiji i krivičnim dokazima iz 1984. i ustanovila funkcije Poverenika za biometriju i Poverenika za nadzorne kamere, odgovorne za donošenje odluka o nacionalnoj bezbednosti i kontrolu nad upotrebom i zadržavanjem biometrije.

Dodatno, Poglavlje 2 prvog dela PoFA predviđa posebnu zaštitu biometrijskih podataka dece u školama, zahtevajući saglasnost roditelja i obezbeđujući alternativna sredstva za decu koja se protive obradi njihovih biometrijskih podataka. Ako se dete protivi obradi biometrijskih podataka, čak i ako roditelj pristane, škola mora da obezbedi razuman alternativni način za učešće deteta u školskim aktivnostima.

Uloga Poverenika za biometriju, uspostavljena u okviru PoFA, nezavisna je od vlade i ima ograničen obim u razmatranju upotrebe biometrijskih podataka. Četiri posebne funkcije Poverenika uključuju:

- analizu zadržavanja i upotrebe DNK uzoraka;
- određivanje aplikacija za zadržavanje DNK profila i otisaka prstiju;
- preispitivanje odluka o nacionalnoj bezbednosti; i
- podnošenje izveštaja ministru unutrašnjih poslova Ujedinjenog Kraljevstva.

Iako je delokrug ograničen, Poverenik može da se bavi temama izvan svog neposrednog delokruga zahvaljujući ovlašćenju da izveštava o bilo kom pitanju koje se odnosi na njegove funkcije.

Poverenik za nadzorne kamere ima tri osnovne funkcije:

- podsticanje poštovanja kodeksa prakse nadzornih kamera;
- preispitivanje funkcionisanja kodeksa; i
- davanje saveta vladi u vezi sa izmenama ili kršenjem kodeksa.

Definicija „sistema nadzornih kamera“ koju koristi Poverenik za nadzorne kamere pokriva CCTV i svaki sistem asociran ili povezan s njim, uključujući video biometriju. Mada Poverenik nema funkcije sprovođenja ili ovlašćenja inspekcije, on daje savete o efikasnom i odgovarajućem korišćenju sistema nadzornih kamera, uključujući biometrijske tehnologije, koje mora biti opravdano, proporcionalno i za navedenu svrhu. Ažurirani kodeks prakse pruža smernice o korišćenju tehnologije za prepoznavanje lica uživo od strane policijskih starešina, uključujući uspostavljanje procesa autorizacije i kriterijuma za primenu.

Uloge dva poverenika, za biometriju i za nadzorne kamere, za Englesku i Vels spojene su u martu 2021. godine u jednu funkciju, što su raniji poverenici kritikovali.[665] Nema zakona koji bi definisao ovu novu ulogu i očekuje se da pravna osnova ostane ista. Vlada je u septembru 2021. predložila da bi funkcije Poverenika mogle biti integrisane u ICO, što je potez koji je izgleda krenuo u realizaciju 2023.

Prilike u Škotskoj donekle su drugačije od Engleske i Velsa. Škotski poverenik za biometriju (Scottish Biometrics Commissioner, SBC) imenovan je 2020. godine na temelju relevantnog zakona.[666] SBC je 2022. doneo obavezujući Kodeks prakse za obradu biometrijskih podataka u radu policije.[667] Kada je u pitanju kontrola rada policije, SBC ima i istražna ovlašćenja. Kako je opisano ovde i kasnije u poglavlju Praksa, policijska upotreba prepoznavanja lica uživo u javnim prostorima bila je učestala u Engleskoj i Velsu, dok do danas ovi sistemi još nijednom nisu primenjeni u Škotskoj.

PRAVNA PRAKSA

Odluka Evropskog suda za ljudska prava u slučaju S. i Marper protiv Ujedinjenog Kraljevstva (2008) imala je ključnu ulogu u tumačenju uticaja obrade biometrijskih podataka na ljudska prava.[668] ESLJP je zaključio da prikupljanje biometrijskih podataka o osobi, „koje omogućava njenu

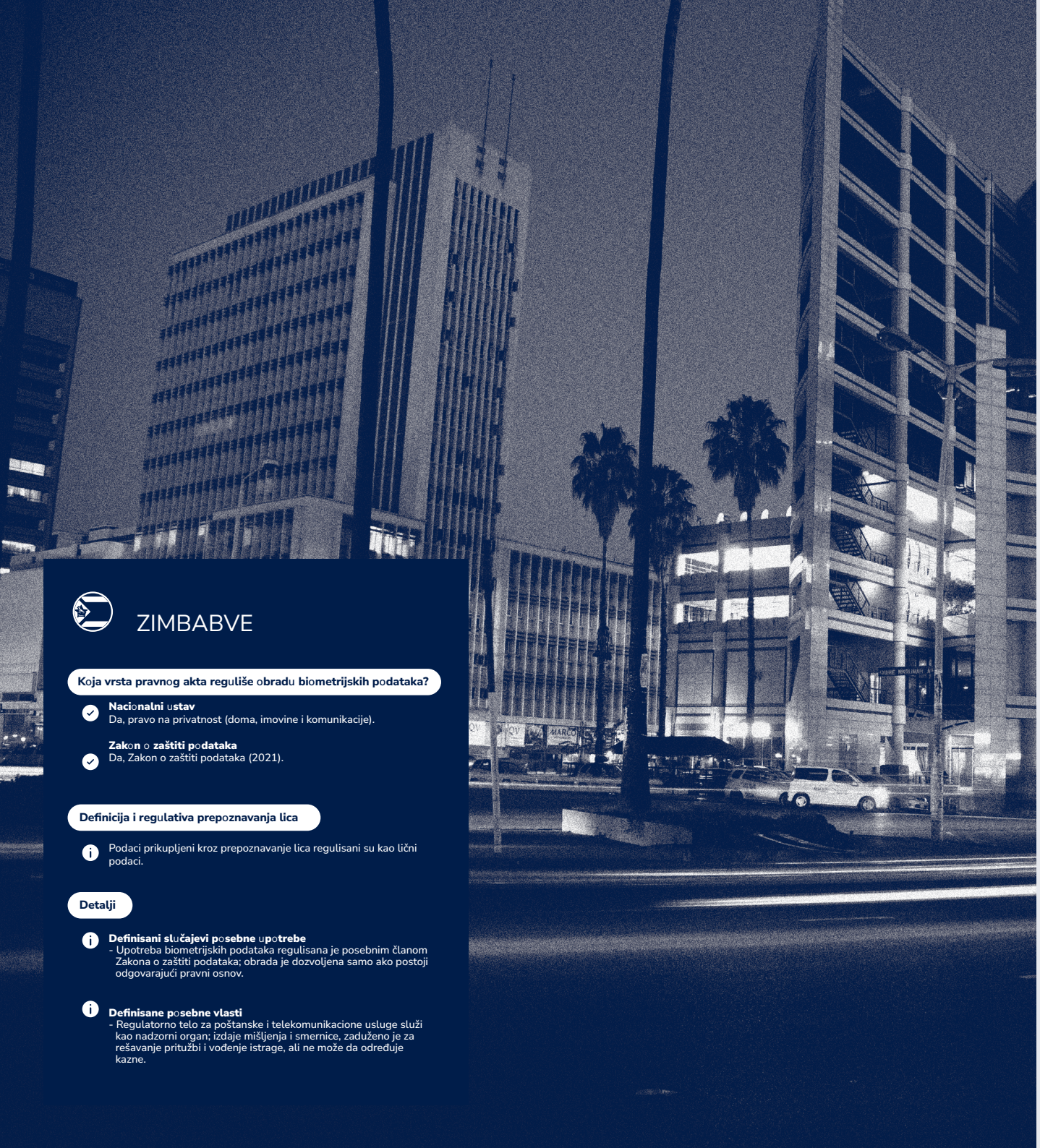
preciznu identifikaciju u širokom spektru okolnosti“, može da „utiče na njen privatni život“ i izaziva „značajnu zabrinutost za privatni život“.

Takođe, da bi prikupljanje i zadržavanje biometrijskih podataka bilo zakonito, Sud je utvrdio da je neophodno imati „jasna, detaljna pravila koja regulišu obim i primenu mera, kao i minimalne zaštitne mehanizme koji se tiču, između ostalog, trajanja, skladištenja, upotrebe, pristupa trećih strana, procedura za očuvanje integriteta i poverljivosti podataka i procedura za njihovo uništavanje, čime se obezbeđuju dovoljne garancije protiv rizika od zloupotrebe i arbitrarnosti“.

Slučaj R (Bridges) protiv šefa policije Južnog Velsa (2020) ticao se policijske primene tehnologije automatskog prepoznavanja lica uživo (LFR) na većim grupama ljudi.[669] Apelacioni sud je utvrdio da je policijska upotreba LFR bila nezakonita jer krši pravo na privatnost, zakone o zaštiti podataka i propise o jednakosti. Takođe je smatrao da testiranje LFR tehnologije od strane policije Južnog Velsa nije zadovoljilo uslov „usklađenosti sa zakonom“ čime je prekršen član 8 EKLJP, pošto je pravni okvir bio nedovoljan da zaštiti prava pojedinca. Sud je istakao da se član 8 primenjuje kad god se biometrijski podaci prikupljaju, čuvaju ili obrađuju, čak i nakratko.

Ako je neka mera u suprotnosti sa članom 8 EKLJP a u skladu je sa zakonom, sledeći korak je razmatranje da li je neophodna i proporcionalna u demokratskom društvu. To zahteva utvrđivanje legitimnog cilja, procenu da li je odstupanje od člana 8 EKLJP srazmerno ostvarenju tog cilja i da li su sredstva delotvorna. Proporcionalnost se procenjuje četvorostepenim testom koji je uspostavio Vrhovni sud UK u predmetu Bank Mellat v HM Treasury iz 2013.[670]

Četiri faze testa su formulisane u obliku pitanja: (1) da li je cilj primenjene mere dovoljno važan da opravda ograničenje osnovnog prava; (2) da li je u razumnoj vezi s legitimnim ciljem; (3) da li je primenjiva manje intruzivna mera koja ne kompromituje cilj; i (4) da li je uspostavljena pravična ravnoteža između prava pojedinca i interesa zajednice, uzimajući u obzir težinu posledica.



ZIMBABVE

Koja vrsta pravnog akta reguliše obradu biometrijskih podataka?

Nacionalni ustav
Da, pravo na privatnost (doma, imovine i komunikacije).

Zakon o zaštiti podataka
Da, Zakon o zaštiti podataka (2021).

Definicija i regulativa prepoznavanja lica

Podaci prikupljeni kroz prepoznavanje lica regulisani su kao lični podaci.

Detalji

Definisani slučajevi posebne upotrebe
- Upotreba biometrijskih podataka regulisana je posebnim članom Zakona o zaštiti podataka; obrada je dozvoljena samo ako postoji odgovarajući pravni osnov.

Definisane posebne vlasti
- Regulatorno telo za poštanske i telekomunikacione usluge služi kao nadzorni organ; izdaje mišljenja i smernice, zaduženo je za rešavanje pritužbi i vođenje istrage, ali ne može da određuje kazne.

ZIMBABVE

KONTEKST

Politička klima u Zimbabveu tokom vladavine Roberta Mugabea, koja je trajala više od 30 godina, okrenula je ovu državu od Zapada i otvorila je za kineski uticaj.[671] Mugabeov režim je vremenom doveo zemlju do ekonomske i demokratske propasti. Promena vlasti usledila je 2017. posle državnog udara, da bi naredne godine za predsednika bio izabran Emerson Mnangagva. Međutim, pod vladavinom novog predsednika Zimbabve je i dalje na putu „demokratske regresije" dok se „sužava građanski prostor i onlajn i oflajn, jer režim primenjuje niz zakonskih i vanzakonskih mera da suzbije neslaganje".[672]

Kineski uticaj ogleda se u finansijskoj pomoći, ali i značajnom učešću kineskih kompanija (posebno Huawei) u izgradnji internet i telekom infrastrukture u zemlji.[673] Novu zgradu parlamenta, otvorenu 2023. godine, u potpunosti je finansirala Kina kao „poklon" Zimbabveu.[674] Kinesko učešće u različitim nabavkama takođe je veliko, posebno kada je u pitanju moderna tehnologija nadzora koja, prema medijskim izveštajima, uključuje i tehnologiju prepoznavanja lica za svrhe sprovođenja zakona.[675]

Tokom posete predsednika Mnangagve Kini 2018, spekulisalo se da će tehnologija za prepoznavanje lica biti kupljena od kineske kompanije Cloudwalk Technology Go.[676] Iste godine vlada je pokrenula „inicijativu za pametne održive gradove Zimbabvea",[677] povezanu s planovima za primenu alata za prepoznavanje lica u većim gradovima,[678] kao i planovima Kine da saradnju sa zemljama poput Zimbabvea koristi za trening svoje tehnologije na „crnoj populaciji".[679] Prema pojedinim izveštajima, 2018. se već počelo sa instaliranjem

tehnologije za prepoznavanje lica na granicama.[680] Drugi izveštaji sugerišu da je 2020. godine počela nabavka tehnologije za prepoznavanje lica od kompanija Huawei, CloudWalk Technology i Hikvision.[681] Navodi se da CloudWalk Technology „već prikuplja podatke miliona građana Zimbabvea kroz biometrijsku registraciju birača, a koji se skladište i obrađuju u Kini".[682]

Najnoviji projekat u vezi sa korišćenjem prepoznavanja lica zove se „Zim Cyber City" a namenjen je za Novi Harare – područje planirano za novo sedište vlade na periferiji postojećeg glavnog grada Zimbabvea.[683] Projekat je pokrenut 2022. i još uvek je u ranoj fazi razvoja. Međutim, glavni investitor – kompanija Mulk International iz Dubaija – već najavljuje da će jedna od mnogih „pametnih" karakteristika projekta biti „tehnologija nadzora koja je direktno povezana sa organima za sprovođenje zakona", sa ciljem čuvanja „bezbednosti ljudi koji tamo žive i rade".[684] Tek ćemo videti kako će se odvijati realizacija ovog projekta, kao i kuda vodi interes Emirata za razvoj tehnologije zasnovane na prepoznavanju lica u mnogo siromašnijoj zemlji poput Zimbabvea.

Mada postoji mnogo indicija da javni organi u Zimbabveu već koriste tehnologije za prepoznavanje lica, ili bar prikupljaju podatke svojih građana za razvoj ove tehnologije, nema nedvosmislenih dokaza o takvoj praksi i njenim razmerama, što predstavlja zaseban problem.

PRAVNI OKVIR

Ustav Zimbabvea reguliše pravo na privatnost u svom odeljku 57, koji pokriva zaštitu doma, imovine i komunikacije građana, ali ne pominje zaštitu bilo kakvih ličnih podataka – sa izuzetkom zdravstvenih podataka koji su izričito zaštićeni od otkrivanja.

Zakon koji reguliše pitanja ličnih podataka donet je u decembru 2021. godine.[685] Tokom procedure usvajanja, radni naziv propisa bio je Predlog zakona o sajber bezbednosti i zaštiti podataka, da bi bio usvojen pod nazivom Zakon o zaštiti podataka.[686] Ovaj propis reguliše pitanja koja se odnose i na sajber bezbednost i na zaštitu ličnih podataka, a njegovim tekstom se menjaju Zakon o kodifikaciji i reformi (krivični zakonik), Zakon o krivičnom postupku i dokazima i Zakon o presretanju komunikacija.[687]

Takav pristup, kao i formulacija niza odredbi, naišli su na kritiku jer nova pravila nose značajan rizik od zloupotrebe u cilju političke represije – posebno u delu zakona o sajber bezbednosti, kao što su pravila o suzbijanju širenja lažnih informacija koja zapravo „podrivaju slobodu govora i slobodu medija".[688]

Čini se da odredbe o zaštiti ličnih podataka, na prvi pogled, prate modernu pravnu logiku kojom se rukovodi Evropska unija. Zimbabveanski Zakon o zaštiti podataka ima odredbe koje se odnose na pravni osnov za obradu podataka, reguliše prava subjekata podataka, kao i dužnosti rukovalaca i obrađivača. Zakon se primenjuje na svaku organizaciju, uključujući vladine organe. Regulatorna agencija za poštu i telekomunikacije (Postal and Telecommunications Regulatory Authority of Zimbabwe, POTRAZ) imenovan je kao organ za zaštitu podataka zadužen za sprovođenje Zakona.

U novembru 2024. godine, POTRAZ je na osnovu svojih ovlašćenja iz zakona doneo podzakonski akt u vezi sa zaštitom podataka (Statutory Instrument 155, SI 155) koji detaljnije reguliše pitanje licenciranja i imenovanja službenika za zaštitu podataka.[689]

Kada je u pitanju regulisanje biometrijskih podataka, tačnije prepoznavanja lica, Zakon ne ulazi previše u detalje. Naprotiv, biometrijski podaci nisu definisani zakonom. Međutim, SI 155 nadoknađuje ovu pravnu prazninu i u svojoj definiciji biometrijskih podataka izričito navodi prepoznavanje lica. Takođe vredi napomenuti da Zakon razlikuje osetljive podatke, koja obuhvata: (1) informacije koje mogu otkriti rasno ili etničko poreklo osobe, njena politička, verska ili filozofska uverenja, članstvo u profesionalnom ili trgovačkom udruženju, seksualni život, krivično, obrazovno, finansijsko ili radno iskustvo, rod, uzrast, bračni ili porodični status; (2) zdravstvene informacije; (3) genetske informacije; ili (4) bilo koju informaciju za koju se može smatrati da predstavlja veliki rizik za prava osoba na koje se podaci odnose. U nedostatku zvaničnih uputstava ili sudske prakse, uključujući i to da definicija biometrijskih podataka iz SI 155 ne rešava ovu dilemu, možemo samo da nagađamo da li se biometrija svrstava u poslednju kategoriju osetljivih podataka iz Zakona. Za pravno tumačenje indikativno je da su genetske i zdravstvene informacije izričito navedene kao osetljivi podaci, dok biometrijski podaci nisu.

Što se tiče pravila iz SI 155, biometrijski podaci se pominju samo u kontekstu obaveze za rukovaoce koji obrađuju takve podatke da o tome obaveste POTRAZ, bez dalje regulative o svrsi ili sadržini tog obaveštenja.

Pravila koja se direktno bave biometrijskim podacima sadržana su samo u odeljku 12 Zakona, naslovljenom „Genetski podaci, biometrijski osetljivi podaci i zdravstveni podaci“. Važan aspekt za pravno tumačenje može biti da se ovaj naslov odnosi na biometrijske „osetljive“ podatke, dok zakonska odredba iz stava 1 glasi: „Obrada genetskih podataka, biometrijskih podataka i zdravstvenih podataka [...]“, izostavljajući reč „osetljivi“. Da li to može da implicira da postoje biometrijski podaci koji jesu osetljivi i drugi koji nisu? Opet, teško je doneti bilo kakav zaključak bez zvaničnog uputstva.

U odeljku 12 dalje se kaže da je obrada genetskih podataka, biometrijskih podataka i zdravstvenih podataka zabranjena bez saglasnosti, ili ako ako se ne primenjuje jedan od izuzetaka. Izuzeci, između ostalog, uključuju situacije kada je obrada neophodna, odnosno zahtevana: (1) u oblasti zakona o zapošljavanju; (2) za sprovođenje zakona o nacionalnoj bezbednosti; (3) za unapređenje i zaštitu javnog zdravlja, uključujući medicinski pregled stanovništva; (4) za značajan javni interes; (5) za zaštitu vitalnih interesa pojedinca; ili (6) radi sprečavanja neposredne opasnosti ili ublažavanja posledica određenog krivičnog dela. Postoji i nekoliko izuzetaka inspirisanih GDPR-om, na primer ako je osoba na koju se podaci odnose javno objavila podatke ili je obrada neophodna za odbranu zakonskih prava.

Ova lista izaziva zabrinutost zbog nekoliko nejasnih i širokih izuzetaka koje bi državni organi mogli da koriste u kontekstu različitih agendi. Taj rizik je prepoznao advokat za ljudska prava Kelvin Kabaya, koji je tvrdio da član nije u skladu sa Ustavom. Prema njegovom mišljenju, odredba je „postavljena preširoko i može se zloupotrebiti. Fraze kao što je 'značajan interes' nemaju precizno značenje. Ova odredba može da padne na ustavnoj proveri, jer je nejasna i potencijalno narušava pravo na privatnost.“[690]

Konačno, odeljak 12 detaljnije reguliše obradu genetskih i zdravstvenih podataka, ali ne pominje ništa drugo u vezi sa biometrijom.

Jedna odredba Zakona koja potencijalno može poslužiti kao zaštita u nekim slučajevima upotrebe prepoznavanja lica i drugih biometrijskih alata za nadzor, jeste član 25 koji reguliše automatizovano odlučivanje. Prema tom članu, jasno inspirisanim GDPR-om, osobe na koje se podaci odnose imaju pravo da ne budu predmet odluke zasnovane isključivo na automatizovanoj obradi, uključujući profilisanje, a koja ima pravno dejstvo ili na sličan način može značajno da utiče na subjekta podataka. Postoje dva izuzetka od ovog pravila: ako je osoba pristala na takvu odluku, ili ako je odluka zasnovana na odredbi utvrđenoj zakonom. Strogo tumačenje drugog izuzetka trebalo bi da znači da postoji poseban zakon koji bi regulisao određeni automatizovani proces odlučivanja.

Sve u svemu, čini se da kenijski Zakon o zaštiti podataka ne reguliše obradu biometrijskih podataka na sveobuhvatan i zadovoljavajući način. Nedostatak pravne definicije, otvorenost za različita tumačenja prirode biometrijskih podataka, preširoki i dvosmisleni pravni osnov za njihovo prikupljanje i nedostatak bilo kakvih značajnih zaštitnih mehanizama u pogledu njihovog korišćenja u organima javnih vlasti, predstavljaju povod za zabrinutost kada vlada počne da sprovodi najavljene projekte zasnovane na tehnologiji za prepoznavanje lica.

Sudeći po zvaničnom sajtu POTRAZ-a, trenutno ne postoje podzakonski akti ili uputstva koja se bave bilo kojim aspektom biometrijske obrade.

PRAVNA PRAKSA

Sudovi u Zimbabveu do sada nisu odlučivali o pitanjima u vezi sa biometrijskim masovnim nadzorom, niti je POTRAZ donosio pojedinačne odluke o takvim stvarima.

Međutim, jedan slučaj vezan za presretanje komunikacija može biti relevantan u smislu onoga što se može dogoditi u Zimbabveu kada vlada koristi zakone u svoje svrhe. Naime, 2019, nakon najave da će gorivo poskupeti za 150% izbili su protesti.[691] Vlada je na to reagovala ukidanjem interneta u zemlji, naređujući telekomima da prestanu da pružaju internet usluge.[692] Usledila je hitna pravna reakcija dve organizacije, Instituta za medije za južnu Afriku i Zimbabveanskih pravnika za ljudska prava, koji su osporili primenu Zakona o presretanju komunikacija za potpuno obustavljanje internet komunikacija.[693] Visoki sud je presudio u korist podnosilaca predstavke i vladinu naredbu (koju je izdao nadležni ministar) proglasio nezakonitom, jer nije izdata u skladu sa Zakonom o presretanju komunikacija. Odluka je bila zasnovana na činjenici da je predsednik, a ne ministar, taj koji ima ovlašćenje da izdaje naloge takve vrste. Sud stoga nije morao odlučivati o kršenju ustavnih prava građana, uključujući slobodu govora, niti je odlučivao o tome da li Zakon o presretanju komunikacija dozvoljava takve neselektivne mere.[694] Odlukom je Visoki sud takođe naložio telekomunikacionim kompanijama da bezuslovno i bez odlaganja nastave sa pružanjem internet usluga.[695]

PRAKSA

UVOD

Poslednje poglavlje, fokusirano na niz konkretnih primera, u prvi plan stavlja odluke i politike za primenu tehnologija za prepoznavanje lica. Dok izraz „masovni biometrijski nadzor“ podrazumeva svaku primenu takvih sistema, od vitalnog je značaja da se ovim opštim terminom obuhvate i njihove arbitrarne primene. Tako i baze podataka i drugi delovi tehničke infrastrukture čine sastavni deo koncepta masovnog biometrijskog nadzora, što nas vodi do široke i sveobuhvatne definicije. To je od suštinske važnosti jer, da bi izbegle preispitivanje, vlade često tvrde da je upotreba ovih tehnologija uvek „ciljana“.

Iz perspektive povreda prava, oslanjajući se na radove autora kao što su Nathalie Smuha, Harini Suresh i John Guttag, u ovom poglavlju težište je na značaju sagledavanja štete uzrokovane biometrijskim nadzorom ne samo na nivou pojedinca, već i na nivou celokupnog društva. Kada umesto tehnocentričnog favorizujemo sociološki pristup, jasnije ćemo videti da svaki element ovih tehnoloških sistema, uključujući podatke koji ih hrane, predstavlja produkt moći i istorije.

To je očigledno iz nekoliko ovde ispitanih slučajeva u kojima iz državne upotrebe prepoznavanja lica nastaje mašinerija nasilja kao, na primer, u Mjanmaru i Njujorku. Talas represije koju tamošnja hunta sprovodi poslednjih godina, izložio je demonstrante i političku opoziciju u Mjanmaru nekažnjenom zatvaranju i ubijanju, dok primena prepoznavanja lica za brzu identifikaciju i hapšenje disidenata olakšava, pa čak i podstiče njihov progon.

U Njujorku je porast upotrebe tehnologije za prepoznavanje lica pogoršao već prekomernu policijsku kontrolu crne i drugih rasijalizovanih zajednica, dok je istovremeno čini manje transparentnom. Taj kontrast vidljivosti i neprozirnosti česta je pojava – na primer, fizička vidljivost kamera koju njujorški policajci nose na uniformama, naspram pokušaja da se prikriju rezultati takvih praksi, odnosno povrede prava usled pogrešnih i politički motivisanih hapšenja.

Uprkos toksičnom susretu digitalnog i analognog rasizma, međutim, u Njujorku postoje dobri primeri otpora. Zajednice i nevladine organizacije kao što su Amnesty International i Američka unija za građanske slobode (American Civil Liberties Union, ACLU) razotkrivaju takve prakse i pokreću sudske parnice za veću transparentnost. Izveštaj nezavisnog nadzornog organa njujorške policije (Komptroler), jedan je od retkih primera u svetu da su javnosti date tačne i relevantne informacije o policijskoj upotrebi sistema veštačke inteligencije. Nadu daje i slučaj Srbije, gde su pokušaji da se legalizuje upotreba kineskih nadzornih kamera koje su preplavile glavni grad, naišli na snažan otpor javnosti što je, bar za sada, dovelo do odustajanja od izmena zakona.

Slučajevi upotrebe, zasnovane na tvrdnjama o „nacionalnoj bezbednosti“, pokazuju sistematsko spajanje primene sporne tehnologije za nacionalnu i javnu bezbednost. Takođe pokreću pitanje ko je zapravo bezbedniji kada su naša lica i tela izložena stalnom nadzoru.

Ovo pitanje je posebno relevantno u slučaju nadzora ljudi u pokretu. U Grčkoj, tehnologija nadzora granica, uključujući biometriju, povezana je sa nasilnim odvraćanjem ljudi koji traže azil – dok su finansijska sredstva namenjena oporavku od pandemije kovida-19, tajno preusmeravana na ulaganja u sisteme za praćenje. Mnoge od ovih primera podržava ogroman industrijski kompleks za nadzor granica. Na iste probleme nailazimo u Centralnoj Americi, gde biometrija olakšava sprečavanje ljudi pri traženju azila, što je očigledan primer kršenja međunarodnog prava.

U Palestini vidimo verovatno najočigledniji primer kako se uređaji, softveri i baze podataka uklapaju u sistem biometrijskog nadzora i ugnjetavanja koji daleko prevazilazi puki zbir njegovih činilaca. Konkretno, ta studija slučaja pokazuje koliko je ograničen pristup usmeren na povrede prava nastale u različitim tačkama društveno-tehničkog sistema. Nemoguće je umanjiti razmere u kojima su Palestinci izloženi biometrijskom i drugim vrstama nadzora koji sprovodi izraelska vojska, a koja se čak hvali takozvanim „Fejsbukom za Palestince“. Ni tehnički „najsavršeniji“ sistem ne bi mogao da ublaži rutinsku kontrolu i ugnjetavanje koji se vrše uz pomoć biometrijskih alata. U trenutku kada je objavljeno prvo izdanje ove knjige, rat u Gazi još nije počeo; u međuvremenu, otkriveni su razni drugi načini na koje izraelska vojska zloupotrebljava sisteme masovnog biometrijskog nadzora za lociranje i ubijanje ljudi, često civila.

U kontekstu maloprodaje i usluga – i u javnom i u privatnom sektoru – primena ovih tehnologija označila je sveobuhvatno praćenje društvenih medija. Mada regulatori reaguju na odsustvo dovoljnog osnova za upotrebu ovih sistema, prodavnice, banke i drugi servisi u Australiji, SAD i UK

ubrzano ih implementiraju. Jedan primer tiče se tinejdžera koji je pogrešno optužen za krađu zahvaljujući profilisanju koje su ovi sistemi omogućili.

Konačno, analiza francuskih Olimpijskih i Paraolimpijskih igara i krunisanja kralja Čarlsa u Londonu, otkriva porast upotrebe biometrijskih sistema u radu policije i kontroli javnih prostora i masovnih događaja. Uprkos tvrdnjama o naprednom režimu zaštite podataka, obe zemlje zapravo eksperimentišu sa sistemima koji prate ljude dok uživaju u sportskom događaju ili javnoj proslavi (ili demonstriraju protiv proslave). Pitanje protesta je posebno relevantno za Ujedinjeno Kraljevstvo, budući da se mnoge primene prepoznavanja lica uživo – bez odgovarajućih ovlašćenja i uz ozbiljne rizike od diskriminacije – odvijaju u vreme kada su usvojeni novi zakoni za ograničavanje više oblika protesta.

Ukratko, ovo poglavlje otkriva dramatične razmere neuspeha da se zakonima, razmatranim u prethodnom poglavlju, građani zaštite od kršenja prava prilikom primene biometrijskog nadzora. Uprkos zapanjujućem odsustvu dokaza o efikasnosti i mnoštvu dokaza o povredama prava, vlade i kompanije grozničavo raspoređuju sisteme biometrijskog nadzora, ne uzimajući u obzir njihove posledice. Takvi postupci samo utvrđuju postojeće strukture moći.

Nakon detaljne analize tehničkih karakteristika biometrijskog nadzora i zakona koji (ne) regulišu njegovu upotrebu u prethodnim poglavljima ove knjige, ovde ćemo se posvetiti praktičnoj primeni tih tehnologija širom sveta. Slučajevi upotrebe su brojni zato što vlade i kompanije svesno eksperimentišu sa načinima na koje se ti sistemi mogu koristiti, često pre nego što procene sve potencijalne rizike. To se posebno odnosi na upotrebu biometrijskih tehnologija u svrhe koje se svode na masovno praćenje stanovništva, što se često operacionalizuje pod maskom javne sigurnosti i nacionalne bezbednosti. Peter Königs tvrdi da je aktuelna postavka državnog nadzora građana u velikim razmerama učinila da ove prakse prima facie izgledaju mnogo manje intruzivne kroz upotrebu automatizovanih sistema i drugih digitalnih tehnologija u nastajanju, što ponekad društvima otežava da shvate obim potencijalnih zloupotreba i već postojećih povreda prava.[696]

Dok su sredstva za nadzor stanovništva danas možda manje vidljiva, istina je, međutim, da su obim i prodor ovih sistema u eksponencijalnom rastu. Stoga je važno razgovarati o takozvanoj etici biometrijskog nadzora i sagledati načine na koje se nadzor sprovodi širom sveta, da bismo bolje razumeli kako se on opravdava i zloupotrebljava.

ŠTA JE MASOVNI BIOMETRIJSKI NADZOR?

Prema definiciji Saveta Evrope, strateški ili masovni nadzor predstavlja arbitraran oblik nadzora čiji je cilj sprečavanje, a ne ublažavanje posledica teških dela, i po prirodi je manje selektivan od „ciljanog“ nadzora kao što su prisluškivanje telefona, praćenje i slično, za šta je u načelu potrebna neka vrsta ovlašćenja kao što je sudski nalog.[697] U praksi, masovna upotreba bi značila upotrebu tehnologija nadzora za aktivno praćenje stanovništva kao vid kontrole, umesto za identifikaciju konkretne osobe od interesa koja predstavlja jasnu i neposrednu pretnju po imovinu, život i javnu bezbednost.

Jedna od glavnih karakteristika masovnog nadzora jeste to što se smatra neciljanim, što znači da se ne tiče samo konkretnih pojedinaca od interesa. Definiše ga neselektivni pristup koji može obuhvatiti prikupljanje podataka o zajednicama, pa čak i čitavom društvu. Drugi važan aspekt jeste način na koji se ovi podaci prikupljaju, jer u slučaju masovnog nadzora nije potrebna osnova ili razumna sumnja da bi se sistem stavio u upotrebu. Stoga, u skladu sa radnom definicijom koju koristimo u ovoj knjizi, masovni biometrijski nadzor se odnosi na neciljano prikupljanje, obradu ili analizu biometrijskih podataka, obično u javno dostupnom prostoru. Ova vrsta široko rasprostranjenog nadzora lako može izazvati tzv. efekat zebnje, odnosno odvratiti građane od učešća u javnom životu ili ograničiti njihovu slobodu izražavanja i druga osnovna ljudska prava.

Kako objašnjava italijanska agencija za zaštitu podataka, Garante Privacy, čak i kada vlasti traže određenog osumnjičenog, činjenica da se podaci svake osobe moraju obraditi kako bi se utvrdilo da li je to osoba za kojom se traga ili ne, znači da je takva praksa zapravo (biometrijski) „masovni nadzor“.[698] Ovo tumačenje je zaista važno jer mnogi državni organi širom sveta netačno tvrde da je potraga za osobama koje se nalaze na listi za praćenje „ciljana“, kako bi opravdali upotrebu biometrijskih sistema na načine koji ipak predstavljaju masovni nadzor.

Mreža European Digital Rights (EDRi) objašnjava da je daljinska biometrijska identifikacija (remote biometric identification, RBI), na primer prepoznavanje lica u javnom prostoru, jedan od glavnih stubova biometrijske prakse masovnog nadzora. RBI podrazumeva upotrebu biometrijskih sistema u javnim prostorima na neciljani ili arbitrarno ciljani način, što je inherentno dizajnu ovih sistema, kako napominje Garante Privacy.[699] Međutim, sporne tačke postoje čak i u Evropskoj uniji koja je

učinila neke značajne korake da ograniči i reguliše biometriju, i gde se većina članova Evropskog parlamenta 2021. obavezala da će zabraniti masovni biometrijski nadzor.[700] Zvanični stav Saveta EU, usvojen u decembru 2022. godine, omogućio bi policiji da koristi RBI u javnim prostorima iz raznih razloga i ne zabranjuje drugim akterima njegovu upotrebu.[701] Taj dokument takođe daje revidiranu definiciju sistema veštačke inteligencije kao sistema koji su razvijeni kroz pristupe mašinskom učenju, kao i pristupe zasnovane na logici i znanju. Ovaj potez izazvao je negodovanje digitalnih i organizacija za ljudska prava, koje tvrde da će ove promene ublažiti pristup regulatora jer suštinski dehumanizuju ove sisteme. Početkom avgusta 2024. godine, na snagu je stupila Uredba o veštačkoj inteligenciji kojom je RBI u realnom vremenu (real-time) propisana kao zabranjena praksa u načelu, ali dozvoljava da se koristi u policijske svrhe ako su ispunjeni određeni uslovi za izuzeće od zabrane. S druge strane, naknadna RBI je svrstana u visokorizične prakse i može se koristiti pod uslovima koji su prethodno opisani u delu publikacije koji se bavi pravnim aspektima.[702]

Takođe je važno ponoviti da se prakse masovnog biometrijskog nadzora obično oslanjaju na aktivnosti prikupljanja podataka u velikim razmerama kao i na ekspanzivne tehnološke infrastrukture, koje su istovremeno skrivene i vidljive. Ove biometrijske infrastrukture masovnog nadzora obuhvataju baze koje sadrže podatke iz ličnih karata, zdravstvenih kartona ili druge lične podatke koje skladište državni organi ili privatne organizacije (kao što je ozloglašeni Clearview AI, o kome se detaljno govori u ovoj knjizi).

Takve zbirke mogu da sadrže ogromne količine ličnih podataka, ali su često izostavljene iz rasprava o biometrijskom masovnom nadzoru usled navodnog nedostatka tehnološke inovativnosti – mada se u prvom delu ove knjige ističe da je masovno prikupljanje biometrijskih podataka često zapravo prethodnica nadzora. Aktuelne aktivnosti na prikupljanju i obradi biometrijskih informacija nisu jedini put ka povredama prava: postojeće baze podataka, građene više godina, pa čak i decenija, podjednako predstavljaju rizičnu polaznu osnovu za kršenje privatnosti.

Kada se koriste pod izgovorom sigurnosnih ili bezbednosnih razloga, uglavnom se koriste za ciljanje određenih zajednica kao što su ljudi u pokretu, rasijalizovane i druge obespravljene grupe. U tom smislu, ove baze podataka nose potencijal da pogoršaju vrlo specifične i štetne vrste prekomerne policijske kontrole i diskriminatornog ciljanja određenih grupa, što se ugrađuje u prikupljene podatke, a zatim pogrešno čita kao „neutralno". Zato je od velikog značaja da se arbitrarno ciljana primena takođe posmatra kao masovni biometrijski nadzor, jer je „ciljana" na način koji zapravo progoni čitave zajednice.

USPON BIOMETRIJE

Biometrijski sistemi postaju nezaobilazni deo svakodnevnog života, od nižeg nivoa lične upotrebe (na primer, za otključavanje telefona) do većih razmera primene u korporacijama i državama. Vlade i zagovornici ovih tehnologija spremno ističu navodne prednosti, koje se pretežno tiču zaštite javne bezbednosti. Pristalice sistema biometrijskog nadzora, za koji tvrdimo da predstavlja masovni nadzor, navode da je primena takvih sistema u radu policije ključno sredstvo za sprečavanje i otkrivanje kriminalnih aktivnosti. Argument glasi da upotreba ove vrste tehnologije omogućava policiji da interveniše pre nego što se zločin dogodi, ili da reaguje veoma brzo nakon što se dogodi, što potencijalno može da sačuva živote i spreči štetu pojedincima i društvu u celini.

Pored toga, pristalice neciljanog nadzora tvrde da je to neophodan odgovor na evoluirajuću prirodu kriminala, koji se sve češće odigrava u onlajn verzijama javnih prostora ne mareći za nacionalne granice. Međutim, nema dokaza da masovni biometrijski nadzor zapravo doprinosi sigurnijim društvima ili većoj stopi rešavanja krivičnih dela.[703] Stručnjaci ističu da praktični slučajevi primene ovih tehnologija zapravo podrivaju tvrdnje o legitimnosti i neophodnosti masovnog biometrijskog nadzora. Statistika na koju se oslanja upotreba ovih sistema uglavnom je generalizovan zaključak izveden iz male količine podataka i potpuno zanemaruje ljudski faktor u procesu evaluacije.[704] S druge strane, sudski procesi u Francuskoj i Holandiji tokom 2019. pokazali su da je pozivanje na rezultate poklapanja iz alata za prepoznavanje lica duboko problematično i može dovesti do odbacivanja tužbe.[705]

Jedan od razloga za manjak podataka o delotvornosti ovih sistema jeste taj što se sistemi primenjuju na nejasan način uz ograničenu javnu ili institucionalnu kontrolu. Anegdotalni izveštaji sugerišu da se od probnih primena koje nisu bile delotvorne – za koje se može pretpostaviti da čine ogromnu većinu, jer bi se uspešne probe verovatno naširoko reklamirale – često u tišini odustaje, što dodatno onemogućava kontrolu. Kako su ove tehnologije proteklih godina došle u centar pažnje vlada koje obećavaju bespoštednu borbu protiv kriminala, raste zabrinutost zbog načina na koji se

ti sistemi primenjuju, te zbog raspodele odgovornosti za njihovo održavanje i odgovornu distribuciju. Ovi sistemi, ali i celokupna oblast biometrije i podataka zasnovanih na biometriji, njihovo prikupljanje i promena svrhe njihove upotrebe, otvaraju brojna pitanja etike i ljudskih prava.

U svom radu „S one strane individualnog: Upravljanje društvenom štetom od AI", Nathalie Smuha iznosi argumente o razlikama između individualne, kolektivne i društvene štete koja može nastati usled nepravilne upotrebe sistema veštačke inteligencije poput sistema za prepoznavanje lica.[706] Svaka od ove tri vrste štete jedinstvena je po načinu na koji utiče na pojedince i zajednice izložene državnom nadzoru. Smuha tvrdi da je šteta po društvo prouzrokovana nadzorom najrasprostranjenija, te da je opasna i za pojedince i za zajednicu upravo zbog dalekosežnosti potencijalne štete za društvo u celini. Društvena šteta je zbir individualnih, kao što su pojedinačna dela rasne diskriminacije koji mogu nastati kao rezultat pristrasne tehnologije prepoznavanja lica (ili nesrazmerne upotrebe ovih alata protiv rasijalizovanih i minorizovanih ljudi). Ta šteta može narušiti prava i pojedinaca i zajednica, ali Smuha ističe da se takođe mora posmatrati kao štetna po ljudska prava. Ona to opisuje kao „štetu interesima društva u celini, koji prevazilaze zbir pojedinačnih interesa" zbog strukturalne i sistemske prirode takve štete.[707]

Postoje brojna istraživanja o štetnim posledicama masovnog nadzora na izražavanje i uživanje drugih osnovnih prava i sloboda, kao i o rizicima koje predstavlja nedovoljno regulisana i netransparentna upotreba biometrijske tehnologije.[708] Naspram tih istraživanja, međutim, nema ni približno dovoljno verodostojnih dokaza koji bi mogli opravdati upotrebu ovih tehnologija. Takođe je važno imati u vidu efekat koji tehnologije mogu imati na ljudsko ponašanje, uključujući posledice njihove primene za suzbijanje građanskih sloboda, kao što su slučajevi gušenja demonstracija ili uvođenje sistema socijalnog kredita.[709]

ŠTETNOST BMS

Predrasude ugrađene u podatke za trening i odluke o dizajnu alata za prepoznavanje lica, kako je opisano u prvom poglavlju ove knjige, predstavljaju glavni povod za brigu u mnogim organizacijama civilnog društva, kao i među članovima društva na koje oni direktno utiču. Već je sprovedeno više studija koje su pokazale da sistemi veštačke inteligencije iznova greše u identifikaciji ljudi koji se po etničkom poreklu, demografskim i rodnim karakteristikama razlikuju od istorijski glavnog subjekta podataka za trening – belih, telesno sposobnih muškaraca.[710]

To može dovesti do veće stope lažno pozitivnih rezultata za minorizovane grupe, što uključuje ljude sa nestandardnim crtama lica, i može doprineti održavanju i jačanju postojećih predrasuda u policiji i javnoj upravi, što dovodi do diskriminatornih praksi i rezultata. Kritičari tvrde da policijska primena tehnologija za prepoznavanje lica i drugih biometrijskih alata za nadzor može narušiti poverenje u policiju, posebno u rasijalizovanim zajednicama koje su kroz istoriju bile izložene diskriminaciji i nepravičnom postupanju.[711] Kako bi se pozabavili ovim problemima, jedni pozivaju na strožu regulativu tehnologije i izradu policijskih procedura koje bi smanjile mogućnost za pristrasnost i diskriminaciju. Drugi se, međutim, zalažu za abolicionistički pristup i traže da se ove tehnologije u potpunosti uskrate policiji.

U studiji koju je sprovela mreža EDRi, posebno se ističe to kako regulatori i tehnološke kompanije koje proizvode sisteme zasnovane na veštačkoj inteligenciji, tretiraju predrasude sa čisto tehnološkog stanovišta.[712] EDRi objašnjava način na koji donosioci odluka često zanemaruju različite predrasude i nejednakosti koje mogu biti ugrađene u alate za prepoznavanje lica i druge sisteme zasnovane na veštačkoj inteligenciji. Fokus se stavlja na „pristrasnost" kao matematički problem za rešavanje, što često znači da će se diskriminacija u primeni ovih sistema tretirati kao puka statistička greška i tehnički problem.

Ovaj tehnocentrični pristup, međutim, u suštini negira uticaj strukturalne diskriminacije, koja je stalno prisutna u društvima u kojima ovi sistemi funkcionišu svakodnevno. Konačno, takav pristup „prebacuje složene socio-tehničke probleme u domen dizajna, a time i u ruke tehnoloških kompanija".[713] Jedna od ključnih posledica jeste to da su civilno društvo, zagovornici privatnosti i drugi aktivisti za ljudska prava često isključeni iz razgovora o zaštitnim merama u primeni tehnologije prepoznavanja lica i sistema zasnovanih na veštačkoj inteligenciji – a kamoli o tome da li bi oni uopšte trebalo da postoje ili ne. Ovo isključenje značajno ometa zvanične rasprave o biometrijskim tehnologijama, usled odsustva kritičke perspektive aktera sa prvih linija fronta zaštite građanskih sloboda.

Suresh i Guttag razmatraju „sedam izvora štete u mašinskom učenju", odnosno ključne tačke na kojima se predrasude i druge povrede prava uključuju u životni ciklus sistema mašinskog učenja.[714] Ovi izvori štete su od

suštinskog značaja za razumevanje i širenje diskusije o korišćenju masovnog biometrijskog nadzora od strane vlasti. U mnogim slučajevima, predrasuda se razmatra na krajnje površnom nivou, što korisnicima takvih tehnologija omogućava da neometano pravdaju njihovu primenu. Dodatnom razradom nijansi između različitih vrsta štete koje mogu nastati u procesima mašinskog učenja, kao i politizovanjem samog koncepta „pristrasnosti podataka" kako bi se pokazalo da su podaci zapravo vrlo subjektivni artefakti utisnuti u kontekst u kojem su nastali, Suresh i Guttag su omogućili temeljniju, sociotehničku perspektivu o načinima na koje se zloupotrebe takvih sistema mogu klasifikovati i potencijalno osporiti.

Istorijska predrasuda, prvi izvor štete po klasifikaciji Suresh i Guttaga, već jeste jedna od prepoznatljivih kategorija u diskursu pristrasnosti i odnosi se na načine na koje se prethodno znanje koristi da bi se perpetuiralo ono što se može nazvati reprezentaciona šteta. Ovo znanje se, potom, odnosi na nametanje stereotipa o određenim grupama ljudi u populaciji na osnovu netačne pretpostavke da su istorijski podaci neutralni, što može imati bitan negativan uticaj na način na koji tehnologije kasnije funkcionišu. Pošto se algoritmi kodiraju uz pomoć tih prethodnih struktura znanja, istorijske nejednakosti i obrasci diskriminacije će biti kodirani u osnove tih tehnologija.[715] Budući da su automatizovane tehnologije prepoznavanja lica naslednice analogne fotografije, podložne su istim predrasudama koje su bile prisutne u procesima razvoja te prethodne tehnologije. Istraživanja su pokazala da je istorijska rasna diskriminacija prisutna od samog početka fotografije, pri čemu su podešavanja kamere i oprema optimizovani da daju prioritet vernom prikazu bele kože.[716]

Na primer, analiza iz 2016. godine pokazala je kako je utvrđeno da pretvaranje reči u vektore (word embedding), trenirano na osnovu tekstova iz Googleovog servisa za vesti, sadrži brojne rodne stereotipe.[717] Ovaj postupak podrazumeva reprezentaciju tekstualnih podataka koji imaju semantičko značenje kao vektora u brojnim operacijama mašinskog učenja i obrade prirodnog jezika (natural language processing, NLP) te su stoga sastavni deo finalnog proizvoda. U analiziranim podacima, veća je verovatnoća da određene rodno neutralne reči [na engleskom jeziku!] kao što su domaćica (homemaker), recepcioner (receptionist), frizer (hairdresser) i medicinska sestra (nurse) budu asocirane sa rečju 'žena', dok su štićenik (protege), kapetan (skipper), filozof i šef bili asocirani uz reč 'muškarac'. Utvrđeno je da su automatski generisane analogije koje funkcionišu u dihotomiji on/ona veoma pristrasne, sa primerima kao što su berberin/frizerka, farmacija/kozmetika i arhitekta/dizajnerka enterijera. Korpus analiziranih tekstova za to istraživanje sadrži više od tri miliona reči iz novinskih članaka profesionalnih novinara. Rezultati studije pokazali su da je implicitna i eksplicitna rodna pristrasnost široko rasprostranjena u odabranim podacima. Autori su naveli da neki budući pokušaji čišćenja ovih sistema od predrasuda mogu makar biti od pomoći pri uklanjanju ili smanjenju rodnih predrasuda u društvu, kao i da buduća istraživanja budu pravičnija.

Šteta od reprezentacione pristrasnosti (representation bias), koja je poznata i kao pristrasnost uzorkovanja, bavi se nedovoljnom zastupljenošću određenih delova populacije u skupovima podataka na kojima se ovi sistemi kasnije treniraju i koje na kraju primenjuju. Ključni problem nastaje usled toga što ljudi za koje (ili protiv kojih) se sistemi koriste nisu dovoljno zastupljeni u skupu podataka za trening. Tako, na primer, skup podataka možda ne uključuje rasijalizovane i minorizovane ljude (čak i kada su tehnologije namenjene za upotrebu protiv njih) a može i da previđa određene podatke. Prema izveštaju Nacionalnog instituta za standarde i tehnologiju (NIST), analizirani algoritmi su najbolje rezultate davali za lica označena kao muška, dok su za lica označena kao ženska, posebno iz minorizovanih grupa, rezultati bili najmanje tačni.[718]

U svom ključnom radu „Senke roda", Joy Buolamwini i Timnit Gebru ističu kako automatizovani algoritmi za analizu lica mogu perpetuirati pristrasnost prilikom određivanja roda i rase.[719] Ispitujući ove sisteme, istraživačice su ustanovile da aktuelni sistemi za prepoznavanje lica beleže više stope grešaka kod osoba tamnije puti, posebno kod žena, kao i kod žena sa neuobičajenim frizurama. Njihova studija je pokazala da sistemi veštačke inteligencije nisu potpuno neutralni i, dakle, nisu osposobljeni da se bave razlikama unutar ljudskih populacija, što treba da podrazumeva dodatni trening i metriku za rodove i boje kože. Istraživanje poziva na veću odgovornost komercijalnih programera i vlada u obezbeđivanju da se tehnologija prepoznavanja lica ne koristi za održavanje predrasuda ili nanošenje štete marginalizovanim zajednicama.[720]

Sledeća šteta izvire iz pristrasnosti merenja, koja se odnosi na definiciju proksija koji se koristi za prikupljanje podataka u skup. Proksiji su karakteristike ili mere koje se koriste za predstavljanje određenih koncepata na kvantitativan način, a koji zauzvrat pružaju korisne informacije za skup podataka. To bi značilo da bi u slučaju merenja određenog stanja ili fenomena, proksi značio pregled i prikupljanje već dostupnih informacija

o toj konkretnoj temi. To bi onda omogućilo sistemu da iznese predviđanje o datim podacima i klasifikuje ih u okviru skupa. Recimo, neka kompanija tretira fakultetsku diplomu kao proksi prilikom procene kvalifikacija kandidata za posao. Taj proksi možda ne odražava precizno stvarne veštine ili poslovno iskustvo kandidata. Takođe, oni koji nisu pohađali fakultet, ali imaju relevantno radno iskustvo mogu biti nepravedno isključeni iz razmatranja, dok kandidati koji imaju diplomu, ali nemaju praktične veštine mogu biti precenjeni. Tako nastaje pristrasnost merenja u procesu zapošljavanja i rezultira u manje raznolikoj i manje kvalifikovanoj radnoj snazi. Ova vrsta pristrasnosti može da izazove probleme kada su proksiji nejasni ili ne predstavljaju precizno koncept koji treba da definišu, kada se tačnost merenja ne primenjuje podjednako u grupama za testiranje ili kada se metode merenja razlikuju od grupe do grupe. Što je najvažnije, o tim merenjima odlučuju ljudi – a to otvara prostor za štetu zasnovanu na njihovim uverenjima, predrasudama i pretpostavkama.

Fokus analize koju je 2016. sprovela ProPublica bio je alat kompanije Northpointe pod nazivom Profilisanje u upravljanju prestupnicima za alternativne sankcije (Correctional Offender Management Profiling for Alternative Sanctions, COMPAS), koji su koristile policijske i tužilačke službe u SAD. Istraživači su otkrili da je algoritam korišćen za procenu češće predviđao višu stopu recidivizma za crne osuđenike, dok su osuđeni belci često pogrešno označavani kao manje skloni riziku nego što su to zapravo bili.[721] Procene rizika su pravljene na osnovu bodovanja koje je za svakog osuđenog generisano iz odgovora na upitnik. To očigledno znači da su bodovani odgovori optuženih sadržali informacije o ranijim prestupima koji bi ih svrstali u kategoriju sklonih riziku. Pitanja iz upitnika se jasno mogu protumačiti kao rasijalizovana, imajući u vidu ogroman disparitet u stopama hapšenja i zatvaranja u SAD između belaca i pripadnika drugih rasa.[722] Stoga se može zaključiti da je proksi „različito meren“ za ove zajednice jer je uključivao veću stopu lažno pozitivnih rezultata usled razlike u policijskoj praksi u određenim zajednicama.[723] Tako je, na primer, verovatnije da će crne i latinoameričke osobe biti označene kao rizične jer je veća verovatnoća da su već ranije hapšene ili dolazile u sukob sa policijom. Ovu vrstu „pristrasnosti predviđanja“ ustanovili su i programeri i policijski službenici koji su koristili takav softver.[724]

U slučaju pristrasnosti agregacije, šteta izvire iz opštih modela koji zanemaruju specifičnosti podataka. U osnovi ove vrste pristrasnosti, kako objašnjavaju Suresh i Guttag, nalazi se pretpostavka da je unos za proces označavanja konzistentan u svim podacima, kao kad istraživači pogrešno pretpostave da trendovi u agregiranim podacima važe za sve pojedinačne tačke podataka.[725] Ovo stanovište potencijalno previđa mnoge skrivene obrasce ili njihovo odsustvo, navodeći na pogrešnu klasifikaciju određenih podataka u nastojanju da se oni uklope u univerzalni i uspostavljeni sistem, što zauzvrat može dovesti do netačnih zaključaka kroz trendove i predikcije. Na primer, prilikom analize objava na društvenim mrežama uz pomoć alata za obradu prirodnog jezika, zanemarivanje kulturnog, društvenog i drugog konteksta specifičnog za grupu može značajno uticati na rezultate. Nijanse između podskupova određenih podataka mogu se pogrešno tumačiti u pokušaju standardizacije skupova, čime se generišu potencijalno štetni rezultati.

U studiji koja je razmatrala tvitove mladih iz uličnih bandi Čikaga, istraživači su zaključili da je oko 50 odsto reči korišćenih u tvitovima pogrešno ili uopšte nije definisano u onlajn rečnicima i postojećim bazama.[726] Cilj istraživanja bio je da utvrdi razlike između označavanja govora kao agresivnog sa direktnim pretnjama, kao uvrede ili kao naznake tuge ili gubitka. Zaključak je bio da uobičajeni NLP alati koji se koriste za klasifikaciju onlajn govora nisu precizni ni reprezentativni za određene podskupove zajednice, pa bi bili pogrešno protumačeni ako bi se analizirali zajedno sa dominantnim i standardizovanim značenjima i kontekstima. Takođe je utvrđeno da je veća verovatnoća da pojedini dijalekti neće biti ni označeni u postojećim skupovima podataka.

Pristrasnost u učenju, četvrta šteta koju su definisali Suresh i Guttag, javlja se kad sistem počne da favorizuje određene ishode u odnosu na druge, što dovodi do isključivanja većih odstupanja ili ulaznih informacija koje algoritmi mogu posmatrati kao anomaliju. Podaci koji značajno odstupaju od zadatog seta nisu česti i sistem im može pripisati netačne vrednosti u analizi, jer je zasnovan na statistici i verovatnoćama. U mašinskom učenju, algoritam se trenira na skupu podataka da identifikuje obrasce i pravi predviđanja. Dok algoritam pravi predviđanja, procenjuje se njegova tačnost, a greške se koriste za ažuriranje parametara i unapređenje performansi. Međutim, ova povratna sprega može postati problem kada su podaci za trening pristrasni ili je metrika evaluacije loša. Ako su podaci za trening pristrasni u korist određenih grupa ili ishoda, algoritam će naučiti da pravi predviđanja koja favorizuju te grupe ili ishode, čak i ako nisu reprezentativni u realnom svetu. To može postati začarani krug koji održava i pojačava sve pristrasnosti prisutne u podacima, a model zasnovan na tome počinje

dosledno da proizvodi sve pristrasnija predviđanja. Ako se takva predviđanja koriste u donošenju odluka ili informisanju politika, otvara se prostor za perpetuiranje i jačanje sistemskih predrasuda i nejednakosti.

Istraživanje britanskog Guardiana otkrilo je da alati veštačke inteligencije sa zadatkom da analiziraju i obeleže neprikladne slike objavljene na društvenim mrežama, obično to rade sa slikama ženskih tela.[727] Pritom, nije reč o fotografijama koje su na bilo koji način seksualno eksplicitne ili neprikladne, već naprosto prikazuju delove ženske anatomije. Slike ženskih tela, na primer žene koje rade jogu, alati su označavali kao „provokativne", ali ne i slike muškaraca koji vežbaju bez majice. Kada su ovi algoritmi, koje su razvili Microsoft, Google i druge velike tehnološke kompanije, testirani na slikama pacijentkinja iz medicinskih baza podataka, slike koje prikazuju pregled dojke ili trudnica označavali su kao „eksplicitne i seksualno sugestivne prirode".[728] Takve oznake rezultirale su prikrivenim ograničavanjem naloga na mrežama, gde se sadržaj ne uklanja sa platforme, ali je njegov doseg značajno limitiran zbog navodno eksplicitnog sadržaja. Dalja analiza je takođe pokazala da je za vrednovanje potpune tačnosti, algoritmima bio dovoljan prikaz grudnjaka, pa bi takva slika bila označena kao „provokativna" ili seksualno eksplicitna. Jasno je da su kroz takvu dekontekstualizaciju odevnog predmeta ili dela tela, zasnovanu na unapred zamišljenim rodnim predrasudama, ovi sistemi veštačke inteligencije već naučili da diskriminišu i objektivizuju određene delove populacije.

Peta šteta – pristrasnost evaluacije u mašinskom učenju – odnosi se na prisustvo sistematskih grešaka ili netačnosti u proceni performansi modela. Javlja se kada metrika evaluacije ili testni skup podataka, odnosno referentni podaci koji se koriste za merenje tačnosti i efikasnosti modela, nisu reprezentativni za scenarije iz stvarnog sveta u kojima će model biti primenjen. Na primer, referentni podaci prikupljeni od komercijalnih alata za analizu lica mogu dovesti do pristrasnih rezultata i previđanja karakteristika kao što su rod i rasa, što može biti posledica istorijske, reprezentacione ili pristrasnosti merenja. Pored toga, izbor referentnih podataka takođe može uticati na performanse modela, u zavisnosti od prirode problema i kompromisa između različitih metrika evaluacije. Nereprezentativni skupovi referentnih podataka mogu dovesti do lošeg rada sistema kada se koriste na drugim podskupovima podataka, čime se dodatno širi obim potencijalne štete u procesu. Da bi se umanjio rizik od pristrasnosti evaluacije, važno je pažljivo odabrati testne podatke i metriku evaluacije, kao i imati u vidu potencijalne izvore pristrasnosti koji mogu biti uvedeni tokom izrade modela.

U nastojanju da sačine inkluzivni i intersekcionalni skup podataka za treniranje sa ciljem da eliminiše dobro poznate predrasude, Deborah Raji i saradnici su opisali neke od najvećih aktuelnih prepreka s kojima se ovi sistemi suočavaju. Prilikom revizije referentnih podataka, identifikovan je niz problema, kao što su ograničenja markera u širokoj upotrebi, poput referenci na etničke ili rasne kategorije ili binarne rodne oznake koje bi dovele do isključenja određenih delova populacije. Istraživački tim je takođe ukazao da za skupove referentnih podataka treba jasno navesti svrhe za koje se mogu koristiti, da ne bi bili pogrešno tumačeni i primenjivani u širim kontekstima, što bi moglo da dovede do preteranog izlaganja označenih podataka i prevazilaženja ograničenja predviđene namene skupa referentnih podataka.[729]

Pristrasnost primene tiče se ljudskog odlučivanja koje može da učestvuje u procesu interpretacije podataka. Iako su ovi sistemi stvoreni i testirani u donekle autonomnom okruženju, jednom kada uđu u primenu nastaje niz faktora koji utiču na način na koji se oni koriste, kao i na odgovornost za evaluaciju i tumačenje prikupljenih podataka. To može da zavisi od vlada, privatnih subjekata i organizacija koje mogu imati privilegovan uvid u upotrebu takvih sistema. Stoga tvrdimo da su čak i sistemi za prepoznavanje lica koji su u teoriji besprekorni (šta god to podrazumevalo) i dalje u riziku od zamki pristrasnosti i štete, pošto je prethodno iskustvo pokazalo da policija često primenjuje tehnologije nadzora nesrazmerno protiv rasijalizovanih, migrantskih i siromašnih zajednica.

Naročito u slučajevima tehnologije prepoznavanja lica koja se koristi u policiji, nema dovoljno informacija o ljudskom faktoru u procesu donošenja odluka. U analizi uvođenja kamera za prepoznavanje lica Metropolitan policije na ulice Londona, Pete Fussey ističe da se statistički podaci o efikasnosti sistema striktno bave njegovim tehničkim karakteristikama. Drugim rečima, ove procene ne uzimaju u obzir lažno pozitivne rezultate koji nastaju kao rezultat grešaka policijskih službenika u identifikaciji prilikom upotrebe ovih sistema u istrazi i rešavanju krivičnih dela.[730]

Važno je napomenuti da nije bilo moguće uočiti i pouzdano identifikovati sve predrasude koje se mogu pojaviti u slučajevima o kojima se govori u ovom poglavlju, što se delom tiče i načelnog pitanja uskraćivanja informacija civilnom društvu. Međutim, naša je namera da demistifikujemo različite

predrasude koje se mogu javiti, a u nekim slučajevima su se već javile sa primenom takvih tehnologija na terenu. Šteta koja može nastati usled tih predrasuda poslužiće kao vodič za mnoge probleme koji su još uvek veoma prisutni kada razgovaramo o implikacijama upotrebe ovih tehnologija, posebno imajući u vidu sveopšti nedostatak odgovarajućeg nadzora i regulatornih ograničenja.

STUDIJE SLUČAJA

Pored razmatranja tehničkih karakteristika i regulatornih okvira koji se razvijaju u i oko ove tehnologije, važno je analizirati i osporiti njene primene na terenu. Kako zemlje širom sveta pristupaju regulisanju prepoznavanja lica, biometrije i ličnih podataka na više različitih načina, sledeći primeri potvrđuju da primena takvih sistema na globalnom nivou može biti podjednako raznolika.

Primeri u ovom poglavlju ne predstavljaju iscrpan prikaz onoga što se dešava u zemljama i regionima širom sveta, pa čak ni u svakoj od oblasti interesovanja definisanih u ovoj knjizi. Radije, služe kao opisni primeri za razvoj šireg razumevanja načina na koji se ove tehnologije primenjuju, te njihovih potencijalnih nedostataka, rizika i povreda. Cilj je bio pronaći slučajeve iz različitih zemalja i regiona, sa primenama koje su uticale na različite društvene, etničke i verske zajednice, ne bi li se ova pitanja sagledala iz što više perspektiva. Opet, ne tvrdimo da se radi o reprezentativnom uzorku, već o raznolikom uzorku koji bi mogao pomoći u identifikaciji sličnih obrazaca, kao i razlika.

Slučajevi su podeljeni u četiri opšte oblasti od interesa koje predstavljaju okvir za analizu. Svaka od kategorija doprinosi sveobuhvatnijem pogledu na to kako se ove tehnologije primenjuju, kao i kako se njihova primena opravdava. S obzirom na to da nam je osnovni cilj da predstavimo što više dostupnih informacija o svakom slučaju, važno je napomenuti da su neki od razmatranih slučajeva istraženi dublje od drugih i stoga sadrže više detalja. To ne znači da smatramo da su neki slučajevi važniji od drugih koji su ovde predstavljeni i dali smo sve od sebe da svaki slučaj analiziramo što je moguće sveobuhvatnije.

ORVELIJANSKA NACIONALNA BEZBEDNOST

Zaštita nacionalne bezbednosti jedan je od najčešćih argumenata za razvoj i implementaciju tehnologije prepoznavanja lica, a time i intruzivnih sistema čija se upotreba svodi na masovni biometrijski nadzor. Koncept nacionalne bezbednosti je, u zavisnosti od situacije, u većini slučajeva namerno nejasan i rastegljiv. Kako navodi Lucia Zedner, početak novog milenijuma sa terorističkim napadima u Americi 11. septembra 2001, kao i kasnijim napadima u Londonu i Madridu, doprineo je „normalizaciji vanrednih ovlašćenja" u oblasti nacionalne bezbednosti.[731] Bezbednost u ovom slučaju postaje više praksa nego krajnji cilj, pa se i kao argument rutinski poteže. Štaviše, postalo je nemoguće zamisliti mere bezbednosti kao nezavisne od neke vrste nadzora. Sve češće se preklapaju u sličnim taktikama upotrebe, kao i u svrhe poput praćenja, uticaja i kontrole kretanja.[732]

Ovakva postavka nacionalne bezbednosti omogućava vladama da opravdaju svoju nameravanu ili tekuću upotrebu tehnologija za nadzor. Štaviše, argument nacionalne bezbednosti često se dovodi u vezu sa javnom bezbednošću – ciljem koji, iako važan, nije dovoljno ozbiljan da bi dozvolio iste izuzetne mere kao u svrhe nacionalne bezbednosti. Nije teško razumeti zašto je to slučaj, jer ova racionalizacija omogućava vlastima da prošire svoj domet i opravdaju narušavanje privatnosti i ličnih sloboda. Stoga se masovni nadzor takođe predstavlja kao siguran način da se garantuje bolja bezbednost u javnim prostorima. Do danas još uvek nema značajnih dokaza o bilo kakvoj korelaciji između nadzora javnih prostora i smanjenja kriminala ili unapređenja nivoa javne bezbednosti.

Naprotiv, rezultati različitih studija o tačnosti ovakvih sistema koje koriste vlasti pokazuju suprotno, pri čemu je većina ljudi manje bezbedna pod masovnim biometrijskim nadzorom.[733] U ovim diskusijama takođe treba otvoriti pitanje (odsustva) odgovornosti tehnoloških kompanija, pošto se one rutinski služe svojim načelima profita (na primer, zaštitom intelektualne svojine, kako je objašnjeno u prvom poglavlju ove knjige) da bi izbegle odgovornost. U izveštaju koji je objavio Access Now o primeni tehnologija biometrijskog nadzora širom Latinske Amerike, napominje se da pojedine kompanije nude ove sisteme vladama besplatno kako bi testirale njihove kapacitete bez ikakvih obzira za rizike po ljudska prava koje ti sistemi predstavljaju.[734]

CCTV PUČ – SUZBIJANJE DEMOKRATSKIH PROTESTA U MJANMARU

Tehnologija prepoznavanja lica odigrala je značajnu ulogu u nasilnom i smrtonosnom gušenju mirnih demokratskih protesta u Mjanmaru posle vojnog udara u februaru 2021. Mirni demokratski protesti pokrenuti su kada je vojska preuzela vlast i pritvorila izabrane zvaničnike, među kojima i Aung San Suu Kyi. Mediji su izveštavali da vlada hunte koristi CCTV sisteme sa kapacitetima za prepoznavanje lica da identifikuje i prati demonstrante u realnom vremenu[735] kao i retrospektivno, nakon čega su usledila hapšenja, pritvaranja, zatvorske kazne i pogubljenja.[736] Ove tehnologije su samo jedan element u širem nastojanju hunte da uspostavi potpuni digitalni nadzor nad stanovništvom u Mjanmaru. To podrazumeva onlajn cenzuru, gašenje interneta,[737] skok cena za protok podataka i telefonske pozive, naredbe operatorima da instaliraju tehnologije za nadzor kako bi presretali komunikaciju bez dovoljnog osnova, kao i značajno pooštravanje uslova za registraciju SIM kartica i IMEI.[738]

Prema izveštajima, tri kineske kompanije, Dahua, Huawei i Hikvision, snabdevale su režim autoritarne hunte CCTV kamerama.[739] Ove kompanije su već pod sankcijama Sjedinjenih Država zbog uloge u omogućavanju kineskoj vladi da sprovodi genocid i ugnjetavanje manjina u Sinđijangu.[740] Implementacija projekta CCTV kamera poverena je dvema lokalnim kompanijama, od kojih su obe tesno povezane sa represivnim aparatom Mjanmara. Predsednik jedne od izabranih kompanija, Fisca Security & Communication, jeste penzionisani zamenik komesara mjanmarskih policijskih snaga. Druga, Naung Yoe Technologies, ima istoriju obezbeđivanja opreme za vojsku.[741]

Reakcija vojne hunte na proteste bila je žestoka represija. Prema izveštajima, uhapšeno je više od 20.000 ljudi, a preko 17.000 je još uvek u pritvoru.[742] Procenjuje se da je nekoliko hiljada demonstranata izgubilo živote pod udarom represivnog režima hunte.[743] Da bi ušla u trag demonstrantima, hunta poredi biometrijske podatke sa CCTV kamera sa podacima iz nacionalne baze ličnih karata. CCTV kamere, koje skeniraju lica i registarske tablice vozila na javnim mestima, automatski upozoravaju vlasti na podudarnosti sa poternicama.[744] Vojna hunta je upregla tehnologiju za identifikaciju i targetiranje osoba koje su učestvovale u protestima, što je rezultiralo privođenjima i hapšenjima više stotina građana. Mnogi od njih podvrgnuti su mučenju i drugim oblicima kršenja ljudskih prava, što je u pojedinim slučajevima izvesno bilo lakše izvršiti uz pomoć biometrijskih tehnologija masovnog nadzora.[745]

Slab pravni okvir koji uređuje upotrebu tehnologije za prepoznavanje lica u Mjanmaru ostavlja malo ili nimalo prostora za kontrolu. Zakon o elektronskim transakcijama i Zakon o razvoju računarskih nauka izmenjeni su u februaru 2021. kako bi se proširio masovni nadzor građana. Prvi propis omogućava hapšenje stanovnika zbog nepoželjnog onlajn ponašanja (prvenstveno njihovih aktivnosti na društvenim mrežama) uključujući, ali ne ograničavajući se na širenje lažnih informacija ili narušavanje inostranih odnosa,[746] dok drugi obavezuje sve korisnike interneta da registruju svoja prava imena i druge lične podatke, što anonimnost na mreži čini praktično nemogućom.[747]

Međunarodna zajednica je uvela sankcije režimu vojne hunte, vojnim i privatnim kompanijama, individualnim preduzetnicima, političarima i administratorima. Mada nije jasno kakav je stvarni uticaj ovih sankcija, očigledno je da nisu doprinele odvraćanju od represije, već je režim samo pojačao svoj autoritarni obračun sa građanima koji izražavaju neslaganje.[748] Upotreba tehnologije za prepoznavanje lica i CCTV kamera za targetiranje mirnih demokratskih protesta predstavlja jasno kršenje privatnosti, građanskih sloboda i ljudskih prava. Slab pravni okvir koji reguliše upotrebu ove tehnologije, uz odsustvo kontrole i odgovornosti usled autoritarne prirode režima, omogućio je vojnoj hunti da tehnologiju koristi nekažnjeno.

Slučaj Mjanmara osvetljava jednu neprijatnu istinu – tehnologije biometrijskog nadzora, koje su u razvijenim demokratijama prepoznate kao potencijalna pretnja slobodama i pravima građana, često se koriste od strane iliberalnih demokratskih i autokratskih režima širom sveta upravo kao sredstva za gušenje prava i sloboda.[749] Vojna hunta u Mjanmaru koristila je tehnologije za prepoznavanje lica kako bi identifikovala i targetirala mirne demonstrante koji su protestovali zbog državnog udara. Tehnologije nadzora, koje primenjuju politički sistemi koje karakteriše pogoršanje ili odsustvo vladavine prava, često postaju sredstvo nelegitimnog kršenja osnovnih građanskih i političkih prava, kao što su sloboda izražavanja i okupljanja. Upotreba tehnologija masovnog biometrijskog nadzora za progon određenih grupa podseća na izvorne ideje koje leže u njihovoj osnovi, kao što je prvi veliki program biometrijskog identiteta, odnosno upotreba otisaka prstiju za kontrolu, koji su sprovodili britanski kolonisti u Indiji,[750] ili facijalna metrika koju je primenjivao nacistički režim.[751]

Globalna dostupnost i široka primena takvih tehnologija direktno doprinosi opštem trendu pogoršanja demokratskih vrednosti i praksi, jer dodatno jača autokratske režime.[752] U pojedinim delovima Mjanmara situacija na terenu se može opisati samo kao permanentni građanski rat, dok se u drugim oblastima izvesno može govoriti o zločinima protiv čovečnosti.[753] Kao takve, tehnologije prepoznavanja lica nisu samo pogodne za konsolidaciju moći autoritarnih država i jačanje totalitarne stege nad društvom, već i za efikasno sprovođenje ratnih zločina i zverstava.

HILJADE KAMERA U BEOGRADU

Borba za zabranu tehnologija biometrijskog nadzora, posebno prepoznavanja lica, u Beogradu traje već šest godina. Organizacije civilnog društva i zagovornici privatnosti poput SHARE Fondacije, oštro su se usprotivili uvođenju ovih sistema, posebno nakon procene uticaja na zaštitu podataka (Data Protection Impact Assessment, DPIA) koju je Ministarstvo unutrašnjih poslova sprovelo 2019. godine.[754] Pošto je procena uticaja dostavljena Povereniku za zaštitu podataka o ličnosti u okviru revizije planova za postavljanje kamera za prepoznavanje lica širom Beograda, Poverenik je ocenio da procena ne ispunjava ni formalne ni materijalne uslove propisane Zakonom o zaštiti podataka o ličnosti.

Poverenik je ocenio da sistem ne zadovoljava uslove po dve tačke i obustavio njegovu primenu dok se ne sprovede adekvatna procena uticaja.[755] Prema mišljenju Poverenika, neselektivni sistem masovnog nadzora koji predlaže MUP ne može biti opravdan jer mu nedostaje konkretna svrha zasnovana na dobro utvrđenim činjenicama. Najveći problem do danas predstavlja to što Vlada nije pružila dovoljan argument za neophodnost sistema, niti je mogla da opravda takvo zadiranje u privatnost.

Prvi slučaj zabeležen u javnosti da su u gradu postavljene kamere sa biometrijskim funkcijama – slične modelima koji su razmatrani u prvom poglavlju ove knjige – datira iz juna 2019.[756] Međutim, do masovne instalacije ovih kamera širom Beograda došlo je 2020. u vreme pandemije kovida-19 i posledičnih mera zabrane kretanja. Iako je to policiji olakšalo postavljanje kamera po gradu, stanovnici su ove slučajeve marljivo beležili

i slali ih na Tviter pod haštagom Hiljade kamera, što je inicijativa koju je pokrenula SHARE Fondacija.[757] Cilj inicijative je bio da se mapiraju sve nadzorne kamere postavljene širom grada, ali i da se podigne svest građana o planu za život pod stalnim nadzorom.

Postavljanje biometrijskih kamera sa ugrađenim kapacitetima za prepoznavanje lica širom Beograda osvetlila je načine na koje se kineska tehnologija pojavljuje i primenjuje širom sveta; to se jasno vidi u studiji slučaja o Mjanmaru. Kineski tehnološki gigant Huawei glavni je dobavljač opreme za nadzor namenjene službama za sprovođenje zakona u Srbiji. Ova saradnja datira još od 2011. godine, kada su Vlada Srbije i Huawei započeli pregovore o implementaciji projekta „Bezbedno društvo" koji obuhvata uvođenje sistema masovnog nadzora.[758] Dve strane su 2014. potpisale Memorandum o razumevanju.[759] Postavljanje 1000 kamera za nadzor na 800 lokacija u Beogradu najavljeno je na sajtu kompanije Huawei 2019. godine uz link ka projektu „Bezbedan grad". Stranica je brzo uklonjena, ali je SHARE fondacija pre toga uspela da je arhivira.[760] Ta veb stranica predstavljala je vitalni deo slagalice, kome civilno društvo inače ne bi imalo pristup, zahvaljujući netransparentnoj praksi kompanija i vlada u vezi sa biometrijskim nadzorom.

Posle odbijene procene uticaja iz 2019, Ministarstvo unutrašnjih poslova je u martu 2020. dostavilo Povereniku novu, unapređenu verziju svog zahteva.[761] Međutim, prerađena procena i dalje nije ispunjavala uslove za opravdanost takvog projekta, uz obilje proizvoljne terminologije. Primera radi, druga procena uticaja je predstavila plan da se detekcija lica vrši kod svih osoba koja prolaze kroz zonu pokrivenu sistemom video-nadzora, a da policija koristi sistem za profilisanje, iako iz dokumenta nije bilo jasno šta bi profilisanje konkretno podrazumevalo. Sve u svemu, vlada ponovo nije bila u stanju da obezbedi dovoljan pravni osnov za obradu biometrijskih podataka prikupljenih preko nadzornih kamera.

Neophodnost i proporcionalnost stalno izostaju u argumentima Vlade Srbije za uspostavljanje tako invazivnog sistema. U septembru 2021. MUP je objavio Nacrt zakona o unutrašnjim poslovima sa odredbama koje uređuju upotrebu tehnologije masovnog biometrijskog nadzora u javnim prostorima.[762] Da je usvojen, taj zakon bi Srbiju učinio prvom evropskom zemljom koja je legalizovala sprovođenje neselektivnog nadzora svojih stanovnika u javnim prostorima. Tokom obavezne javne rasprave, SHARE Fondacija je dostavila komentare na Nacrt ističući da bi takav zakon praktično legalizovao masovni biometrijski nadzor.[763] Fondacija je zatražila da se bez odlaganja povuku odredbe Nacrta zakona koji se odnose na biometrijski nadzor, kao i da se proglasi moratorijum na upotrebu biometrijskih tehnologija i sistema masovnog nadzora. Usred šire javne kritike, Nacrt zakona je povučen samo nekoliko dana kasnije.[764]

Međutim, nakon godinu dana sve se vratilo na početak. Krajem 2022. MUP je ponovo objavio revidirani Nacrt zakona o unutrašnjim poslovima,[765] zajedno sa Nacrtom zakona o evidencijama i obradi podataka u oblasti unutrašnjih poslova[766] i revidiranom Procenom uticaja.[767] SHARE Fondacija je utvrdila da se vlasti u Srbiji još uvek nisu adekvatno pozabavile rizicima od neselektivnog i proizvoljnog praćenja i prakse prepoznavanja lica. Novim nacrtom predviđalo se da se biometrijski podaci stanovnika izdvajaju sa nadzornih snimaka i zadržavaju u periodu od 72 sata, što znači da je proces neselektivan i omogućava potencijalno grubo kršenje prava na privatnost.[768]

Zahvaljujući zajedničkim naporima organizacija civilnog društva i pomoći međunarodne zajednice, uključujući poslanike Evropskog parlamenta, nacrti zakona su povučeni iz procedure na samom kraju 2022. godine.[769] Vlada je izrazila želju da se pre novih izmena dodatno konsultuje sa stručnjacima iz oblasti zaštite podataka i privatnosti uopšte.[770] To je signaliziralo pozitivan korak u borbi protiv masovnog biometrijskog nadzora, ne samo u Srbiji, već i šire u Evropi, budući da je čitav slučaj otkrio jasno nezadovoljstvo javnosti i demokratskih predstavnika, naročito po pitanju odsustva transparentnosti i odgovornosti u poduhvatu sa tako visokim ulogom.

SHARE Fondacija, zajedno sa drugim organizacijama civilnog društva i zagovornicima privatnosti, stoji na stanovištu da upotreba biometrijskih tehnologija masovnog nadzora treba da bude zabranjena. Od novembra 2020. godine, preko osamdeset organizacija civilnog društva širom Evrope, uključujući SHARE fondaciju, učestvuju u kampanji za zabranu biometrijskih sistema masovnog nadzora u javnim prostorima.[771]

Mada nisu podneti novi predlozi za legalizaciju biometrijskog nadzora, novija istraživanja pokazuju da je tehnologija za prepoznavanje lica u školama, studentskim domovima, kao i na pijacama i u javnim preduzećima nabavljena i korišćena u najmanje 12 gradova i opština u Srbiji.[772] Druga istraživanja pokazuju da je u poslednjih nekoliko godina broj gradova u Srbiji koji su prekriveni sistemima za nadzor premašio 40.[773]

BIOMETRIJA VELIKE JABUKE: SLUČAJ NJUJORŠKE POLICIJE

Neki od najznačajnijih primera negativnih posledica upotrebe tehnologije bez kontrole, mogu se naći u Sjedinjenim Državama, posebno u vezi sa policijskom primenom prepoznavanja lica u javnim prostorima – tehnologije koja predstavlja jedan od najistaknutijih i najmoćnijih oblika masovnog biometrijskog nadzora. Do sad je objavljeno više izveštaja o osobama iz rasijalizovanih grupa, posebno crne zajednice, koje su pogrešno identifikovane i nepravedno hapšene.[774] Uprkos ubrzanom usvajanju prepoznavanja lica u mnogim policijskim upravama, zakonodavci su bili spori u uspostavljanju pravnog okvira koji bi obezbedio odgovornost i transparentnost u korišćenju takvih tehnologija. Kao ilustrativan primer, ova studija slučaja se bavi upotrebom prepoznavanja lica u njujorškoj policiji (NYPD). Procedure i politike NYPD-a su dugo bile pod lupom javnosti i predmet intenzivnih političkih debata usled nesrazmernog targetiranja minorizovanih grupa.[775]

U analizi upotrebe prepoznavanja lica u NYPD-u, od suštinskog je značaja uzeti u obzir sveobuhvatni pravni okvir i politike države u vezi sa primenom programa mašinskog učenja – ili, tačnije, njihovo odsustvo. Kako se može videti u izveštaju državnog kontrolora iz februara 2023. godine, javnim službama grada Njujorka, uključujući policiju, nedostaju etičke i pravne smernice za korišćenje programa za mašinsko učenje kao što su algoritamsko modeliranje, prepoznavanje lica i druge vrste softvera za nadgledanje građana.[776] U izveštaju se dalje pojašnjava da „[grad Njujork] nema efikasan okvir upravljanja veštačkom inteligencijom. Mada se od službi zahteva da dostavljaju izveštaje o određenim vrstama upotrebe veštačke inteligencije na godišnjem nivou, ne postoje pravila ili smernice za upotrebu veštačke inteligencije“.[777] Usled nedostatka zajedničkog okvira, svaka njujorška služba razvija različit pristup. Izveštaj kontrolora ističe dve glavne oblasti za koje postoji zabrinutost: modeliranje rizika u sistemu socijalne zaštite dece i tehnologiju prepoznavanja lica koju koristi NYPD.

NYPD je izložen javnoj kritici jer ne održava bazični inventar svojih alata veštačke inteligencije, a uprava očigledno nije u potpunosti svesna svih sistema koje koristi.[778] Dok NYPD tvrdi da koristi samo sisteme veštačke inteligencije koje je odobrio Nacionalni institut za standarde i tehnologiju (National Institute of Standards and Technology, NIST), nije procenio rezultate NIST evaluacije tehnologije prepoznavanja lica. Izveštaj kontrolora takođe otkriva da NYPD nije uspostavio potreban ili prihvatljiv nivo tačnosti za svoj sistem prepoznavanja lica.[779] Iako služba nastoji da razvije odgovarajuće politike i procedure za specifične tehnologije, one se ne odnose konkretno na veštačku inteligenciju, već su pre priručnici za upotrebu bilo kakvih tehnoloških alata. Ovo se loše odražava na sposobnost i iskrenost NYPD-a u postavljanju delotvornih zaštitnih mehanizama i proceni rizika povezanih sa upotrebom tehnologija biometrijskog nadzora.

Izveštaj kontrolora jedan je od retkih slučajeva da je javnost dobila tačne i relevantne informacije o policijskoj upotrebi sistema veštačke inteligencije. Od uvođenja tehnologije prepoznavanja lica (već 2011), policijska uprava je efikasno uskraćivala javnosti bilo kakve relevantne informacije o svojoj upotrebi tehnologija za prepoznavanje lica. Dok je upotreba tehnologija za prepoznavanje lica u NYPD skrivena, brojne CCTV i kamere koje se nose na uniformi postale su vidljiv i stalni podsetnik na sistem masovnog nadzora građana. Dok je 2017. prijavljeno „samo“ 6.000 kamera za video nadzor,[780] prema procenama iz 2023. ima ih više od 25.000[781] – što je rast od preko 400% za nešto više od šest godina. Štaviše, NYPD-ov program kamera

za nošenje na uniformi najveći je te vrste u SAD, sa 24.000 policijskih službenika opremljenih kamerama.[782] Policiji su tako na raspolaganju video snimci sa oko 50.000 kamera, koji se mogu koristiti za biometrijsku analizu.

Njujorška policija navodi da se tehnologija prepoznavanja lica koristi za identifikaciju osumnjičenih čije su slike snimljene dok su činili krivično delo.[783] Međutim, tvrdi se da poklapanje ne služi kao osnov za hapšenje, već se tretira kao trag za dodatne istražne korake. Policija takođe tvrdi da ne koristi prepoznavanje lica za praćenje i identifikaciju ljudi u masi ili na skupovima. Štaviše, video snimci sa kamera koje se nose na uniformi ne dostavljaju se redovno na biometrijsku analizu, niti se slike neidentifikovanih osumnjičenih rutinski porede sa drugim državnim bazama fotografija (što je, navodno, rezervisano za slučajeve u vezi sa terorizmom).[784]

Pa ipak, valjalo bi zadržati oprez i ne uzimati te tvrdnje zdravo za gotovo. Možda bi čak bilo prikladnije da se informacije o tehnologiji za prepoznavanje lica koje saopštava policija tretiraju kao nepouzdane. Za početak, NYPD se aktivno bori protiv strateških parnica kojima je cilj da rasvetle stvarne prakse i alate koje koristi policijska uprava.[785] Pored toga, njujorška policija ima loše rezultate po pitanju transparentnosti operacija u kojima se koristi prepoznavanje lica, a čak je u određenim slučajevima dovodila javnost u zabludu. Zahvaljujući tome, narušeni su i poverenje javnosti i reputacija policije.

Clearview AI, kompanija koja je sakupila 30 milijardi slika sa Facebooka i drugih društvenih medija i opskrbila NYPD tehnologijom za prepoznavanje lica, detaljno je obrađena na više mesta u ovoj knjizi, ali vredi je ponovo pomenuti u jednom od najgorih primera namernog obmanjivanja javnosti. Njujorška policija je relativizovala svoj odnos sa Clearview AI, tvrdeći čak da nema ni formalne ni neformalne odnose sa kompanijom. Međutim, 2021. godine otkriveno je da je NYPD koristila alat kompanije tokom dugog probnog perioda, a pojedini pripadnici policije su nastavili da ga koriste i pošto je probni period završen.[786] Iako NYPD nije potpisala ugovor sa Clearview AI, policija države Njujork jeste i, kako je saopšteno, sprovela je više od 5.100 pretraga kako bi prikupila potencijalne tragove.[787] Uprkos tvrdnjama da ne koristi tehnologiju prepoznavanja lica na demonstrantima, NYPD aktivno pokušava da uskrati informacije o biometrijskim podacima prikupljenim tokom protesta Black Lives Matter.[788]

Branitelji privatnosti otkrili su 2021. značajan tajni fond za nadzor i pokazali da NYPD nije morala da traži odobrenje od gradskog veća ili bilo kog drugog gradskog funkcionera da koristi ova sredstva. Od 2007. godine, preko svog Fonda za posebne troškove, NYPD je potrošila zapanjujućih 159 miliona dolara na različite alate i servise za nadzor.[789] Tokom 2014. policija je potrošila 800.000 dolara na petogodišnji ugovor sa najvećim izraelskim odbrambenim izvođačem, Elbit Systems, koji je obezbedio mobilne rendgene navodno sposobne da skeniraju vozila u potrazi za oružjem sa daljine od 450 metara. Uprkos upozorenjima zdravstvenih zvaničnika o potencijalnim rizicima od raka koji su povezani sa ovom tehnologijom, policija nije obavestila javnost o njenoj upotrebi.

Policija Njujorka je takođe nabavila simulatore mobilnih lokacija od KeyW Corporation, poznate i kao „otrovne raže“, koji oponašaju antene mobilne telefonije i evidentiraju identifikacione informacije svakog telefona koji se poveže, što policiji omogućava da prati određene osobe bez sudskog naloga.[790] Takođe, policija je nezakonito održavala bazu podataka o otiscima prstiju maloletnika uprkos njenoj nezakonitosti, i redovno unosila slike maloletnika u svoju bazu za prepoznavanje lica.[791]

Javni diskurs oko policijske upotrebe prepoznavanja lica sličan je borbi njujorške zajednice protiv zloglasne politike „zaustavi i pretresi“ – dve prakse koje su, u rukama NYPD, ideološki isprepletene. Prema podacima njujorške policije, od 2002. godine bilo je više od pet miliona slučajeva zaustavljanja i pretresa. Velika većina takvih pretresa vršena je nad pripadnicima rasijalizovanih zajednica, a većina ljudi koji su podvrgnuti pretresima bili su nevini.[792] Bivši gradonačelnik Bill de Blasio, koji je dužnost preuzeo 2014. godine, obećao je da će ukinuti ovu praksu, i zaista, broj zaustavljanja i pretresanja se značajno smanjio.[793] Međutim, nagli pad slučajeva zaustavljanja i pretresanja zabeležen je pre 2014. godine, verovatno zbog tužbi podnetih protiv njujorške policije, ali i kao rezultat oštre kritike javnosti. Bez obzira na zabeleženi pad, rasni disparitet i dalje je visok – mladi crni i Latino muškarci čine samo 5 odsto populacije, u poređenju sa 38 odsto prijavljenih zaustavljanja od strane NYPD. Ne iznenađuje onda što su primenu prepoznavanja lica, sa nižim nivoima preciznosti za rasijalizovane ljude uopšte (a posebno za obojene žene) pomno pratili aktivisti za ljudska prava i privatnost.[794] U svetlu sedam šteta koje su definisali Suresh i Guttag, ovaj primer ilustruje kako se u toksičnom mulju digitalnog i analognog rasizma spajaju sve definisane štete – a posebno istorijske i reprezentativne pristrasnosti, pristrasnost u proceni i pristrasnost u primeni.

U Njujorku postoji upadljiva korelacija između prekomerne policijske kontrole i prekomernog nadzora, gde je nadzor kamerama koje se nalaze na uniformama policajaca najbolji primer. Izveštaj organizacije Amnesty International iz 2022. pokazuje da ovo važi i za CCTV kamere, posebno u crnim i latino kvartovima.[795] Analiza u okviru izveštaja pokazuje da se u popisnim oblastima sa većom koncentracijom rasijalizovanih u Bronksu, Bruklinu i Kvinsu nalazi veći broj kamera u javnom vlasništvu. Štaviše, naselja sa većom stopom incidenata zaustavljanja i pretresa povezana su sa postavljanjem većeg broja CCTV kamera. Analizom su čak identifikovane rute koje pokazuju značajno viši CCTV nadzor i veću verovatnoću pretresa. Kako ističe Matt Mahmoudi iz Amnesty Internationala: „Odavno znamo da je zaustavljanje i pretresanje u Njujorku rasistička policijska taktika. Sada znamo da su zajednice koje su najviše na meti ove prakse takođe izložene većem riziku od diskriminatorne policijske kontrole putem invazivnog nadzora.“[796]

Javna dostupnost podataka koji potvrđuju nesrazmerno targetiranje rasijalizovanih grupa, omogućila je aktivistima da stave politiku zaustavljanja i pretresanja NYPD-a pod lupu. Međutim, sada su od javnosti skriveni relevantni podaci o upotrebi prepoznavanja lica, gde možemo da se oslonimo samo na odabrane i potencijalno nepouzdane podatke koje „proaktivno“ objavljuje policija. Na primer, prema NYPD, u njihovoj primeni tehnologije za prepoznavanje lica između 2011. i 2017. zabeleženo je samo pet slučajeva pogrešne identifikacije. S druge strane, advokat-supervizor Jerome Greco iz organizacije Legal Aid Society, koja zastupa klijente u slučajevima prepoznavanja lica što je bilo od ključnog značaja u naporima da se njujorška policija primora da otkrije 58 ugovora sa kompanijama za nadzor, tvrdi da su kriterijumi za određivanje šta predstavlja grešku u poređenju nejasni.[797] Drugo pitanje je odsustvo bilo kakvih smernica ili standarda u vezi sa slikama koje policija može da dostavi na analizu za prepoznavanje lica. U praksi, na analizu se šalje veliki broj „fotografija iz istrage“, uključujući izmenjene fotografije, crteže, pa čak i slike ljudi koji liče na slavne ličnosti. Zbog lošeg kvaliteta fotografija osumnjičenih, njujorška policija je čak pribegavala korišćenju fotografija glumca Woodyja Harrelsona i košarkaša gradskog tima u odvojenim slučajevima u kojima su policajci verovali da osumnjičeni liče na poznate ličnosti.[798] U okviru projekta javne kontrole nadzorne tehnologije (Surveillance Technology Oversight Project, STOP)[799] pribavljena je evidencija koja potvrđuje da je NYPD koristila prepoznavanje lica približno 22.000 puta u periodu od 2016. do 2019.[800] Uprkos tvrdnji NYPD-a da nije bilo nezakonitih hapšenja, protiv policije je podneto najmanje pola tuceta tužbi u vezi sa korišćenjem tehnologije za prepoznavanje lica.

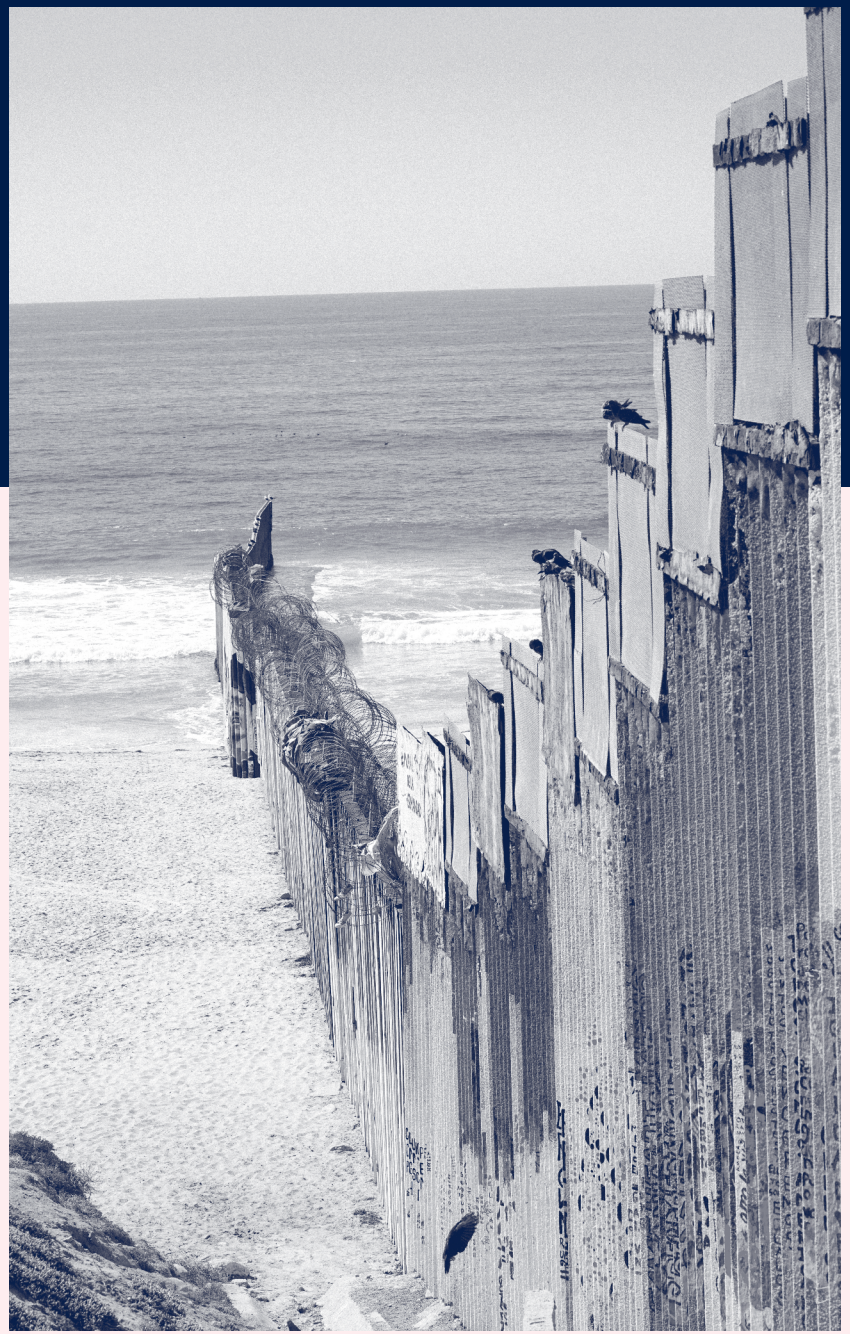
Istaknuti aktivista pokreta Black Lives Matter, Derrick Ingram, optužen je 2020. za napad na policajca jer je vikao u megafon blizu uha policajca. Kada je policija došla u Ingramov stan, navodno je posedovala dokument pod nazivom Informativni izveštaj odseka za identifikaciju lica, čime je nenamerno potvrdila da je NYPD koristila prepoznavanje lica na učesnicima demonstracija pokreta Black Lives Matter.[801] Dostupni dokazi sugerišu da je NYPD, uprkos svojim zvaničnim politikama, koristila prepoznavanje lica za identifikaciju demonstranta i, čini se, za te potrebe izmislila krivičnu prijavu, dok su neosnovan četvoročasovan pretres stana u vojnom stilu policijske snage iskoristile da pošalju političku poruku aktivistima.[802] Kada je policija odustala od prekršajne prijave, Ingram je podneo tužbu tvrdeći da je žrtva kampanje zastrašivanja, uznemiravanja i manipulacije, pri čemu se policija oslanjala na izmišljene dokaze kao opravdanje za brutalnu represiju.[803]

Dok država Njujork trenutno nema propise koji bi to sprečili, kako je opisano u pravnom poglavlju ove knjige, pet američkih država (Vašington, Kolorado, Mejn, Virdžinija i Alabama) zabranjuju svojim službama za sprovođenje zakona da koriste poklapanje iz alata za prepoznavanje lica kao osnovanu sumnju onako kako je to NYPD izgleda uradila u Ingramovom slučaju. U tom konkretnom primeru vidimo da je, mada su u igri verovatno bile mnoge štete kako su ih definisali Suresh i Guttag, izvor štete bila ogromna pristrasnost u primeni.

Spoj nekoliko faktora doprineo je razvoju ekspanzivnog sistema policijskog nadzora u Njujorku. Služba je koristila skrivene tokove finansiranja da bi pribavila napredne tehnologije za nadzor. Takođe, njujorška policija je izradila interne procedure i smernice za korišćenje takvih tehnologija, što je doprinelo stvaranju sistema kojem praktično u svakoj tački nedostaje transparentnost i odgovornost.[804] Još uvek ima mnogo nepoznanica u vezi sa efikasnošću primene tehnologije za prepoznavanje lica. S obzirom na njenu istoriju neprikladnog postupanja, dok se ne pruže dodatni dokazi sve podatke koje je njujorška policija dostavila javnosti na ovu temu treba posmatrati kao nepouzdane i selektivne.

Slučaj iz Njujorka ilustruje opravdana očekivanja da će upotreba tehnologije nadzora verovatno pojačati postojeće rasne disparitete u ishodima i posledicama aktuelne policijske prakse i politike. Rasijalizovane zajednice nalaze se na meti prekomerne policijske kontrole i nadzora,

što može da izazove efekat zebnje na korišćenje prava i sloboda njihovih članova – na primer, koliko se osećaju sigurno i slobodno da se pridruže protestu pokreta Black Lives Matter. To uvećava verovatnoću pogrešne identifikacije pripadnika rasijalizovanih zajednica (jer su statistički više izloženi nepreciznim tehnologijama), što je dodatno otežano činjenicom da je tehnologija za prepoznavanje lica sklona greškama pri identifikaciji ne-belih ljudi. Čini se da je produbljivanje rasnih dispariteta neizbežan ishod korišćenja tehnologije za nadzor i intenziviranje policijske kontrole rasijalizovanih i minorizovanih zajednica.



BANOPTIKON: JEDNAKOST DISKRIMINACIJE LJUDI U POKRETU

U ovom poglavlju smo već razmotrili kako tehnologije za prepoznavanje lica i drugi oblici (masovnog) biometrijskog nadzora imaju naročit uticaj na minorizovane, rasijalizovane i obespravljene grupe. Ništa drugačija situacija nije ni kada je u pitanju nadzor državnih granica. U povremenim izbegličkim krizama na spoljnim granicama EU i SAD, iznova se pokazuje kako ljudi u najranjivijem položaju snose najveći teret eksperimentalnih tehnologija koje se primenjuju pod maskom nacionalne bezbednosti i navodne humanitarne zaštite.

Mada se implementacija biometrijskog sistema Evropske unije za ulazak i izlazak (Entry/Exit System, EES), koji će olakšati prelazak granice za sve stanovnike šengenskog prostora, već više puta odlaže zbog rizika u sistemu,[805] to se ne može reći za nekoliko aktivnih sistema nadzora luka i granica koji se koriste za praćenje ljudi u pokretu, posebno izbegličke i migrantske populacije. Vlade širom sveta eksperimentišu sa upotrebom prepoznavanja lica i drugih biometrijskih tehnologija na svojim granicama, gde se ljudi u pokretu nepravedno profilišu, a njihovi lični podaci prikupljaju i čuvaju bez odgovarajuće saglasnosti, što takođe predstavlja rizik kriminalizacije već i same namere migriranja (što predstavlja kršenje međunarodnog izbegličkog prava).[806] U mnogim zemljama, ova tehnologija je takođe povezana sa praksama nasilnog potiskivanja, tj. kolektivnog proterivanja, obično pre nego što stignu do određene zemlje ili teritorije, često na veoma opasne načine.[807] Povrh svega, analize pokazuju da je širom evropskih zemalja minorizovana i ne-zapadna imigrantska populacija izložena većem riziku od diskriminacije i kriminalizacije od strane nacionalnih policijskih struktura.[808]

Profesor Didier Bigo problematizuje koncept „banoptikona“ (ban, eng. zabrana; igra reči koja tradicionalni pojam panoptikona stavlja u kontekst kontrole, odnosno zabrane pristupa) objašnjavajući kako određene društvene grupe postaju predmet stalnog nadzora u vezi sa transnacionalnim bezbednosnim praksama. Kao takav, banoptikon postavlja targetiranu grupu (minorizovani ljudi u pokretu) kao isključenu iz normalizovanih

društvenih struktura zbog njihovog budućeg potencijala za poremećaje (kroz profilisanje), na čemu se zasniva pravno isključenje i podupire sprovođenje uskraćivanja slobodnog kretanja (normativni imperativ mobilnosti).[809] To strukturama moći omogućava da kod većine stvore osećaj sigurnosti, uprkos stalnoj klimi straha i neizvesnosti koja muči nacionalne države pod preuveličanim pretnjama terorističkih ili drugih oblika napada na suverenitet. Grupe „Drugih“ u pokretu podvrgavaju se preteranoj kontroli onako kako pripadnici većine nikada neće biti, što isključene grupe dovodi u veći rizik od praksi dehumanizacije, obično u ime bezbednosti.[810] Još jedan ključni Bigoov uvid kaže da, za razliku od Panoptikona, ove strukture nisu centralizovane ili homogenizovane, što im omogućava da zabace mnogo širu mrežu i koriste različite tehnike da ostvare svoje namere.

HIPERION I KENTAUR: POLITIKA NADZORA NA GRANICAMA GRČKE

Industrijski kompleks za nadzor granica postaje sve veća realnost za zemlje na graničnom frontu masovnih migracija.[811] U Evropi je primarna tačka ulaska ljudi u pokretu najčešće Grčka, što ovu zemlju pozicionira kao testni poligon za neke od najvećih državnih agencija EU gde isprobavaju tehnologije i metode protiv ljudi u pokretu. Među njima je i Evropska agencija za graničnu i obalsku stražu, Frontex, koja se bavi bezbednošću granica i obale u zemljama članicama EU i zemljama Šengena.[812] Već godinama, tačnije od migrantske krize 2015, i Grčka i međunarodne policijske službe nalaze se pod pojačanom pažnjom javnosti zbog primene invazivnih tehnologija nadzora. Sistemi nadzora takođe su, po pravilu, u upotrebu uvedeni na netransparentan i štetan način, često uzrokuju diskriminaciju tražilaca azila i koriste se u masovnim nasilnim potiskivanjima na moru, što predstavlja kršenje međunarodnog izbegličkog prava. Samo tokom 2022. godine, pokazala je jedna analiza, zabeleženo je preko 200.000 nezakonitih potiskivanja sa spoljnih granica EU, pri čemu je Grčka odgovorna za više od 26.000 slučajeva.[813]

Šteta koju ovi sistemi nanose ljudima u pokretu temeljno je dokumentovana i dokazano doprinosi stvaranju neprijateljske klime za ljude koji žele da migriraju u druge zemlje usled rata, gladi, pretnji progonom ili ekonomskih problema. U svom izveštaju za 2022, Balkanska istraživačka mreža (BIRN) konstatuje da je sredstva za oporavak od pandemije koja je obezbedila EU, Grčka koristila za implementaciju dva nova sistema za praćenje ljudi u

pokretu i u improvizovanim izbegličkim kampovima, čiji je razvoj planiran od 2020. Ta dva sistema, nazvana Hiperion i Kentaur, prate ulaske i izlaske iz azilantskih kampova u zemlji uz pomoć algoritama za analizu ponašanja, kao i identifikaciju otisaka prstiju, i šalju CCTV i snimke sa dronova direktno Ministarstvu za migracije i azil.[814] U svojim zvaničnim dokumentima, Ministarstvo o ovim algoritmima ili sistemu za otiske prstiju ne govori kao o biometriji. BIRN-ovo istraživanje utvrdilo je da pre uvođenja ovih sistema nisu utvrđene odgovarajuće zaštitne mere (ako su takve mere uopšte moguće, s obzirom na ogromnu neravnotežu moći), pri čemu grčka vlada nije imenovala službenika za zaštitu podataka niti je sprovela procene uticaja za oba sistema, uprkos obavezama iz GDPR-a. U martu 2022. godine, brojne organizacije iz Grčke i širom Evrope podnele su zahtev za istragu ovih sistema, što je Helenska uprava za zaštitu podataka i učinila.[815] Međutim, nema napretka u tom slučaju, a Uprava nije objavila nikakve dodatne informacije.

Jedna od istraživačkih NVO, grčka organizacija Homo Digitalis, ranije je takođe izrazila zabrinutost u vezi sa namerama Obalske straže Grčke da nabavi sisteme za praćenje društvenih medija koji bi se koristili za praćenje aktivnosti tražilaca azila, kao i za pristup njihovim informacijama, uključujući privatnu komunikaciju, slike, video snimke i tekstualne objave.[816] Obim sistema koje grčke vlasti uspostavljaju za praćenje tražilaca azila ozbiljno narušava ljudska prava i slobode koje su zajednicama u pokretu garantovane nizom međunarodnih dokumenata. Duboko invazivne strukture za nadzor predstavljaju ozbiljnu pretnju i rizik od opasnog presedana koji bi mogao da podstakne druge zemlje da slede njihov primer. Nezakonite i dehumanizujuće prakse u kontroli granica već su dokumentovane u drugim članicama EU, kao što su Mađarska[817] i Hrvatska,[818] koje bi mogle biti potencijalne buduće tačke za primenu biometrijskih tehnologija masovnog nadzora. To bi doprinelo kontinuiranoj sekuritizaciji zaštite granica i kriminalizaciji migracija. Takav primer takođe naglašava zašto je toliko važno da naša definicija masovnog biometrijskog nadzora obuhvati arbitrarno ciljani nadzor, kao što je nadzor ljudi u pokretu.

Pismo upućeno 2022. donosiocima odluka u EU, koje je inicirala grupa organizacija civilnog društva, uključujući Access Now, European Digital Rights (EDRi), Platformu za međunarodnu saradnju u slučajevima nedokumentovanih migranata (PICUM) i Laboratoriju za izbegličko pravo, zahtevalo je jačanje garancija za zaštitu zajednica gurnutih na marginu, kao i ljudi u pokretu, u odredbama o visokorizičnim sistemima veštačke inteligencije iz predloga zakona o veštačkoj inteligenciji.[819] Pismo su potpisale 42 organizacije, a u njemu se detaljno opisuju načini na koje su ove zajednice izložene većem riziku targetiranja sistema. U apelu se posebno pominju nove tehnologije koje se testiraju na graničnim prelazima, kao što su daljinska biometrijska identifikacija (RBI), prepoznavanje emocija, biometrijska kategorizacija i automatizovane procene rizika.

Nagoveštavajući važnu pobedu, dva odbora Evropskog parlamenta glasala su početkom maja 2023. godine za unošenje zaštitnih mera u predlog zakona o veštačkoj inteligenciji, kojima bi se zabranilo nekoliko vrsta upotrebe tehnologije za prepoznavanje emocija (uključujući primene za sprovođenje zakona i kontrolu migracija), biometrijska kategorizacija, daljinska biometrijska identifikacija u javno dostupnim prostorima i prediktivni policijski sistemi.[820] Iako su ovaj potez pozdravile mnoge organizacije civilnog društva širom Evrope, ističe se da još uvek predstoji dug put kada su prediktivni sistemi u pitanju. Na primer, sistemi prediktivne analitike koji nisu bili obrađeni u nacrtu uredbe, čine ključnu komponentu za policijsko praćenje i ometanje migratornih kretanja. Štaviše, kao što se u ovoj knjizi navodi u odeljku o pravu EU, iako je Evropski parlament kroz uredbu o veštačkoj inteligenciji uveo fomalnu zabranu RBI u javnim prostorima, čini se da ova zabrana ne uključuje granične prelaze, prihvatne centre i/ili kampove. Naime, prema uredbi, policija sme da koristi nadzorne sisteme sa biometrijskim kapacitetima na graničnim prelazima i pri nadgledanju populacija u pokretu, izbeglica i migranata koji prelaze granice i nastoje da uđu u EU.[821]

Takođe je važno napomenuti da je početkom 2025. Evropski sud za ljudska prava proglasio Grčku krivom za „sistematsko“ odbijanje tražilaca azila i njihovo proterivanje preko granice na teritorije susednih zemalja.[822] Presuda iz Strazbura potvrdila je sumnje organizacija za ljudska prava koje su godinama tvrdile da su ove nezakonite deportacije faktički bile u skladu sa zvaničnom imigracionom politikom ove članice EU.[823] Korišćenje tehnologija za prepoznavanje lica i prikupljanje drugih biometrijskih podataka od marginalizovanih grupa koje su već među najobespravljenjim društvenim grupama, predstavlja flagrantnu zloupotrebu i derogaciju ljudskih prava i sloboda.

FACEBOOK ZA PALESTINCE: DRAKONSKA UPOTREBA BIOMETRIJSKOG NADZORA U IZRAELU

Prekomerna policijska kontrola palestinskih stanovnika Izraela decenijama raste, u čemu biometrijski sistemi nadzora imaju sve značajniju ulogu. Izraelska vlada je 1999. godine počela da koristi softver za prepoznavanje lica na Palestincima kako bi nadgledala osobe sa radnim vizama koje ulaze na teritoriju.[824] Izrael kontroliše sve ulazne i izlazne tačke na Zapadnoj obali, a ova kontrola je efektivno pojednostavljena korišćenjem široke CCTV mreže i baza podataka, uključujući biometrijske podatke Palestinaca.[825] Takva postavka savršeno ilustruje kako se softver, hardver i baze podataka uklapaju u sistem kažnjavanja i ugnjetavanja. Pravo palestinskog naroda na kretanje i pravo na privatnost grubo su narušeni ovim praksama, u kojima su tretirani kao hodajući bar-kodovi, što bi trebalo da služi kao alarmantno upozorenje na razmere zloupotreba do kojih masovni biometrijski nadzor može da dovede u zajednicama širom sveta.

Noviji razvoj događaja u Izraelu istražen je u izveštaju „Automatizovani aparthejd“, koji je Amnesty International objavio 2023. sa fokusom na sistem nazvan „Crveni vuk“.[826] Ovaj sofisticirani sistem masovnog biometrijskog nadzora povezuje lica Palestinaca snimljena na terenu sa postojećim ličnim podacima koji se skladište u vladinim i vojnim bazama podataka. Takođe omogućava izraelskoj vojsci da trenira sistem povezujući lica civila sa ličnim dokumentima, sve dok ne počne automatski da prepoznaje pojedince i proverava prethodno prikupljene informacije kako bi procenio da li mogu da prođu vojne kontrolne punktove ili ih treba zaustaviti i uhapsiti. Sve se to, naravno, radi bez saglasnosti, niti su Palestinci informisani o načinu na koji se njihovi lični podaci čuvaju i koriste, ili koliko dugo. Kapaciteti ovog sistema još uvek nisu do kraja jasni spoljnim istraživačima, pa ni Palestincima koji su mu podvrgnuti. Amnesty International je takođe identifikovao Hikvision i TKH Security sa sedištem u Holandiji kao dobavljače većeg dela tehnologije za nadzor koja se tamo koristi.[827]

Osim što koristi biometrijske sisteme za prepoznavanje lica, Izrael je takođe duboko upleten u njihovo stvaranje. AnyVision Interactive Technologies je izraelski tehnološki startap koji proizvodi i distribuira sisteme za prepoznavanje lica sa obimnim kapacitetima za masovni biometrijski nadzor. Kompanija tvrdi da se njihov softver povezuje sa bilo kojom kamerom i da se njime lako upravlja, čak i ako operatori imaju ograničene računarske veštine ili resurse.[828] Ova kompanija se takođe povezuje sa strogo poverljivim projektima izraelske vojske u vezi sa nadgledanjem Palestinaca na kontrolnim punktovima. Takođe, pojavile su se informacije da je njihov softver korišćen na Zapadnoj obali za stalno posmatranje stanovnika te teritorije.[829]

Izraelska vlada je radila na integraciji svojih baza podataka sa biometrijskim podacima palestinskih stanovnika, dok oprema vojne snage telefonima sa tehnologijom prepoznavanja lica. Pametni telefoni pristupaju bazama podataka preko skenova lica, što vojnicima omogućava da na licu mesta ispituju ili pritvaraju Palestince koji pokušaju da prođu kroz kontrolne punktove, pa i unutar granica Zapadne obale. Ovaj sistem je poznat kao „Plavi vuk“ i predstavlja ekstenziju baze „Čopor vukova“, u kojoj se sve privatne informacije inicijalno skladište. Prema izveštajima, vojnici ga među sobom nazivaju „Fejsbuk za Palestince“.[830] Za ovako intruzivan slučaj upotrebe, taksonomija štete koju su ponudili Suresh i Guttag verovatno je ograničena: jasno je da čak ni tehnički najsavršeniji sistem ne bi učinio ništa da ublaži razmere u kojima su Palestinci rutinski izloženi kontroli i ugnjetavanju na načine koje omogućavaju biometrijski alati za masovni nadzor.

Od početka okupacije Gaze u oktobru 2023. godine, izraelska vojska se značajno oslanja na primenu nadzornih i biometrijskih tehnologija za sprovođenje napada na Palestince. „Lavanda“ predstavlja jedan od najsofisticiranijih AI alata koji gotovo u potpunosti eliminiše takozvani ljudski faktor pri kreiranju „spiska za odstrel“, koji navodno sadrži imena palestinskih vojnika i članova Hamasa, ali u realnosti cilja mnogo veći broj

civila, uključujući žene i decu. Kako se navodi u izveštajima, tokom prvih meseci rata, izraelske odbrambene snage su koristile ovaj sistem kako bi odredile mete za bombardovanje i atentate. Drugi automatizovani sistem, „Where's Daddy", korišćen je kako bi se mete locirale, ali i da bi se sačekala potvrda da su ušle u svoj dom pre nego što bi se lansirao napad, što povećava šanse da žrtva bude eliminisana, često sa čitavom svojom porodicom.[831] Korišćenje ovih sistema otkriveno je nakon početka rata i pokazuje na koji način se veštačka inteligencija razvija kao sredstvo ratovanja sa dvojakim svojstvom – prvo, sistem preuzima „odgovornost" za donošenje odluka i samim tim doprinosi otklanjanju osećaja krivice ili oklevanja vojnika kada dobiju naredbu da pokrenu napad, i drugo, automatizuju napade što omogućava dodatnu dehumanizaciju i distanciranje od nevidljivih žrtava koje su napadnute iz udaljenih dronova po direkcijama sistema bez lica.

IZMEĐU DVA ZLA: CENTRALNA AMERIKA I JUŽNA GRANICA SAD

Princip nevraćanja u represivnu državu predstavlja fundamentalni aspekt međunarodnog migracionog pravnog sistema, koji se nažalost krši prisilnim potiskivanjem, pritvaranjem i deportacijom tražilaca azila u treće zemlje, koje se često pogrešno nazivaju „sigurna treća zemlja" ili „prva zemlja azila".[832] Poslednjih decenija, u usponu je globalni trend eksternalizacije, ofšoringa i autsorsovanja obrade zahteva za azil u susednim, pa čak i udaljenim zemljama. Ovakav pristup je pokušaj da se tražioci azila spreče da uopšte stignu do granice željene države.[833] Kako smo u ovom poglavlju već pokazali, to se može videti na granicama EU i SAD.

Nesputana prisilna potiskivanja izbeglica kroz presretanje na moru, uz mogućnost pritvaranja u Gvantanamu ili deportacije u daleke latinske zemlje, gurnulo je tražioce azila na nove migratorne rute dalje od obale. To se jasno pokazalo 2013. kada je Meksiko (zemlja porekla mnogih američkih imigranata) postao tranzitna zemlja, a četvrt miliona migranata uhapšeno na američko-meksičkoj granici. U poslednjoj deceniji, SAD su mnogo uložile u autsorsovanje operacija koje se bave ljudima u pokretu, a sve sa ciljem da ih spreče da ikada stignu do meksičke granice. Tako je od 2020. godine Panama u svojoj južnoj provinciji Darijen pritvorila mnoge

transkontinentalne tražioce azila, uključujući 2000 Haićana.[834] Panamske službe za upravljanje migracijama dobijaju značajnu podršku američkog Ministarstva za unutrašnju bezbednost. Sjedinjene Države su sa Meksikom i sve tri zemlje tzv. Severnog trougla (El Salvador, Gvatemala i Honduras) potpisale sporazume o „sigurnoj trećoj zemlji", odnosno o saradnji u pitanjima azila.[835]

Pored autsorsovanja sprovođenja migratornih politika, razmena biometrijskih i drugih ličnih podataka izbeglica i migranata je još jedan element širokog okvira saradnje osmišljene da fizički spreči grupe u pokretu da stignu do američke granice. Sjedinjene Države su potpisale neobavezujuće memorandume sa Meksikom 2017.[836] a 2019. sa zemljama Severnog trougla,[837] koji uređuju razmenu biometrijskih podataka ljudi u pokretu u okviru Međunarodnog programa za razmenu biometrijskih informacija (International Biometric Information Sharing Program, IBIS).[838]

Međutim, ne postoji odgovornost država i aktera usled odsustva transparentnosti, nejasne prirode operacija na terenu, kao i uopštenog jezika i neobavezujuće prirode sporazuma.[839] To otežava, a praktično i onemogućava sprovođenje nezavisne procene uticaja na ljudska prava (mada je posledična ljudska patnja vrlo vidljiva). Organizacije za civilnu kontrolu predlažu uvođenje mera za zaštitu ljudskih prava migranata koje bi podrazumevale usvajanje zakona o zaštiti podataka u svim relevantnim zemljama; zabranu masovnog profilisanja, prediktivnih analiza i intruzivnog praćenja geolokacije; ograničavanje pristupa ličnim podacima; obezbeđivanje posebne zaštite dece; obavezu pribavljanja informisane saglasnosti za obradu biometrijskih podataka; i obezbeđivanje sprovođenja prava na zaštitu podataka (posebno u pogledu pristupa, ispravke, brisanja i prigovora).[840]

Razmena podataka sa inostranstvom duboko se ukorenila u upravljanje migracijama u SAD, što je rezultiralo brojnim kršenjima pravičnog postupka i građanskih prava. Neproverene informacije inostranih policijskih snaga dele se preko mreže i stavljaju na raspolaganje američkoj Carinskoj i graničnoj službi (Customs and Border Protection, CBP) kao i Službi za imigraciju i carinu (Immigration and Customs Enforcement, ICE). Dok službenici CBP-a proveravaju ljude na granici sa SAD, pripadnici ICE-a koriste dostavljene informacije kao osnovu za pritvor i/ili deportaciju.[841] Međutim, dokumentovani incidenti pokazuju ozbiljne probleme sa tačnošću ovih podataka. Podatke su dostavile strane policijske snage za koje je američka administracija konstatovala da rutinski krše ljudska prava i slobode i da se upuštaju u koruptivno ponašanje. Na primer, jedan tražilac azila sklonio se iz svoje zemlje jer su ga policajci zastrašivali i tražili od njega da lažno svedoči, da bi se našao u pograničnom pritvoru zbog zlonamernih podataka o njemu koje je dostavila ista policija od koje je bežao.[842] Prilikom odlučivanja o slučajevima migracija, administracija i pravosuđe SAD često koriste informacije o navodnim vezama sa kriminalnim bandama, uprkos tome što ne postoje nikakva jasna sredstva za proveru validnosti ili osnova. Organizacija National Immigrant Justice Center pružila je pravno savetovanje za više od stotinu roditelja razdvojenih od svoje dece i utvrdila da su u najvećem broju slučajeva ljudi bivali označeni kao povezani sa kriminalnom bandom bez odgovarajućeg postupka ili pratećih dokaza.[843]

Sprovođenje migracione politike SAD imalo je očigledno štetan uticaj na prava i slobode ljudi u pokretu. Nesputano prisilno potiskivanje na pomorskim migratornim rutama preusmerilo je ljude u pokretu na kontinentalne puteve, što je povećalo migracioni pritisak na američko-meksičku granicu i podstaklo SAD da ulože velika sredstva u kapacitete zemalja Severnog trougla da pronađu, privedu i deportuju migrante. To je migrante prinudilo da se kreću sve opasnijim rutama van domašaja lokalnih vlasti koje finansiraju SAD. Jedna takva ruta je ozloglašeni Darien Gap – oblast bez puteva[844] i zakona u planinskim prašumama Kolumbije i Paname,[845] gde su „pljačka, silovanje i trgovina ljudima podjednaka opasnost kao divlje životinje, insekti i nedostatak pijaće vode".[846]

Teško je izračunati konačnu ljudsku cenu američke imigracione politike.[847] Ovaj ogroman poduhvat, čiji je jedini cilj da ljude u pokretu spreči da se približe američkoj granici, oslanja se na eksternalizaciju i autsorsovanje izvršnih operacija u zemlje Centralne Amerike, što ne bi bilo moguće bez prekogranične razmene ličnih podataka ljudi, uključujući i biometriju. Mada ti podaci nisu pouzdani (posebno informacije o vezama sa kriminalnim bandama), uzimaju se zdravo za gotovo, i određuju sudbinu migranata i njihovih porodica. Negativne uticaje na ljudska prava zanemaruju i SAD i zemlje Centralne Amerike – prve su se zadovoljile širenjem dometa sprovođenja svoje politike dalje od granice kroz eksternalizaciju i autsorsovanje, a druge nastoje da sačuvaju i prošire američka ulaganja u eksternalizaciju i autsorsovanje procesuiranja tražilaca azila.

U avgustu 2024. godine u javnost je dospela informacija da je američko ministarstvo za unutrašnju bezbednost počelo da istražuje načine kako da uspostavi višegodišnje praćenje migranata i izbeglica uz pomoć tehnologija za prepoznavanje lica. Posebno zabrinjava to što se korišćenje ovakvih tehnologija razmatra i u slučajevima maloletne dece, čak i kada imaju samo nekoliko godina, što predstavlja neistraženu teritoriju i postavilo bi opasan presedan.[848]

PRIVATIZACIJA TEHNOSOLUCIONIZMA: UPOTREBA BIOMETRIJE U PRIVATNOM SEKTORU

Ova oblast donekle se razlikuje od slučajeva koji su već obrađeni u ovoj knjizi, u kojima su države odgovorne za praksu masovnog biometrijskog nadzora. U prethodnim slučajevima, privatne kompanije su igrale različite sporedne uloge, kao fasilitatori i podstrekači, ali ovde zauzimaju centralno mesto. Tradicionalno, za razliku od vlada, privatni subjekti nisu odgovorni za dobrobit građana i stanovnika. Motivisani su profitom i stoga rade u interesu njegovog generisanja – kako je tehnički deo ove knjige jasno pokazao. Ipak, kompanije nisu lišene svake odgovornosti i takođe bi trebalo da odgovaraju za tehnologije koje primenjuju. Zapravo, sa pojavom Vodećih principa UN-a o poslovanju i ljudskim pravima, sve više pravnih sistema razmatra ili implementira jasne obaveze kompanija u poštovanju ljudskih prava.[849] U ovom odeljku razmatramo tri specifična aspekta privatne, profitne implementacije biometrijskih sistema nadzora koja je u porastu širom sveta.

NASMEŠENA LICA I KONTROLISANI PROSTORI: BIOMETRIJA U MALOPRODAJI

Na prvi pogled, upotreba tehnologije za prepoznavanje lica i drugih biometrijskih tehnologija mogla bi da evocira slike kupaca koji robu plaćaju selfijima ili otiskom prsta – što po sebi predstavlja rizik, kako ćemo objasniti u jednoj od narednih studija slučaja. Ali načini na koje se kupci mogu pratiti dok se kreću kroz prodavnice predstavlja urgentan problem koji je dosad retko bio u prvom planu. CCTV i drugi „tradicionalni“ sistemi za nadzor već dugo se koriste u maloprodajnoj industriji. Međutim, pojedini maloprodajni lanci u poslednje vreme unapređuju svoje sisteme kako bi uključili upotrebu tehnologija za prepoznavanje lica, koje su intruzivnije jer se često oslanjaju na biometrijske podatke.

Glavno opravdanje za korišćenje nadzora u prodavnicama obično se nalazi u bezbednosnim razlozima. Međutim, mi tvrdimo da bezbednost ne pruža dovoljno opravdanje za prikupljanje i zadržavanje ličnih podataka, s obzirom na dostupnost manje intruzivnih alternativa. To je posebno tačno kada kupci nisu ni svesni da su pod nadzorom u prodavnicama, kao što je bio slučaj sa tri velika australijska maloprodajna lanca.[850]

Nakon što je grupa potrošača otkrila da australijski maloprodajni giganti Bunnings, Kmart i The Good Guys tajno koriste tehnologije prepoznavanja lica za praćenje kupaca, pokrenuta je šira rasprava u javnosti o korišćenju i zadržavanju ličnih podataka. CHOICE, grupa za zastupanje potrošača, ispitala je više vodećih maloprodajnih lanaca u Australiji i otkrila da samo tri prikupljaju i čuvaju biometrijske podatke preko svog softvera za prepoznavanje lica. Grupa je takođe istakla da su fizički znaci postavljeni u prodavnicama, koji bi trebalo da obaveste kupce da će u prodavnicama biti podvrgnuti tehnologiji prepoznavanja lica, bili premali, odnosno da ih je lako prevideti.[851]

Obe ove prakse predstavljaju potencijalno kršenje australijskog Zakona o privatnosti, koji predviđa proporcionalnost prikupljanja osetljivih podataka, uključujući biometriju. Zakon takođe obavezuje rukovaoce da prikupljanje podataka mora odgovarati svrhama poslovanja, što bi zahtevalo detaljnije objašnjenje kompanija koje koriste ove tehnologije. U skladu sa svojim zapažanjima, CHOICE je zatražio od Kancelarije australijskog poverenika za informacije (OAIC) da istraži praksu trgovaca u vezi sa korišćenjem prepoznavanja lica i prikupljanja biometrijskih podataka.[852] Čim je OAIC najavio istragu, sve tri kompanije su obustavile upotrebu tehnologije.[853] U februaru 2023, OAIC je najavio da će istraga Kmarta i Bunningsa biti završena do jula.[854] Nakon kratke pauze, istraga je zvanično pokrenuta na leto 2024. pa je sredinom novembra zvanično utvrđeno da je Bunnings prekršio privatnost stotina hiljada građanki i građana svojim neselektivnim nadzorom svih kupaca u periodu od 2018. do 2022. godine.[855] Iako je australijski poverenik jasno ukazao na činjenicu da je hipermarket narušio privatnost svojih kupaca, Bunnings je najavio žalbu na odluku i tvrdi da je tehnologije za nadzor u svojim radnjama koristio u skladu sa zakonom.

Kancelarija poverenika takođe je saopštila da je odustala od istrage lanca The Good Guys, jer je kompanija na početku istrage saopštila da će obustaviti upotrebu prepoznavanja lica.[856] Pritužba koju je podneo CHOICE 2022. zbog korišćenja biometrijskih podataka, u velikoj meri se oslanjala na prethodni slučaj u vezi sa lancem megamarketa 7-Eleven, koji je koristio prepoznavanje lica na svojim tabletima u prodavnicama kako bi ocenio zadovoljstvo kupaca. Kompanija je tvrdila da obrada slika lica ne predstavlja kršenje Zakona o privatnosti, tvrdeći da se podaci ne koriste za identifikaciju i praćenje pojedinaca. Međutim, praksa je prekinuta nakon istrage OAIC-a, u kojoj je utvrđeno da nema dokaza da su biometrijski podaci neophodni za procenu iskustva kupaca u radnji, a 7-Eleven je obavezan da izbriše sve prethodno prikupljene podatke o kupcima.[857]

U sličnom slučaju, Amazon, koji je 2021. hvaljen jer je navodno zabranio policiji da koristi njegov softver za prepoznavanje lica, bio je umešan u dva slučaja obmanjujućeg prikupljanja biometrijskih podataka u svojim fizičkim prodavnicama „Go“ u Njujorku.[858] Podnosioci tužbe su naveli da prodavnica nije na odgovarajući način istakla tablu sa obaveštenjem da se na ulazu prikupljaju biometrijski podaci kupaca.[859]

Drugi slučajevi otkrivaju kako se prepoznavanje lica koristi za dodatno praćenje kupaca, na primer sistemi koji sprečavaju kupce da skeniraju pogrešnu stvar na samouslužnim kasama.[860] Pored toga, raste zabrinutost zbog hiperpersonalizovanih cena, pošto ne postoji izvodljiv način da se utvrdi gde maloprodajne prodavnice podvlače crtu kada imaju pristup tako osetljivim informacijama o potrošačima.[861] To bi značilo da prodavnice mogu da targetiraju pojedine kupce koji često koriste aplikacije za kupovinu njihovih proizvoda i doteruju cene na osnovu prikupljenih informacija. Iako su prakse hiperpersonalizacije u primeni duže od decenije,[862] uvođenje tehnologije za prepoznavanje lica otvara sasvim novo područje rizika, posebno ako se ove prakse previše koriste i nedovoljno regulišu.[863] Zahvaljujući takvoj upotrebi tehnologija biometrijskog nadzora, sveprisutno onlajn praćenje, na primer na platformama društvenih medija, protiv kog se grupe za digitalna prava bore godinama, preliva se u oflajn prostore.

Stoga je transparentnost ključno sredstvo u nastojanjima da zloupotrebe takvih praksi ne ostanu van kontrole (ili da se spreče) i može podstaći kompanije da pažljivije rukuju podacima svojih klijenata. To posebno važi za proizvode koji prikupljaju osetljive podatke, kao što je Amazonova Alexa, koja prikuplja i čuva glasovne podatke, kao i druge proizvode koji se oslanjaju na biometrijske karakteristike i senzore.[864]

Korišćenje biometrijskih podataka za identifikaciju kupaca potencijalno predstavlja brojne oblike štete – kao prvo, pogrešna identifikacija će se sigurno desiti, a već je bilo takvih slučajeva sa tehnološkim gigantima poput Applea.[865] Kompanija je optužena da je pogrešno identifikovala kradljivca preko svog softvera za prepoznavanje lica i podnela prijavu policiji protiv tinejdžera koji ne samo da nikada nije ušao u prodavnicu u kojoj se incident odigrao, već ni u državu u kojoj se prodavnica nalazi.

Nemar prikazan u tom slučaju otkriva duboko ukorenjene probleme u okviru kojih takvi sistemi funkcionišu. Prema podnetoj tužbi, Apple i firma koja mu pruža usluge obezbeđenja, Security Industry Specialists (SIS), svesno su pogrešno identifikovali osobu optuženu za krađu u jednoj od prodavnica kroz loše upravljanje sistemom nadzora. Kako je utvrđeno, usled ljudske greške nije uhapšen pravi počinilac, jer je posedovao ukradenu vozačku dozvolu osumnjičenog tinejdžera. Snimci sa nadzornih kamera povezani su sa dozvolom bez dodatnih provera, dok policija nije ni pokušala da proveri identitet osumnjičenog.[866] Jedina karakteristika koja povezuje dvojicu muškaraca bila je njihova rasa.

U drugim jurisdikcijama takođe su zabeleženi slučajevi maloprodajnih firmi koje ubrzano uvode prepoznavanje lica i druge vrste biometrijskog nadzora u svoje prodavnice. U Ujedinjenom Kraljevstvu, supermarket Co-op našao se na meti javnosti zbog korišćenja tehnologije za identifikovanje i sprečavanje kupaca koje su druge maloprodajne firme stavile na listu za posmatranje – bez dokaza ili nezavisne procene da li su ljudi na listama za praćenje počinili ili pokušali da počine bilo kakvo delo.[867] U Evropi, holandska kompanija VisionLabs jedna je od mnogih koje nude biometrijske sisteme za profilisanje kupaca dok se kreću po prodavnici – uključujući i put kojim idu, predmete za koje se čini da ih zanimaju, njihove emocije i drugo.[868]

U SAD raste pritisak na velike trgovce da obustave upotrebu prepoznavanja lica u svojim prodavnicama. Aktivistički kolektiv Fight for the Future pokrenuo je kampanju za zabranu prepoznavanja lica u prodavnicama, dok potrošače informiše o trgovcima koji koriste spornu tehnologiju u svojim radnjama, kao i onima koji su se obavezali da će se uzdržati od njene upotrebe.[869] Privatne kompanije su dužne da usklade svoju upotrebu sistema nadzora sa lokalnim zakonima, a na promenu prakse mogu ih privoleti pritužbe potrošača i opomene javnih službenika. Razmere javne kontrole i potencijalni prostor za uticaj zaista zavise od konkretne zemlje u kojoj kompanije posluju, pa su i rezultati ovakvih kampanja različiti.[870]

PRIVATNA TEHNOLOGIJA U JAVNOJ SLUŽBI

Dosad smo se bavili načinima na koje vlade pravdaju upotrebu tehnologija biometrijskog nadzora nacionalnom i bezbednošću granica i luka. Međutim, još jedan argument kojim se vlade služe u usvajanju biometrije odnosi se na društveno-ekonomski razvoj. Širom sveta, male i velike zemlje pronalaze nove načine da ugrade upotrebu osetljivih podataka svojih stanovnika u svakodnevnu praksu.

Važno je napomenuti da nijedan tehnološki napredak nije lišen rizika. Vlade treba ozbiljno da razmotre pretnje po privatnost tokom razvoja i prilagođavanja novih tehnologija svojim i potrebama svojih stanovnika, kao i da pažljivo procene dobavljače trećih strana s kojima će raditi na njihovoj implementaciji.

Bezbednost ličnih podataka građana može da ima značajan uticaj na odluke vlada da koriste biometrijske tehnologije u svakodnevnom životu. Bezbedna interakcija i zadovoljstvo stanovnika javnim e-uslugama postaje sve veći izazov za vlade, posebno u uslovima pandemije kovida-19, koja je od 2020. bitno uticala na sektore sa šalterima – što čini većinu vladinih usluga. Kao rezultat, činilo se da su vlade pomerile fokus na pronalaženje novih načina za pomeranje digitalnih granica u nastojanju da se pozabave pitanjima bezbednosti ličnih podataka, ali su u tom procesu izgleda zanemarile brigu za privatnost. Pristup polisama životnog osiguranja i medicinskim podacima, upravljanje finansijama i bezbedna onlajn komunikacija sa javnim službama zahtevaju neki oblik verifikacije identiteta. Iako su lozinke i dalje najrasprostranjeniji oblik, mnoge kompanije sve više nude navodno naprednija tehnološka „rešenja“. To predstavlja očigledne izazove, budući da e-usluge najvećim delom razvijaju nezavisni dobavljači. Neki provajderi usluga, poput banaka, odlučuju se za integraciju biometrijskih tehnologija koje koriste velike tehnološke kompanije poput Applea i Samsunga, a koje su u prošlosti kritikovane zbog odsustva modela ugrađene privatnosti (privacy by design).

U Aziji, biometrija postaje sve važniji deo svakodnevnih aktivnosti državnih službi. Tajland je već dodao prepoznavanje lica za unapređenje autentifikacije novih bankarskih klijenata kroz integraciju platforme nacionalnih digitalnih ličnih karata.[871] Ova platforma je u vlasništvu privatne kompanije za usluge digitalnog identiteta, koja tvrdi da pojednostavljuje procese verifikacije identiteta za kompanije i usluge u različitim sektorima kao što su bankarstvo, zdravstvena zaštita, naplata poreza i osiguranje.[872] Početkom 2022. godine, platforma je ušla u partnerstvo sa Mastercardom kako bi svoje usluge verifikacije ponudila van zemlje, što omogućava proširenje liste potencijalnih klijenata na međunarodnom nivou.[873] Ovakva ekspanzija u relativno kratkom vremenskom periodu pripisana je regulatornom izuzeću koje im je omogućilo da u realnom vremenu testiraju svoje usluge na stanovnicima, ne brinući za kršenje propisa o privatnosti. Izuzeće je pružilo kompaniji carte blanche u prikupljanju dokaza o efikasnosti tehnologije. Dok je u slučaju Tajlanda ovaj eksperiment navodno pomogao državi da poveća svoj digitalni BDP, za koji se očekuje da će iznositi trećinu ukupnog BDP-a zemlje u narednih pet godina,[874] ulozi su previsoki da bi se zanemarili potencijalni problemi integrisanih sistema koji sadrže biometrijske podatke stanovnika.

U Rusiji, država je razvila i finansirala Jedinstveni biometrijski sistem (JBS) koji stanovnicima omogućava pristup i korišćenje brojnih usluga širom zemlje.[875] Sistem je razvijen u saradnji sa Bankom Rusije i Rostelekomom, najvećim ruskim provajderom telekomunikacionih usluga, i prikuplja biometrijske identifikatore ljudi kao što su glas i lice. JBS je postao centralni element tehnologije biometrijske identifikacije koja se distribuira među ruskim bankama i drugim preduzećima od 2018. Prikupljanje ličnih podataka koje vrše banke obavlja se kroz dvostruki proces – prvo banka prikuplja biometrijske podatke ljudi za sopstvene bezbednosne svrhe, a zatim se podaci prikupljaju da bi se prosleđivali u JBS.[876] Iako je prikupljanje biometrijskih podataka za JBS i dalje na dobrovoljnoj osnovi, u dostupnim izveštajima se navodi da je vlada najavila integraciju sistema u obezbeđene prostore kao što

su odbrambeni i nuklearni objekti.[877] Međutim, 2022. godine, donji dom ruskog parlamenta usvojio je zakon kojim se bankama nalaže da dostavljaju biometrijske podatke klijenata vladi bez njihove prethodne saglasnosti.[878] Stručnjaci za privatnost povezuju masovnu centralizaciju biometrijskih podataka u Rusiji sa organizovanim nastojanjem da se što više informacija o građanima stavi pod kontrolu, budući da su naredbu bankama da dostave biometrijske podatke klijenata izdale državne službe bezbednosti.[879]

Centralizacija sistema koji obrađuju lične podatke može predstavljati brojne pretnje po privatnost građana, od krađe do zloupotrebe podataka, a rizici samo rastu kada je u kombinaciji i biometrija.

BAZA OD MILIJARDU LICA: CLEARVIEW AI

Privatni sektor je na čelu ekspanzije upotrebe prepoznavanja lica i drugih biometrijskih tehnologija širom sveta, što ima sve veći uticaj na interese i prava građana. Privatne kompanije javljaju se i kao dobavljači (programeri) i kao kupci biometrijske tehnologije. S druge strane, zakoni koji regulišu upotrebu prepoznavanja lica i drugih vrsta biometrijskog nadzora često nisu dovoljni da se izbore sa razmerama štete, kako je opisano u pravnom poglavlju ove knjige.

Shodno tome, privatne kompanije često razvijaju proizvode, biznis planove i marketinške strategije ne uzimajući dovoljno u obzir negativne eksterne posledice kao što su diskriminacija, narušavanje privatnosti i rizici po druga ljudska prava. Često se široj javnosti ostavlja da generiše pritisak na vladu da uvede odgovarajuće propise, dok aktivisti za privatnost i branitelji ljudskih prava pokreću strateške parnice kako bi obuzdali upotrebu takvih tehnologija. Slučaj Clearview AI upravo ilustruje takve prilike – gde su zloupotrebe biometrijskih podataka toliko brojne da smo probleme ove kompanije u različitim jurisdikcijama dosad već više puta istražili u ovoj knjizi.

Kompanija Clearview AI izašla je na zao glas zbog svog servisa za prepoznavanje lica, koji se oslanja na biometrijsku databazu izgrađenu skrejpovanjem ličnih fotografija sa interneta, prvenstveno sa društvenih mreža.[880] Osnovni poslovni model i sam alat temelje se na krajnje nelegitimnoj

obradi ličnih podataka i smatra se potpuno nezakonitim prema GDPR-u. U Evropskoj uniji, Clearview AI se suočio sa nizom novčanih kazni koje su rezultat strateških parnica aktivista za zaštitu privatnosti, kao i postupaka koje su po službenoj dužnosti preduzimali poverenici za zaštitu podataka iz različitih evropskih država. Konkretno, službe iz tri države članice EU izrekle su kazne od 20 miliona evra za Clearview AI: u Italiji (mart 2022),[881] Grčkoj (jul 2022)[882] i Francuskoj (oktobar 2022).[883] Pre ovih odluka, britanski ICO je kompaniji izrekao kaznu od 7,5 miliona funti (decembar 2021).[884] U maju 2023. francuska služba za zaštitu podataka izrekla je još jednu kaznu od 5,2 miliona evra zbog nepoštovanja prethodne odluke o novčanoh kazni.[885] Austrijska agencija za zaštitu podataka je takođe ocenila poslovanje kompanije kao nezakonito, ali nije izrekla novčanu kaznu.[886]

Do 2020. Clearview AI je prodavao svoje usluge i privatnim kompanijama i javnim vlastima. Međutim, ovom biznis planu suprotstavila se tužba Američke unije za građanske slobode (American Civil Liberties Union, ACLU) koja je rezultirala zabranom prodaje usluga privatnim kompanijama u Sjedinjenim Državama.[887] Međutim, kompanija i dalje pruža svoje usluge službama za sprovođenje zakona, što daje posebnu težinu aktuelnoj debati o upotrebi i regulativi prepoznavanja lica u SAD, posebno u svetlu jačanja i pogoršavanja rasizma u radu policije. Tehničke aspekte koji se odnose na tačnost tehnologije prepoznavanja lica detaljno smo razmotrili u prvom poglavlju, dok su štetne društvene posledice opisane u studiji slučaja koja opisuje kako NYPD koristi tehnologije za prepoznavanje lica.

Pored bankarskog i sektora maloprodaje, potražnju za tehnologijama prepoznavanja lica i drugim biometrijskim alatima podstiču službe za sprovođenje zakona, uključujući i službe nacionalne bezbednosti. Clearview AI je privukao pažnju javnosti zbog svoje krajnje problematične prakse obrade podataka, ali i zahvaljujući popularnosti među policijskim upravama u SAD. Šira javnost uglavnom postaje svesna upotrebe tehnologije za prepoznavanje lica samo kad ona direktno utiče na policijske procedure na terenu, kojima ljudi i sami svedoče ili kojima bivaju podvrgnuti. S druge strane, netransparentnost i odsustvo javne kontrole tipične su za mnoge kompanije koje isporučuju tehnologiju biometrijskog nadzora širim strukturama za sprovođenje zakona. Istraživanja pokazuju da je u poslednje dve decenije američka vlada potpisala ugovore za tehnologije za prepoznavanje lica, koji nisu klasifikovani kao poverljivi, u vrednosti od 76 miliona dolara.[888] Procenjuje se da je vrednost poverljivih ugovora federalnih službi za sprovođenje zakona ili vojske daleko veća.

Mada velikih biometrijskih kompanija i dobavljača tehnologije ima širom sveta, čini se da su, možda usled nedostatka federalnih propisa o kojima smo govorili u prethodnom poglavlju, američke kompanije naročito spremne da se „kreću brzo i razorno“. Ovakav pristup neobuzdanom razvoju i prodaji alata i usluga za prepoznavanje lica nedavno su dovele u pitanje i same privatne kompanije. Pojedine su čak navodno zaustavile razvoj ili ograničile prodaju takvih alata. Na primer, Microsoft je odlučio da ograniči svoju ponudu veštačke inteligencije i povukao alate za prepoznavanje emocionalnog stanja iz analize lica zbog netačnosti i diskriminatornih primena – mada, kako smo istakli u prvom poglavlju, i dalje postoji zabrinutost koliko je zapravo realan i efikasan taj moratorijum.

Ipak, čini se da Clearview AI ne usporava – tokom 2024. je broj fotografija lica u bazi premašio 50 milijardi, dok je broj pretraga u bazi od strane policijskih službi prešao dva miliona.[889] Baza se takođe koristi u Ukrajini kako bi pomogla u identifikovanju poginulih ruskih i ukrajinskih vojnika, kao i za obaveštavanje porodica.[890] Uprkos svojim netransparentnim poslovnim praksama i komotne saradnje sa organima vlasti, čini se da nedostaje ozbiljniji i opširniji razgovor o posledicama tehnološkog napretka koji često ide na uštrb ljudskih prava i sloboda.

OČI, UŠI I SVEST: KONTROLA JAVNIH PROSTORA

Normalizacija stalnog nadzora javnih prostora izaziva zabrinutost u pogledu privatnosti i građanskih sloboda. Građani imaju pravo na privatnost i ne bi trebalo da se osećaju kao da ih neko neprestano posmatra i prati svaki njihov pokret. Ogromni fudbalski stadioni i druge sportske arene širom sveta postali su jedan od najpogodnijih poligona za testiranje novih tehnologija za nadzor. Vlade su shvatile da su veliki sportski događaji vrlo zgodna prilika za uvođenje i pravdanje masovne primene tehnologija za nadzor, kao proba pre njihove šire upotrebe. Zbog toga većinu slučajeva nadzora javnog prostora, kao što su FIFA Svetsko prvenstvo u Kataru 2022.[891] i Olimpijske igre u Francuskoj 2024,[892] uvek prate kontroverze tehnosolucionizma. Takođe, vredi napomenuti da nadzor sa prepoznavanjem lica posetilaca stadiona uključuje finansijski aspekt, jer kompanijama omogućava da zaštite svoje interese. To je bio slučaj kada se FIFA obračunavala sa navijačima zbog nošenja određene boje na Svetskom prvenstvu 2010. jer je sumnjala da vode kampanju za brend koji je želeo da se reklamira na utakmici, ali nije bio zvanični sponzor.[893] Sa 15.000 kamera raspoređenih za Svetsko prvenstvo u Kataru 2022. godine, glavni tehnološki direktor kompanije koja je upravljala nadzornom infrastrukturom na događaju, opisao je sistem kao „oči, uši i svest svih stadiona u isto vreme“.[894] Ovo kršenje privatnosti pothranjuje kulturu straha i ometa lične slobode, što končano potkopava demokratsko tkivo društva.

VIVE LA NADZOR! – OLIMPIJSKE IGRE U FRANCUSKOJ 2024.

Nacionalna bezbednost često je šifra za državnu primenu tehnologija za prepoznavanje lica, posebno u prilikama kao što su parade, festivali ili sportski događaji. Zato ne čudi da su Olimpijske igre glavna tačka spora kada vlade pokušavaju da nađu ravnotežu između bezbednosti i privatnosti. U knjizi „Bezbednosne igre: Nadzor i kontrola na mega-događajima“ Colin Bennett i Kevin Haggerty tvrde da ovi mega-događaji služe kao plodno tlo za eksperimentisanje sa nadgledanjem i nadzorom javnih prostora, dok zaobilaze diskusiju o zaštitnim merama koje unapred treba postaviti. Autori takođe primećuju da je „bezbednost postala integralni deo olimpijskog rituala“.[895]

Jedan od glavnih podsticaja za rast sekuritizacije mega-događaja bili su napadi u Americi 11. septembra 2001, što je vladama dalo blanko ovlašćenje da eksperimentišu sa invazivnim tehnologijama. Kako smo pokazali u pregledu upotrebe nadzora u kontekstu nacionalne bezbednosti, dodatni sloj je prisutan u organizaciji velikih događaja, posebno onih međunarodnog karaktera koji privlače brojnu publiku, kao što su Svetsko prvenstvo u fudbalu ili Olimpijske igre. Ove manifestacije imaju društveni, ekonomski i nacionalni značaj za zemlju domaćina, i stoga su obično pozornica za demonstraciju sposobnosti zemlje da upriliči i kontroliše takve događaje. Nažalost, pojačan nadzor publike postao je glavna takmičarska kategorija.

U središtu jednog od najregulisanijih delova sveta, Evropske unije, sekuritizacija Olimpijskih igara postala je tema dugotrajne diskusije. Francuska je kao domaćin Letnjih olimpijskih i paraolimpijskih igara na leto 2024. godine, prošla je težak put usaglašavanja oko pristupa nadzoru i bezbednosti na ceremoniji. U novembru 2022, francuska vlada je obećala da neće koristiti tehnologiju prepoznavanja lica, navodeći to kao „crvenu liniju“ u smislu kršenja privatnosti.[896] Međutim, u martu 2023, parlament je usvojio član 7 zakona o Olimpijskim igrama, koji predviđa korišćenje automatizovanog bihevioralnog nadzora javnih prostora tokom trajanja sportskih, rekreativnih ili kulturnih događaja. Vlada tvrdi da to ne podrazumeva kapacitete za jedinstvenu identifikaciju.[897]

Uprkos snažnom protivljenju evroposlanika i organizacija civilnog društva,[898] francuska vlada je uspela da obezbedi podršku i zakon je usvojen u maju 2023. Tome je pomogla činjenica da je u to vreme u fokusu javnosti bila kontroverzna reforma penzionog sistema, što nije ostavilo mnogo prostora za javnu debatu i podizanje svesti šire javnosti o biometrijskom nadzoru. Zagovornici privatnosti i građanskih prava ukazivali su da zakon predstavlja opasan presedan ne samo u Francuskoj, već i šire u Evropi. Takođe su kritikovali vladine tvrdnje da tehnologija automatizovanog video nadzora nije biometrija niti je na bilo koji način koristi, i isticali da je to očigledna zabluda, obmanjujuće tumačenje i zloupotreba pravnih koncepata.[899] Tehnologija automatizovanog nadzora treba da pomogne policiji u praćenju i označavanju „sumnjivog ponašanja“ na događaju. U vreme prvog izdanja našeg istraživanja, vlada još nije izdala uredbu kojom bi se definisala označena ponašanja, ali je tada zaključeno da bi na meti nadzora bilo hodanje suprotnim putem od mase, ležanje na ulici, trčanje itd. Softver za nadzor u realnom vremenu u stanju je da detektuje predmete i ponašanja koje bi vlasti mogle da označe kao rizične.[900]

Razvoj tehnologije nadzora koja se koristi u svrhe nacionalne bezbednosti na velikim događajima u stalnom je porastu, po kvantitetu i po sofisticiranosti. Prema nekim procenama, dok su budžeti za bezbednost na Olimpijskim igrama 2000. bili milionski, posle napada u Americi 11. septembra 2001. ti iznosi su prerasli u milijarde.[901] Međutim, kada se analiziraju mnoge oblasti u kojima je ranije korišćena tehnologija nadzora kakva je primenjena na Olimpijskim igrama, uočićemo prekomerni nadzor nad osiromašenim, minorizovanim i rasijalizovanim zajednicama, dokumentovan već na Olimpijskim igrama u Riju 2016. godine.[902] Upotreba tehnologije omogućava vlastima da odluče ko može da bude prisutan gde i na koji način. Još uvek nema kritičkog ispitivanja potencijalne štete od zloupotrebe takve tehnologije tokom, ali i nakon događaja.

Francuski zakon o Olimpijskim igrama je još jedan primer kako vlade koriste velike događaje da proguraju bezbednosni program i promovišu ekonomske interese. Takođe pogoduje velikoj francuskoj industriji algoritamskog video nadzora da reguliše upotrebu ovih tehnologija, što akterima omogućava da povećaju svoju proizvodnju i testiraju i prodaju svoje sisteme državi.[903]

U maju 2023. francuski ustavni sud je odobrio zakon i podržao vladino uvođenje sistema algoritamske obrade. Eksperimentalna faza će trajati do aprila 2025, dugo nakon završetka Olimpijskih igara.[904] Drugi veliki problem je to što su, prema francuskoj vladi, biometrijski podaci povezani samo sa prepoznavanjem lica, što zanemaruje analizu ponašanja kao deo obrade biometrijskih podataka. Dakle, ograničenje koje je postavio Ustavni sud može se tumačiti kao čisto simbolično, bez mnogo praktičnih posledica iz pravne perspektive.

Konačno, tokom letnjih olimpijskih i paraolimpijskih igara u Francuskoj, posetioci, turisti i sportisti bili su 24 časa pod budnim okom 485 kamera koje su bile kontrolisane uz pomoć veštačke inteligencije. Ove kamere proizvodile su fotografije i video sadržaje čitave dve nedelje u Parizu i drugim gradovima, nakon čega su materijali slati na obradu uz pomoć sistema koji prepoznaje pokrete i ponašanja.[905] U oktobru je objavljeno da će sistem koji je bio instaliran za nadzor tokom trajanja igara postati stalni deo bezbednosne infrastrukture zemlje, uprkos obećanjima zvaničnika da će biti uklonjen.[906]

Ovaj slučaj naglašava značaj široke definicije biometrijskih podataka u pravnom okviru. U suprotnom, vrlo je realan rizik da će vlade tražiti rupe i utvrđivati proizvoljne razlike između praksi za koje priznaju da su previše štetne i onih za koje tvrde da su prihvatljive jer nisu pokrivene tehničkom definicijom.

KRUNSKI DRAGULJ KONTROLE – KRUNISANJE U UK

Tokom protekle decenije, Ujedinjeno Kraljevstvo (UK) se pozicioniralo kao jedna od najdinamičnijih zemalja Evrope u pogledu primene biometrijskih sistema masovnog nadzora u javnim prostorima. Neki od najistaknutijih primera obuhvataju tajno partnerstvo između londonske metropolitenske policije (Met) i investitora oko putničkog čvorišta Kings Cross od 2016. do 2018;[907] nadzor božićnih kupaca 2017. i mirnih demonstranata 2018. godine koje je sprovodila policija Južnog Velsa;[908] novčanu kaznu izrečenu muškarcu koji je pokrio lice da bi izbegao prepoznavanje lica uživo 2019;[909] i policijsko targetiranje crnih zajednica na karnevalu u Notting Hillu (godišnja proslava londonske afro-karipske zajednice) 2017.[910] Primeri su posebno alarmantni u svetlu nezavisne analize iz 2023. godine koja je otkrila da je Met policija još uvek „institucionalno rasistička“,[911] decenijama nakon što je sistemska diskriminacija u Metu prvi put javno obznanjena.

Ovi i mnogi drugi zabrinjavajući primeri pokrenuli su nevladine organizacije kao što su Liberty i Big Brother Watch da se suprotstave usvajanju tehnologija za prepoznavanje lica kao navodno lakom rešenju praktično svakog društvenog ili kriminalnog pitanja u Ujedinjenom Kraljevstvu.[912] Organizacije ukazuju na značajne pretnje po rasnu pravdu, pri čemu se mnoge primene odvijaju bez ikakvog razmatranja pristrasnosti sistema za prepoznavanje lica ili diskriminatornih struktura unutar kojih se oni primenjuju, što rezultira targetiranjem rasijalizovanih zajednica.

Takođe, nekoliko vodećih akademika analiziralo je testiranje biometrijskog nadzora u britanskoj policiji, uključujući istaknutu studiju iz 2019. koju su

sproveli profesor Pete Fussey i dr Daragh Murray.[913] Njihovo istraživanje bilo je prva nezavisna studija o korišćenju prepoznavanja lica u britanskoj policiji, a koja je utvrdila ozbiljne operativne propuste, značajan nedostatak kontrole i razne prakse koje bi se verovatno smatrale nezakonitim ako bi se osporile na sudu. Drugi vodeći stručnjaci, kao što je profesorka Lorna McGregor iz Projekta za ljudska prava, velike podatke i tehnologiju (Human Rights, Big Data and Technology, HRBDT), primenili su svoja interdisciplinarna znanja o ljudskim pravima da problematizuju nepromišljenu državnu primenu tehnologija za prepoznavanje lica.[914]

Međutim, nisu samo državni organi odgovorni za naglu ekspanziju biometrije u Ujedinjenom Kraljevstvu. Supermarketi se užurbano upuštaju u eksperimentisanje s takvim alatima. Lanac supermarketa Co-op koristio je prepoznavanje lica za sprovođenje politike zabrane ulaska.[915] Takođe, u širokom spektru usluga (uključujući velike lance supermarketa kao što su Sainsbury's i Tesco, uz poštanske službe) testirani su sistemi zasnovani na biometriji za verifikaciju starosne dobi kupaca, prilikom odobravanja kupovine proizvoda za koje postoji relevantno ograničenje.[916] Slične prakse su predstavljene u ovom poglavlju, u studiji slučaja iz Australije.

Britanska kompanija za biometrijsku proveru uzrasta, Yoti, udružila se sa velikim onlajn platformama poput Instagrama,[917] uprkos otvorenim pitanjima o kompatibilnosti njihove prakse sa ljudskim pravima. Kako ističe nevladina organizacija Privacy International, nagli rast primene servisa kao što je Yoti podržan je posebnim ciljem vlade Ujedinjenog Kraljevstva da podstakne globalni uspon svoje industrije „digitalnog identiteta".[918]

Biometrijski institut, udruženje sa sedištem u UK, takođe je privukao pažnju civilnog društva promocijom interesa biometrijske industrije, iako se predstavljao kao nepristrasna grupacija.[919] Kako stoje stvari, biometrijska industrija je toliko značajna za ekonomiju Ujedinjenog Kraljevstva, da se procenjuje da je 2022. vredela preko pola milijarde funti.[920] Stoga je jasno da se, pored društvene kontrole i tehnosolucionizma, širenje upotrebe prepoznavanja lica i drugih biometrijskih sistema u Ujedinjenom Kraljevstvu takođe vodi ekonomskim interesima. Konkretno, država sponzoriše nastojanje da se izgradi najveće tržište za biometriju na svetu – što je aspiracija kojoj, prema istraživanjima opisanim u pravnom poglavlju ove knjige, očigledno parira i kineska vlada. Mada nije svaka upotreba biometrije ujedno i masovni nadzor, doprinosi stvaranju osnovnih uslova i infrastrukture koja će omogućiti procvat praksi biometrijskog masovnog nadzora.

Konkretno, čini se da je široko rasprostranjena komercijalna upotreba biometrijskih sistema – uz ogromnu mrežu CCTV kamera u Ujedinjenom Kraljevstvu (najveću u Evropi, sa jednom kamerom na svakih 13 ljudi)[921] – doprinela nesvesnoj normalizaciji masovnog biometrijskog nadzora. Takve prakse dodatno umanjuju oprez i uslovljavaju nižu svest o rizicima po prava i slobode.

U kontekstu nemarnih eksperimenata vođenih profitom i verom u tehnološki nadzor kao rešenje za praktično svaki problem, krunisanje kralja Čarlsa precizno je pokazalo zašto je upotreba prepoznavanja lica u javnim prostorima u UK toliko zabrinjavajuća. Pre svega, asocirana je uz nesrazmerno grube reakcije i na proslavi i na protestu protiv krunisanja, na način koji demonstrira moć ovih sistema da kontrolišu i guše pravo na korišćenje javnih prostora.

Krunisanje kralja Čarlsa Trećeg 6. maja 2023. bio je događaj koji je naglasio polarizovane stavove građana i stanovnika Ujedinjenog Kraljevstva prema monarhiji. Uoči događaja, mnogi ljudi i zajednice su se pripremali za ulične zabave i slična slavlja. Drugi su se pripremali za proteste i druge vrste zakonitog izražavanja svog neslaganja. Nekoliko takvih protesta ticalo se kritike institucije monarhije u širem smislu, ali i konkretnih postupaka britanske kraljevske porodice.[922] Mnogi su se protivili ogromnim javnim izdacima za krunisanje u vreme kada milioni dece u UK ne mogu da priušte tri obroka dnevno.[923]

Nekoliko dana pre krunisanja, Met policija je najavila da će nastaviti sa svojom, dosad najširom primenom prepoznavanja lica uživo, u sklopu kontrole nad događajem, što je profesor Fussey okarakterisao kao „verovatno najveću ikada viđenu u Evropi".[924] Policija je navela da krunisanje vidi kao priliku da koristi prepoznavanje lica „da bi privela osobe tražene zbog nekog krivičnog dela ili čije se ime povezuje s nekim nalogom".[925]

Korišćenje javnih proslava i protesta kao prilike za policiju da otkrije tražene osobe nezavisno od tih aktivnosti, sugeriše da policijski napori nisu usmereni na zaštitu prava učesnika da koriste javne prostore. Umesto toga, ove legitimne, zakonite aktivnosti se vide kao šansa za realizaciju drugih ciljeva. To sugeriše da policijski resursi i pažnja nisu bili usredsređeni na očuvanje bezbednosti slavljenika i demonstranata. Pravo na protest je u više

navrata podržao Evropski sud za ljudska prava i dužnost je države da poštuje i obezbedi to pravo.[926]

Poznato je da tehnologije biometrijskog nadzora izazivaju tzv. efekat zebnje koji može da odvrati ljude od ostvarivanja prava i sloboda, posebno prava na okupljanje i udruživanje.[927] Uprkos tome, Met policija ih svesno koristi na protestima. Moguće je da je policija smatrala da je prepoznavanje lica uživo, očigledan oblik masovnog biometrijskog nadzora, podesan način za preventivno obeshrabrivanje ljudi da koriste svoje pravo na protest. U prilog takvom tumačenju govore oštre reči u objavama Met policije na društvenim mrežama, u kojima su ljudi upozoravani da ne protestuju, dok su protesti nazivani „ometanjem" uz jasne nagoveštaje da će demonstranti biti hapšeni.[928] Takve objave su naišle na opštu osudu na društvenim mrežama, kao represivne i autoritarne. Upotreba tehnologije za prepoznavanje lica uživo očigledno je duboko povezana sa načelnim problemima u radu policije.

Mada se prima facie može činiti legitimnim napor policije da locira tražene osobe, istog dana kada je Met najavio upotrebu prepoznavanja lica uživo na krunisanju, stupio je na snagu novi britanski zakon o javnom redu.[929] Uz zakon o policiji, kriminalu, presudama i sudovima[930] novi propisi su žestoko kritikovani zbog kriminalizacije određenih oblika protesta, i to na način koji je dovoljno nejasan da potencijalno obeshrabri značajan broj ljudi od učešća u protestima ili drugom zakonitom izražavanju neslaganja – tako da bi policija mogla da hapsi čak i demonstrante koji se drže za ruke.[931] Ministarstvo unutrašnjih poslova Ujedinjenog Kraljevstva navodno se obratilo grupi Republic neposredno pre krunisanja, sa upozorenjem članovima da su novi zakoni osmišljeni tako da obeshrabre proteste na velikim javnim događajima ili druge „remetilačke" akcije.[932]

Novi zakoni pružaju Met policiji ovlašćenje da hapsi demonstrante, kriminalizujući pravo na slobodno protivljenje krunisanju, kao i pravo na slobodno okupljanje. Zauzvrat, sistem za prepoznavanje lica uživo omogućava policiji da locira i identifikuje demonstrante, što će kod svake razumne osobe umanjiti osećaj da se protestovati može komforno i bezbedno, s obzirom na svest da ih je lako pratiti u realnom vremenu. Takvo postupanje Met policije dodatno učvršćuje represivnu moć upotrebe tehnologije za prepoznavanje lica uživo i ulogu masovnog biometrijskog nadzora u progonu ljudi koji pokušavaju da uživaju svoje osnovno pravo na protest.

Konačno, pitanja oko policijske primene sistema za prepoznavanje lica koja su postavljena na početku ovog poglavlja, poput odsustva transparentnosti i zanemarivanja visokog rizika od diskriminacije, nikada nisu formalno rešavana. To dodatno otežava povrede i demonstrira flagrantno ignorisanje ljudskih prava prilikom odlučivanja policije da koristi prepoznavanje lica uživo na krunisanju. Posle događaja, britanski komesar za biometriju i nadzorne kamere, Fraser Samson, upozorio je da su „kontrola i regulativa u ovoj, sve važnijoj oblasti javnog života nepotpune, nedosledne i nejasne".[933]

Sve u svemu, ovaj slučaj verno prikazuje masovni biometrijski nadzor kao jedinstven alat u širem arsenalu tehnika države za kontrolu i oblikovanje javnih prostora. Tehnologija za prepoznavanje lica uživo, posebno u radu londonske policije, koristi se za kažnjavanje običnog ponašanja kao što je pokrivanje lica u javnosti, za kriminalizovanje demokratskih akcija poput protesta, kao i za preciznije targetiranje crne i drugih rasijalizovanih zajednica. Nadovezujući se na normalizaciju javnog nadzora zahvaljujući ogromnoj mreži CCTV kamera u Ujedinjenom Kraljevstvu, policija je u velikoj meri uspela da priguši protivljenje masovnom biometrijskom nadzoru, uprkos značajnim naporima nevladinih organizacija i stručne javnosti.

U tom kontekstu, supermarketi i drugi privatni subjekti užurbano isprobavaju primenu biometrijskih ili podataka zasnovanih na biometriji za druge funkcije, kao što je provera uzrasta kupaca. Uz rasprostranjenu primenu u policiji, komercijalnim primenama se podsvesno normalizuju biometrijski sistemi za širok spektar upotrebe u UK.

Dok Ujedinjeno Kraljevstvo sve više pribegava upotrebi najosetljivijih ličnih podataka kako bi se uspostavila kontrola ko može, a ko ne može da koristi javne prostore, resurse i osnovna prava, istovremeno se uklanjaju ionako nedovoljne mere zaštite od biometrijskog masovnog nadzora. Poverenik Samson upozorava da će jedini obavezujući zakonski okvir koji postoji u Ujedinjenom Kraljevstvu za prakse biometrijskog nadzora uskoro biti ukinut, „a da nisu ponuđene odredbe koje bi ga zamenile".[934]

BELEŠKE

1 SHARE Fondacija, „Evropska promocija knjige SHARE Fondacije o biometrijskom nadzoru“, 7. decembar 2023. https://sharefoundation.info/evropska-promocija-knjige-share-fondacije-o-biometrijskom-nadzoru/

2 IBM, “What is Computer Vision?”, https://www.ibm.com/topics/computer-vision

3 S. Lewis, “The Racial Bias Built Into Photography”, The New York Times, 25. april 2019. https://www.nytimes.com/2019/04/25/lens/sarah-lewis-racial-bias-photography.html

4 V. Joler, M. Pasquinelli, “The Nooscope Manifested: AI as Instrument of Knowledge Extractivism”, 2020. https://nooscope.ai/

5 K. Crawford, T. Paglen, “Excavating AI: The Politics of Images in Machine Learning Training Sets”, The AI Now Institute, 19. septembar 2019. https://excavating.ai

6 R. Mac, “Facebook Apologizes After A.I. Puts ‘Primates’ Label on Video of Black Men”, The New York Times, 3. septembar 2019. https://www.nytimes.com/2021/09/03/technology/facebook-ai-race-primates.html; M. Zhang, “Google Photos Tags Two African-Americans As Gorillas Through Facial Recognition Software”, Forbes, 1. juli 2015. https://www.forbes.com/sites/mzhang/2015/07/01/google-photos-tags-two-african-americans-as-gorillas-through-facial-recognition-software/

7 J. Vincent, “Google ‘fixed’ its racist algorithm by removing gorillas from its image-labeling tech”, The Verge, 12. januar 2018. https://www.theverge.com/2018/1/12/16882408/google-racist-gorillas-photo-recognition-algorithm-ai

8 “Labeled Faces in the Wild”, University of Massachusetts - Computer Vision Lab, http://vis-www.cs.umass.edu/lfw/

9 G. Bae et al., “DigiFace-1M: 1 Million Digital Face Images for Face Recognition”, Winter Conference on Applications of Computer Vision 2023, https://microsoft.github.io/DigiFace1M/

10 European Digital Rights (EDRi), “Remote biometric identification: a technical & legal guide”, 23. januar 2023. https://edri.org/our-work/remote-biometric-identification-a-technical-legal-guide/

11 National Human Genome Research Institute, “Fact Sheet: Eugenics and Scientific Racism”, https://www.genome.gov/about-genomics/fact-sheets/Eugenics-and-Scientific-Racism

12 L. Lee-Morrison, “Portraits of Automated Facial Recognition: On Machinic Ways of Seeing the Face”, Transcript-Verlag, 2019, str. 85-87 https://lucris.lub.lu.se/ws/portalfiles/portal/70768307/LLM_manu.pdf

13 M. Rouse, “Pixel”, Techopedia, 31. avgust 2020. http://www.techopedia.com/definition/24012/pixel

14 L. Lee-Morrison, “Portraits of Automated Facial Recognition: On Machinic Ways of Seeing the Face”, str. 67

15 L. Sirovich, M. Kirby, “Low-Dimensional Procedure for the Characterization of Human Faces”, Journal of the Optical Society of America. A, Optics and image science 4 (3): 519-24, 1987, DOI:10.1364/JOSAA.4.000519, https://www.researchgate.net/publication/19588504_Low-Dimensional_Procedure_for_the_Characterization_of_Human_Faces, str. 520-521

16 Wiktionary, “Eigen”, https://en.wiktionary.org/wiki/eigen#German

17 L. Lee-Morrison, “Portraits of Automated Facial Recognition: On Machinic Ways of Seeing the Face”, str. 72

18 Ibid.

19 Izvor: M. Dussenbery, “On Eigenfaces: Creating ghost-like images from a set of faces.”, 22. januar 2015. https://mikedusenberry.com/on-eigenfaces

20 M. Turk, A. Pentland, “Eigenfaces for Recognition”, Journal of Cognitive Neuroscience 3 (1): 71-86, 1991, https://doi.org/10.1162/jocn.1991.3.1.71, str. 72

21 Ibid. str. 71

22 Ibid. str. 86

23 L. Krahulcova, “Techno solutionism—very few things actually need to be an app.”, Digital Rights Watch, 25. mart 2021. https://digitalrightswatch.org.au/2021/03/25/technosolutionism; M. Rouse, “Technodeterminism”, Techopedia, 19. novembar 2012. https://www.techopedia.com/definition/28194/technodeterminism

24 V. Joler, M. Pasquinelli, “The Nooscope Manifested: AI as Instrument of Knowledge Extractivism”, 2020. https://nooscope.ai/

25 M. Schaake, “Trade secrets shouldn’t shield tech companies’ algorithms from oversight”, Brookings TechStream, 4. maj 2020. https://www.brookings.edu/techstream/trade-secrets-shouldnt-shield-tech-companies-algorithms-from-oversight/

26 Merriam-Webster.com Dictionary, “Biometrics.”, https://www.merriam-webster.com/dictionary/biometrics

27 S. Minaee et al., “Biometrics Recognition Using Deep Learning: A Survey”, arXiv:1912.00271v3 [cs.CV], https://doi.org/10.48550/arXiv.1912.00271, str. 1-2

28 V. Joler, M. Pasquinelli, “The Nooscope Manifested: AI as Instrument of Knowledge Extractivism”, 2020. https://nooscope.ai/

29 Ibid.

30 Amazon Web Services, “What is a Neural Network?”, https://aws.amazon.com/what-is/neural-network/

31 A. Trafton, “Study urges caution when comparing neural networks to the brain”, MIT News Office, 2. novembar 2022. https://news.mit.edu/2022/neural-networks-brain-function-1102

32 Amazon Web Services, “What is a Neural Network?”, https://aws.amazon.com/what-is/neural-network/

33 Izvor: F. van Veen, “The Neural Network Zoo”, The Asimov Institute, 14. septembar 2016. https://www.asimovinstitute.org/neural-network-zoo/

34 IBM, “What are convolutional neural networks?”, https://www.ibm.com/topics/

convolutional-neural-networks

35 M. Rouse, “RGB Color Model (RGB)”, Techopedia, 19. septembar 2015. https://www.techopedia.com/definition/5555/rgb-color-model-rgb

36 Y. Gavrilova, “Convolutional Neural Networks for Beginners”, SeroKell, 3. avgust 2021. https://serokell.io/blog/introduction-to-convolutional-neural-networks

37 Ibid.

38 Ibid.

39 IBM, “What are convolutional neural networks?”, https://www.ibm.com/topics/convolutional-neural-networks

40 Google Research, “Google Brain”, https://research.google/teams/brain/

41 Microsoft Research, “Deep Learning Group”, https://www.microsoft.com/en-us/research/group/deep-learning-group/

42 V. Joler, M. Pasquinelli, “The Nooscope Manifested: AI as Instrument of Knowledge Extractivism”, 2020. https://nooscope.ai/

43 B. Ammanath, K. Firth-Butterfield, “How deep learning can improve productivity and boost business”, World Economic Forum, 12. januar 2022. https://www.weforum.org/agenda/2022/01/deep-learning-business-productivity-revenue/

44 Kada je Srbija u pitanju, druga verzija Procena uticaja obrade na zaštitu podataka o ličnosti upotrebom savremenih tehnologija video nadzora u okviru projekta “Sigurno društo” koju je Ministarstvo unutrašnjih poslova objavilo 2020. godine sadržala je podatke o 8100 uređaja koji će biti nabavljeni za ovaj sistem: fiksne i pokretne kamere na uličnim stubovima, fiksne kamere montirane na policijska vozila, kamere za policijske uniforme i ručni eLTE terminali. Više na: SHARE Fondacija, “Kamere bez upotrebne dozvole / Procena uticaja 2.0”, 31. juli 2020. https://www.sharefoundation.info/sr/kamere-bez-upotrebne-dozvole-procena-uticaja-2-0/

45 B. Ammanath, “Facial Recognition: Here’s looking at you”, Deloitte AI Institute, 2021. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology/us-ai-institute-facial-recognition.pdf, str. 5

46 J. Cox, J. Koebler, “Ransomware Group Claims Hack of Amazon’s Ring”, Vice / Motherboard, 14. mart 2023. https://www.vice.com/en/article/ransomware-group-claims-hack-of-amazons-ring/

47 J. Kelley, M. Guariglia, “Ring Reveals They Give Videos to Police Without User Consent or a Warrant”, EFF, 15. juli 2022. https://www.eff.org/deeplinks/2022/07/ring-reveals-they-give-videos-police-without-user-consent-or-warrant

48 Electronic Privacy Information Center (EPIC), “Drones and Aerial Surveillance”, https://epic.org/issues/surveillance-oversight/aerial-surveillance/

49 Za foto referencu videti: T. Paglen, “Untitled (Reaper Drone)”, Institute of Contemporary Art Boston, 2012. https://www.icaboston.org/art/trevor-paglen/untitled-reaper-drone

50 J. Honovich, “How to Design a Video Surveillance Solution”, IPVM, 4. januar 2012. https://ipvm.com/reports/how-to-design-video-surveillance-solution

51 X. Fu, “Design of Facial Recognition System Based on Visual Communication Effect”, Computational Intelligence and Neuroscience, vol. 2021, 2021. https://doi.org/10.1155/2021/1539596, str. 2

52 Ibid, str. 3

53 MEP Patrick Breyer, “Expect biometric mass surveillance in Paris in 2024: French Parliament approves automated monitoring of public spaces for ‘suspicious behaviour’”, Patrick-Breyer.de, 24. mart 2023. https://www.patrick-breyer.de/en/expect-biometric-mass-surveillance-in-paris-in-2024-french-parliament-approves-automated-monitoring-of-public-spaces-for-suspicious-behaviour/

54 P. Rueckert, “France Wants to Make Olympics-Style Surveillance Permanent”, Jacobin, 23. oktobar 2024. https://jacobin.com/2024/10/france-olympics-surveillance-ai-policing

55 J. Hendel, “Why suspected Chinese spy gear remains in America’s telecom networks”, Politico, 21. juli 2022. https://www.politico.com/news/2022/07/21/us-telecom-companies-huawei-00047045

56 E. Morozov, “The Huawei war”, Le Monde diplomatique, novembar 2020. https://mondediplo.com/2020/11/10huawei

57 Huawei, “Huawei Launches Ascend 910, the World’s Most Powerful AI Processor, and MindSpore, an All-Scenario AI Computing Framework”, 23. avgust 2019. https://www.huawei.com/au/news/au/2019/huawei-launches-ascend-910-the-worlds-most-powerful-ai-processor

58 Huawei, “Atlas 900 PoD (Model: 9000)”, https://e.huawei.com/en/products/computing/ascend/atlas-900-pod-9000

59 Huawei, “Atlas 900 AI Cluster”, https://e.huawei.com/en/products/computing/ascend/atlas-900-ai

60 Datagen, “ResNet-50: The Basics and a Quick Tutorial”, https://datagen.tech/guides/computer-vision/resnet-50/

61 J. E. Hillman, M. McCalpin, “Watching Huawei’s ‘Safe Cities’”, Center for Strategic and International Studies, 4. novembar 2019. https://www.csis.org/analysis/watching-huaweis-safe-cities

62 C. Zhihui, “Nowhere to hide: Building safe cities with technology enablers and AI”, Huawei, juli 2016. https://www.huawei.com/en/huaweitech/publication/winwin/ai/nowhere-to-hide

63 Sadržaj stranice sa studijom slučaja sačuvan je na servisu za onlajn arhiviranje: https://archive.li/pZ9HO

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

65 Huawei, “Huawei Safe City Solution: Safeguards Serbia”, 23. avgust 2018. dostupno na: https://archive.li/pZ9HO

66 NEC, “NEC Face Recognition Technology Ranks First in NIST Accuracy Testing”, 3. oktobar 2019. https://www.nec.com/en/press/201910/global_20191003_01.html; NEC, “NEC Face Recognition Technology Ranks First in NIST Accuracy Testing”, 23. avgust 2021. https://www.nec.com/en/press/202108/global_20210823_01.html

67 NEC, "NEC Unveils 'NEC Group AI and Human Rights Principles'", 2. april 2019. https://www.nec.com/en/press/201904/global_20190402_01.html

68 NEC, "NEC Group AI and Human Rights Principles", 2. april 2019. https://www.nec.com/en/press/201904/images/0201-01-01.pdf

69 F. Ragazzi et al., "Biometric and Behavioural Mass Surveillance in EU Member States", The Greens/EFA in the European Parliament, 1. oktobar 2021. https://www.greens-efa.eu/biometricsurveillance/

70 R. Mahmud, "Brunei receives facial recognition equipment", Borneo Bulletin, 15. mart 2022. https://borneobulletin.com.bn/brunei-receives-facial-recognition-equipment-2/

71 NEC, "NeoFace Watch", https://www.nec.com/en/global/solutions/biometrics/face/neofacewatch.html

72 Ibid.

73 NEC Corporation of America, "The most accurate and fastest face recognition platform available: NeoFace Watch", 2017. https://www.necam.com/docs/?id=3d1b0643-1d6e-4a9a-8195-a9ba79fe4b14

74 I. Burrington, "Why Amazon's Data Centers Are Hidden in Spy Country", The Atlantic, 8. januar 2016. https://www.theatlantic.com/technology/archive/2016/01/amazon-web-services-data-center/423147/

75 Amazon, "AWS Global Infrastructure", https://aws.amazon.com/about-aws/global-infrastructure/

76 D. Harwell, "Oregon became a testing ground for Amazon's facial-recognition policing. But what if Rekognition gets it wrong?", The Washington Post, 30. april 2019. https://www.washingtonpost.com/technology/2019/04/30/amazons-facial-recognition-technology-is-supercharging-local-police/

77 Amazon, "We are implementing a one-year moratorium on police use of Rekognition", 10. juni 2020. https://www.aboutamazon.com/news/policy-news-views/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition

78 J. Dastin, "Amazon extends moratorium on police use of facial recognition software", Reuters, 18. maj 2021. https://www.reuters.com/technology/exclusive-amazon-extends-moratorium-police-use-facial-recognition-software-2021-05-18/

79 Amazon, "What is Amazon Rekognition?", https://docs.aws.amazon.com/rekognition/latest/dg/what-is.html

80 IBM, "What is an API (application programming interface)?", https://www.ibm.com/topics/api

81 Amazon, "How Amazon Rekognition works", https://docs.aws.amazon.com/rekognition/latest/dg/how-it-works.html

82 R. Sauer, "Six principles to guide Microsoft's facial recognition work", Microsoft, 17. decembar 2018. https://blogs.microsoft.com/on-the-issues/2018/12/17/six-principles-to-guide-microsofts-facial-recognition-work/

83 Microsoft, "What is Azure", https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-azure/

84 Microsoft, "What is the Azure AI Face service?", 30. april 2024. https://learn.microsoft.com/en-us/azure/cognitive-services/computer-vision/overview-identity

85 Ibid.

86 N. Crampton, "Microsoft's framework for building AI systems responsibly", Microsoft, 21. jun 2022. https://blogs.microsoft.com/on-the-issues/2022/06/21/microsofts-framework-for-building-ai-systems-responsibly/

87 S. Bird, "Responsible AI investments and safeguards for facial recognition", Microsoft, 21. jun 2022. https://azure.microsoft.com/en-us/blog/responsible-ai-investments-and-safeguards-for-facial-recognition/

88 Microsoft, "Use cases for Azure Face service", 29. septembar 2022. https://learn.microsoft.com/en-us/legal/cognitive-services/face/transparency-note

89 Autoriteit Persoonsgegevens, "AP: Pas op met camera's met gezichtsherkenning", 29. oktobar 2020. https://autoriteitpersoonsgegevens.nl/actueel/ap-pas-op-met-cameras-met-gezichtsherkenning (na holandskom jeziku)

90 Microsoft, "Use cases for Azure Face service", 29. septembar 2022. https://learn.microsoft.com/en-us/legal/cognitive-services/face/transparency-note

91 Ibid.

92 E. Jakubowska, "Do no harm? How the case of Afghanistan sheds light on the dark practice of biometric intervention", Heinrich Böll Stiftung EU, 19. oktobar 2021. https://eu.boell.org/en/2021/10/19/do-no-harm-how-case-afghanistan-sheds-light-dark-practice-biometric-intervention

93 EDPB-EDPS Zajedničko mišljenje 5/2021 o Predlogu uredbe Evropskog parlamenta i Veća o utvrđivanju usklađenih pravila o veštačkoj inteligenciji (Akt o veštačkoj inteligenciji) 18. juna 2021. https://www.edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_hr.pdf

94 Thales Group, "About Thales", https://www.thalesgroup.com/en/global/group

95 Thales Group, "Biometric Solutions", https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics

96 Thales Group, "Designing an ethical, socially accountable facial recognition system: A vision from Thales", 2021, https://www.thalesgroup.com/sites/default/files/database/document/2021-11/gov-wp-facial-recognition-2021.pdf, str. 10

97 Thales Group, "Video-based facial recognition - Thales Facial Recognition Platform", https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-software/live-face-identification-system

98 European Digital Rights (EDRi), "European Parliament: Make sure the AI act protects peoples' rights!", 19. april 2023. https://edri.org/wp-content/uploads/2023/04/PDF-FINAL-Statement-European-Parliament-Make-sure-the-AI-act-protects-peoples-rights.pdf

99 Thales Group, "Video-based facial recognition - Thales Facial Recognition Platform", https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-software/live-face-identification-system

100 European Digital Rights (EDRi), "IBM's facial recognition: the solution cannot be left to companies", 17. juli 2020. https://edri.org/our-work/ibm-facial-recognition-solution-cannot-be-left-to-companies/

101 Videti, na primer, analizu francuske NVO La Quadrature du Net (LQDN) u kojoj se

objašnjava zašto bi takve podatke trebalo smatrati biometrijskim: La Quadrature du Net, "Loi J.O: refusons la surveillance biométrique", https://www.laquadrature.net/biometrie-jo/ (na francuskom)

102 IPVM, "Huawei / Megvii Uyghur Alarms", 8. decembar 2020. https://ipvm.com/reports/huawei-megvii-uygur

103 BBC, "Who are the Uyghurs and why is China being accused of genocide?", 24. maj 2022. https://www.bbc.co.uk/news/world-asia-china-22278037

104 IPVM, "Huawei / Megvii Uyghur Alarms", 8. decembar 2020. https://ipvm.com/reports/huawei-megvii-uygur

105 Ibid.

106 Amazon, "What is Amazon Rekognition?", https://docs.aws.amazon.com/rekognition/latest/dg/what-is.html

107 Amazon, "Guidelines on face attributes", https://docs.aws.amazon.com/rekognition/latest/dg/guidance-face-attributes.html

108 M. Wood, "Thoughts On Machine Learning Accuracy", AWS News Blog, 27. juli 2018. https://aws.amazon.com/blogs/aws/thoughts-on-machine-learning-accuracy/

109 Amazon, "FaceDetail - Amazon Rekognition", https://docs.aws.amazon.com/rekognition/latest/APIReference/API_FaceDetail.html

110 Amazon, "Emotion - Amazon Rekognition", https://docs.aws.amazon.com/rekognition/latest/APIReference/API_Emotion.html

111 Microsoft, "Use cases for Azure AI Face service", 17. novembar 2023. https://learn.microsoft.com/en-us/legal/cognitive-services/face/transparency-note

112 S. Bird, "Responsible AI investments and safeguards for facial recognition", Microsoft, 21. juni 2022. https://azure.microsoft.com/en-us/blog/responsible-ai-investments-and-safeguards-for-facial-recognition

113 Microsoft, "Face detection, attributes, and input data", 30. april 2024. https://learn.microsoft.com/en-us/azure/cognitive-services/computer-vision/concept-face-detection

114 Amazon, "Gender - Amazon Rekognition", https://docs.aws.amazon.com/rekognition/latest/APIReference/API_Gender.html

115 Amazon, "KnownGender - Amazon Rekognition" https://docs.aws.amazon.com/rekognition/latest/APIReference/API_KnownGender.html

116 Microsoft, "Face detection, attributes, and input data", 30. april 2024. https://learn.microsoft.com/en-us/azure/cognitive-services/computer-vision/concept-face-detection

117 Amazon, "Landmark - Amazon Rekognition" https://docs.aws.amazon.com/rekognition/latest/APIReference/API_Landmark.html

118 Huawei, "Huawei Intelligent Video Surveillance Product Brochure", 8. mart 2019. https://e.huawei.com/en/material/local/8cc4272f73664757977a5fd128e-53a6c

119 Ibid.

120 Ibid.

121 Huawei, "NVR800 User Guide - Features", 31. oktobar 2020. https://support.huawei.com/hedex/hdx.do?docid=EDOC1100166735&id=EN-US_TOPIC_0222303676, str. 10

122 Huawei, "NVR800 Distribution Solution 3.0 - Residential District", 20. januar 2022. https://support.huawei.com/enterprise/en/doc/EDOC1100206847/691710f4/residential-district

123 Amazon, "People pathing - Amazon Rekognition", https://docs.aws.amazon.com/rekognition/latest/dg/persons.html

124 F. Cheng, M. Pivida, "Transitioning from Amazon Rekognition people pathing: Exploring other alternatives", AWS Machine Learning Blog, 24. oktobar 2024. https://aws.amazon.com/blogs/machine-learning/transitioning-from-amazon-rekognition-people-pathing-exploring-other-alternatives/

125 NEC Corporation of America, "The most accurate and fastest face recognition platform available: NeoFace Watch", 2017. https://www.necam.com/docs/?id=3d1b0643-1d6e-4a9a-8195-a9ba79fe4b14

126 Ibid.

127 A. Hern, "TechScape: Clearview AI was fined £7.5m for brazenly harvesting your data – does it care?", The Guardian, 25. maj 2022. https://www.theguardian.com/technology/2022/may/25/techscape-clearview-ai-facial-recognition-fine

128 CNIL, "Facial recognition: 20 million euros penalty against Clearview AI", 20. oktobar 2022. https://web.archive.org/web/20221021005057/https://www.cnil.fr/en/facial-recognition-20-million-euros-penalty-against-clearview-ai

129 Clearview AI, "Clearview AI Wins Appeal Against U.K. Information Commissioner Office (ICO) Fine", 19. oktobar 2023. https://www.clearview.ai/press-room/clearview-ai-wins-appeal-against-uk-information-commissioner-office-ico-fine

130 European Data Protection Board, "Facial recognition: Italian SA fines Clearview AI EUR 20 million", 10. mart 2022. https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en

131 CNIL, "Facial recognition: the CNIL imposes a penalty payment on Clearview AI", 10. maj 2023. dostupno na: https://web.archive.org/web/20230614161044/https://www.cnil.fr/en/facial-recognition-cnil-imposes-penalty-payment-clearview-ai

132 Autoriteit Persoonsgegevens, "Dutch DPA imposes a fine on Clearview because of illegal data collection for facial recognition", 3. septembar 2024. https://www.autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-imposes-a-fine-on-clearview-because-of-illegal-data-collection-for-facial-recognition

133 Office of the Privacy Commissioner of Canada, "Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta", 2. februar 2021. https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/

134 ACLU of Illinois, "In Big Win, Settlement Ensures Clearview AI Complies With Groundbreaking Illinois Biometric Privacy Law", 9. maj 2022. https://www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-com-

plies-with-groundbreaking-illinois

135 J. Clayton, B. Derico, "Clearview AI used nearly 1m times by US police, it tells the BBC", BBC News, 27. mart 2023. https://www.bbc.com/news/technology-65057011

136 Clearview AI, "Company Overview", https://www.clearview.ai/overview

137 R. Mac, C. Haskins, A. Pequeño IV, "Police In At Least 24 Countries Have Used Clearview AI. Find Out Which Ones Here.", BuzzFeed News, 25. avgust 2021. https://www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table

138 European Data Protection Board, "Swedish DPA: Police unlawfully used facial recognition app", 12. februar 2021. https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en

139 NOYB, "Complaint under Article 77(1), 80(1) GDPR, noyb Case-No: C043", 26. maj 2021. https://noyb.eu/sites/default/files/2021-05/Clearview%20AI%20-%20EN%20DE%20-%20noyb%20-%20redacted.pdf, str. 3-5

140 PimEyes, "PimEyes: Face Search Engine Reverse Image Search", https://pimeyes.com/en

141 Big Brother Watch, "Big Brother Watch files legal complaint against facial recognition 'search engine', Pimeyes", 8. novembar 2022. https://bigbrotherwatch.org.uk/press-releases/pimeyes-press-release/

142 PimEyes, "PimEyes' Statement on allegations made by Big Brother Watch", https://pimeyes.com/en/blog/pimeyes-statement-on-allegations-made-by-big-brother-watch

143 PimEyes, "More about PimEyes' database and opt-out service", https://pimeyes.com/en/blog/more-about-pimeyes-database-and-opt-out-service

144 Council of the European Union, "Artificial intelligence (AI) act: Council gives final green light to the first worldwide rules on AI", 21. maj 2024. https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/

145 Uredba Evropskog parlamenta i Veća o utvrđivanju usklađenih pravila o veštačkoj inteligenciji (Akt o veštačkoj inteligenciji) i izmeni određenih zakonodavnih akata Unije, 13. juna 2024. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

146 "Enhanced face recognition in video - US9355301B2", Google Patents, https://patents.google.com/patent/US9355301B2/

147 Ibid.

148 "Sharing video footage from audio/video recording and communication devices for parcel theft deterrence - US10210727B2", Google Patents, https://patents.google.com/patent/US10210727B2/

149 Ibid.

150 "Grouping and ranking images based on facial recognition data - US9773156B2", Google Patents, https://patents.google.com/patent/US9773156B2/

151 Ibid.

152 "Face recognition in video content - US8494231B2", Google Patents, https://patents.google.com/patent/US8494231B2/

153 "Verifying identity based on facial dynamics - US10282530B2", Google Patents, https://patents.google.com/patent/US10282530B2/

154 "Adaptive image cropping for face recognition - US10872258B2", Google Patents, https://patents.google.com/patent/US10872258B2/

155 Clearview AI, "Clearview AI's Revolutionary Facial Recognition Platform Awarded U.S. Patent", 31. januar 2022. https://www.clearview.ai/press-room/clearview-ais-revolutionary-facial-recognition-platform-awarded-us-patent

156 "Methods for Providing Information about a Person Based on Facial Recognition - US20210042527A1", Google Patents, https://patents.google.com/patent/US20210042527A1/

157 Ibid.

158 Ibid.

159 Ibid.

160 Ibid.

161 L. Rhue, "Racial Influence on Automated Perceptions of Emotions", 9. novembar 2018. https://dx.doi.org/10.2139/ssrn.3281765

162 Clearview AI, "Clearview AI Awarded U.S. Patent for Highly Accurate, Bias-Free Facial Recognition Algorithm", 28. septembar 2022. https://www.clearview.ai/clearview-ai-awarded-us-patent-for-highly-accurate-bias-free-facial-recognition-algorithm

163 "Scalable training data preparation pipeline and efficient distributed trainer for deep neural networks in facial recognition - US11443553B1", Google Patents, https://patents.google.com/patent/US11443553B1/

164 Ibid.

165 Y. Gorokhovskaia, A. Shahbaz, A. Slipowitz, "Freedom in the World 2023: Marking 50 Years in the Struggle for Democracy", Freedom House, 2023. https://freedomhouse.org/report/freedom-world/2023/marking-50-years

166 A. Shahbaz, A. Funk, K. Vesteinsson, "Freedom on the Net 2022: Countering an Authoritarian Overhaul of the Internet", Freedom House, 2022. https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet

167 E. Jakubowska, H. Maryam, M. Mahmoudi, "Retrospective facial recognition surveillance conceals human rights abuses in plain sight", Euronews, 14. april 2023. https://www.euronews.com/2023/04/14/retrospective-facial-recognition-surveillance-conceals-human-rights-abuses-in-plain-sight

168 J. Mudditt, "The nation where your 'faceprint' is already being tracked", BBC, 24. jun 2022. https://www.bbc.com/future/article/20220616-the-nation-where-your-faceprint-is-already-being-tracked; J. Blakkarly, "Push for new law to regulate facial recognition technology", CHOICE, 27. septembar 2022. https://www.choice.com.au/consumers-and-data/data-collection-and-use/how-your-data-is-used/articles/new-law-to-regulate-facial-recognition; M. Andrejevic et al., "How should we regulate the use of facial recognition in Australia?", Monash University, 21. juni 2022. https://lens.monash.edu/@politics-socie-

ty/2022/06/21/1384816/how-should-we-regulate-the-use-of-facial-recognition-in-australia

169 R. Crozier, "Govts agree on national face matching database", iTnews, 5. oktobar 2017. https://www.itnews.com.au/news/govts-agree-on-national-face-matching-database-474759; C. Petrie, "Identity-matching Services Bill 2019 and Australian Passports Amendment (Identity-matching Services) Bill 2019", Bills Digest No. 21, 2019–20, Parliament of Australia, 26. avgust 2019. https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd1920a/20bd021#_Toc16773923

170 Australia's Federal Relations Architecture, "Intergovernmental Agreement on Identity Matching Services", 5. oktobar 2017. https://federation.gov.au/about/agreements/intergovernmental-agreement-identity-matching-services, odeljak 8.

171 J. Hendry, "First states upload data to national facial recognition system", ITnews, 17. septembar 2019. https://www.itnews.com.au/news/first-states-upload-data-to-national-facial-recognition-system-531084; L. Pascu, "Western Australia joins national facial biometrics matching database", Biometric Update, 2. april 2020. https://www.biometricupdate.com/202004/western-australia-joins-national-facial-biometrics-matching-database; C. Petrie, "Identity-matching Services Bill 2019 and Australian Passports Amendment (Identity-matching Services) Bill 2019", Bills Digest No. 21, 2019–20, Parliament of Australia; 26. avgust 2019. https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd1920a/20bd021#_ftnref74

172 A. Macdonald, "Pending bill delays biometric data upload to drivers' license database in Australia", Biometric Update, 13. oktobar 2020. https://www.biometricupdate.com/202010/pending-bill-delays-biometric-data-upload-to-drivers-license-database-in-australia; C. Tonkin, "Government building national facial recognition database", Australian Computer Society, 1. februar 2022. https://ia.acs.org.au/article/2022/government-building-national-facial-recognition-database.html

173 S. Martin, "Committee led by Coalition rejects facial recognition database in surprise move", The Guardian, 24. oktobar 2019. https://www.theguardian.com/australia-news/2019/oct/24/committee-led-by-coalition-rejects-facial-recognition-database-in-surprise-move

174 C. Petrie, "Identity-matching Services Bill 2019 and Australian Passports Amendment (Identity-matching Services) Bill 2019", Bills Digest No. 21, 2019–20, Parliament of Australia, 26. avgust 2019. https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd1920a/20bd021#_Toc16773923

175 Izveštaj komiteta dostupan je ovde: Parliamentary Joint Committee on Intelligence and Security, "Advisory report on the Identity-matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019", Parliament of Australia, 2019. https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024343/toc_pdf/AdvisoryreportontheIdentity-matchingServicesBill2019andtheAustralianPassportsAmendment(Identity-matchingServices)Bill2019.pdf

176 J. Brookes, "Govt mulls facial recognition bill reheat", InnovationAus.com, 16. januar 2023. https://www.innovationaus.com/govt-mulls-facial-recognition-bill-reheat/

177 Office of the Australian Information Commissioner, "Variation to extend term of MOU in relation to National Facial Biometric Matching Capability 2020", 30. juni 2020. https://www.oaic.gov.au/about-the-OAIC/our-corporate-information/memorandums-of-understanding/current-memorandums-of-understanding/national-facial-biometric-matching-capability/variation-to-extend-term-of-mou-in-relation-to-national-facial-biometric-matching-capability-2020

178 Sažete informacije o ovom zakonskom aktu se mogu naći na sajtu australijske Vlade ovde: https://www.digitalidsystem.gov.au/what-is-digital-id/digital-id-act-2024#what-is-the-digital-id-act

179 I. Aldridge and G. Pecora, "New Digital ID Bill raises serious privacy concerns for Australians", Lawyers Weekly, 17. jun 2024. https://www.lawyerweekly.com.au/politics/39896-new-digital-id-bill-raises-serious-privacy-concerns-for-australians

180 J. Taylor, "Calls to stop NSW police trial of national facial recognition system over lack of legal safeguards", The Guardian, 30. jun 2021. https://www.theguardian.com/australia-news/2021/jul/01/calls-to-stop-nsw-police-trial-of-national-facial-recognition-system-over-lack-of-legal-safeguards

181 J. Taylor, "Calls to stop NSW police trial of national facial recognition system over lack of legal safeguards", The Guardian, 30. jun 2021. https://www.theguardian.com/australia-news/2021/jul/01/calls-to-stop-nsw-police-trial-of-national-facial-recognition-system-over-lack-of-legal-safeguards; J. Hendry, "Facial recognition use 'misunderstood': NSW Police", InnovationAus.com, 11. oktobar 2022. https://www.innovationaus.com/facial-recognition-use-misunderstood-nsw-police/

182 E. Tlozek, "SA Police could use Adelaide city facial recognition technology, despite being asked not to", ABC News, 19. jun 2022. https://www.abc.net.au/news/2022-06-20/sa-police-could-use-adelaide-city-facial-recognition-technology/101166064

183 C. Kelly, "Protesters 'should expect' Australian police to use facial recognition", The New Daily, 13. jun, 2020. https://thenewdaily.com.au/news/2020/06/13/facial-recognition-police-protest/; J. Brookes, "Facial recognition and the NSW protest crowds", InnovationAus.com, 27. jul 2021. https://www.innovationaus.com/facial-recognition-and-the-nsw-protest-crowds/

184 B. Kaye, "Australia's two largest states trial facial recognition software to police pandemic rules", Reuters, 17. septembar, 2021. https://www.reuters.com/world/asia-pacific/australias-two-largest-states-trial-facial-recognition-software-police-pandemic-2021-09-16/

185 S. Grill, "CHOICE raises concern over Bunnings, Kmart and the Good Guys use of facial recognition technology", ABC News, 15. jun 2022. https://www.abc.net.au/news/2022-06-15/choice-investigation-major-retailers-using-facial-recognition/101153384

186 J. Taylor, "7-Eleven took photos of some Australian customers' faces without consent, privacy commissioner rules", The Guardian, 14. oktobar 2021. https://www.theguardian.com/australia-news/2021/oct/14/7-eleven-took-photos-of-some-australian-customers-faces-without-consent-privacy-commissioner-rules

187 Office of the Australian Information Commissioner, "OAIC and UK's ICO open

joint investigation into Clearview AI Inc.", 9. juli 2020. https://www.oaic.gov.au/newsroom/oaic-and-uks-ico-open-joint-investigation-into-clearview-ai-inc.

188 A. Bogle, "Australian federal police tested controversial facial recognition search engine, FOI documents reveal", The Guardian, 26. oktobar 2023. https://www.theguardian.com/australia-news/2023/oct/24/australian-federal-police-afp-pimeyes-facial-recognition-facecheck-id-search-engine-platform

189 Australian Human Rights Commission, "Technology and Human Rights", https://humanrights.gov.au/our-work/technology-and-human-rights; Australian Human Rights Commission, "Australians Deserve Technology that Protects Human Rights", 27. maj 2021. https://humanrights.gov.au/about/news/media-releases/australians-deserve-tech-protects-their-rights

190 N. Davis, L. Perry, E. Santow, "Facial recognition technology: Towards a model law", Human Technology Institute, The University of Technology Sydney, septembar 2022. https://www.uts.edu.au/sites/default/files/2022-09/Facial%20recognition%20model%20law%20report.pdf

191 Združeni parlamentarni komitet za ljudska prava (PJCHR) ustanovljen je Zakonom o ljudskim pravima iz 2011: Parliament of Australia, Human Rights (Parliamentary Scrutiny) Act 2011, No. 186, https://www.legislation.gov.au/Details/C2016C00195; osnovna funkcija komiteta jeste da preispita sve zakone i pravne instrumente sa stanovišta njihove usklađenosti sa ljudskim pravima, kako su ta prava definisana zakonom, videti: Australian Human Rights Commission, "Parliamentary Joint Committee on Human Rights", https://humanrights.gov.au/our-work/rights-and-freedoms/parliamentary-joint-committee-human-rights

192 A. Fletcher, "Government surveillance and facial recognition in Australia: a human rights analysis of recent developments", Griffith Law Review, 32:1, 30-61, 2023. https://doi.org/10.1080/10383441.2023.2170616

193 Istorija najvažnijih amandmana dostupna je ovde: Office of the Australian Information Commissioner, "History of the Privacy Act", https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act/history-of-the-privacy-act

194 Najnovija verzija dostupna je ovde: Parliament of Australia, Privacy Act 1988, No. 119, https://www.legislation.gov.au/Details/C2022C00361

195 Office of the Australian Information Commissioner, "Biometric scanning", https://www.oaic.gov.au/privacy/your-privacy-rights/surveillance-and-monitoring/biometric-scanning

196 Ovaj aspekt regulisanja biometrijskih informacija u Zakonu o privatnosti kritikovan je kao neadekvatan i zastareo, videti: S. Burns et al., "Facial recognition and artificial intelligence in Australia. Do we need more rules?", Gilbert + Tobin, 25. juli 2022. https://www.gtlaw.com.au/knowledge/facial-recognition-artificial-intelligence-australia-do-we-need-more-rules

197 Prema tumačenju OAIC, postoje četiri ključna elementa pristanka: osoba je adekvatno informisana pre davanja pristanka, osoba daje pristanaj dobrovoljno, pristanak je ažuran i konkretan, i osoba je sposobna da razume i komunicira svoj pristanak; videti: Office of the Australian Information Commissioner, "Australian Privacy Principles guidelines", Odeljak B, 21. decembar 2022. https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-b-key-concepts#consent

198 Tačka 3.4.(a) Principa 3 Australijskih principa privatnosti.

199 Tačka 3.4. (d) Principa 3 Australijskih principa privatnosti.

200 N. Davis, L. Perry, E. Santow, "Facial recognition technology: Towards a model law", Human Technology Institute, The University of Technology Sydney, septembar 2022. https://www.uts.edu.au/sites/default/files/2022-09/Facial%20recognition%20model%20law%20report.pdf, str. 37

201 Office of the Australian Information Commissioner, "OAIC and UK's ICO open joint investigation into Clearview AI Inc.", 9. juli 2020. https://www.oaic.gov.au/newsroom/oaic-and-uks-ico-open-joint-investigation-into-clearview-ai-inc.

202 Office of the Australian Information Commissioner, "OAIC and ICO conclude joint investigation into Clearview AI", 3. novembar 2021. https://www.oaic.gov.au/newsroom/oaic-and-ico-conclude-joint-investigation-into-clearview-ai

203 Tekst odluke dostupan je ovde: Australian Information Commissioner, "Commissioner initiated investigation into Clearview AI, Inc. (Privacy) [2021] AICmr 54", 14. oktobar 2021. http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2021/54.html

204 Office of the Australian Information Commissioner, "Clearview AI breached Australians' privacy", 3. novembar 2021. https://www.oaic.gov.au/newsroom/clearview-ai-breached-australians-privacy

205 Ibid.

206 J. Siganto, "Clearview AI Australia Found To Have Breached Privacy Laws", Privacy 108, 18. mart 2022. https://privacy108.com.au/insights/clearview-ai-australia-privacy-breach/

207 Tekst odluke dostupan je ovde: Australian Information Commissioner, "Commissioner Initiated Investigation into the Australian Federal Police (Privacy) [2021] AICmr 74", 26. novembar 2021. http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2021/74.html

208 Office of the Australian Information Commissioner, "AFP ordered to strengthen privacy governance", 16. decembar 2021. https://www.oaic.gov.au/newsroom/afp-ordered-to-strengthen-privacy-governance

209 C. Wilson, "'World's most controversial company' Clearview AI still being used to solve Australian police cases", Crikey., 25. januar 2024. https://www.crikey.com.au/2024/01/25/clearview-ai-australian-police-operation-renewed-hope/

210 Office of the Australian Information Commissioner, "Statement on Clearview AI", 21. avgust 2024. https://www.oaic.gov.au/news/media-centre/statement-on-clearview-ai

211 Sistem veštačke inteligencije dizajniran da identifikuje osobe sa daljine upoređivanjem njihovih biometrijskih podataka sa podacima uskladištenim u referentnoj bazi podataka ili spremištu podataka.

212 F. Ragazzi et al., "Biometric and Behavioural Mass Surveillance in EU Member States", The Greens/EFA in the European Parliament, 1. oktobar 2021. https://www.greens-efa.eu/biometricsurveillance/

213 E. De Marco, Aeris, "Impacts of the use of biometric and behavioural mass surveillance technologies on human rights and the rule of law", The Greens/ EFA

in the European Parliament, februar 2022. https://extranet.greens-efa-service.eu/public/media/file/1/7487

214 VIS – vizni informacioni sistem (Visa Information System), SIS – šengenski informacioni sistem (Schengen Information System), ECRIS – evropski sistem krivičnih dosijea (European Criminal Records System), ETIAS – evropski sistem za putne informacije i autorizaciju (European Travel Information and Authorisation System), EES – sistem ulaz/izlaz (Entry/Exit System).

215 European Union's Fundamental Rights Agency, "Facial recognition technology: fundamental rights considerations in the context of law enforcement", 2020. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

216 European Digital Rights (EDRi), "New EU law amplifies risks of state overreach and mass surveillance", 7. septembar 2022. https://edri.org/our-work/new-eu-law-amplifies-risks-of-state-over-reach-and-mass-surveillance/

217 P. De Hert, G. Bouchagiar, "Visual and biometric surveillance in the EU. Saying 'no' to mass surveillance practices?", Information Polity 27, 193-217, 2022. https://content.iospress.com/download/information-polity/ip211525?id=information-polity%2Fip211525

218

219 M. Heikkila, "European Parliament calls for a ban on facial recognition", Politico, 6. oktobar 2021. https://www.politico.eu/article/european-parliament-ban-facial-recognition-brussels/

220 C. Thorbecke, "Citing human rights risks, UN calls for ban on certain AI tech until safeguards are set up", ABC News, 15. septembar 2021. https://abcnews.go.com/Technology/citing-human-rights-risks-calls-ban-ai-tech/story?id=80034073

221 L. Peets et al., "European Parliament Votes in Favor of Banning the Use of Facial Recognition in Law Enforcement", Covington Inside Privacy, 12. oktobar 2021. https://www.insideprivacy.com/artificial-intelligence/european-parliament-votes-in-favor-of-banning-the-use-of-facial-recognition-in-law-enforcement/

222 European Data Protection Board, "EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination", 21. jun 2021. https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en

223 Amnesty International, "Amnesty International and more than 170 organisations call for a ban on biometric surveillance", 7. jun 2021. https://www.amnesty.org/en/latest/press-release/2021/06/amnesty-international-and-more-than-170-organisations-call-for-a-ban-on-biometric-surveillance/

224 Reclaim Your Face, https://reclaimyourface.eu/

225 E. Pollina, F. Maccioni, "Italy outlaws facial recognition tech, except to fight crime", Reuters, 14. novembar 2022. https://www.reuters.com/technology/italy-outlaws-facial-recognition-tech-except-fight-crime-2022-11-14/

226 M. Heikkila, "German coalition backs ban on facial recognition in public places", Politico, 24. novembar 2021. https://www.politico.eu/article/german-coalition-backs-ban-on-facial-recognition-in-public-places/

227 Reclaim Your Face, "Portugal: Proposed law tries to sneak in biometric mass surveillance", 15. novembar 2021. https://reclaimyourface.eu/portugal-proposed-law-tries-to-sneak-in-biometric-mass-surveillance/

228 A. Lodie, S. Celis Juarez, "AI-Assisted Security at the Paris 2024 Olympic Games: From Facial Recognition to Smart Video", AI Regulation, 27. januar 2023. https://ai-regulation.com/ai-driven-systems-paris-olympics/

229 MEP Patrick Breyer, "Expect biometric mass surveillance in Paris in 2024: French Parliament approves automated monitoring of public spaces for 'suspicious behaviour'", Patrick-Breyer.de, 24. mart 2023. https://www.patrick-breyer.de/en/expect-biometric-mass-surveillance-in-paris-in-2024-french-parliament-approves-automated-monitoring-of-public-spaces-for-suspicious-behaviour/

230 MEP Patrick Breyer, "Vote to stop a future of biometric mass surveillance in Europe!", Patrick-Breyer.de, 17. mart 2023. https://www.patrick-breyer.de/wp-content/uploads/2023/03/MEP-letter-to-FR-MPs-about-biometric-mass-surveillance-in-2024-Olympic-law.pdf

231 N. Aszódi, "Open letter: the German government should stand up for a strong ban on biometric surveillance in the Council of EU negotiations regarding the AI Act", AlgorithmWatch, 8. novembar 2022. https://algorithmwatch.org/en/open-letter-german-government-biometric-surveillance-ai-act/

232 Uredba (EU) 2016/679 Evropskog parlamenta i Veća od 27. aprila 2016. o zaštiti lica u vezi s obradom podataka i o ličnosti i slobodnom kretanju takvih podataka te o stavljanju van snage Direktive 95/46/EZ (Opšta uredba o zaštiti podataka) (Tekst značajan za EGP) 2016. https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:32016R0679

233 Direktiva (EU) 2016/680 Evropskog parlamenta i Veća od 27. aprila 2016. o zaštiti lica u vezi s obradom podataka o ličnosti od strane nadležnih tela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih dela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju van snage Okvirne odluke Veća 2008/977/PUP, 2016. https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:32016L0680

234 GDPR, član 4 (14); LED, član 3 (13).

235 Article 29 Data Protection Working Party, "Opinion 3/2012 on developments in biometric technologies", 27. april 2012. https://www.pdpjournals.com/docs/87998.pdf

236 GDPR, član 9, paragraf 1; LED, član 10.

237 S. Barros Vale, G. Zanfir-Fortuna, "Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities", The Future of Privacy Forum, maj 2022. https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf, str. 41

238 Uredba Evropskog parlamenta i Veća o utvrđivanju usklađenih pravila o veštačkoj inteligenciji (Akt o veštačkoj inteligenciji) i izmeni određenih zakonodavnih akata Unije, 13. jun 2024. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

239 European Data Protection Board, "EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination", 21. jun 2021. https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-auto-

mated-recognition-human-features-publicly-accessible_en

240 Council of the European Union, "Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights", 6. decembar 2022. https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/

241 European Parliament, "AI Act: a step closer to the first rules on Artificial Intelligence", 11. maj 2023. https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence

242 European Parliament, "MEPs ready to negotiate first-ever rules for safe and transparent AI", 14. jun 2023. https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai

243 European Digital Rights (EDRi), "EU Parliament calls for ban of public facial recognition, but leaves human rights gaps in final position on AI Act", 14. jun 2023. https://edri.org/our-work/eu-parliament-plenary-ban-of-public-facial-recognition-human-rights-gaps-ai-act/; Access Now, "Historic vote in the European Parliament: dangerous AI surveillance banned, but not for migrant people at the borders", 14. jun 2023. https://www.accessnow.org/press-release/historic-vote-in-the-european-parliament-dangerous-ai-surveillance-banned-but-not-for-migrant-people-at-the-borders/

244 European Digital Rights (EDRi), "European Parliament calls loud and clear for a ban on biometric mass surveillance in AI Act", 14. septembar 2022. https://edri.org/our-work/european-parliament-calls-loud-and-clear-for-a-ban-on-biometric-mass-surveillance-in-ai-act/

245 L. R. Helfer, E. Voeten, "International Courts as Agents of Legal Change: Evidence from LGBT Rights in Europe", 68 International Organization 77-110, 2014. https://scholarship.law.duke.edu/faculty_scholarship/2402/

246 M. Brkan, "The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core", European Constitutional Law Review, Volume 14, Issue 2, juni 2018. str. 332 - 368, https://doi.org/10.1017/S1574019618000159

247 European Court of Human Rights, "Case of S. and Marper v. the United Kingdom", 4. decembar 2008. https://rm.coe.int/168067d216

248 European Court of Human Rights, "Gaughran v. The United Kingdom", 13. februar 2020. https://hudoc.echr.coe.int/en?i=002-12731

249 European Court of Human Rights, "Case of Uzun v. Germany", 2. septembar 2010. https://hudoc.echr.coe.int/en?i=001-100293

250 The Court of Justice of the European Union, "La Quadrature du Net and Others", 6. oktobar 2020. https://curia.europa.eu/juris/liste.jsf?language=en&num=c-511/18&td=ALL

251 Article 19, "When bodies become data: Biometric technologies and freedom of expression", april 2021. https://www.article19.org/wp-content/uploads/2021/05/Biometric-Report-P3-min.pdf

252 European Data Protection Board, "Facial recognition in school renders Sweden's first GDPR fine", 22. avgust 2019. https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_sv

253 CNIL, "Expérimentation de la reconnaissance faciale dans deux lycées: la CNIL précise sa position", 29. oktobar, 2019. https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position (na francuskom); European Data Protection Board, "Fine for processing students' fingerprints imposed on a school", 5. mart 2020. https://www.edpb.europa.eu/news/national-news/2020/fine-processing-students-fingerprints-imposed-school_en; S. Weale, "ICO to step in after schools use facial recognition to speed up lunch queue", The Guardian, 18. oktobar 2021. https://www.theguardian.com/education/2021/oct/18/privacy-fears-as-schools-use-facial-recognition-to-speed-up-lunch-queue-ayrshire-technology-payments-uk; Tribunal Administratif de Marseille, "Laquadrature du net et autres", 27. februar, 2020. https://www.laquadrature.net/wp-content/uploads/sites/8/2020/02/1090394890_1901249.pdf (na francuskom).

254 European Data Protection Board, "Swedish DPA: Police unlawfully used facial recognition app", 12. februar 2021. https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en

255 Garante per la Protezione dei Dati Personali, "Facial recognition: the SARI Real Time system is not compliant with privacy laws", 16. april 2021. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9575842

256 European Data Protection Board, "News", https://edpb.europa.eu/news/news_en

257 Prema ovom izveštaju: Common Cause, Lokniti – Centre for the Study Developing Societies (CSDS), "Status of Policing in India Report 2023: Surveillance and the Question of Privacy", 2023. https://www.commoncause.in/wotadmin/upload/REPORT_2023.pdf; policija u Indiji ima opsežne planove za prediktivan policijski rad, dok će se uloga FRT u njegovoj primeni tek videti.

258 Internet Freedom Foundation, Panoptic, "About", https://panoptic.in/about

259 Broj varira u zavisnosti od izvora; od 440.000 prema: P. Bischoff, "Surveillance Camera Statistics: Which City has the Most CCTV Cameras?", Comparitech, 23. maj 2023. https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/; do 900.000 prema: Q. Inzamam, H. Qadri, "This Part of India Is on the Verge of Becoming a Complete Surveillance State", Slate, 13. juli 2022. https://slate.com/technology/2022/07/telangana-india-surveillance-state.html

260 Amnesty International, "Ban The Scan Hyderabad", https://banthescan.amnesty.org/hyderabad/#num-14

261 R. R. Jain, "Facial recognition wielded in India to enforce COVID policy", AP News, 20. decembar 2022. https://apnews.com/article/technology-health-india-hyderabad-law-enforcement-9b5e249d7ef5cefd3c6dc74c2c4b5b84

262 Indijske nacionalne mreže i sistemi za praćenje kriminala i počinilaca (Crime and Criminal Tracking Networks and Systems, CCTNS), što je naziv za nacionalnu bazu koja sadrži milione slika kriminalaca i nestalih: Q. Inzamam, H. Qadri, "This Part of India Is on the Verge of Becoming a Complete Surveillance State", Slate, 13. juli 2022. https://slate.com/technology/2022/07/telangana-india-surveillance-state.html

263 Al Jazeera, "Facial recognition taken to court in India's surveillance hotspot", 20. januar 2022. https://www.aljazeera.com/news/2022/1/20/india-surveil-

lance-hotspot-telangana-facial-recognition-court-lawsuit-privacy; R. R. Jain, "Facial recognition wielded in India to enforce COVID policy", AP News, 20. decembar 2022. https://apnews.com/article/technology-health-india-hyderabad-law-enforcement-9b5e249d7ef5cefd3c6dc74c2c4b5b84

264 V. Bansal, "Meet the man who sued an Indian state over police facial recognition technology", The Record, 20. februar 2022. https://therecord.media/meet-the-man-who-sued-an-indian-state-over-facial-recognition-technology; K. Bapat, "Telangana High Court issues notice in India's first legal challenge to the deployment of Facial Recognition Technology", Internet Freedom Foundation, 3. januar 2022. https://internetfreedom.in/telangana-high-court-issues-notice-in-indias-first-legal-challenge-to-the-deployment-of-facial-recognition-technology/

265 A. Ghosh, "Facial Recognition Is Out of Control in India", Vice, 13. jun 2022. https://www.vice.com/en/article/akew98/facial-recognition-is-out-of-control-in-india

266 N.T. Sarasvati, "How facial recognition-based surveillance restricted this Hyderabad resident's freedoms", MediaNama, 10. januar 2023. https://www.medianama.com/2023/01/223-facial-recognition-surveillance-tactics-hyderabad-resident-constitutional-freedoms/

267 H. Suresh, "Why Hyderabad became India's surveillance capital", The News Minute, 7. decembar, 2021. https://www.thenewsminute.com/article/why-hyderabad-became-india-s-surveillance-capital-158466; K. Sambhav, "EXCLUSIVE: Telangana Offered Its Own 360 Degree Citizen Tracking System To Modi Govt", HuffPost, 18. mart 2020. https://www.huffpost.com/archive/in/entry/telangana-samagram-system-social-registry_in_5e721e19c5b-63c3b64881b30; K. Sambhav, "EXCLUSIVE: Telangana Offered Its Own 360 Degree Citizen Tracking System To Modi Govt", The Reporters' Collective, 19. mart 2020. https://www.reporters-collective.in/stories/exclusive-telangana-offered-its-own-360-degree-citizen-tracking-system-to-modi-govt

268 Al Jazeera, "India's Telangana to test facial recognition in local elections", 22. januar 2020. https://www.aljazeera.com/news/2020/1/22/indias-telangana-to-test-facial-recognition-in-local-elections

269 Grad pod najvećim nadzorom u Indiji, mada ima pet puta manje stanovnika od najnaseljenijeg, jeste Indor, videti: P. Bischoff, "Surveillance Camera Statistics: Which City has the Most CCTV Cameras?", Comparitech, 23. maj 2023. https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/; M. Lu, "Ranked: The World's Most Surveilled Cities", Visual Capitalist, 6. oktobar 2022. https://www.visualcapitalist.com/ranked-the-worlds-most-surveilled-cities/

270 S. Santoshini, "Indian police use facial recognition to persecute Muslims and other marginalized communities", Coda Story, 11. oktobar, 2022. https://www.codastory.com/authoritarian-tech/india-police-facial-recognition/; Hindustan Times, "2 yrs after Delhi riots: 2,456 held, 2 convicted", 24. februar 2022. https://www.hindustantimes.com/cities/delhi-news/2-yrs-after-delhi-riots-2456-held-2-convicted-101645660761884.html

271 A. Jain, "Delhi Police's claims that FRT is accurate with a 80% match are 100% scary", Internet Freedom Foundation, 17. avgust 2022. https://internetfreedom.in/delhi-polices-frt-use-is-80-accurate-and-100-scary/

272 Hindustan Times, "India's use of facial recognition tech during protests causes stir", 20. avgust 2022. https://tech.hindustantimes.com/tech/news/india-s-use-of-facial-recognition-tech-during-protests-causes-stir-story-IL-6fRtv9K43vrwWhuowA2M.html

273 NDTV, "Facial Recognition For Entry To Indian Airports Begins", 2. decembar 2022. https://www.ndtv.com/india-news/at-3-airports-in-india-facial-recognition-based-entry-from-today-3568817; N. Deuskar, "Facial recognition system rollout at Indian airports raises privacy concerns", Scroll, 14. decembar 2022. https://scroll.in/article/1038975/facial-recognition-system-roll-out-at-indian-airports-raises-privacy-concerns

274 N. Deuskar, "Facial recognition system rollout at Indian airports raises privacy concerns", Scroll, 14. decembar 2022. https://scroll.in/article/1038975/facial-recognition-system-roll-out-at-indian-airports-raises-privacy-concerns

275 A. Kimery, "India set to stand up world's largest government facial recognition database for police use", Biometric Update, 11. mart 2020. https://www.biometricupdate.com/202003/india-set-to-stand-up-worlds-largest-government-facial-recognition-database-for-police-use

276 A. Jain, "NCRB's National Automated Facial Recognition System", 7. jun 2023. https://panoptic.in/case-study/ncrbs-national-automated-facial-recognition-system; A. Sinha, "The Landscape of Facial Recognition Technologies in India", Tech Policy Press, 13. mart 2024. https://www.techpolicy.press/the-landscape-of-facial-recognition-technologies-in-india/

277 D. Verma, "Why a massive leak in Tamil Nadu Police's FRT database must herald the end of police use of surveillance technologies", Internet Freedom Foundation, 17. maj 2024. https://internetfreedom.in/leak-in-tamil-nadu-polices-frt-database/

278 N. Ohri, "India lets banks use face recognition, iris scan for some transactions - sources", Reuters, 13. januar 2023. https://www.reuters.com/world/india/india-lets-banks-use-face-recognition-iris-scan-some-transactions-sources-2023-01-13/; R. Jain, "Indian government to add facial recognition, iris scan for digital payments", Business Insider India, 17. februar 2020. https://www.businessinsider.in/tech/news/indian-government-to-add-facial-recognition-iris-scan-for-digital-payments/articleshow/74176902.cms

279 R. C. Bajpai, S. Yadav, "Use of Facial Recognition Technology in India: A Function Creep Breaching Privacy", Oxford Human Rights Hub, 11. januar 2021. https://ohrh.law.ox.ac.uk/use-of-facial-recognition-technology-in-india-a-function-creep-breaching-privacy/

280 R. K. George, A. Tom, "Update on withdrawal of the personal data protection bill, 2019", Lexology, 10. avgust 2022. https://www.lexology.com/library/detail.aspx?g=0c082211-6ba5-402c-9623-32c5e4165d45; Times of India, "Centre withdraws Personal Data Protection Bill, 2019: Will present new legislation, says IT minister", 3. avgust 2022. https://timesofindia.indiatimes.com/india/centre-withdraws-personal-data-protection-bill/articleshow/93323625.cms

281 Nacrt zakona je dostupan ovde: Ministry of Electronics & Information Technology of India, The Digital Personal Data Protection Bill, 2022. https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Potection%20Bill%2C%202022_0.pdf; sažetak je dostupan ovde: PRS Legislative Research, Draft Digital Personal Data Protection Bill, 2022. https://prsindia.org/billtrack/draft-the-digital-personal-data-protection-bill-2022; kao i ovde: KPMG, Digital Personal Data Protection Bill, 2022. https://kpmg.com/in/en/

home/insights/2022/12/privacy-digital-personal-data-protection-bill-2022.html

282 Tekst zakona je dostupan ovde: Parliament of India, The Digital Personal Data Protection Act, 2023. https://egazette.gov.in/WriteReadData/2023/248045.pdf

283 D. Christopher, A. Dutta, A. Kabra, "India – The Digital Personal Data Protection Act, 2023 finally arrives", Linklaters, 23. avgust 2023. https://www.linklaters.com/en/insights/blogs/digilinks/2023/august/india-the-digital-personal-data-protection-act

284 Access Now, "India's Digital Personal Data Protection Bill passed: 'it's a bad law'", 9. avgust 2023. https://www.accessnow.org/press-release/indias-digital-personal-data-protection-bill-passed/

285 Hunton Privacy Blog, "India Passes Digital Personal Data Protection Act", 22. avgust 2023. https://www.huntonprivacyblog.com/2023/08/22/india-passes-digital-personal-data-protection-act/

286 Poziv za javnu raspravu dostupan je na sajtu indijske Vlade: https://innovateindia.mygov.in/dpdp-rules-2025/

287 Tekst Zakona o IT dostupan je ovde: Parliament of India, The Information Technology Act, 2000. https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY

288 Tekst Pravila SPDI dostupan je ovde: Ministry of Communications and Information Technology of India, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. https://www.dataguidance.com/legal-research/information-technology-reasonable-security-practices-and-procedures-and-sensitive

289 A. Jain, P. Waghre, "IFF's first read of the draft Digital Personal Data Protection Bill, 2023", Internet Freedom Foundation, 3. avgust 2023. https://internetfreedom.in/iffs-first-read-of-the-draft-digital-personal-data-protection-bill-2023/; S. Saigal, "Data Protection Bill: Granting government exemption causes great concern, says Justice Srikrishna", The Hindu, 8. juli 2023. https://www.thehindu.com/news/national/justice-srikrishna-on-draft-data-protection-bill-granting-govt-exemption-causes-great-concern/article67049892.ece; The Wire Staff, "Digital Personal Data Protection Bill Could Have Adverse Impact on Press Freedom, Say Editors Guild and DIGIPUB", The Wire, 7. avgust 2023. https://thewire.in/media/digital-personal-data-protection-bill-adverse-impact-press-freedom-editors-guild

290 Access Now, "India's Digital Personal Data Protection Bill passed: 'it's a bad law'", 9. avgust 2023. https://www.accessnow.org/press-release/indias-digital-personal-data-protection-bill-passed/

291 R. Roy, G. Zanfir-Fortuna, "The Digital Personal Data Protection Act of India, Explained", Future of Privacy Forum, 15. avgust 2023. https://fpf.org/blog/the-digital-personal-data-protection-act-of-india-explained/

292 Videti Odeljak 7(c) Zakona o zaštiti digitalnih ličnih podataka.

293 Videti Odeljak 17 (2) (b) Zakona o zaštiti digitalnih ličnih podataka.

294 The Wire Staff, "Digital Personal Data Protection Bill Could Have Adverse Impact on Press Freedom, Say Editors Guild and DIGIPUB", The Wire, 7. avgust 2023. https://thewire.in/media/digital-personal-data-protection-bill-adverse-impact-press-freedom-editors-guild

295 S. Saigal, "Data Protection Bill: Granting government exemption causes great concern, says Justice Srikrishna", The Hindu, 8. juli 2023. https://www.thehindu.com/news/national/justice-srikrishna-on-draft-data-protection-bill-granting-govt-exemption-causes-great-concern/article67049892.ece

296 Hunton Privacy Blog, "India Passes Digital Personal Data Protection Act", 22. avgust 2023. https://www.huntonprivacyblog.com/2023/08/22/india-passes-digital-personal-data-protection-act/

297 Tekst zakona dostupan je ovde: Parliament of India, Criminal Procedure (Identification) Act, 2022. https://www.indiacode.nic.in/bitstream/123456789/19029/1/a2022-11_pdf

298 A. Jain, "Delhi Police's claims that FRT is accurate with a 80% match are 100% scary", Internet Freedom Foundation, 17. avgust 2022. https://internetfreedom.in/delhi-polices-frt-use-is-80-accurate-and-100-scary/

299 Z. Mateen, M. Sebastian, "CPC: Criminal Procedure Identification Bill raises fears of surveillance in India", BBC, 13. april 2022. https://www.bbc.com/news/world-asia-india-61015970

300 Unique Identification Authority of India, "What is Aadhaar", https://uidai.gov.in/en/my-aadhaar/about-your-aadhaar.html

301 Daijiworld, "'Adhaar' most sophisticated ID programme in the world: World Bank", 16. mart 2017. https://www.daijiworld.com/news/newsDisplay.aspx?newsID=442948

302 Money Control, "Economic Survey 2023: 135.2 crore Aadhaar numbers generated till November 2022", 31. januar 2023. Arhivirana verzija: https://web.archive.org/web/20230131231837/https://www.moneycontrol.com/news/business/budget/economic-survey-2023-135-2-crore-aadhaar-numbers-generated-till-november-2022-9971821.html

303 Setopati, "Aadhar is constitutional but don't make it mandatory: Indian SC to govt", 26. septembar 2018. https://en.setopati.com/political/131199

304 Al Jazeera, "India's top court rules privacy is a fundamental right", 24. avgust 2017. https://www.aljazeera.com/news/2017/8/24/indias-top-court-rules-privacy-is-a-fundamental-right; BBC, "Indian Supreme Court in landmark ruling on privacy", 24. avgust 2017. https://www.bbc.com/news/world-asia-india-41033954

305 Pavithraa, "Aadhaar card: An Invasion to privacy", Legal Service India, https://www.legalserviceindia.com/legal/article-34-aadhaar-card-an-invasion-to-privacy.html

306 D. Dutta Roy, "Aadhaar Card Not Mandatory, Supreme Court Rules", NDTV, 11. avgust 2015. https://www.ndtv.com/india-news/aadhaar-card-not-mandatory-supreme-court-rules-1206134

307 Z. Saberin, "India's top court upholds constitution validity of Aadhaar card", Al Jazeera, 26. septembar 2018. https://www.aljazeera.com/news/2018/9/26/indias-top-court-upholds-constitution-validity-of-aadhaar-card; tekst odluke je dostupan ovde: Supreme Court of India, "Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others", 26. septembar 2018. https://uidai.gov.in/images/Aadhaar_Judgment.pdf

308 Deccan Herald, "Aadhaar verdict: What stays, what is struck down", 26. septembar 2018. https://www.deccanherald.com/national/aadhaar-verdict-what-stay-what-694678.html

309 D. Grey, "SC upholds Aadhaar's Constitutional Validity, but partially addresses Privacy Concerns", CJP, 26. septembar 2018. https://cjp.org.in/sc-upholds-aadhaars-constitutional-validity-but-partially-addresses-privacy-concerns/

310 M. Safi, "Indian court upholds legality of world's largest biometric database", The Guardian, 26. septembar 2018. https://www.theguardian.com/world/2018/sep/26/indian-court-upholds-legality-of-worlds-largest-biometric-database

311 Supreme Court of India, "Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others", 26. septembar 2018. https://uidai.gov.in/images/Aadhaar_Judgment.pdf, str.559.

312 N. Nambiar, "Unique Identification Authority of India's face recognition system ready for Maharashtra's various services", The Times of India, 20. avgust 2022. https://timesofindia.indiatimes.com/city/pune/unique-identification-authority-of-indias-face-recognition-system-ready-for-maharashtras-various-services/articleshow/93669134.cms

313 Unique Identification Authority of India, "Resources - Videos", https://uidai.gov.in/en/media-resources/resources/videos.html

314 H. Swart, "Face-off: South Africa's population register is on course to becoming a criminal database – with your mugshot", Daily Maverick, 3. mart 2021. https://www.dailymaverick.co.za/article/2021-03-03-face-off-south-africas-population-register-is-on-course-to-becoming-a-criminal-database-with-your-mugshot/

315 K. Hao, H. Swart, "South Africa's private surveillance machine is fueling a digital apartheid", MIT Technology Review, 19. april 2022. https://www.technologyreview.com/2022/04/19/1049996/south-africa-ai-surveillance-digital-apartheid/; M. Kwet, "Smart CCTV Networks Are Driving an AI-Powered Apartheid in South Africa", Vice, 22. novembar 2019. https://www.vice.com/en/article/pa7nek/smart-cctv-networks-are-driving-an-ai-powered-apartheid-in-south-africa; S. Mungadze, "Professor decries Joburg's private surveillance networks", ITWeb, 3. septembar 2019. https://www.itweb.co.za/content/Pero37ZgoYJMQb6m; K. Allen, I. van Zyl, "Who's watching who? Biometric surveillance in Kenya and South Africa", ENACT, novembar 2020. https://enact-africa.s3.amazonaws.com/site/uploads/2020-11-11-biometrics-research-paper.pdf; H. Swart, A. Munoriyarwa, "Video Surveillance in Southern Africa: Case studies of security camera systems in the region", Media Policy and Democracy Project, maj 2020. https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/video_surveillance_in_southern_africa_-_security_camera_systems_in_the_region.pdf

316 Department of Home Affairs of South Africa, "What is ABIS?", http://www.dha.gov.za/index.php/civic-services/abis

317 BusinessTech, "Home Affairs proposes big change for IDs in South Africa", 26. avgust 2022. https://businesstech.co.za/news/government/620051/home-affairs-proposes-big-change-for-ids-in-south-africa/

318 A. Macdonald, "Delays persist in South Africa's automated biometric identi- fication project completion", Biometric Update, 16. mart 2021. https://www.biometricupdate.com/202103/delays-persist-in-south-africas-automated-biometric-identification-project-completion; M. Illidge, "The truth about South Africa's undelivered R432-million biometrics database", MyBroadband, 12. septembar 2022. https://mybroadband.co.za/news/government/460005-the-truth-about-south-africas-undelivered-r432-million-biometrics-database.html

319 Parliament of South Africa, "Media Statement: Home Affairs Committee Disappointed With Lack of Progress in Migrating to Automated Biometric Identification System", 10. maj 2023. https://www.parliament.gov.za/press-releases/media-statement-home-affairs-committee-disappointed-lack-progress-migrating-automated-biometric-identification-system

320 Parlamentary Monetary Group, "Automated Biometric Information System (ABIS) update; IEC Commissioner Vacancy & salary increase; with Deputy Minister Home Affairs", 12. septembar 2023. https://pmg.org.za/committee-meeting/37466/

321 S. Mzekandaba, "Home affairs ramps up biometrics-driven movement system", ITWeb, 9. maj 2023. https://www.itweb.co.za/content/o1Jr5MxPKNBMKdWL; A. Macdonald, "South Africa to expand biometric border control system", Biometric Update, 11. maj 2023. https://www.biometricupdate.com/202305/south-africa-to-expand-biometric-border-control-system

322 Najava se može naći ovde: Department of Home Affairs of South Africa, "Biometrics capturing process", https://www.flysaa.com/documents/51855150/0/Biometrics+Poster+without+bleeds.pdf/

323 A. Opiah, "South Africa adopts biometrics for social protection, following India's example", Biometric Update, 22. novembar 2024. https://www.biometricupdate.com/202411/south-africa-adopts-biometrics-for-social-protection-following-indias-example

324 D. Rajgopaul, "Sars announces major facial recognition eFiling change", IOL, 6. novembar 2024. https://www.iol.co.za/business/advice/sars-announces-major-facial-recognition-efiling-change-b5928ac5-7a54-40b5-86fd-c4d44d1b2ceb

325 University of Johannesburg, "UJ implements Facial Recognition for a secure registration, a first for a South African university", 24. januar 2024. https://news.uj.ac.za/news/uj-implements-facial-recognition-for-a-secure-registration-a-first-for-a-south-african-university/

326 Član 14 Ustava Republike Južne Afrike (1996) dostupan je ovde: Constitution of the Republic of South Africa, Chapter 2: Bill of Rights, 1996. https://www.gov.za/documents/constitution/chapter-2-bill-rights#14; Južna Afrika je potpisnica Međunarodnog pakta o građanskim i političkim pravima.

327 Tekst na engleskom jeziku dostupan je ovde: Parliament of South Africa, Protection of Personal Information Act (POPIA) 4 of 2013, https://www.gov.za/documents/protection-personal-information-act

328 Sajt na engleskom dostupan je ovde: Information Regulator South Africa, https://inforegulator.org.za/; ovo telo je takođe nadležno za pristup informacijama.

329 POPIA, članovi 26 i 27.

330 Prema definiciji iz POPIA, "odgovorna strana" odgovara definiciji "rukovaoca" iz GDPR, i označava javno ili privatno telo ili drugog subjekta koji, sam ili u saradnji s drugima, određuje svrhu i način obrade ličnih informacija.

331 Information Regulator South Africa, "Guidance Notes", https://inforegulator.org.za/guidance-notes/

332 POPIA, član 33.

333 Vredi napomenuti da Južna Afrika ima zakon koji reguliše presretanje komunikacija i propisuje da službe za sprovođenje zakona treba da traže sudsko ovlašćenje za presretanje: Parliament of South Africa, Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002, https://www.gov.za/documents/regulation-interception-communications-and-provision-communication-related-information--13

334 Information Regulator South Africa, "Prior Authorisation", https://inforegulator.org.za/prior-authorisation/

335 Činjenice i zakon sažeti su ovde: S. de Gouveia, K. Robertson, "Vumacam (Pty) Ltd v Johannesburg Roads Agency and Others", Schindlers Attorneys, 1. septembar 2020. https://www.schindlers.co.za/vumacam-pty-ltd-v-johannesburg-roads-agency-and-others/?pdf=12974; kao i ovde: J. Nash, "A 2020 court fight in South Africa reveals dominance of biometric surveillance industry", Biometric Update, 21. april 2022. https://www.biometricupdate.com/202204/a-2020-court-fight-in-south-africa-reveals-dominance-of-biometric-surveillance-industry; odluka Visokog suda može se naći ovde: South Gauteng High Court, "Vumacam (Pty) Ltd v Johannesburg Roads Agency and Others (14867/20) [2020] ZAGPJHC 186", 20. avgust 2020. http://www.saflii.org/za/cases/ZAGPJHC/2020/186.html

336 Presuda, paragrafi 6 i 7: South Gauteng High Court, "Vumacam (Pty) Ltd v Johannesburg Roads Agency and Others (14867/20) [2020] ZAGPJHC 186", 20. avgust 2020. http://www.saflii.org/za/cases/ZAGPJHC/2020/186.html

337 Presuda, paragraf 16: South Gauteng High Court, "Vumacam (Pty) Ltd v Johannesburg Roads Agency and Others (14867/20) [2020] ZAGPJHC 186", 20. avgust 2020. http://www.saflii.org/za/cases/ZAGPJHC/2020/186.html

338 S. Mungadze, "Johannesburg Road Agency loses CCTV court appeal", ITWeb, 5. oktobar 2020. https://www.itweb.co.za/content/kYbe97XDrV27AWpG

339 R. Mac, C. Haskins, A. Pequeño IV, "Police In At Least 24 Countries Have Used Clearview AI. Find Out Which Ones Here.", BuzzFeed News, 25. avgust 2021. https://www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table

340 Office of the Privacy Commissioner of Canada, "RCMP's use of Clearview AI's facial recognition technology violated Privacy Act, investigation concludes", 10. jun 2021. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/nr-c_210610/

341 Office of the Privacy Commissioner of Canada, "Announcement: Clearview AI ordered to comply with recommendations to stop collecting, sharing images", 14. decembar 2021. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/an_211214/

342 M. Forrest, "RCMP's use of facial recognition extends well beyond Clearview AI", Politico, 30. septembar 2022. https://www.politico.com/news/2022/09/30/rcmps-facial-recognition-clearview-ai-00059639

343 Office of the Privacy Commissioner of Canada, "Recommended legal framework for police agencies' use of facial recognition", 2. maj 2022. https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2022/s-d_prov_20220502/

344 P. Kelly, "Facial Recognition Technology and the Growing Power of Artificial Intelligence", House of Commons of Canada Standing Committee on Access to Information, Privacy and Ethics, oktobar 2022. https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP11948475/ethirp06/ethirp06-e.pdf

345 Internet Policy & Public Interest Clinic (CIPPIC), "Facial Recognition at a Crossroads: Transformation at our Borders & Beyond ", septembar 2020. https://cippic.ca/uploads/FR_Transforming_Borders.pdf

346 International Civil Liberties Monitoring Group, "Ban on use of facial recognition surveillance by federal law enforcement and intelligence agencies", 8. juli 2020. https://iclmg.ca/wp-content/uploads/2020/07/facial-recognition-letter-08072020.pdf

347 J. Bongiorno, "Facial recognition technology gains popularity with police, intensifying calls for regulation", The Canadian Press, 30. jun 2024. https://www.cbc.ca/news/politics/facial-recognition-ai-police-canada-1.7251065

348 H. Ravia, D. Hammer, "Guidelines for Use of Facial Recognition by Ontario Police", Pearl Cohen - Client Updates. 3 mart 2024. https://www.pearlcohen.com/guidelines-for-use-of-facial-recognition-by-ontario-police/

349 Dostupno na sajtu regionalne policije Jorka: https://www.yrp.ca/en/crime-prevention/facial-recognition-technology.asp

350 Department of Justice of Canada, The Canadian Charter of Rights and Freedoms, https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/

351 Parliament of Canada, Revised Statutes of Canada, Privacy Act (1985, c. P-21), poslednja izmena 2022. https://laws-lois.justice.gc.ca/eng/ACTS/P-21/index.html

352 Parliament of Canada, Statutes of Canada, Personal Information Protection and Electronic Documents Act (2000, c. 5), poslednja izmena 2019. https://laws-lois.justice.gc.ca/eng/acts/p-8.6/

353 The Government of Canada, Directive on Automated Decision-Making, 2019. https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592

354 Parliament of Canada, C-27 (44-1), 2022. https://www.parl.ca/legisinfo/en/bill/44-1/c-27

355 Office of the Privacy Commissioner of Canada, "Summary of privacy laws in Canada", januar 2018. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/

356 P. Backman, C. Kennedy, "Biometric Identification and Privacy Concerns: A Canadian Perspective", Aird & Berlis LLP, https://www.airdberlis.com/docs/default-source/articles/biometric-identification-and-privacy-concerns.pdf

357 Office of the Privacy Commissioner of Canada, "Announcement: OPC updates guidance regarding sensitive information", 13. avgust 2021. https://priv.gc.ca/en/opc-news/news-and-announcements/2021/an_210813/

358 Parliament of Canada, C-27 (44-1), Odeljak 63, 2022. https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading

359 Innovation, Science and Economic Development Canada, "The Artificial In-

telligence and Data Act (AIDA) – Companion document", 13. mart 2023. https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document

360 National Assembly of Quebec, Act to establish a legal framework for information technology C-1.1, 2001. https://www.legisquebec.gouv.qc.ca/en/document/cs/c-1.1

361 P. Kelly, "Facial Recognition Technology and the Growing Power of Artificial Intelligence", House of Commons of Canada Standing Committee on Access to Information, Privacy and Ethics, oktobar 2022. https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP11948475/ethirp06/ethirp06-e.pdf, str. 58.

362 Ibid, str. 54.

363 Supreme Court of Canada, "R. v. Dyment", 8. decembar 1988. https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/375/index.do

364 Supreme Court of Canada, "R. v. Spencer", 13. jun 2014. https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do

365 Federal Court of Appeal of Canada, "Wansink v. Telus Communications Inc.", 1. januar 2007. https://decisions.fca-caf.gc.ca/fca-caf/decisions/en/item/35446/index.do

366 Canadian HR Reporter, "Employer can't use finger scan system to clock employees", 29. januar 2007. https://www.hrreporter.com/focus-areas/employment-law/legal-briefs/287904

367 L. McGrady, M. Koroneos, "Employee Privacy Rights in the Workplace", Faculty of Law Center for Law in the Contemporary Workplace – Queen's University, 22. novembar 2013. https://clcw.queenslaw.ca/sites/clcwwww/files/files/Powerpoints%20Papers/Privacy/Leo%20McGrady%20Employee%20Privacy%20Rights%20in%20the%20Workplace.pdf

368 Izveštaj iz 2021. o istoriji i praksama nadzora u Keniji: G. Mutung'u, "Surveillance Law in Africa: a review of six countries, Kenya country report", Institute of Development Studies, 2021. https://opendocs.ids.ac.uk/ndownloader/files/48184981; integralni izveštaj za šest zemalja Afrike: T. Roberts, "Surveillance Law in Africa: a review of six countries", Institute of Development Studies, 2021. https://opendocs.ids.ac.uk/articles/report/Surveillance_Law_in_Africa_a_Review_of_Six_Countries/26435920

369 O nadzoru tokom pandemije kovida 19, videti izveštaj dostupan ovde: Article 19 Eastern Africa, Kenya ICT Action Network, Pollicy, "Unseen Eyes, Unheard Stories Surveillance, data protection, and freedom of expression in Kenya and Uganda during COVID-19", 21. april 2021. https://www.article19.org/wp-content/uploads/2021/04/EAF-Surveillance-Report_Final-min.pdf; nadzor elektronskih komunikacija povod je za zabrinutost, usled izmena zakona o službenim tajnama: B. Andere, "Kenya's sneak attack on the right to privacy", Access Now, 13. januar 2023. https://www.accessnow.org/kenya-right-to-privacy/

370 Privacy International, "Data Protection Impact Assessments and ID systems: the 2021 Kenyan ruling on Huduma Namba", 27. januar 2022. https://privacyinternational.org/news-analysis/4778/data-protection-impact-assessments-and-id-systems-2021-kenyan-ruling-huduma

371 Arhivirana verzija sajta dostupna je ovde: Huduma Namba, https://web.archive.org/web/20230510154147/https://www.hudumanamba.go.ke/

372 M. Obar, "Ruto Issues New Order Over Huduma Namba", Kenyans.co.ke, 27. januar 2023. https://www.kenyans.co.ke/news/84755-ruto-makes-new-orders-over-huduma-namba

373 L. Danflow, "ICT CS Owalo: Kenyans to have digital IDs by March 2024", The Star, 17. maj 2023. https://www.the-star.co.ke/news/realtime/2023-05-17-ict-cs-owalo-kenyans-to-have-digital-ids-by-march-2024/

374 D. Mwangi, "CS Kindiki reveals details of new upgraded ID cards set to be launched", Pulse, 24. maj 2023. https://www.pulselive.co.ke/news/local/interior-cs-kithure-kindiki-reveals-plans-for-upgraded-identification-cards/zc8dskc

375 B. Makong, "Kenya pursues upgraded Biometric Identification System for enhanced security measures", Capital News, 24. maj 2023. https://www.capitalfm.co.ke/news/2023/05/kenya-pursues-upgraded-biometric-identification-system-for-enhanced-security-measures/; M. Kinyanjui, "Kindiki: Kenyans to get ID with machine-readable chip, QR code", The Star, 24. maj 2023. https://www.the-star.co.ke/news/2023-05-24-kindiki-kenyans-to-get-id-with-machine-readable-chip-qr-code/

376 M. Akuchie, "Kenya plans to tackle identity theft with an improved biometric system", Technext, 25. maj 2023. https://technext24.com/2023/05/25/kenya-identity-theft-biometric/

377 D. Mwangi, "CS Kindiki reveals details of new upgraded ID cards set to be launched", Pulse, 24. maj 2023. https://www.pulselive.co.ke/news/local/interior-cs-kithure-kindiki-reveals-plans-for-upgraded-identification-cards/zc8dskc

378 J. Thiong'o, "Inside President Ruto's bid to ditch Huduma Namba, adopt Digital Identity project", The Standard, 1. jun 2023. https://www.standardmedia.co.ke/article/2001474305/inside-president-rutos-bid-to-ditch-huduma-namba-adopt-identity-project

379 Al Kags, "Maisha Namba: Thoughts about Kenya's evolution of identity", Al Kags, 2. septembar 2024. https://alkags.me/maisha-namba/

380 Ibid.

381 Ayang Macdonald, "Kenya's digital ID delivery back on: Court sets aside latest injunction", Biometric Update, 13. avgust 2024. https://www.biometricupdate.com/202408/kenyas-digital-id-delivery-back-on-court-sets-aside-latest-injunction

382 P. Wanjama, "Police Launch Facial Recognition System to Nab Criminals", Kenyans.co.ke, 18. septembar 2018. https://www.kenyans.co.ke/news/33249-police-launch-facial-recognition-system-nab-criminals; C. Burt, "Kenyan police launch facial recognition on urban CCTV network", Biometric Update, 24. septembar 2018. https://www.biometricupdate.com/201809/kenyan-police-launch-facial-recognition-on-urban-cctv-network; Business Today Kenya, "Big brother gets bigger: Police acquire face recognition capabilities", 18. septembar 2018. https://businesstoday.co.ke/big-brother-gets-bigger-police-acquire-face-recognition-capabilities/

383 Prema izveštaju dostupnom ovde: INCLO, "In Focus Facial Recognition Tech Stories And Rights Harm Around The World", januar 2021. https://www.inclo.

net/pdf/in-focus-facial-recognition-tech-stories.pdf

384 C. Burt, "NEC facial recognition border tech for Kenya as airport biometrics rollouts continue", Biometric Update, 7. oktobar 2019. https://www.biometricupdate.com/201910/nec-facial-recognition-border-tech-for-kenya-as-airport-biometrics-rollouts-continue; International Organization for Migration, "Facial Recognition System Installed at Moi International Airport", 7. oktobar 2019. https://www.iom.int/news/facial-recognition-system-installed-moi-international-airport

385 F. Hersey, "850 Kenyan hospitals sue national insurance fund over biometric patient registration", Biometric Update, 4. avgust 2021. https://www.biometricupdate.com/202108/850-kenyan-hospitals-sue-national-insurance-fund-over-biometric-patient-registration; L. Igadwah, "850 private hospitals sue NHIF in biometric registration dispute", Business Daily, 3. avgust 2021. https://www.businessdailyafrica.com/bd/economy/rural-based-hospitals-sue-nhif-biometric-registration-dispute-3496384

386 E. Weiss, "Kenya Replaces Insurance Cards With Fingerprint Biometrics", FindBiometrics, 9. juli 2021. https://findbiometrics.com/kenya-replaces-insurance-cards-with-fingerprint-biometrics-070904/; B. Otieno, "Uhuru launches biometric Universal Health Coverage registration", The Star, 31. oktobar 2020. https://www.the-star.co.ke/news/2020-10-31-uhuru-launches-biometric-universal-health-coverage-registration/; A. Macdonald, "Biometric registration drive in Kenya for health insurance scheme", Biometric Update, 15. jun 2021. https://www.biometricupdate.com/202106/biometric-registration-drive-in-kenya-for-health-insurance-scheme

387 S. Kiplagat, "Safaricom and Airtel want enjoined in fresh SIM cards registration case", Business Daily, 6. april 2022. https://www.businessdailyafrica.com/bd/corporate/companies/safaricom-and-airtel-want-enjoined-sim-cards-registration-case-3773596; C. Burt, "Subscribers scramble for biometric SIM registrations in Kenya as deadline extended", Biometric Update, 20. april 2022. https://www.biometricupdate.com/202204/subscribers-scramble-for-biometric-sim-registrations-in-kenya-as-deadline-extended

388 Access Now, "Open letter: Safaricom must delete all biometric data collected unlawfully during Kenya's SIM card registration exercise", 14. decembar 2022. https://www.accessnow.org/press-release/open-letter-safaricom-privacy-kenya/

389 Tekst Ustava dostupan je ovde: Constitution of Kenya, 2010. http://www.kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=Const2010

390 Tekst KDPA na engleskom dostupan je ovde: Parliament of Kenya, The Data Protection Act, 2019. https://www.odpc.go.ke/dpa-act/

391 DLA Piper, "Global Data Protection Laws of the World - Kenya", 12. januar 2023. https://www.dlapiperdataprotection.com/index.html?t=law&c=KE

392 Office of the Data Protection Commissioner of Kenya, https://www.odpc.go.ke/

393 Objavljene smernice: Office of the Data Protection Commissioner of Kenya, "General Guidelines", https://www.odpc.go.ke/general-guidlines/

394 Detaljna analiza pravnog okvira u Keniji: R. Reeve et al., "Data Privacy and Protection in Kenya: A Regulatory Review", FSD Kenya, januar 2022. https://www.fsdkenya.org/wp-content/uploads/2022/01/Dapa-January-26th.pdf

395 Sva regulativa podataka na engleskom jeziku: Office of the Data Protection Commissioner of Kenya, "Data Protection Regulations", https://www.odpc.go.ke/data-protection-regulation/

396 Postoji javno dostupan registar sa obaveznom registracijom, ali sadrži samo osnovne detalje o registrovanim rukovaocima i obrađivačima, a ne i vrste registrovanih aktivnosti obrade. Javni registar: Office of the Data Protection Commissioner of Kenya, "Register Of Data Controllers And Data Processors", https://www.odpc.go.ke/registered-data-processors-and-controllers/

397 Član 46 KDPA posebno reguliše samo obradu medicinskih podataka.

398 Transfer podataka, uključujući osetljive podatke, detaljno je regulisan u Glavi II (Opšte) regulative zaštite podataka (2021).

399 Prvenstveno su sadržane u članu 28(2) KDPA koji reguliše situacije u kojima se podaci mogu prikupljati indirektno: (a) kada su podaci sadržani u javnoj evidenciji; (b) kada je osoba na koju se podaci odnose namerno objavila podatke; (c) kada su osoba na koju se podaci odnose ili njen staratelj dali saglasnost za prikupljanje iz drugog izvora; (d) kada prikupljanje iz drugog izvora ne bi štetilo interesima osobe na koju se podaci odnose; i (e) kada je prikupljanje podataka iz drugog izvora neophodno: (1) za sprečavanje, otkrivanje, istragu, krivično gonjenje i kažnjavanje zločina; (2) za sprovođenje zakona koji predviđa novčanu kaznu; ili (3) radi zaštite interesa osobe na koju se podaci odnose ili druge osobe.

400 Član 6(1)(e) (Opšte) regulative zaštite podataka (2021).

401 Objavljene smernice dostupne su ovde: Office of the Data Protection Commissioner of Kenya, "General Guidelines", https://www.odpc.go.ke/general-guidlines/

402 Istorija pravnih procedura: Privacy International, "Data Protection Impact Assessments and ID systems: the 2021 Kenyan ruling on Huduma Namba", 27. januar 2022. https://privacyinternational.org/news-analysis/4778/data-protection-impact-assessments-and-id-systems-2021-kenyan-ruling-huduma

403 Tekst odluke na engleskom jeziku: High Court of Kenya at Nairobi, "Nubian Rights Forum & 2 others v. Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2020] eKLR", 30. januar 2020. http://kenyalaw.org/caselaw/cases/view/189189/

404 Videti paragrafe presude broj 781, 784, 910, 919, 922 i 1038. Više detalja o odluci: Privacy International, "Kenyan Court Ruling on Huduma Namba Identity System: the Good, the Bad and the Lessons", 24. februar 2020. https://privacyinternational.org/long-read/3373/kenyan-court-ruling-huduma-namba-identity-system-good-bad-and-lessons

405 Videti paragraf 1047 presude. Sud je, između ostalog, odlučivao o ustavnosti i zakonitosti mera u vezi sa javnim učešćem u zakonodavnom procesu; o tome da li postoji kršenje prava na privatnost (da li je prikupljanje ličnih podataka preterano, intruzivno i nesrazmerno, da li postoji kršenje prava dece na privatnost, da li postoje dovoljne zakonske zaštite i okviri za zaštitu podataka); i da li je postojalo kršenje prava na jednakost i nediskriminaciju.

406 Tekst presude na engleskom jeziku: High Court of Kenya at Nairobi (Milimani Law Courts), "Republic v. Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology & 2 others; Katiba Institute & another (Exparte); Immaculate Kasait, Data Commissioner (Interested Party) (Judicial

Review Application E1138 of 2020) [2021] KEHC 122 (KLR) (Judicial Review)", 14. oktobar 2021. http://kenyalaw.org/caselaw/cases/view/220495/; analiza presude: Privacy International, "Data Protection Impact Assessments and ID systems: the 2021 Kenyan ruling on Huduma Namba", 27. januar 2022. https://privacyinternational.org/news-analysis/4778/data-protection-impact-assessments-and-id-systems-2021-kenyan-ruling-huduma; Media Defence, "Advanced Modules on Digital Rights and Freedom of Expression Online in sub-Saharan Africa, Module 4: Privacy and Security Online, Collection of Biometric Data and Facial Recognition", https://www.mediadefence.org/ereader/publications/advanced-modules-on-digital-rights-and-freedom-of-expression-online/module-4-privacy-and-security-online/collection-of-biometric-data-and-facial-recognition/; The Open Society Justice Initiative, "New Kenya High Court Judgment Sets Important Precedent for Digital ID Privacy Protections and Processes", 15. oktobar 2021. https://www.justiceinitiative.org/newsroom/new-kenya-high-court-judgment-sets-important-precedent-for-digital-id-privacy-protections-and-processes

407 Paragraf 104 presude.

408 Paragraf 119 presude.

409 A. Macdonald, "Kenya mulls digital ID scheme changes and new uses for controversial Huduma Namba", Biometric Update, 16. januar 2023. https://www.biometricupdate.com/202301/kenya-mulls-digital-id-scheme-changes-and-new-uses-for-controversial-huduma-namba

410 A. Macdonald, "Activists urge Kenya not to repeat mistakes of Huduma Namba in new digital ID plan", Biometric Update, 22. maj 2023. https://www.biometricupdate.com/202305/activists-urge-kenya-not-to-repeat-mistakes-of-huduma-namba-in-new-digital-id-plan

411 C. Burt, "Kenyan rights groups warn digital ID program repeating past mistakes", Biometric Update, 15. septmbar 2023. https://www.biometricupdate.com/202309/kenyan-rights-groups-warn-digital-id-program-repeating-past-mistakes

412 "Kenyan Digital Identity System Shelved Over Data Protection Concerns", Dark Reading, 8. decembar 2023. https://www.darkreading.com/data-privacy/kenyan-digital-identity-system-shelved-data-protection-concerns

413 C.Burt, "Maisha Namba issuance to resume as Kenyan High Court lifts injunction", Biometric Update, 23. februar 2024. https://www.biometricupdate.com/202402/maisha-namba-issuance-to-resume-as-kenyan-high-court-lifts-injunction

414 B. Marita, "High Court suspends rollout of new digital IDs", Star, 25. jul 2024. https://www.the-star.co.ke/news/2024-07-25-high-court-suspends-rollout-of-new-digital-ids

415 A. Macdonald, "Kenya's digital ID delivery back on: Court sets aside latest injunction", Biometric Update, 13. avgust 2024. https://www.biometricupdate.com/202408/kenyas-digital-id-delivery-back-on-court-sets-aside-latest-injunction

416 Office of the Data Protection Commissioner of Kenya, "Office of the Data Protection Commissioner Issues a Penalty Notice against Oppo Kenya", 28. januar 2023. https://www.odpc.go.ke/download/office-of-the-data-protection-commissioner-issues-a-penalty-notice-against-oppo-kenya; G. Ndung'u, Issaias,T. Mwango, "Kenya: The Office of the Data Protection Commissioner issues decisions in the determination of complaints", Bowmans, 19. januar 2023. https://bowmanslaw.com/insights/data-protection/kenya-the-office-of-the-data-protection-commissioner-issues-decisions-in-the-determination-of-complaints/

417 D. Gershgorn, "China's 'Sharp Eyes' Program Aims to Surveil 100% of Public Space", OneZero, 2. mart 2021. https://onezero.medium.com/chinas-sharp-eyes-program-aims-to-surveil-100-of-public-space-ddc22d63e015

418 Ibid.

419 Y. Li, M. Elfstrom, "Does Greater Coercive Capacity Increase Overt Repression? Evidence from China", Journal of Contemporary China, 2021. 30:128, 186-211, https://doi.org/10.1080/10670564.2020.1790898

420 A. Polyakova, C. Meserole, "Exporting digital authoritarianism: The Russian and Chinese models", Brookings, 2019. https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf

421 Ibid.

422 AFP, "Sinister or safer? China takes the lead in using facial recognition technology", Hong Kong Free Press, 21. oktobar 2017. https://hongkongfp.com/2017/10/21/sinister-safer-china-takes-lead-using-facial-recognition-technology/

423 J. Vincent, "Chinese police are using facial recognition sunglasses to track citizens", The Verge, 8. februar 2018. https://www.theverge.com/2018/2/8/16990030/china-facial-recognition-sunglasses-surveillance

424 AFP, "Sinister or safer? China takes the lead in using facial recognition technology", Hong Kong Free Press, 21. oktobar 2017. https://hongkongfp.com/2017/10/21/sinister-safer-china-takes-lead-using-facial-recognition-technology/

425 D. Gershgorn, "China's 'Sharp Eyes' Program Aims to Surveil 100% of Public Space", OneZero, 2. mart 2021. https://onezero.medium.com/chinas-sharp-eyes-program-aims-to-surveil-100-of-public-space-ddc22d63e015

426 D. Byler, "Because There Were Cameras, I Didn't Ask Any Questions", ChinaFile, 30. decembar 2020. https://www.chinafile.com/extensive-surveillance-china; IPVM, "Huawei / Megvii Uyghur Alarms", 8. decembar 2020. https://ipvm.com/reports/huawei-megvii-uygur

427 A. Polyakova, C. Meserole, "Exporting digital authoritarianism: The Russian and Chinese models", Brookings, 2019. https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf

428 Ibid.

429 Ibid.

430 D. Byler, "Because There Were Cameras, I Didn't Ask Any Questions", ChinaFile, 30. decembar 2020. https://www.chinafile.com/extensive-surveillance-china

431 J. Tang, "China casts its 'SkyNet' far and wide, pursuing tens of thousands who flee overseas", Radio Free Asia, 4. maj 2022. https://www.rfa.org/english/news/china/skynet-repatriation-05042022151054.html

432 A. Polyakova, C. Meserole, "Exporting digital authoritarianism: The Russian and Chinese models", Brookings, 2019. https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf

433 M. Carney, "Leave no dark corner", ABC News, 17. septembar 2018. https://www.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-a-digital-dictatorship/10200278; P. Mozur, "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras", The New York Times, 8. juli 2018. https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html

434 J. Chin, L. Lin, "Surveillance state : inside China's quest to launch a new era of social control", St. Martin's Press, 2022. https://archive.org/details/surveillancestat0000chin; R. Andersen, "The Panopticon Is Already Here", The Atlantic, septembar 2020. https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/; D. Tang, "Chinese AI 'can check loyalty of party members'", The Sunday Times, 4. juli 2022. https://www.thetimes.co.uk/article/chinese-ai-can-check-loyalty-of-party-members-92d97hgwv; S. Chestnut Greitens, "Dealing With Demand For China's Global Surveillance Exports", Brookings, april 2020. https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200428_china_surveillance_greitens_v3.pdf

435 J. E. Hillman, M. McCalpin, "Watching Huawei's 'Safe Cities'", Center for Strategic & International Studies, 4. novembar 2019. https://www.csis.org/analysis/watching-huaweis-safe-cities

436 R. Standish, "The Fight In Serbia Over Chinese-Style Surveillance (Part 1)", Radio Free Europe/ Radio Liberty, 22. novembar 2022. https://www.rferl.org/a/serbia-chinese-surveilllance-backlash-standish/32142771.html

437 Human Rights in China, "Regulatory framework, Surveillance industry in China", 15. februar 2019. https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Surveillance/HUMAN_RIGHTS_IN_CHINA.pdf

438 Ibid.

439 Ibid.

440 International Association of Lawyers, "A Constitutional View of Privacy Rights in China", 19. oktobar 2020. https://www.uianet.org/en/news/constitutional-view-privacy-rights-china

441 Nezvanični prevod na engleski: Civil Code of the People's Republic of China (2020)https://www.trans-lex.org/601705/_/civil-code-of-the-peoples-republic-of-china-/

442 D. Luo, Y. Wang, "China - Data Protection Overview", DataGuidance, novembar 2022. https://www.dataguidance.com/notes/china-data-protection-overview

443 National People's Congress, Personal Information Protection Law of the People's Republic of China (2021) http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm

444 DataGuidance, Cybersecurity Law (2016) https://www.dataguidance.com/legal-research/cybersecurity-law-2016-unofficial-translation

445 National People's Congress, Data Security Law of the People's Republic of China (2021) http://en.npc.gov.cn.cdurl.cn/2021-06/10/c_689311.htm

446 Nezvanični prevod na engleski: National Security Law (2015) https://www.chinalawtranslate.com/en/2015nsl/

447 Nezvanični prevod na engleski: Counter-Terrorism Law (2015, sa amandmanima iz 2018) https://www.chinalawtranslate.com/en/counter-terrorism-law-2015/

448 Nezvanični prevod na engleski: PRC National Intelligence Law (2017, sa amandmanima iz 2018) https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/

449 Human Rights in China, "Regulatory framework, Surveillance industry in China", 15. februar 2019. https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Surveillance/HUMAN_RIGHTS_IN_CHINA.pdf

450 G. Interesse, "China Issues New Regulations on Network Data Security Management", China Briefing, 2. oktobar 2024. https://www.china-briefing.com/news/china-issues-new-regulations-on-network-data-security-management-effective-january-1-2025/

451 J. Ye, "China changing its stance on facial recognition", Reuters, 8. avgust 2023. https://www.reuters.com/technology/china-drafts-rules-using-facial-recognition-technology-2023-08-08/

452 S. Yang, "The Privacy, Data Protection and Cybersecurity Law Review: China", The Law Review, 27. oktobar 2022. https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/china

453 B. Nguyen, "China is backing away from facial recognition technology — at least in hotels", Quartz, 26. april 2024. godine. https://qz.com/china-stop-facial-recognition-technology-hotels-privacy-1851437900

454 Sažetak na engleskom je objavljen na sajtu Vrhovnog narodnog suda Narodne republike Kine: Supreme People's Court of the People's Republic of China, "New rules to curb misuse of facial recognition tech", 29. juli 2021. https://perma.cc/3YPC-CPV4

455 Ibid.

456 Tekst na engleskom: National Standard of the People's Republic of China, "Information security technology – Personal information (PI) security specification", 2020. https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf

457 Nezvaničan prevod nacrta na engleski: "Information Security Technology Security - Requirements for Facial Recognition Data" (2021) https://www.chinalawtranslate.com/en/draft-facial-recognition-standards/

458 Član 2 Zakona o sajber bezbednosti.

459 S. Xuanfeng Ning, H. Wu, "Data Protection Laws and Regulations China 2024", The International Comparative Legal Guides, 2022. https://iclg.com/practice-areas/data-protection-laws-and-regulations/china

460 S. Yang, "The Privacy, Data Protection and Cybersecurity Law Review: China", The Law Review, 27. oktobar 2022. https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/china

461 Ibid.

462 Y. Luo, R. Guo, "Facial Recognition in China: Current Status, Comparative Approach and the Road Ahead", 25 U. Pa. J.L. & Soc. Change 153, 2021. https://

scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1269&context=jlasc, str. 164.

463 Hronologija usvajanja dostupna ovde: Digital Policy Alert, "China: Information Security Technology Face Recognition Data Security Requirements", https://digitalpolicyalert.org/change/1859-information-security-technology-face-recognition-data-security-requirements

464 Garrigues, "China's Supreme People's Court sets rules for facial recognition technology", 2. avgust 2021. https://www.garrigues.com/en_GB/new/chinas-supreme-peoples-court-sets-rules-facial-recognition-technology

465 X. Shen, "China's first facial-recognition lawsuit comes to an end with new ruling and new questions about the fate of individuals' data", South China Morning Post, 12. april 2021. https://www.scmp.com/tech/policy/article/3129226/chinas-first-facial-recognition-lawsuit-comes-end-new-ruling-and-new

466 G. Du, L. Qiang , "China's First Facial Recognition Case", China Justice Observer, 2. maj 2021. https://www.chinajusticeobserver.com/a/china-s-first-facial-recognition-case

467 Y. Du, "China's First Face Recognition Case Study", HG.org Legal Resources, https://www.hg.org/legal-articles/china-s-first-face-recognition-case-study-58943

468 Y. Ye, "Hangzhou Court Rules in Landmark Facial Recognition Case", Sixth Tone, 21. novembar 2020. https://www.sixthtone.com/news/1006479

469 G. Du, L. Qiang , "China's First Facial Recognition Case", China Justice Observer, 2. maj 2021. https://www.chinajusticeobserver.com/a/china-s-first-facial-recognition-case

470 Y. Du, "China's First Face Recognition Case Study", HG.org Legal Resources, https://www.hg.org/legal-articles/china-s-first-face-recognition-case-study-58943

471 S. Yang, "The Privacy, Data Protection and Cybersecurity Law Review: China", The Law Review, 27. oktobar 2022. https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/china

472 X. Ying , Y. Suwen, "About Face", NewsChina Magazine, http://www.newschinamag.com/newschina/articleDetail.do?article_id=7219&section_id=17&magazine_id=81

473 J. Deng, "China's highest court clarifies judicial rules in civil disputes related to face recognition technology", 2. avgust 2021. https://www.mondaq.com/china/civil-law/1098184/chinas-highest-court-clarifies-judicial-rules-in-civil-disputes-related-to-face-recognition-technology

474 CIPESA, "State of Internet Freedom in Africa 2022: The Rise of Biometric Surveillance", 29. septembar 2022. https://cipesa.org/2022/09/state-of-internet-freedom-in-africa-2022-the-rise-of-biometric-surveillance/; H. Swart, A. Munoriyarwa, "Video Surveillance in Southern Africa: Case studies of security camera systems in the region", Media Policy and Democracy Project, maj 2020. https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/video_surveillance_in_southern_africa_-_security_camera_systems_in_the_region.pdf

475 Izveštaji o ovom uticaju iz američke perspektive: United States-China Economic and Security Review Commission, "Hearing On China's Strategic Aims In Africa", 2020. https://www.uscc.gov/sites/default/files/2020-06/May_8_2020_Hearing_Transcript.pdf ili u EPIC nastavcima dostupnim ovde: B. Jili, "The Rise of Chinese Surveillance Technology in Africa (deo 1 od 6)", EPIC, 31. maj, 2022. https://epic.org/the-rise-of-chinese-surveillance-technology-in-africa/; B. Jili, "The Rise of Chinese Surveillance Technology in Africa (deo 2 od 6)", EPIC, 29. juni 2022. https://epic.org/the-rise-of-chinese-surveillance-technology-in-africa-2/; B. Jili, "The Rise of Chinese Surveillance Technology in Africa (deo 3 od 6)", EPIC, 29. juli 2022. https://epic.org/the-rise-of-chinese-surveillance-technology-in-africa-part-3-of-6/; B. Jili, "The Rise of Chinese Surveillance Technology in Africa (deo 4 od 6)", EPIC, 25. avgust 2022. https://epic.org/the-rise-of-chinese-surveillance-technology-in-africa-part-4-of-6/; B. Jili, "The Rise of Chinese Surveillance Technology in Africa (deo 5 od 6)", EPIC, 22. septembar 2022. https://epic.org/the-rise-of-chinese-surveillance-technology-in-africa-part-5-of-6/; B. Jili, "The Rise of Chinese Surveillance Technology in Africa (deo 6 od 6)", EPIC, 21. oktobar 2022. https://epic.org/the-rise-of-chinese-surveillance-technology-in-africa-part-6-of-6/

476 Africa Business, "How the European Union's General Data Protection Regulations influenced data privacy law in Africa", 9. jun 2022. https://africabusiness.com/2022/06/09/how-the-european-unions-general-data-protection-regulations-influenced-data-privacy-law-in-africa/; P. Boshe, M. Hennemann, "Data Protection Laws in Northern Africa - Regulatory Approaches, Key Principles, Selected Documents", Konrad-Adenauer-Stiftung, septembar 2022. https://www.kas.de/en/web/rspno/single-title/-/content/data-protection-laws-in-northern-africa-regulatory-approaches-key-principles-selected-documents

477 M. Badillo, "Navigating the complexities of facial recognition for public security in Latin America", International Bar Association, 9. maj 2023. https://www.ibanet.org/facial-recognition-security-latin-america

478 Access Now, "Made Abroad, Deployed at Home", avgust 2021. https://www.accessnow.org/wp-content/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf

479 C. Caeiro, "Regulating facial recognition in Latin America", Chatham House, 11. novembar 2022. https://www.chathamhouse.org/2022/11/regulating-facial-recognition-latin-america

480 J. Ramos, "Latin Americans Are Furious", The New York Times, 8. novembar 2019.https://www.nytimes.com/2019/11/08/opinion/contributors/latin-america-protest-repression.html

481 F. Fascendini, F. Roveri, "Your software is my biology: The mass surveillance system in Argentina", Global Information Society Watch (GISWatch), 2014. https://giswatch.org/en/country-report/communications-surveillance/argentina

482 Ibid.

483 Área Digital Asociación por los Derechos Civiles, "Cuantificando identidades en América Latina", maj 2017. https://adc.org.ar/wp-content/uploads/2019/06/029-cuantificando-identidades-en-america-latina-05-2017.pdf (na španskom).

484 D. Gershgorn, "The US Fears Live Facial Recognition. In Buenos Aires, It's a Fact of Life", OneZero, 4. mart 2020. https://onezero.medium.com/the-u-s-fears-live-facial-recognition-in-buenos-aires-its-a-fact-of-life-52019eff454d

485 European Digital Rights (EDRi), "Dangerous by design: A cautionary tale about facial recognition", 12. februar 2020. https://edri.org/our-work/dangerous-by-design-a-cautionary-tale-about-facial-recognition/

486 M. Badillo, "Judge declares Buenos Aires' Fugitive Facial Recognition System Unconstitutional", Future of Privacy Forum, 30. septembar 2022. https://fpf.org/blog/judge-declares-buenos-aires-fugitive-facial-recognition-system-unconstitutional/

487 A. Mascellino, "Brazil deploys ISS facial recognition to secure São Paulo metro", Biometric Update, 9. decembar 2022. https://www.biometricupdate.com/202212/brazil-deploys-iss-facial-recognition-to-secure-sao-paulo-metro

488 A. Makoni, "Brazil's Embrace Of Facial Recognition In Schools Is Worrying Its Black Communities", POCIT, 17. maj 2022. https://peopleofcolorintech.com/general/brazils-embrace-of-facial-recognition-in-schools-is-worrying-black-communities/

489 DataGuidance, "Brazil: ViaQuatro is fined BRL 100,000 for improper facial recognition practices at subway stations", 11. maj 2021. https://www.dataguidance.com/news/brazil-viaquatro-fined-brl-100000-improper-facial

490 M. Garrote, N. Paschoalini, M. Meira, "Why should we all pay attention to the Brazilian Digital ID system?", Data Privacy Brasil Research Association, 23. novembar 2022. https://www.dataprivacybr.org/why-should-we-all-pay-attention-to-the-brazilian-digital-id-system-2/

491 B. Bioni et al., "Between visibility and exclusion: mapping the risks associated with the National Civil Identification System and the usage of its database by the gov.br platform", Data Privacy Brasil Research Association, 2022. https://www.dataprivacybr.org/wp-content/uploads/2022/11/Policy-paper-Data-Privacy-Brazil-Research-BETWEEN-VISIBILITY-AND-EXCLUSION.pdf

492 Access Now, "Joint statement: Mexico, Guatemala, Honduras, El Salvador and the United States must terminate their agreements on cross-border transfers of migrants' biometric data", 23. mart 2023. https://www.accessnow.org/press-release/statement-terminate-agreements-biometric-data-migrants/

493 C. Caeiro, "06 To ban or to regulate facial recognition in Latin America? The debate", Chatham House, 11. novembar 2022. https://www.chathamhouse.org/2022/11/regulating-facial-recognition-latin-america/06-ban-or-regulate-facial-recognition-latin

494 Access Now, "Made Abroad, Deployed at Home" (zaključak), avgust 2021. https://www.accessnow.org/wp-content/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf

495 Coding Rights, "Legislators from all regions of Brazil present bills to ban facial recognition in public spaces", 22. juni 2022. https://medium.com/codingrights/legislators-from-all-regions-of-brazil-present-bills-to-ban-facial-recognition-in-public-spaces-31d8da0d3822

496 DLA Piper, "Global Data Protection Laws of the World - Chile", 28. januar 2023. https://www.dlapiperdataprotection.com/index.html?t=law&c=CL

497 Guyer & Regules, "Global Data Protection Law Guide - Uruguay", Multilaw, 2023. https://www.multilaw.com/Multilaw/Data_Protection_Laws_Guide/DataProtection_Guide_Uruguay.aspx

498 DLA Piper, "Global Data Protection Laws of the World - Mexico", 12. januar 2023. https://www.dlapiperdataprotection.com/index.html?t=law&c=MX

499 DLA Piper, "Global Data Protection Laws of the World - Costa Rica", 26. januar 2023. https://www.dlapiperdataprotection.com/index.html?t=law&c=CR

500 B. Fernandez Nieto, "Habeas Data and Personal Data Protection in Latin America", Data-Pop Alliance, 25. avgust 2022. https://datapopalliance.org/habeas-data-and-personal-data-protection-in-latin-america/

501 AlSur, "Facial recognition in Latin America", 2021. https://www.alsur.lat/sites/default/files/2021-10/ALSUR_Reconocimiento%20facial%20en%20Latam_EN_Final.pdf

502 Ministério dos Transportes do Brasil, Portaria Denatran N° 1515, 2018. https://www.legisweb.com.br/legislacao/?id=372479 (na portugalskom).

503 Legislatura de la Ciudad Autónoma De Buenos Aires, Sistema Integral De Seguridad Pública De La Ciudad Autónoma De Buenos Aires, Ley Q - N° 5.688, 2016. https://digesto.buenosaires.gob.ar/documento/download/Ley%20Ciudad-5688__68dc0cdd582d3dd01f4f976a796c5cda9d7ab7dd.pdf (na španskom).

504 Congreso de la República de Colombia, Código Electoral Colombiano, PL 234-20, 2020. http://leyes.senado.gov.co/proyectos/index.php/textos-radicados-senado/p-ley-2020-2021/2021-proyecto-de-ley-234-de-2020 (na španskom).

505 Constitution for the Argentine Nation, http://www.biblioteca.jus.gov.ar/argentina-constitution.pdf

506 Congress of the Argentine Nation, Act 25.326, 2000. http://www.jus.gob.ar/media/3201023/personal_data_protection_act25326.pdf

507 Télam, "La Legislatura aprobó el uso de reconocimiento facial para la detención de prófugos", 22. oktobar 2020. https://www.telam.com.ar/notas/202010/527676-la-legislatura-aprobo-el-uso-de-reconocimiento-facial-para-la-detencion-de-profugos.html (na španskom).

508 Diario Judicial, "Sonría, lo estamos filmando", 22. oktobar 2020. https://www.diariojudicial.com/news-87691-sonria-lo-estamos-filmando (na španskom).

509 OHCHR, "Statement to the media by the United Nations Special Rapporteur on the right to privacy, on the conclusion of his official visit to Argentina, 6-17 May 2019", 23. maj 2019. https://www.ohchr.org/en/statements/2019/05/statement-media-united-nations-special-rapporteur-right-privacy-conclusion-his

510 E. Ferreyra, "Facial recognition in Latin America: Towards a human rights-based legal framework to protect public spaces from mass surveillance", Global Campus of Human Rights, 2020. https://repository.gchumanrights.org/items/b6fb1ba9-95d2-436a-a4ef-a2471b54a9cf

511 M. Peruzzotti, "Argentina: Draft bill on personal data protection", IAPP, 28. oktobar 2022. https://iapp.org/news/a/argentina-draft-bill-on-personal-data-protection/

512 Agencia de Acceso a la Información Pública de Argentina, Resolución 4/2019, 2019. https://servicios.infoleg.gob.ar/infolegInternet/anexos/315000-319999/318874/norma.htm (na španskom)

513 Privacy International, "Privacy International's submission Argentina's draft law on the protection of personal data, 2022", septembar 2022. https://privacyinternational.org/sites/default/files/2022-11/PI%20comments%20on%20Propuesta%20de%20anteproyecto%20de%20ley%202022.pdf

514 Ministerio de Seguridad, Resolución 710/2024, Ciudad de Buenos Aires, 26. juli 2024. https://www.boletinoficial.gob.ar/detalleAviso/primera/311381/20240729

515 H. Barber, "Argentina will use AI to 'predict future crimes' but experts worry for citizens' rights", 1. avgust 2024. https://www.theguardian.com/world/article/2024/aug/01/argentina-ai-predicting-future-crimes-citizen-rights

516 Constitution of the Federative Republic of Brazil, 3rd Edition, 2010. https://www.globalhealthrights.org/wp-content/uploads/2013/09/Brazil-constitution-English.pdf

517 Presidency of Brazil, Marco Civil Law of the Internet in Brazil, Law No. 12.965, 2014. https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180

518 National Congress of Brazil, Brazilian Data Protection Law (LGPD), as amended by Law No. 13.853, 2019. https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/

519 DataGuidance, "Brazil: House of Representatives approves constitutional amendment on the protection of personal data", 1. septembar 2021. https://www.dataguidance.com/news/brazil-house-representatives-approves-constitutional

520 Câmara dos Deputados, "Exposição de Motivos: Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal", 2019. https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf (na portugalskom).

521 „Regulating Facial Recognition in Brazil", The Cambridge Handbook of Facial Recognition in the Modern State, pp. 228-241, Cambridge University Press, 2024 https://www.cambridge.org/core/books/cambridge-handbook-of-facial-recognition-in-the-modern-state/regulating-facial-recognition-in-brazil/CEEA7751492156D1FFE96E029CB014AD

522 Assembléia Legislativa do Ceará, Lei N.° 16.873, 2019. https://belt.al.ce.gov.br/index.php/legislacao-do-ceara/organizacao-tematica/cultura-e-esportes/item/6638-lei-n-16-873-de-10-05-19-d-o-10-05-19 (na portugalskom)

523 Assembléia Legislativa de Minas Gerais, Lei N° 21737, 2015. https://www.legisweb.com.br/legislacao/?id=287944 (na portugalskom)

524 Assembléia Legislativa de Alagoas, Lel N° 8.113, 2019. https://sapl.al.al.leg.br/media/sapl/public/normajuridica/2019/1594/lei_no_8.113_de_29.05.2019.pdf (na portugalskom)

525 Assembléia Legislativa do Estado do Rio de Janeiro, Lei N° 7123, 2015. https://www.legisweb.com.br/legislacao/?id=384128 (na portugalskom).

526 Câmara Legislativa do Distrito Federal, Lei N° 6.712, 2020. https://www.tjdft.jus.br/institucional/relacoes-institucionais/arquivos/lei-no-6-712-de-10-de-novembro-de-2020.pdf (na portugalskom)

527 E. Sakiotis et al., "Brazil's Senate Committee Publishes AI Report and Draft AI Law", Covington Inside Privacy, 27. januar 2023. https://www.insideprivacy.com/emerging-technologies/brazils-senate-committee-publishes-ai-report-and-draft-ai-law/

528 L.Liang, "Brazilian groups call for ban on facial recognition", Biometric Udate, 16. oktobar 2024. https://www.biometricupdate.com/202410/brazilian-groups-call-for-ban-on-facial-recognition

M. Borak, "As Brazil debates AI bill, calls for facial recognition bans emerge", Biometric Update, 8. jul 2024. https://www.biometricupdate.com/202407/as-brazil-debates-ai-bill-calls-for-facial-recognition-bans-emerge

529 K. Silva, "Brazilian court declares data protection a fundamental right in landmark decision", Global Data Review, 11. maj 2020. https://globaldatareview.com/article/brazilian-court-declares-data-protection-fundamental-right-in-landmark-decision

530 Access Now, "Privacy win for 350,000 people in São Paulo: court blocks facial recognition cameras in metro", 12. maj 2021. https://www.accessnow.org/press-release/sao-paulo-court-bans-facial-recognition-cameras-in-metro/

531 Global Freedom of Expression, "The Case of São Paulo Subway Facial Recognition Cameras", Global Freedom of Expression, 7. maj 2021. https://globalfreedomofexpression.columbia.edu/cases/the-case-of-sao-paulo-subway-facial-recognition-cameras/

532 M. Badillo, "Judge declares Buenos Aires' Fugitive Facial Recognition System Unconstitutional", Future of Privacy Forum, 30. septembar 2022. https://fpf.org/blog/judge-declares-buenos-aires-fugitive-facial-recognition-system-unconstitutional/

533 C. Garrison, V. Hilaire, "Mexico's top court strikes down controversial cell-phone registry with biometric data", Reuters, 25. april 2022. https://www.reuters.com/world/americas/mexicos-top-court-strikes-down-creation-cell-phone-registry-with-biometric-user-2022-04-25/

534 Fight for the Future, "Ban Facial Recognition", https://www.banfacialrecognition.com/map/

535 N. Turner Lee, C. Chin, "Police surveillance and facial recognition: Why data privacy is imperative for communities of color", The Brookings Institution, 12. april 2022. https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/; R. Brandom, "Most US government agencies are using facial recognition", The Verge, 25. avgust 2021. https://www.theverge.com/2021/8/25/22641216/facial-recognition-gao-report-agency-dhs-cbp-fbi; Mordor Intelligence, "United States Facial Recognition Market Size & Share Analysis - Growth Trends & Forecasts (2023 - 2028)", https://www.mordorintelligence.com/industry-reports/united-states-facial-recognition-market

536 NYCLU, "What You Need to Know About New York's Temporary Ban on Facial Recognition in Schools", 2. juli 2021. https://www.nyclu.org/en/publications/what-you-need-know-about-new-yorks-temporary-ban-facial-recognition-schools

537 Predlog iz Masačusetsa: Massachusetts General Court, Bill H.142, An Act establishing the Massachusetts Information Privacy Act, 2021. https://malegislature.gov/Bills/192/H142

538 Videti odeljak o Vermontu.

539 Neki od predloga mogu se naći ovde: Y. D. Clarke, "Reps. Clarke, Pressley & Tlaib Announce Bill to Ban Public Housing Usage of Facial Recognition & Biometric Identification Technology", Clarke.Senate.gov, https://clarke.house.gov/nobiometricsbarriers/; D. Beyer, "Beyer, Lieu Reintroduce Legislation To Block Law Enforcement From Using Facial Recognition Technology With Body Cam Footage", Beyer.House.gov, 21. juni 2022. https://beyer.house.gov/news/documentsingle.aspx?DocumentID=5619; C. Coons, "Facial recognition tech: Sens. Coons, Lee bill requires court orders for law enforcement use of facial recognition technology", Coons.Senate.gov, 14. novembar 2019. https://www.coons.senate.gov/news/press-releases/facial-recognition-tech-sens-coons-lee-bill-requires-court-orders-for-law-enforcement-use-of-facial-recognition-technology

540 United States Congress, S.2052 - Facial Recognition and Biometric Technology Moratorium Act of 2021, https://www.congress.gov/bill/117th-congress/senate-bill/2052?s=1&r=1&q=%7B%22search%22%3A%5B%22Facial+Recognition+and+Biometric+Technology+Moratorium+Act+of+2021%22%5D%7D

541 United States Congress, Facial Recognition and Biometric Technology Moratorium Act of 2023, https://www.markey.senate.gov/imo/media/doc/facial_recognition_and_biometric_technology_moratorium_act_-_2023.pdf

542 E. Markey, "Markey, Merkley, Jayapal Lead Colleagues on Legislation to Ban Government Use of Facial Recognition and Other Biometric Technology", Markey.Senate.gov, 7. mart 2023. https://www.markey.senate.gov/news/press-releases/markey-merkley-jayapal-lead-colleagues-on-legislation-to-ban-government-use-of-facial-recognition-and-other-biometric-technology; J. Lyons Hardcastle, "Law bill seeks to ban Feds' use of facial recognition tech", The Register, 7. mart 2023. https://www.theregister.com/2023/03/07/us_ban_facial_recognition; Passett, "US Congress Members Reintroduce Serious Facial Recognition Bill", TechZone360, 8. mart 2023. https://www.techzone360.com/topics/techzone/articles/2023/03/08/455203-us-congress-members-reintroduce-serious-facial-recognition-bill.htm

543 United States Congress, H. R. 9061, 2022. https://www.congress.gov/bill/117th-congress/house-bill/9061/text?s=1&r=9

544 J. Laperruque, "The Facial Recognition Act: A Promising Path to Put Guardrails on a Dangerously Unregulated Surveillance Technology", Lawfare, 1. novembar 2022. https://www.lawfareblog.com/facial-recognition-act-promising-path-put-guardrails-dangerously-unregulated-surveillance-technology

545 CaseGuard, "The Facial Recognition Act of 2022, New Proposed Law", 28. oktobar 2022. https://caseguard.com/articles/the-facial-recognition-act-of-2022-new-proposed-law/

546 J. Laperruque, "Limiting Face Recognition Surveillance: Progress and Paths Forward", Center for Democracy and Technology, 23. avgust 2022. https://cdt.org/insights/limiting-face-recognition-surveillance-progress-and-paths-forward/

547 A. Kak, "Regulating Biometrics: Global Approaches and Open Questions", AI Now Institute, 1. septembar 2020. https://ainowinstitute.org/publication/regulating-biometrics-global-approaches-and-open-questions

548 Ibid., str. 90. Na primer, zabrane na gradskom nivou usvojene su u San Francisku (Kalifornija): San Francisco Administrative Code, Sec. 19b.2. Board of Supervisors Approval of Surveillance Technology Policy, https://codelibrary.amlegal.com/codes/san_francisco/latest/sf_admin/0-0-0-61746; Oklendu (Kalifornija): City of Oakland, Code of Ordinances, 9.64.045 – Prohibition on City's acquisition and/or use of Biometric Surveillance Technology and Predictive Policing Technology, https://library.municode.com/ca/oakland/codes/code_of_ordinances?nodeId=TIT9PUPEMOWE_CH9.64REACUS-SUTE_9.64.045PRACUSBISUTEPRPOTE; Portlandu (Oregon): The City of Portland, Council Ordinance, 190113 Prohibit the acquisition and use of Face Recognition Technologies by City bureaus ordinance, 2020. https://efiles.portlandoregon.gov/Record/139452; i Mineapolisu (Minesota): Minneapolis Code of Ordinances, Title 2, Chapter 41, Article II. - Facial Recognition Technology, https://library.municode.com/mn/minneapolis/codes/code_of_ordinances?nodeId=COOR_TIT2AD_CH41INGO_ARTIIFARETE

549 A. Kak, "Regulating Biometrics: Global Approaches and Open Questions", AI Now Institute, 1. septembar, 2020. https://ainowinstitute.org/publication/regulating-biometrics-global-approaches-and-open-questions, str. 91-92.

550 AP News, "Virginia lawmakers ban police use of facial recognition", 29. mart 2021. https://apnews.com/article/technology-legislature-police-law-enforcement-agencies-legislation-033d77787d4e28559f08e5e31a5cb8f7

551 X. Landen, "Attorney general's office asks lawmakers to loosen ban on facial recognition", VTDigger, 25. februar 2021. https://vtdigger.org/2021/02/25/attorney-generals-office-asks-lawmakers-to-loosen-ban-on-facial-recognition/

552 The Editorial Board of Los Angeles Daily News, "Opinion: Calif. Should Extend Facial Recognition Ban", Government Technology, 6. april 2022. https://www.govtech.com/policy/opinion-calif-should-extend-facial-recognition-ban; G. Lee, "California bill would regulate police use of facial recognition technology in body cams", KTVU Fox 2, 9. mart 2023. https://www.fox2detroit.com/news/california-bill-would-regulate-police-use-of-facial-recognition-technology-in-body-cams; CBS San Franciscso, "Bill proposed to regulate facial recognition technology in policing", 8. mart 2023. https://www.cbsnews.com/sanfrancisco/news/bill-proposed-to-regulate-facial-recognition-technology-in-policing/; C. Micheli, "Facial Recognition Legislation in California", California Globe, 4. mart 2023. https://californiaglobe.com/articles/facial-recognition-legislation-in-california/

553 K. Kaye, "Police can use facial recognition again after ban in New Orleans, home to sprawling surveillance", Protocol, 26. juli 2022. https://www.protocol.com/enterprise/new-orleans-surveillance-facial-recognition

554 R. Metz, "First, they banned facial recognition. Now they're not so sure", CNN Business, 5. avgust 2022. https://edition.cnn.com/2022/08/05/tech/facial-recognition-bans-reversed/index.html; J. Parker, "U.S. States and Cities Rethinking Bans, Setting Rules for Law Enforcement Use of Facial Recogni- tion", Security Industry Association, 10. maj 2022. https://www.securityindustry.org/2022/05/10/u-s-states-and-cities-rethinking-bans-setting-rules-for-law-enforcement-use-of-facial-recognition/

555 P. Dave, "U.S. cities are backing off banning facial recognition as crime rises", Reuters, 12. maj 2022. https://www.reuters.com/world/us/us-cities-are-backing-off-banning-facial-recognition-crime-rises-2022-05-12/

556 BIPA reguliše različite vrste biometrije. Prema definiciji, „biometrijski identifika-

tor“ znači sken irisa u oku, ostisak prsta, otisak glasa, sken dlana ili geometrije lica. Tekst BIPA: Illinois General Assembly, Public Act 095-0994, https://www.ilga.gov/legislation/publicacts/95/095-0994.htm

557 Zakon Teksasa za poslovanje i trgovinu 503.001, naslovljen kao zakon o snimanju ili upotrebi biometrijskih identifikatora (Capture or Use of Biometric Identifiers Act, CUBI): Texas State Legislature, Texas Business & Commerce Code 503.001, 2009. https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm

558 J. Goldwater, M. Smigielski, K. Nelson, “State Biometric Legislation Developments”, Lewis Brisbois Bisgaard & Smith LLP, 18. avgust 2021. https://lewisbrisbois.com/newsroom/legal-alerts/state-biometric-legislation-developments

559 J. Lewis, W. Crumpler, “Facial Recognition Technology: Responsible Use Principles and the Legislative Landscape”, Center for Strategic and International Studies, 29. septembar 2021. https://www.csis.org/analysis/facial-recognition-technology-responsible-use-principles-and-legislative-landscape

560 C. W. Savage, “Washington Enacts First-in-the-Nation State Law Regulating Governmental Use of Facial Recognition Technology”, Davis Wright Tremaine, 9. april 2020. https://www.dwt.com/blogs/privacy--security-law-blog/2020/04/washington-state-facial-recognition-tech-law

561 Y. Luo, R. Guo, “Facial Recognition in China: Current Status, Comparative Approach and the Road Ahead”, 25 U. Pa. J.L. & Soc. Change 153, 2021. https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1269&context=jlasc, str. 173.

562 Washington State Legislature, SB 6280 - 2019-20, 2020. https://app.leg.wa.gov/billsummary?BillNumber=6280&Year=2019&Initiative=false#-documentSection

563 E. Lostri, “Washington’s New Facial Recognition Law”, Center for Strategic and International Studies, 3. april 2020. https://www.csis.org/blogs/strategic-technologies-blog/washingtons-new-facial-recognition-law

564 A. Berengaut, “Washington State Passes Bill Limiting Government Use of Facial Recognition”, Covington Inside Privacy, 23. mart 2020. https://www.insideprivacy.com/united-states/state-legislatures/washington-state-passes-bill-limiting-government-use-of-facial-recognition/

565 J. Lee, “We Need a Face Surveillance Moratorium, Not Weak Regula- tions: Concerns about SB 6280”, ACLU of Washington, 31. mart 2020. https://www.aclu-wa.org/story/we-need-face-surveillance-moratorium-not-weak-regulations-concerns-about-sb-6280; E. Lostri, “Washington’s New Facial Recognition Law”,Center for Strategic and International Studies, 3. april 2020. https://www.csis.org/blogs/strategic-technologies-blog/washingtons-new-facial-recognition-law

566 P. Dave, J. Dastin, “Washington State signs facial recognition curbs into law; critics want ban”, Reuters, 31. mart 2020. https://www.reuters.com/article/us-washington-tech-idUSKBN21I3AS; D. Gershgorn, “A Microsoft Employee Literally Wrote Washington’s Facial Recognition Law”, OneZero, 3. april 2020. https://onezero.medium.com/a-microsoft-employee-literally-wrote-washingtons-facial-recognition-legislation-aab950396927; B. Smith, “Finally, progress on regulating facial recognition”, Microsoft, 31. mart 2020. https://blogs.microsoft.com/on-the-issues/2020/03/31/washington-facial-recognition-legislation/

567 A. Berengaut, “Washington State Passes Bill Limiting Government Use of Facial Recognition”, Covington Inside Privacy, 23. mart 2020. https://www.insideprivacy.com/united-states/state-legislatures/washington-state-passes-bill-limiting-government-use-of-facial-recognition/

568 Colorado General Assem- bly, SB22-113, Artificial Intelligence Facial Recognition, 2022. https://leg.colorado.gov/bills/sb22-113; Digital Policy Alert, “United States of America: Colorado: Law on facial recognition technology (Senate Bill 22-113)”, https://digitalpolicyalert.org/change/2828-colorado-law-on-facial-recognition-technology-senate-bill-22-113

569 L. Foster Freedman, “Colorado Law Restricts Use of Facial Recognition Technology by Government Agencies”, Robinson+Cole , 15. juni 2022. https://www.dataprivacyandsecurityinsider.com/2022/06/colorado-law-restricts-use-of-facial-recognition-technology-by-government-agencies/; H. Metzger, “Task force to assess use of facial recognition by Colorado law enforcement, government”, Colorado Politics, 9. jun 2022. https://www.coloradopolitics.com/legislature/task-force-to-assess-use-of-facial-recognition-by-colorado-law-enforcement-government/article_52846144-e83e-11ec-b930-7fe52b4e1214.html

570 General Assembly of Virginia, Code of Virginia, § 15.2-1723.2., 2021. https://law.lis.virginia.gov/vacode/title15.2/chapter17/section15.2-1723.2/; General Assembly of Virginia, Code of Virginia, § 23.1-815.1, 2021. https://lis.virginia.gov/cgi-bin/legp604.exe?212+ful+HB2031ER+hil

571 B. Atkinson, “Virginia Bill to Put De Facto Ban on Facial Recognition Tech”, Government Technology, 8. april, 2021. https://www.govtech.com/policy/virginia-bill-to-put-de-facto-ban-on-facial-recognition-tech.html; Robinson & Cole LLP, “Virginia Law Bans Local Police Use of Facial Recognition Technology”, The National Law Review, 22. april 2021. https://www.natlawreview.com/article/virginia-law-bans-local-police-use-facial-recognition-technology

572 A. Powers, K. Simon, J. Spivack, “From Ban to Approval: What Virginia’s Facial Recognition Technology Law Gets Wrong”, 26 Rich. Pub. Int. L. Rev. 155, 2023. https://scholarship.richmond.edu/cgi/viewcontent.cgi?article=1553&context=pilr

573 S. C. Weston, “Can Police in Virginia Use Facial Recognition if They Suspect Criminal Activity?”, 16. novembar 2022. https://scwestonlaw.com/can-police-in-virginia-use-facial-recognition-if-they-suspect-criminal-activity/

574 A. McGibbon, “Police use of facial recognition tech resumes with guardrails”, VPM, 3. mart 2023. https://www.vpm.org/news/2023-03-03/virginia-facial-recognition-law-enforcement-privacy; ACLU of Virginia, “ACLU-VA’s Statement on Gov. Youngkin’s Actions on Facial Recognition Technology”, 14. april 2022. https://www.acluva.org/en/press-releases/aclu-vas-statement-gov-youngkins-actions-facial-recognition-technology

575 General Assembly of Virginia, SB 741 Facial recognition technology; authorised uses, 2022. https://lis.virginia.gov/cgi-bin/legp604.exe?221+sum+SB741

576 Commonwealth of Virginia, ”State Police Model Facial Recognition Technology Policy”, 31. decembar 2022. https://vsp.virginia.gov/wp-content/uploads/2023/01/State-Police-Model-Facial-Recognition-Technology-Policy.doc

577 Maine State Legislature, 25 Maine Revised Statutes § 6001. Facial surveillance,

2021. https://legislature.maine.gov/statutes/25/title25sec6001.html

578 ACLU of Maine, "Maine Enacts Strongest Statewide Facial Recognition Reg- ulations in the Country", 30. jun 2021. https://www.aclu.org/press-releases/maine-enacts-strongest-statewide-facial-recognition-regulations-country; A. Beyea, M. Kebede, "Maine's facial recognition law shows bipartisan support for protecting privacy", TechCrunch, 20. juli 2021. https://techcrunch.com/2021/07/20/maines-facial-recognition-law-shows-bipartisan-support-for-protecting-privacy/; J. Bryant, "Maine passes statewide facial recognition ban", IAPP, 1. juli 2021, https://iapp.org/news/a/maine-passes-statewide-facial-recognition-ban/; D. Gershgorn, "Maine passes the strongest state facial recognition ban yet", The Verge, 30. jun 2021. https://www.theverge.com/2021/6/30/22557516/maine-facial-recognition-ban-state-law; I. Bonifacic, "Maine bans facial recognition technology from schools and most police work", Engadget, 30. juni 2021. https://www.engadget.com/maine-facial-recognition-law-191252742.html; S. Ikeda, "Maine Becomes First State To Pass Broad Government Ban on Facial Recognition Technology", CPO Magazine, 8. juli 2021. https://www.cpomagazine.com/data-privacy/maine-becomes-first-state-to-pass-broad-government-ban-on-facial-recognition-technology/

579 Statewatch, "EU: Got a driving licence? You're going in a police line-up", 21. februar 2022. https://www.statewatch.org/news/2022/february/eu-got-a-driving-licence-you-re-going-in-a-police-line-up/

580 Utah State Legislature, S.B. 34 Governmental Use of Facial Recognition Technology, 2021. https://le.utah.gov/~2021/bills/static/SB0034.html

581 FindBiometrics, "Utah State Legislature Passes Facial Recognition Bill", 5. mart 2021. https://findbiometrics.com/utah-state-legislature-passes-facial-recognition-bill-030504/; FindBiometrics, "Utah Agency Adopts Internal Guidelines In Lieu of State Facial Recognition Law", 6. oktobar 2020. https://findbiometrics.com/utah-agency-adopts-internal-guidelines-lieu-state-facial-recognition-law-100606/; FindBiometrics, "Utah Poll Finds Public Support for Facial Recognition", 13. februar 2020. https://findbiometrics.com/biometrics-news-utah-poll-finds-public-support-facial-recognition-021308/; rezultati glasanja dostupni su ovde: Suffolk University, Salt Lake Tribune, Utah Poll, januar 2020. https://www.suffolk.edu/-/media/suffolk/documents/academics/research-at-suffolk/suprc/polls/other-states/2020/2_18_2020_marginals_pdftxt.pdf?la=en&hash=440698A-3312913CAF76630A78BD-07E142631D34B

582 Massachusetts General Court, General Laws, Part I, Title II, Chapter 6, Section 220: Facial recognition searches, 2020. https://malegislature.gov/Laws/GeneralLaws/PartI/TitleII/Chapter6/Section220; u Masačusetsu takođe postoji zakon koji reguliše upotrebu FRT u privatnim subjektima: Massachusetts General Court, Bill H.117, An Act to provide facial recognition accountability and comprehensive enforcement, 2021. https://malegislature.gov/Bills/192/H117

583 S. Solis, "Compromise police reform bill heads to Massachusetts Gov. Charlie Baker's desk", MassLive, 23. decembar 2020. https://www.masslive.com/politics/2020/12/compromise-police-reform-bill-heads-to-massachusetts-gov-charlie-bakers-desk.html

584 Zakon sadrži definiciju "drugih vrsta biometrijskog prepoznavanja na daljinu" koja obuhvata hod i glas, ali ne reguliše upotrebu tehnologije za takvo prepoznavanje na daljinu. Oslanja se na takvu definiciju da razjasni situacije u kojima se mogu koristiti alati za prepoznavanje lica. Videti takođe: ACLU of Massachusetts, "Limited face recognition regulations take effect today", 1. juli 2021. https://www.aclum.org/en/news/limited-face-recognition-regulations-take-effect-today; E. Peaslee, "Massachusetts Pioneers Rules For Police Use Of Facial Recognition Tech", NPR, 7. maj 2021. https://www.npr.org/2021/05/07/982709480/massachusetts-pioneers-rules-for-po-lice-use-of-facial-recognition-tech; J. Cote, "Facial recognition: What to know about the Massachusetts police reform bill's restrictions on the controver- sial tech", MassLive, 6. decembar 2020. https://www.masslive.com/police-fire/2020/12/facial-recognition-what-to-know-about-the-massachusetts-police-reform-bills-restrictions-on-the-controversial-tech.html

585 K. Hill, "How One State Managed to Actually Write Rules on Facial Recognition", The New York Times, 27. februar 2021. https://www.nytimes.com/2021/02/27/technology/Massachusetts-facial-recognition-rules.html

586 ACLU of Massachusetts, "Limited face recognition regulations take effect today", 1. juli 2021. https://www.aclum.org/en/news/limited-face-recognition-regulations-take-effect-today

587 ACLU of Massachusetts, "Press Pause on Face Surveillance", juni 2023. https://www.aclum.org/en/campaigns/press-pause-face-surveillance

588 Facial Recognition Commission of Massachusetts, https://frcommissionma.com/

589 Massachusetts General Court, Session Laws, Chapter 253, An Act Relative To Justice, Equity And Accountability In Law Enforcement In The Commonwealth, https://malegislature.gov/Laws/SessionLaws/Acts/2020/Chapter253

590 J. Nash, "Massachusetts panel says use of facial recognition should be restricted to state police", Biometric Update, 24. mart 2022. https://www.biometricupdate.com/202203/massachusetts-panel-says-use-of-facial-recognition-should-be-restricted-to-state-police; W. Katcher, "Massachusetts Facial Recognition Commission issues recommendations on use of controversial technology", MassLive, 22.mart 2022. https://www.masslive.com/news/2022/03/massachusetts-facial-recognition-commission-issues-recommendations-on-use-of-controversial-technology.html; S. Schoenberg, "Commission calls for limiting police use of facial recognition technology", CommonWealth Magazine, 22. mart 2022. https://commonwealthmagazine.org/criminal-justice/commission-calls-for-limiting-police-use-of-facial-recognition-technology/; J. Bonilla, "Should facial recognition be used in Massachusetts? New report says to limit use", wickedlocal.com, 29. juni 2022. https://www.wickedlocal.com/story/regional/massachusetts/2022/06/29/facial-recognition-use-commission-suggests-documenting-limiting-massachusetts-aclu-digital-fourth/9660776002/

591 Alabama Legislature, AL SB56, 2022. https://legiscan.com/AL/bill/SB56/2022

592 Predloženi tekst: Alabama Legislature, AL SB56, Introduced 2022. https://legiscan.com/AL/text/SB56/id/2470282

593 Usluga prepoznavanja lica definisana je kao softver, algoritam, proizvod ili aplikacija koja prikuplja ili elektronski analizira informacije u svrhu identifikacije pojedinca korišćenjem tehnologije koja može jedinstveno da identifikuje ili verifikuje identitet osobe poređenjem i analizom obrazaca prema konturama lica te osobe.

594 M. Maharrey, "Alabama Senate Passes Bill to Limit Warrantless Use of Facial Recognition", Tenth Amendment Center, 2. februar 2022. https://blog.ten-

thamendmentcenter.com/2022/02/alabama-senate-passes-bill-to-limit-warrantless-use-of-facial-recognition/; B. Moseley, "Senate passes bill restricting the use of facial recognition technology by law enforcement", 1819 News, 2. februar 2022. https://1819news.com/news/item/senate-passes-bill-restricting-the use-of-facial-recognition-technology-by-law-en-02-02-2022

595 J. Parker, "U.S. States and Cities Rethinking Bans, Setting Rules for Law Enforcement Use of Facial Recognition", Security Industry Association, 10. maj 2022. https://www.securityindustry.org/2022/05/10/u-s-states-and-cities-rethinking-bans-setting-rules-for-law-enforcement-use-of-facial-recognition/

596 D. Pillion, "Alabama police using facial recognition to ID Capitol riot suspects", AL.com, 9. januar 2021. https://www.al.com/news/2021/01/alabama-police-using-facial-recognition-to-id-capitol-riot-suspects.html; A. Ramey, "Investigating Alabama's use of facial recognition technology", NBC 15 News, 26. februar 2021. https://mynbc15.com/news/local/investigating-alabamas-use-of-facial-recognition-technology

597 Vermont General Assembly, Act No. 166 (S.124), 2020. https://legislature.vermont.gov/bill/status/2020/S.124

598 Poseban propis koji uređuje upotrebu dronova, predviđa izuzetak u pogledu upotrebe dronova u službama za sprovođenje zakona.

599 X. Landen, "Attorney general's office asks lawmakers to loosen ban on facial recognition", VTDigger, 25. februar 2021. https://vtdigger.org/2021/02/25/attorney-generals-office-asks-lawmakers-to-loosen-ban-on-facial-recognition/; J. Parker, "Most State Legislatures Have Rejected Bans and Severe Restrictions on Facial Recognition", Security Industry Association, 9. juli 2021. https://www.securityindustry.org/2021/07/09/most-state-legislatures-have-rejected-bans-and-severe-restrictions-on-facial-recognition/

600 Vermont General Assembly, Act No. 17 (H.195), 2021. https://legislature.vermont.gov/bill/status/2022/H.195

601 Vermont Criminal Justice Council, "Facial Recognition Technology Working Group", https://vcjc.vermont.gov/council/committees/facial-recognition-technology-working-group

602 Kentucky General Assembly, Senate Bill 176, 2022. https://apps.legislature.ky.gov/record/22rs/sb176.html

603 J. Parker, "U.S. States and Cities Rethinking Bans, Setting Rules for Law Enforcement Use of Facial Recognition", Security Industry Association, 10. maj 2022. https://www.securityindustry.org/2022/05/10/u-s-states-and-cities-rethinking-bans-setting-rules-for-law-enforcement-use-of-facial-recognition/

604 Test zakona: https://mgaleg.maryland.gov/2024RS/chapters_noln/Ch_808_sb0182E.pdf

605 J. Parker, "Nation's Strongest Regulations for Law Enforcement Use of Facial Recognition Technology Go Into Effect: Key Provisions of Maryland's New Law", Security Industry Association, 7. oktobar 2024. https://www.securityindustry.org/2024/10/07/nations-strongest-regulations-for-law-enforcement-use-of-facial-recognition-technology-go-into-effect-key-provisions-of-marylands-new-law/

606 Model politike: https://mcac.maryland.gov/wp-content/uploads/2024/10/Final-Facial-Recognition-Model-Policy.pdf

607 AIAAIC, "Robert Williams facial recognition wrongful arrest", april 2021. https://www.aiaaic.org/aiaaic-repository/ai-and-algorithmic-incidents-and-controversies/robert-williams-facial-recognition-wrongful-arrest; T. Ryan-Mosley, "The new lawsuit that shows facial recognition is officially a civil rights issue", MIT Technology Review, 14. april 2021. https://www.technologyreview.com/2021/04/14/1022676/robert-williams-facial-recognition-lawsuit-aclu-detroit-police/

608 E. Anderson, "Controversial Detroit facial recognition got him arrested for a crime he didn't commit", Detroit Free Press, 10. juli 2020. https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/

609 R. Darin Goldberg, "You Can See My Face, Why Can't I? Facial Recognition and Brady", Columbia Human Rights Law Review, 12. april 2021. https://hrlr.law.columbia.edu/hrlr-online/you-can-see-my-face-why-cant-i-facial-recognition-and-brady/#post-1679-footnote-ref-19

610 ACLU of Massachusetts, "ACLU v. Department of Justice", 2019. https://www.aclum.org/en/cases/aclu-v-department-justic

611 R. Mac, K. Hill, "Clearview AI settles suit and agrees to limit sales of facial recognition database.", The New York Times, 9. maj 2022. https://www.nytimes.com/2022/05/09/technology/clearview-ai-suit.html; R. Metz, "Clearview AI agrees to restrict US sales of facial recognition mostly to law enforcement", CNN Business, 9. maj 2022. https://edition.cnn.com/2022/05/09/tech/clearview-ai-aclu-settlement/index.html; ACLU of Illinois, "In Big Win, Settlement Ensures Clearview AI Complies With Groundbreaking Illinois Biometric Privacy Law", 9. maj 2022. https://www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois

612 H. Tsukayama, "Trends in biometric information regulation in the USA", Ada Lovelace Institute, 5. juli 2022. https://www.adalovelaceinstitute.org/blog/biometrics-regulation-usa/; E. Barlow Keener, "Facial Recognition: A New Trend in State Regulation", American Bar Association, 25. april 2022. https://www.americanbar.org/groups/business_law/publications/blt/2022/05/facial-recognition/; neke tužbe nisu bile uspešne: R. Westhead, "Blackhawks resolve lawsuit over alleged use of facial recognition software", TSN, 1. septembar 2021. https://www.tsn.ca/rick-westhead-chicago-blackhawks-illegally-used-facial-recognition-software-on-fans-lawsuit-says-1.1688479; "Plaintiff Abandons BIPA Lawsuit Against Chicago Blackhawks", 8. septembar 2021. https://findbiometrics.com/plaintiff-abandons-bipa-lawsuit-against-chicago-blackhawks-090807/

613 P. McKnight, "Historic Biometric Privacy Suit Settles for $650 Million", Business Law Today from ABA, 28. januar, 2021. https://businesslawtoday.org/2021/01/historic-biometric-privacy-suit-settles-650-million/; J. Bryant, "Facebook's $650M BIPA settlement 'a make-or-break moment'", IAPP, 5. mart 2021. https://iapp.org/news/a/facebooks-650m-bipa-settlement-a-make-or-break-moment/

614 F. M. Trujillo, J. Frankel, "Texas Starts Enforcing its Biometric Law", ZwillGen Blog, 18. februar 2022. https://www.zwillgen.com/privacy/texas-cubi-law-and-biometric-privacy; D. Bartz, "Texas sues Meta's Facebook over fa- cial-recognition practices", Reuters, 14. februar 2022. https://www.reuters.com/technology/texas-sues-meta-over-facebooks-facial-recognition-practices-report-2022-02-14/

615 Hunton Privacy Blog, "Judge Approves $92 Million TikTok Settlement", 9. avgust 2022. https://www.huntonprivacyblog.com/2022/08/09/judge-approves-92-million-tiktok-settlement/; N. Sakin, "TikTok settlement highlights power of privacy class actions to shape US protections", IAPP, 23. mart 2021. https://iapp.org/news/a/tiktok-settlement-highlights-power-of-privacy-class-actions-to-shape-u-s-protections/

616 A. Malik, "Snap agrees to $35 million settlement in Illinois privacy lawsuit", TechCrunch, 24. avgust 2022. https://techcrunch.com/2022/08/24/snap-35-million-settlement-in-illinois-bipa/; Top Class Actions, "Snapchat biometric privacy $35M class action settlement", 1. novembar 2022. https://topclassactions.com/lawsuit-settlements/closed-settlements/snapchat-biometric-privacy-35m-class-action-settlement/

617 K. Hurler, "Google Settles in $100 Million Illinois Photo Privacy Lawsuit", Gizmodo, 14. jun 2023. https://gizmodo.com/with-a-new-developer-framework-building-in-xr-is-easie-1850491958; NBC Chicago, "Everything To Know About Google Class-Action Settlement For Illinois Residents", 1. oktobar 2022. https://www.nbcchicago.com/news/local/everything-to-know-about-google-class-action-settlement-for-illinois-residents/2955833/

618 Xische & Co, "The UAE Can Lead in Facial Recognition", 26. maj 2021. https://www.xische.com/all-articles/2019/7/01/the-uae-can-lead-in-facial-recognition

619 M. Rajagopalan, "IBM, Huawei, And Hikvision Are Battling To Sell Facial Recognition Technology In Dubai", Buzzfeed News, 29. maj 2019. https://www.buzzfeednews.com/article/meghara/dubai-facial-recognition-technology-ibm-huawei-hikvision

620 Minister of State for Artificial Intelligence, Digital Economy & Remote Work Applications Office, UAE National Strategy for Artificial Intelligence 2031. https://ai.gov.ae/strategy/

621 Ibid.

622 UAE PASS, "About", https://selfcare.uaepass.ae/about

623 UAE PASS, https://selfcare.uaepass.ae/

624 Ministry of Cabinet Affairs, "UAE Government to employ biometric face recognition to register customers under 'UAE Pass' app", 7. april 2021. https://www.moca.gov.ae/en/media/news/uae-government-to-employ-biometric-face-recognition-to-register-customers-under-%27uae-pass%27-app

625 Ibid.

626 Z. Husain, "UAE: Facial recognition instead of Emirates ID card readers will now verify identity", Gulf News, 19. oktobar 2021. https://gulfnews.com/living-in-uae/ask-us/uae-facial-recognition-instead-of-emirates-id-card-readers-will-now-verify-identity-1.1634628283290; Z. Husain, "UAE: Three ways you can access the digital version of your Emirates ID for free", Gulf News, 9. februar 2023. https://gulfnews.com/living-in-uae/visa-immigration/uae-three-ways-you-can-access-the-digital-version-of-your-emirates-id-for-free-1.1675855637719

627 Dubai Police, Facebook, 30. oktobar 2021. https://www.facebook.com/dubaipolicehq.en/photos/a.136978203046390/4512542835489883/?type=3; Khaleej Times, "Dubai Police to launch AI-enabled platform for decision-making process", 30. oktobar 2021. https://www.khaleejtimes.com/uae/dubai-police-to-launch-ai-enabled-platform-for-decision-making-process

628 The Official Portal of the UAE Government, "Maintaining safety and security", https://u.ae/en/information-and-services/justice-safety-and-the-law/maintaining-safety-and-security

629 Dubai Police, Facebook, 27. januar 2018. https://www.facebook.com/dubaipolicehq.en/videos/1600201106724085; P. Bhunia, "Dubai Police launches artificial intelligence-based surveillance programme", OpenGov Asia, 29. januar 2018. https://opengovasia.com/dubai-police-launches-artificial-intelligence-based-surveillance-programme/; M. Rajagopalan, "IBM, Huawei, And Hikvision Are Battling To Sell Facial Recognition Technology In Dubai", Buzzfeed News, 29. maj 2019. https://www.buzzfeednews.com/article/meghara/dubai-facial-recognition-technology-ibm-huawei-hikvision

630 A. Al Shouk, "How Dubai's AI cameras helped arrest 319 suspects last year", Gulf News, 18. mart 2019. https://gulfnews.com/amp/uae/how-dubais-ai-cameras-helped-arrest-319-suspects-last-year-1.62750675

631 City Security Magazine, "Dubai Police take personal security to a whole new level", 12. septembar 2022. https://citysecuritymagazine.com/editors-choice/dubai-police-take-personal-security-to-a-whole-new-level; Gulf Business, "Dubai monitored by 300,000 cameras, one of the world's safest cities - Sheikh Mohammed", 14. juli 2021. https://gulfbusiness.com/dubai-monitored-by-300000-cameras-one-of-the-worlds-safest-cities-sheikh-mohammed/; B. Sapra, "Dubai police unveil plan to use drones", WIRED Middle East, 14. juli 2021. https://wired.me/technology/dubai-police-unveil-plan-to-use-drones/

632 A. Al Shouk, "Watch: Facial recognition at Dubai Metro stations to identify wanted criminals", Gulf News, 22. novembar 2020. https://gulfnews.com/uae/government/watch-facial-recognition-at-dubai-metro-stations-to-identify-wanted-criminals-1.75309516

633 L. Pascu, "Abu Dhabi police upgrade patrol cars with live biometric facial recognition", Biometric Update, 19., mart 2020. https://www.biometricupdate.com/202003/abu-dhabi-police-upgrade-patrol-cars-with-live-biometric-facial-recognition; A. Kumar, "These patrol cars can soon spot criminals on UAE streets", Khaleej Times, 10. mart 2020. https://www.khaleejtimes.com/uae/these-patrol-cars-can-soon-spot-criminals-on-uae-streets

634 M. Rajagopalan, "IBM, Huawei, And Hikvision Are Battling To Sell Facial Recognition Technology In Dubai", Buzzfeed News, 29. maj 2019. https://www.buzzfeednews.com/article/meghara/dubai-facial-recognition-technology-ibm-huawei-hikvision

635 J. Lynch, "Iron net: Digital repression in the Middle East and North Africa", European Council on Foreign Relations, 19. juni 2022. https://ecfr.eu/publication/iron-net-digital-repression-in-the-middle-east-and-north-africa/

636 Član 36 Ustava, dostupno na engleskom ovde: Constitution of the United Arab Emirates, https://www.wipo.int/edocs/lexdocs/laws/en/ae/ae030en.pdf

637 UAE Government, Federal Decree Law No. 45 of 2021 regarding the Protection of Personal Data, 2021, https://u.ae/-/media/ Documents-2023/ArFederal-Decree-Law-No-45-of-2021-regarding-the-Protection-of-Personal-Data.ashx (na arapskom); tekst zakona o zaštiti podataka nije javno dostupan na engleskom, ali korisni pregledi mogu se naći ovde: DLA Piper, "Data Protec-

tion Laws of the World UAE - General", 2023. https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country-1=AE; Al Tamimi & Co, "UAE's New Federal Data Protection Law", 6. decembar, 2021. https://www.tamimi.com/news/uaes-new-federal-data-protection-law/; R. Rizvi, "UAE - Data Protection Overview", DataGuidance, april 2023. https://www.dataguidance.com/notes/uae-data-protection-overview

638 The Official Portal of the UAE Government, "Data protection laws", https://u.ae/en/about-the-uae/digital-uae/data/data-protection-laws

639 Al Tamimi & Co, "UAE's New Federal Data Protection Law", 6. decembar 2021. https://www.tamimi.com/news/uaes-new-federal-data-protection-law/

640 R. Rizvi, "UAE - Data Protection Overview", DataGuidance, april 2023. https://www.dataguidance.com/notes/uae-data-protection-overview

641 Član 10 Zakona: UAE Government, Federal Decree Law No. 45 of 2021 regarding the Protection of Personal Data, 2021. https://u.ae/-/media/Documents-2023/ArFederal-Decree-Law-No-45-of-2021-regarding-the-Protection-of-Personal-Data.ashx (na arapskom).

642 Član 21 Zakona: UAE Government, Federal Decree Law No. 45 of 2021 regarding the Protection of Personal Data, 2021. https://u.ae/-/media/Documents-2023/ArFederal-Decree-Law-No-45-of-2021-regarding-the-Protection-of-Personal-Data.ashx (na arapskom).

643 House of Lords of the United Kingdom, "Attorney General's Reference No. 3 of 1999", 14. decembar 2000. https://publications.parliament.uk/pa/ld200001/ldjudgmt/jd001214/agref-1.htm

644 Statewatch, "UK: Police can keep DNA of innocent people indefinitely", 28. mart 2012. https://www.statewatch.org/news/2004/september/uk-police-can-keep-dna-of-innocent-people-indefinitely/

645 P. Fussey, W. Webster, "Interim report on the Abolition of the Office of the Biometrics and Surveillance Camera Commissioner as proposed by the UK Data Protection and Digital Information Bill", Centre for Research into Information, Surveillance and Privacy (CRISP), 11. maj 2023. http://www.crisp-surveillance.com/blog/233253/interim-report-abolition-office-biometrics-and-surveillance-camera-commissioner-proposed

646 V. Dodd, "Met police to use facial recognition software at Notting Hill carnival", The Guardian, 5. avgust 2017. https://www.theguardian.com/uk-news/2017/aug/05/met-police-facial-recognition-software-notting-hill-carnival

647 Izjava je dostupna na sajtu UK Vlade: https://www.gov.uk/government/speeches/prime-minister-keir-starmers-statement-in-downing-street-1-august

648 A. Wagner, "AI Facial Recognition Surveillance in the UK", Tech Policy Press, 22. oktobar 2024. https://www.techpolicy.press/ai-facial-recognition-surveillance-in-the-uk/

649 Nalazi ovog istraživanju su dostupni na Liberty sajtu: https://www.libertyhumanrights.org.uk/fundamental/predictive-policing/

650 https://homeofficemedia.blog.gov.uk/2023/10/29/police-use-of-facial-recognition-factsheet/

651 UK Information Commissioner's Office, "Information Commissioner's Opinion: The use of live facial recognition technology in public places", 18. jun 2021. https://ico.org.uk/media/for-organisations/documents/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf

652 Privacy International, "Civil Society Groups: Live Facial Recognition Technology should not be used in public spaces", avgust 2021. https://privacyinternational.org/sites/default/files/2021-08/LFRT%20Open%20Letter%20Final.pdf

653 P. Collings, M. Guariglia, "Ban Government Use of Face Recognition In the UK", Electronic Frontier Foundation, 26. septembar 2022. https://www.eff.org/deeplinks/2022/09/ban-government-use-face-recognition-uk

654 M. Ryder, "The Ryder Review", Ada Lovelace Institute, juni 2022. https://www.adalovelaceinstitute.org/wp-content/uploads/2022/06/The-Ryder-Review-Independent-legal-review-of-the-governance-of-biometric-data-in-England-and-Wales-Ada-Lovelace-Institute-June-2022.pdf

655 Tekst pisma je dostupan ovde: https://migrantsrights.org.uk/wp-content/uploads/2024/08/Joint-letter-to-Keir-Starmer-re-expansion-of-facial-recognition-technology-090824.pdf

656 Parliament of the United Kingdom, Human Rights Act 1998, https://www.legislation.gov.uk/ukpga/1998/42/contents

657 Government of the United Kingdom, The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019. https://www.legislation.gov.uk/uksi/2019/419/contents/made

658 Parliament of the United Kingdom, Data Protection Act 2018. https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

659 Scottish Biometrics Commissioner, "What are biometrics?", https://www.biometricscommissioner.scot/biometrics/what-are-biometrics/

660 UK Information Commissioner's Office, "Information Commissioner's Opinion: The use of live facial recognition technology by law enforcement in public places", 31. oktobar 2019. https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf

661 UK Information Commissioner's Office, "The use of live facial recognition technology in public places", 18. juni 2021. https://ico.org.uk/media/for-organisations/documents/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf

662 Parliament of the United Kingdom, Police and Criminal Evidence Act 1984. https://www.legislation.gov.uk/ukpga/1984/60/contents

663 Parliament of the United Kingdom, Terrorism Act 2000. https://www.legislation.gov.uk/ukpga/2000/11/contents

664 Parliament of the United Kingdom, Protection of Freedoms Act 2012. https://www.legislation.gov.uk/ukpga/2012/9/contents/enacted

665 S. Rowe, J. Jones, "The Biometrics and Surveillance Camera Commissioner: streamlined or eroded oversight?", Ada Lovelace Institute, 9. oktobar 2020. https://www.adalovelaceinstitute.org/blog/biometrics-surveillance-camera-commissioner/

666 Scottish Parliament, Scottish Biometrics Commissioner Act 2020. https://www.legislation.gov.uk/asp/2020/8/contents

667 Scottish Biometrics Commissioner, "Code of Practice", novembar 2022. https://www.biometricscommissioner.scot/media/5y0dmsq3/biometrics-code-of-practice.pdf

668 European Court of Human Rights, "Case of S. and Marper v. the United Kingdom", 4. decembar 2008. https://rm.coe.int/168067d216

669 England and Wales Court of Appeal, "R (Bridges) v. Chief Constable of South Wales Police", 11. avgust 2020. https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf

670 UK Supreme Court, "Bank Mellat v. HM Treasury", 19. juni 2013. https://www.supremecourt.uk/cases/uksc-2011-0040.html

671 H. Swart, A. Munoriyarwa, "Video Surveillance in Southern Africa: Case studies of security camera systems in the region", Media Policy and Democracy Project, maj 2020. https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/video_surveillance_in_southern_africa_-_security_camera_systems_in_the_region.pdf

672 Global Voices, "How Zimbabwe is building a Big Brother surveillance state", 10. januar 2023. https://globalvoices.org/2023/01/10/how-zimbabwe-is-building-a-big-brother-surveillance-state/

673 Ibid.

674 F. Mutsaka, "Zimbabwe's imposing new Chinese-funded parliament opens-Mutsaka", AP News, 23. novembar 2022. https://apnews.com/article/africa-china-asia-zimbabwe-d7176d0e7ed5997e50c89d226a34d2e9

675 Privacy International, "Huawei and Surveillance in Zimbabwe", 18. novembar 2021. https://privacyinternational.org/long-read/4692/huawei-and-surveillance-zimbabwe

676 MISA Zimbabwe, "Digest: Facial recognition technology and privacy rights", 29. maj 2018. https://zimbabwe.misa.org/2018/05/29/digest-facial-recognition-technology-privacy-rights/; takođe videti: Hawkins, "Beijing's Big Brother Tech Needs African Faces", Foreign Policy, 24. juli 2018. https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/

677 K. Muleya, "African dream of 'smart cities' remains strong", Warp News, 16. oktobar 2021. https://www.warpnews.org/human-progress/african-dream-of-smart-cities-remains-strong/

678 The Standard, "Creating a surveillance state: ED govt zooms in for critics with Chinese help", 1. mart 2020. https://thestandard.newsday.co.zw/2020/03/01/creating-surveillance-state-ed-govt-zooms-critics-chinese-help

679 Ibid; videti takođe: Privacy International, "Huawei and Surveillance in Zimbabwe", 18. novembar 2021. https://privacyinternational.org/long-read/4692/huawei-and-surveillance-zimbabwe

680 P. Masau, "Face of the Future", ChinAfrica, 13. avgust 2018. http://www.chinafrica.cn/Homepage/201808/t20180813_800138079.html

681 Privacy International, "Huawei and Surveillance in Zimbabwe", 18. novembar 2021. https://privacyinternational.org/long-read/4692/huawei-and-surveillance-zimbabwe; Africa Defense Forum, "Zimbabwe Turns to Chinese Technology to Expand Surveillance of Citizens", 17. januar 2023. https://adf-magazine.com/2023/01/zimbabwe-turns-to-chinese-technology-to-expand-surveillance-of-citizens/

682 Global Voices, "How Zimbabwe is building a Big Brother surveillance state", 10. januar 2023. https://globalvoices.org/2023/01/10/how-zimbabwe-is-building-a-big-brother-surveillance-state/

683 A. Macdonald, "Zimbabwe govt faces criticism over biometric surveillance project for new smart city", Biometric Update, 28. februar 2023. https://www.biometricupdate.com/202302/zimbabwe-govt-faces-criticism-over-biometric-surveillance-project-for-new-smart-city

684 S. Matiashe, "Zimbabwe's cyber city: Urban utopia or surveillance menace?", Context, 21. februar 2023. https://www.context.news/surveillance/zimbabwes-cyber-city-urban-utopia-or-surveillance-menace

685 DataGuidance, "Zimbabwe - Summary", https://www.dataguidance.com/jurisdiction/zimbabwe

686 MISA Zimbabwe, "Analysis of the Data Protection Act", 6. decembar 2021. https://zimbabwe.misa.org/2021/12/06/analysis-of-the-data-protection-act/

687 Ibid.

688 T. Kachiko, "Data Protection Bill criticised", NewsDay Zimbabwe, 17. decembar 2021. https://www.newsday.co.zw/2021/12/data-protection-bill-criticised; K. Chimhangwa, "Weaponising the law: Zimbabwe's new frontier in digital rights repression", Global Voices, 26. april 2022. https://globalvoices.org/2022/04/26/weaponising-the-law-zimbabwes-new-frontier-in-digital-rights-repression/

689 Cyber and Data Protection (Licensing of Data Controllers and Appointment of Data Protection Officers) Regulations, 2024. https://zimlii.org/akn/zw/act/si/2024/155/eng@2024-09-13

690 K. Chimhangwa, "Weaponising the law: Zimbabwe's new frontier in digital rights repression", Global Voices, 26. april 2022. https://globalvoices.org/2022/04/26/weaponising-the-law-zimbabwes-new-frontier-in-digital-rights-repression/

691 C. S. Mavhunga, D. McKenzie, "Social media access restored in Zimbabwe by court order", CNN, 23. januar 2019. https://edition.cnn.com/2019/01/21/africa/zimbabwe-protests-internet-shutdown-ruling-intl/index.html

692 Veritas, "Court Watch 1/2019 - The Internet Shutdown: The High Court's Ruling of 21st January", 30. januar 2019. https://www.veritaszim.net/node/3397

693 F. Mudzingwa, "[Breaking] High Court Declares That Internet Blockade Was Illegal And Social Media Access Must Be Restored", Techzim, 21. januar 2019. https://www.techzim.co.zw/2019/01/breaking-high-court-declares-that-internet-blockade-was-illegal/

694 Veritas, "Court Watch 1/2019 - The Internet Shutdown: The High Court's Ruling of 21st January", 30. januar 2019. https://www.veritaszim.net/node/3397

695 M. Dzirutwe, "Zimbabwe court says internet shutdown illegal as more civilians detained", Reuters, 21. januar 2019. https://www.reuters.com/article/us-zimbabwe-politics-idUSKCN1PF11M

696 P. Königs, "Government Surveillance, Privacy, and Legitimacy", Philosophy and Technology 35(8), 2022, https://doi.org/10.1007/s13347-022-00503-9

697 Council of Europe, "Thematic Factsheet: Mass Surveillance", juli 2018. https://rm.coe.int/factsheet-on-mass-surveillance-july2018-docx/16808c168e

698 Garante per la Protezione dei Dati Personali, "Facial recognition: the SARI Real Time system is not compliant with privacy laws", 16. april 2021. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575842#english

699 E. Jakubowska, "Remote biometric identification: a technical & legal guide", EDRi, 23. januar 2023. https://edri.org/our-work/remote-biometric-identification-a-technical-legal-guide/

700 European Parliament, "Report on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters", 17. juli 2021. https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.html

701 Council of the European Union, "Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - General approach", 25. novembar 2022. https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf

702 Future of Life Institute, "High-level summary of the AI Act", 27. februar 2024. https://artificialintelligenceact.eu/high-level-summary/

703 Hindustan Times, "'Only 2 percent accuracy' in Delhi police facial recognition software: High Court told", 23. avgust 2018. https://www.hindustantimes.com/cities/only-2-percent-accuracy-in-delhi-police-facial-recognition-software-high-court-told/story-D4d2oP3PAVn8OwyCqpA4FO.html

704 P. Fussey, A. Sandhu, "Surveillance arbitration in the era of digital policing", Theoretical Criminology 26(1), 3-22, 2022. https://doi.org/10.1177/1362480620967020

705 La Quadrature du Net, "La Reconnaissance Faciale Des Manifestant□es Est Déjà Autorisée", 18. novembar 2019. https://www.laquadrature.net/2019/11/18/la-reconnaissance-faciale-des-manifestants-est-deja-autorisee/

706 N. A. Smuha, "Beyond the Individual: Governing AI's Societal Harm", Internet Policy Review 10(3), 2021. https://doi.org/10.14763/2021.3.1574

707 Ibid. str. 5

708 K. Hao, "This is How We Lost Control of Our Faces", MIT Technology Review, 5. februar, 2021. https://www.technologyreview.com/2021/02/05/1017388/ai-deep-learning-facial-recognition-data-history/; P. Guest, "Singapore's Tech-Utopia Dream is Turning Into a Surveillance State Nightmare", Rest of World, 16. novembar 2021. https://restofworld.org/2021/singapores-tech-utopia-dream-is-turning-into-a-surveillance-state-nightmare/; V. Dodd, "UK police use of live facial recognition unlawful and unethical, report finds", The Guardian, 27. oktobar 2022. https://www.theguardian.com/technology/2022/oct/27/live-facial-recognition-police-study-uk; European Digital Rights (EDRi), "Ban biometric Mass Surveillance", 2020. https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf

709 H. Boghosian, "How Fear of Government Surveillance Influences Our Be- havior", Literary Hub, 15. juli 2021. https://lithub.com/how-fear-of-government-surveillance-influences-our-behavior/

710 A. Najibi, "Racial Discrimination in Face Recognition Technology", Harvard University, 24. oktobar 2020. https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/

711 S. Perkowitz, "The Bias in the Machine: Facial Recognition Technology and Racial Disparities", MIT Case Studies in Social and Ethical Responsibilities of Computing, zima 2021. (februar), https://doi.org/10.21428/2c646de5.62272586

712 European Digital Rights (EDRi), "Beyond Debiasing: Regulating AI and Its Inequalities", 2021. https://edri.org/wp-content/uploads/2021/09/EDRi_Beyond-Debiasing-Report_Online.pdf

713 Ibid. str. 10

714 H. Suresh, J. Guttag, "A Framework for Understanding Sources of Harm Throughout the Machine Learning Life Cycle", Equity and Access in Algorithms, Mechanisms, and Optimization (EAAMO '21), Association for Computing Machinery, 2021. https://doi.org/10.1145/3465416.3483305

715 V. Joler, M. Pasquinelli, "The Nooscope Manifested: AI as Instrument of Knowledge Extractivism", 2020. https://nooscope.ai/

716 D. Leslie, "Understanding the Bias in Facial Recognition Technology: An Explainer", The Alan Turing Institute, 2020. https://www.turing.ac.uk/sites/default/files/2020-10/understanding_bias_in_facial_recognition_technology.pdf

717 T. Bolukbasi et al., "Man is to Computer Programmer as Woman is to Homemaker? Debiasing Word Embeddings", NIPS'16: Proceedings of the 30th International Conference on Neural Information Processing Systems, 4356–4364, decembar 2016. https://dl.acm.org/doi/pdf/10.5555/3157382.3157584

718 M. Ngan, P. Grother, "Face Recognition Vendor Test (FRVT) - Performance of Automated Gender Classification Algorithms, NIST Interagency Report 8052", National Institute of Standards and Technology, april 2015. https://doi.org/10.6028/NIST.IR.8052

719 J. Buolamwini, T. Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", Conference on Fairness, Accountability and Transparency, Proceedings of Machine Learning Research 81:1–15, 2018. http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

720 J. Buolamwini et al., "Gender Shades", Algorithmic Justice League, 2018. http://gendershades.org/overview.html

721 J. Angwin et al., "Machine Bias", ProPublica, 23. maj 2016. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

722 A. Nellis, "The Color of Justice: Racial and Ethnic Disparity in State Prisons", The Sentencing Project, 13. oktobar 2021. https://www.sentencingproject.org/reports/the-color-of-justice-racial-and-ethnic-disparity-in-state-prisons-the-sentencing-project/

723 H. Suresh, J. Guttag, "A Framework for Understanding Sources of Harm Throughout the Machine Learning Life Cycle", str. 5

724 A. Sandhu, P. Fussey, "The 'uberization of policing'? How police negotiate and operationalise predictive policing technology", Policing and Society 31 (1), 66-81, 2021. https://doi.org/10.1080/10439463.2020.1803315, str. 76

725 H. Suresh, J. Guttag, "A Framework for Understanding Sources of Harm Throughout the Machine Learning Life Cycle", str. 5

726 T. Blevins et al., "Automatically Processing Tweets from Gang-Involved Youth: Towards Detecting Loss and Aggression", Proceedings of COLING 2016, the 26th International Conference on Computational Linguistics: Technical Papers, 2196–2206, decembar 2016. https://aclanthology.org/C16-1207.pdf

727 G. Mauro, H. Schellmann, "'There is no standard': investigation finds AI algorithms objectify women's bodies", The Guardian, 8. februar 2023. https://www.theguardian.com/technology/2023/feb/08/biased-ai-algorithms-racy-women-bodies

728 Ibid.

729 I. D. Raji et al., "Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing", AIES '20: Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society, 145–151, februar 2020. https://doi.org/10.1145/3375627.3375820

730 Pete Fussey, @PeteFussey, "1. This is a technical evaluation. Doesn't examine policing uses. While has merit, does not follow that the findings (a) can be generalised (b) legitimate entire FRT use or (c) even fully address issues of bias 2/15", Twitter, 5. april 2023. https://twitter.com/PeteFussey/status/1643721120971993090

731 L. Zedner, "Security", Routledge, 2009, str. 2

732 C. Whelan, "Surveillance, security and sporting mega events: Toward a research agenda on the organisation of security networks", Surveillance and Society 11(4): Surveillance and Sport, 392-404, 2014. http://dx.doi.org/10.24908/ss.v11i4.4722, str. 395

733 C. Reilly, "Facial-recognition software inaccurate in 98% of cases, report finds", CNET, 13. maj 2018. https://www.cnet.com/tech/tech-industry/facial-recognition-software-inaccurate-in-98-of-metropolitan-police-cases-reports/

734 G. Pisanu et al., "Surveillance Tech in Latin America: Made Abroad, Deployed at Home", Access Now, 9. avgust 2021. https://www.accessnow.org/surveillance-tech-in-latin-america-made-abroad-deployed-at-home/

735 E. Hinz, "How Myanmar's junta uses Chinese surveillance technology", Deutsche Welle, 28. juli 2022. https://www.dw.com/en/how-myanmars-junta-is-using-chinese-facial-recognition-technology/a-62624413

736 G. Benjamin, D. Sivaprakasam, W. P. Myint, "Track and target: FAQ on Myanmar CCTV cameras and facial recognition", Access Now, 4. avgust 2022. https://www.accessnow.org/myanmar-cctv-cameras/

737 Access Now, "Resist Myanmar's digital coup: stop the military consolidating digital control", 8. februar 2022. https://www.accessnow.org/press-release/myanmars-digital-coup-statement/

738 G. Benjamin, D. Sivaprakasam, W. P. Myint, "Track and target: FAQ on Myanmar CCTV cameras and facial recognition", Access Now, 4. avgust 2022. https://www.accessnow.org/myanmar-cctv-cameras/

739 Ibid.

740 M. Clark, "Leaked documents link Huawei to China's domestic spying in Xinjiang", The Verge, 15. decembar 2021. https://www.theverge.com/2021/12/14/22834860/huawei-leaked-documents-xinjiang-region-uyghur-facial-recognition-prisons-surveillance

741 G. Benjamin, D. Sivaprakasam, W. P. Myint, "Track and target: FAQ on Myanmar CCTV cameras and facial recognition", Access Now, 4. avgust 2022. https://www.accessnow.org/myanmar-cctv-cameras/

742 M. Maung, "Myanmar's Prisoner Release Still Leaves Thousands Detained", Human Rights Watch, 6. maj 2023. https://www.hrw.org/news/2023/05/06/myanmars-prisoner-release-still-leaves-thousands-detained

743 Asocijacija za pomoć političkim zatvorenicima u Burmi je organizacija za ljudska prava koja zagovara oslobađanje političkih zatvorenika u Burmi kao i unapređenje kvaliteta života tokom i nakon zatvorske kazne: Assistance Association for Political Prisoners Burma, "Home", https://aappb.org/

744 E. Hinz, "How Myanmar's junta uses Chinese surveillance technology", Deutsche Welle, 28. juli 2022. https://www.dw.com/en/how-myanmars-junta-is-using-chinese-facial-recognition-technology/a-62624413

745 Amnesty International, "Myanmar: Detainees tortured to crush opposition to coup", 2. avgust 2022. https://www.amnesty.org/en/latest/news/2022/08/myanmar-detainees-tortured-to-crush-opposition-to-coup/

746 Free Expression Myanmar, "Myanmar's new Electronic Transactions Law Amendment", 18. februar 2021. https://freeexpressionmyanmar.org/myanmars-new-electronic-transactions-law-amendment/

747 G. Benjamin, D. Sivaprakasam, W. P. Myint, "Myanmar IMEI FAQ: how the junta could disconnect the resistance", Access Now, 7. juli 2022. https://www.accessnow.org/myanmar-imei/

748 UN Human Rights Office, "The international community's response to the crisis in Myanmar is failing, and that failure has contributed to a lethal downward spiral that is devastating the lives of millions of people", Tom Andrews, Specijalni izvestilac UN o ljudskim pravima u Mjanmaru ("UN expert urges Japan to step up pressure on Myanmar junta", saopštenje za štampu, 28. april 2023); OHCHR, "UN expert urges Japan to step up pressure on Myanmar junta", 28. april 2023. https://www.ohchr.org/en/press-releases/2023/04/un-expert-urges-japan-step-pressure-myanmar-junta

749 Klasifikacija političkih sistema Wolfganga Merkela: demokratije (ugrađene i defektne) i autokratije (autoritarizam and totalitarizam); W. Merkel, "Embedded and defective democracies", Democratisation 11:5, 33-58, 2004.

750 S. A. Cole, "Imprint of the Raj: How Fingerprinting was Born in Colonial India (review)", Technology and Culture 46(1), 252-253, 2005. Project MUSE, https://doi.org/10.1353/tech.2005.0010

751 B. W. Goossen, "Measuring Mennonitism: Racial Categorization in Nazi Germany and Beyond", Journal of Mennonite Studies, Vol. 34, 2016. https://jms.uwinnipeg.ca/index.php/jms/article/view/1651

752 Y. Gorokhovskaia, A. Shahbaz, A. Slipowitz, "Marking 50 Years in the Struggle for Democracy", Freedom House, mart 2023. https://freedomhouse.org/report/freedom-world/2023/marking-50-years

753 Human Rights Watch, "Myanmar: No Justice, No Freedom for Rohingya 5 Years On", 24. avgust 2022. https://www.hrw.org/news/2022/08/24/myanmar-no-justice-no-freedom-rohingya-5-years

754 Ministarstvo unutrašnjih poslova Republike Srbije, "Procena uticaja obrade na zaštitu podataka o ličnosti korišćenjem sistema video nadzora", septembar

2019. https://www.sharefoundation.info/wp-content/uploads/MUP-Procena-uticaja-obrade-na-zastitu-podataka-o-licnosti-koriscenjem-sistema-video-nadzora.pdf

755 Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti Republike Srbije, "Mišljenje Poverenika na akt Ministarstva unutrašnjih poslova – Procena uticaja obrade na zaštitu podataka o ličnosti korišćenjem sistema video nadzora", novembar 2019. https://praksa.poverenik.rs/predmet/detalji/FB967E2A-AE57-4B2C-8F11-D2739FD85A9B

756 SHARE Conference, @SHAREConference, "Postavljanje Huawei kamera na Trgu Republike", Twitter, 12. jun 2019. https://twitter.com/ShareConference/status/1138774544632680449

757 hiljadekamera Twitter nalog, @hiljadekamera, https://twitter.com/hiljadekamera

758 U službenim dokumentima, Huawei i Ministarstvo unutrašnjih poslova podjednako koriste izraze "Siguran grad" i "Sigurno društvo".

759 D. Krivokapić, M. Bajić, B. Perkov, "Biometrics in Belgrade: Serbia's Path Shows Broader Dangers of Surveillance State", Heinrich Boell Stiftung, 19. maj 2021. https://eu.boell.org/en/2021/05/19/biometrics-belgrade-serbias-path-shows-broader-dangers-surveillance-state

760 Huawei, "Huawei Safe City Solution: Safeguards Serbia", 23. avgust 2018. dostupno na: https://archive.li/pZ9HO

761 Ministarstvo unutrašnjih poslova Republike Srbije, "Procena uticaja obrade na zaštitu podataka o ličnosti upotrebom savremenih tehnologija video nadzora u okviru projekta 'Sigurno društvo' u Beogradu", mart 2020. https://www.sharefoundation.info/wp-content/uploads/Procena_uticaja_2_0.pdf

762 SHARE Fondacija, "Protiv legalizacije masovnog biometrijskog nadzora", 21. septembar 2021. https://www.sharefoundation.info/sr/protiv-legalizacije-masovnog-biometrijskog-nadzora/

763 SHARE Fondacija, "Komentari na Nacrt zakona o unutrašnjim poslovima", septembar 2021. https://www.sharefoundation.info/wp-content/uploads/Komentari-na-Nacrt-zakona-o-unutrasnjim-poslovima-SHARE-Fondacija.pdf

764 SHARE Fondacija, "Povlačenje nacrta korak ka moratorijumu na biometrijski nadzor", 23. septembar 2021. https://www.sharefoundation.info/sr/povlacenje-nacrta-korak-ka-moratorijumu-na-biometrijski-nadzor/

765 Ministarstvo unutrašnjih poslova Republike Srbije, Nacrt zakona o unutrašnjim poslovima, decembar 2022. http://www.mup.gov.rs/wps/wcm/connect/4ceb4620-bcb6-4370-b55a-8f9dbb6f558d/НАЦРТ+ЗАКОНА+О+УНУТРАШЊИМ+ПОСЛОВИМА.pdf?MOD=AJPERES&CVID=ojJiNDS

766 Ministarstvo unutrašnjih poslova Republike Srbije, Nacrt zakona o obradi podataka i evidencijama u oblasti unutrašnjih poslova, decembar 2022. https://shorturl.at/KLn2u

767 Ministarstvo unutrašnjih poslova Republike Srbije, Procena uticaja radnji obrade podataka o ličnosti upotrebom softvera za obradu biometrijskih podataka u sistemu video nadzora Ministarstva unutrašnjih poslova na zaštitu podataka o ličnosti, novembar 2022. https://www.sharefoundation.info/wp-content/uploads/Procena-uticaja-novembar-2022.pdf

768 SHARE Fondacija, "Šta predviđaju novi predlozi policijskih propisa", 16. decembar 2022. https://www.sharefoundation.info/sr/novi-predlozi-policijskih-propisa/

769 Vlada Republike Srbije, "Povlači se Nacrt zakona o unutrašnjim poslovima iz procedure usvajanja", 26. decembar 2022. https://www.srbija.gov.rs/vest/674074/povlaci-se-nacrt-zakona-o-unutrasnjim-poslovima-iz-procedure-usvajanja.php

770 SHARE Fondacija, "Druga runda bitke protiv masovnog biometrijskog nadzora", 9. januar 2023. https://www.sharefoundation.info/sr/druga-runda-bitke-protiv-masovnog-biometrijskog-nadzora/

771 Reclaim Your Face, "The problem", https://reclaimyourface.eu/the-problem/

772 A. Tešić i F. Mirilović, "Mapirana oprema za prepoznavanje lica širom Srbije: Pod nadzorom i škole, vrtići i pijace", BIRN, 23. februar 2024. https://birn.rs/oprema-za-prepoznavanje-lica-u-skolama-i-vrticima/

773 N. Jovanović, "'Mali brat i velike sestre': Stanovnici više od 40 gradova i opština u Srbiji na oku kamera iz Kine", Radio Slobodna Evropa, 17. juli 2023. https://www.slobodnaevropa.org/a/video-nadzor-kineske-kamere-srbija/32507504.html

774 K. Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match", The New York Times, 29. decembar 2020. https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html

775 G. Ridgeway, "Analysis of Racial Disparities in the New York Police Department's Stop, Question, and Frisk Practices", RAND Corporation, 2007. https://www.rand.org/pubs/technical_reports/TR534.html

776 Office of the New York State Comptroller, Division of State Government Accountability, "Artificial Intelligence Governance: Report 2021-N-10", februar 2023. https://www.osc.state.ny.us/files/state-agencies/audits/pdf/sga-2023-21n10.pdf

777 Office of the New York State Comptroller, Division of State Government Accountability, "Artificial Intelligence Governance", 16. februar 2023. https://www.osc.state.ny.us/state-agencies/audits/2023/02/16/artificial-intelligence-governance

778 R. Abraham, "AI Use by Cops, Child Services In NYC Is a Mess: Report says", Vice, 22. februar 2023. https://www.vice.com/en/article/3adxak/nypd-child-services-ai-facial-recognition

779 Office of the New York State Comptroller, Division of State Government Accountability, "Artificial Intelligence Governance: Report 2021-N-10", februar 2023. https://www.osc.state.ny.us/files/state-agencies/audits/pdf/sga-2023-21n10.pdf

780 E. Manis et al., "Scan city - A Decade of NYPD Facial Recognition Abuse", Surveillance Technology Oversight Project (STOP), 8. juli 2021. https://static1.squarespace.com/static/5c1bfc7eee175995a4ceb638/t/60e5dd3bed032877ec8e3be9/1625677116317/2021.7.7_Scan+City_FINAL.pdf

781 Amnesty International, "Inside NYPD's Surveillance Machine", https://banthescan.amnesty.org/decode/

782 The New York Police Department, "Body-Worn Cameras - What you need to know", https://www.nyc.gov/site/nypd/about/about-nypd/equipment-tech/body-worn-cameras.page

783 The New York Police Department, "NYPD Questions and Answers - Facial Recognition", https://www.nyc.gov/site/nypd/about/about-nypd/equipment-tech/facial-recognition.page

784 Ibid.

785 Surveillance Technology Oversight Project (STOP), "NYPD Facial Recognition Lawsuit", https://www.stopspying.org/nypd-facial-rec

786 C. Haskins, "The NYPD Has Misled The Public About Its Use Of Facial Recognition Tool Clearview AI", BuzzFeed, 6. april 2021. https://www.buzzfeednews.com/article/carolinehaskins1/nypd-has-misled-public-about-clearview-ai-use

787 R. Mac et al., "Surveillance Nation", BuzzFeed, 6. april 2021. https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition

788 A. Perala, "Judge Orders NYPD to Release Biometric Surveillance Docs", FindBiometrics, 2. avgust 2022. https://findbiometrics.com/judge-orders-nypd-to-release-biometric-surveillance-docs-508021/

789 S. Fussel, "The NYPD Had a Secret Fund for Surveillance Tools", Wired, 10. avgust 2021. https://www.wired.com/story/nypd-secret-fund-surveillance-tools/

790 Ibid.

791 J. Goldstein, A. Watkins, "She Was Arrested at 14. Then Her Photo Went to a Facial Recognition Database", The New York Times, 1. avgust 2019. https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html

792 New York Civil Liberties Union (NYCLU), "Stop and Frisk Data", https://www.nyclu.org/en/stop-and-frisk-data

793 New York Civil Liberties Union (NYCLU), "Stop and Frisk in the de Blasio era", 14. mart 2019. https://www.nyclu.org/en/publications/stop-and-frisk-de-blasio-era-2019

794 MIT Media Lab, Gender Shades, "Results", https://www.media.mit.edu/projects/gender-shades/results/

795 Amnesty International, "USA: Facial recognition technology reinforcing racist stop-and-frisk policing in New York – new research", 15. februar 2022. https://www.amnesty.org/en/latest/news/2022/02/usa-facial-recognition-technology-reinforcing-racist-stop-and-frisk-policing-in-new-york-new-research/

796 Ibid.

797 S. Goldenberg, J. Anuta, "Adams eyes expansion of highly controversial police surveillance technology", Politico, 8. februar 2022. https://www.politico.com/news/2022/02/08/adams-police-surveillance-technology-00006230

798 C. Garvie, "Garbage in, Garbage out: Face Recognition on Flawed Data", Georgetown Law Center on Privacy and Technology, 16. maj 2019. https://www.flawedfacedata.com/

799 Surveillance Technology Oversight Project (S.T.O.P.) je neprofitna zagovaračka organizacija koja pruža pravne usluge i radi na ukidanju sistema masovnog nadzorna u lokalnim upravama.

800 T. Ryan-Mosley, "A new map of NYC's cameras shows more surveillance in Black and brown neighborhoods", MIT Technology Review, 14. februar 2022. https://www.technologyreview.com/2022/02/14/1045333/map-nyc-cameras-surveillance-bias-facial-recognition/

801 G. Joseph, J. Offenhartz, "NYPD Used Facial Recognition Technology In Siege Of Black Lives Matter Activist's Apartment", Gothamist, 14. avgust 2020. https://gothamist.com/news/nypd-used-facial-recognition-unit-in-siege-of-black-lives-matter-activists-apartment

802 J. Offenhartz et al., "The NYPD Banged On A Black Lives Matter Organizer's Door, Shut Down His Street, Stayed For 5 Hours, Then Left", Gothamist, 7. avgust 2020. https://gothamist.com/news/nypd-banged-black-lives-matter-organizers-door-shut-down-his-street-stayed-5-hours-then-left

803 J. Offenhartz, "Black Activist Targeted In Military-Style NYPD Siege Files Federal Lawsuit", Gothamist, 4. novembar 2021. https://gothamist.com/news/black-activist-targeted-military-style-nypd-siege-files-federal-lawsuit

804 S. Fussel, "The NYPD Had a Secret Fund for Surveillance Tools", Wired, 10. avgust 2021. https://www.wired.com/story/nypd-secret-fund-surveillance-tools/

805 The Local, "UPDATE: EU postpones launch of EES border entry system once again", 19. januar 2023. https://www.thelocal.no/20230119/update-eu-postpones-launch-of-ees-border-entry-system-once-again

806 F. Giandana Gigena, "Cross-border Surveillance Poses a Silent Threat to Migrants", El Faro, 24. april 2023. https://elfaro.net/en/202304/opinion/26819/Cross-border-Surveillance-Poses-a-Silent-Threat-to-Migrants.htm

807 J. Askew, "'Mass surveillance, automated suspicion, extreme power': How tech is shaping EU borders", Euronews, 6. april 2023. https://www.euronews.com/next/2023/04/06/mass-surveillance-automated-suspicion-extreme-power-how-tech-is-shaping-the-eus-borders

808 P. Williams, E. Kind, "Data Driven Profiling", European Network Against Rac- ism (ENAR), novembar 2019. https://www.statewatch.org/media/documents/news/2019/nov/data-driven-profiling-web-final.pdf

809 D. Bigo, "Globalized (in)security: The field and the ban-opticon", in D. Bigo and A. Tsoukala (eds.), Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11, Routledge, 2008. str. 10-48

810 D. Bigo, "Security, exception, ban and surveillance", in D. Lyon (ed.), Theorizing Surveillance, Routledge, 2006. str. 46-68

811 M. Higgins, "How the $68 Billion Border Surveillance Industrial Complex Affects Us All", Vice, 11. jun 2021. https://www.vice.com/en/article/k7873m/how-the-dollar68-billion-border-surveillance-industrial-complex-affects-us-all

812 J. Askew, "'Mass surveillance, automated suspicion, extreme power': How tech is shaping EU borders", Euronews, 6. april 2023. https://www.euronews.com/next/2023/04/06/mass-surveillance-automated-suspicion-extreme-power-how-tech-is-shaping-the-eus-borders

813 11.11.11., "Over 200,000 illegal pushbacks at EU's external borders in 2022", 22. mart 2023. https://pers.11.be/translation-over-200000-illegal-push-backs-at-eus-external-borders-in-2022

814 A. Fotiadis, I. Papangeli, S. Malichudis, "Asylum Surveillance Systems Launched in Greece without Data Safeguards", BIRN, 9. septembar 2022. https://balkaninsight.com/2022/09/09/asylum-surveillance-systems-launched-in-greece-without-data-safeguards/

815 Homo Digitalis, "A major success for civil society in Greece: The Hellenic DPA launches an investigation into the Ministry of Immigration and Asylum re the YPERION and KENTAYROS IT systems", 9. mart 2022. https://www.homodigitalis.gr/en/posts/11024

816 Homo Digitalis, "The Hellenic Coast Guard wants to acquire social media monitoring software: The Hellenic DPA is urged to exercise its investigative and supervisory powers", 15. februar 2022. https://www.homodigitalis.gr/en/posts/10848

817 Hungarian Helsinki Committee, "Hungary: Access to the territory and push backs", Asylum Migration Database (AIDA), 19. april 2023. https://asylumineurope.org/reports/country/hungary/asylum-procedure/access-procedure-and-registration/access-territory-and-push-backs/

818 Human Rights Watch, "Croatia: Ongoing, Violent Border Pushbacks", 3. maj 2023. https://www.hrw.org/news/2023/05/03/croatia-ongoing-violent-border-pushbacks

819 Refugees International, "Letter: The EU AI Act must protect people on the move", 6. decembar 2022. https://www.refugeesinternational.org/reports/2022/12/5/letter-the-eu-ai-act-must-protect-people-on-the-move

820 Border Violence Monitoring Network, "AI Act: European Parliament Endorses Protections Against AI in Migration", 11. maj 2023. https://borderviolence.eu/app/uploads/PR-AI-ACT-PICUM-and-BVMN-v2.pdf

821 PICUM, "A dangerous precedent: how the EU AI Act fails migrants and people on the move", 4. april 2024. https://picum.org/blog/a-dangerous-precedent-how-the-eu-ai-act-fails-migrants-and-people-on-the-move/

822 N. Ionta, "Greece systematically pushing back migrants, rules ECtHR", 07. januar 2025. https://www.euractiv.com/section/politics/news/greece-systematically-pushing-back-migrants-rules-echr/

823 Amnesty International, "Greece: Pushbacks and violence against refugees and migrants are de facto border policy", 23. jun 2021. https://www.amnesty.org/en/latest/press-release/2021/06/greece-pushbacks-and-violence-against-refugees-and-migrants-are-de-facto-border-policy/

824 K. Weitzberg, "Biometrics and counter-terrorism: Case study of Israel/Palestine", Privacy International, maj 2021. https://privacyinternational.org/sites/default/files/2021-06/PI%20Counterterrorism%20and%20Biometrics%20Report%20Israel_Palestine%20v7.pdf

825 M. Cohn, "Israel Is Using a Vast Network of Biometric Cameras to Terrorize Palestinians", Thuthout, 5. maj 2023. https://truthout.org/articles/israel-is-using-a-vast-network-of-biometric-cameras-to-terrorize-palestinians/

826 Amnesty International, "Automated Apartheid: How Facial Recognition Fragments, Segregates and Controls Palestinians In The OPT", 2. maj 2023. https://www.amnesty.org/en/documents/mde15/6701/2023/en/

827 Amnesty International, "Israel/OPT: Israeli authorities are using facial recognition technology to entrench apartheid", 2. maj 2023. https://www.amnesty.org/en/latest/news/2023/05/israel-opt-israeli-authorities-are-using-facial-recognition-technology-to-entrench-apartheid/

828 A. Ziv, "This Israeli Face-recognition Startup Is Secretly Tracking Palestinians", Haaertz, 15. juli 2019. https://www.haaretz.com/israel-news/business/2019-07-15/ty-article/.premium/this-israeli-face-recognition-startup-is-secretly-tracking-palestinians/0000017f-f47b-ddde-abff-fc7fe25c0000

829 A. Ziv, "Israel uses new surveillance technology to distance itself from the occupation. It's not working", Forward, 30. novembar 2021. https://forward.com/opinion/478846/israel-new-surveillance-technology-occupation-palestinians/

830 Amnesty International, "Automated Apartheid: How Facial Recognition Fragments, Segregates and Controls Palestinians In The OPT", 2. maj 2023. https://www.amnesty.org/en/documents/mde15/6701/2023/en/

831 Y. Abraham, "'Lavender': The AI machine directing Israel's bombing spree in Gaza", +972 Magazine, 3. april 2024. https://www.972mag.com/lavender-ai-israeli-army-gaza/

832 Princip nevraćanja (non-refoulement) zabranjuje državama u koje dolaze tražioci azila da uklanjaju te osobe iz svoje jurisdikcije ili zone delotvorne kontrole kada postoji osnovana sumnja da će biti u riziku nepopravljive štete po povratku.

833 A. Erfani, M. Garcia, "Pushing Back Protection – How Offshoring and Externalization Imperil the Right to Asylum", National Immigrant Justice Centre, FWD.us, 3. avgust 2021. https://immigrantjustice.org/research-items/off-shoring-asylum

834 Ibid.

835 Ibid.

836 Statement of Cooperation between the Secretariat of Governance of the United Mexican States, National Migration Institute and the Department of Homeland Security for the United States of America concerning Biometric Immigration Information Sharing, 18. januar 2017. https://r3d.mx/wp-content/uploads/SOC-2017.pdf

837 United States Department of Homeland Security, "Fact sheet: DHS Agreements with Guatemala, Honduras and El Salvador", https://www.dhs.gov/sites/default/files/publications/19_1028_opa_factsheet-northern-central-america-agreements_v2.pdf

838 United States Department of Homeland Security, "DHS/ALL/PIA-095 International Biometric Information Sharing Program (IBIS)", novembar 2022. https://www.dhs.gov/publication/dhsallpia-095-international-biometric-information-sharing-program-ibis

839 Access Now, "Joint statement: Mexico, Guatemala, Honduras, El Salvador and the United States must terminate their agreements on cross-border transfers of migrants' biometric data", 23. mart 2023. https://www.accessnow.org/press-release/statement-terminate-agreements-biometric-data-migrants/

840 Ibid.

841 Ibid.

842 J. Franzblau, "Caught in the Web – The Role of Transnational Data Sharing in the

U.S. Immigration System", National Immigrant Justice Center, decembar 2002. https://immigrantjustice.org/sites/default/files/content-type/research-item/documents/2022-12/NIJC_Policy_Brief_Foreign_data_sharing_December-2022.pdf

843 Ibid.

844 To je jedini prekid na 30.000 km dugom pan-američkom autoputu, koji se proteže od Aljaske do Argentine.

845 D. Wolfe, "The Darién Gap: migrant route of last resort", World Vision, 8. avgust 2023. https://www.worldvision.ca/stories/child-protection/darien-gap-migrant-route

846 Izjava Jeana Gougha, direktora UNICEF-a za Latinsku Ameriku i Karibe, prema: D. Wolfe, "The Darién Gap: migrant route of last resort", World Vision, 8. avgust 2023. https://www.worldvision.ca/stories/child-protection/darien-gap-migrant-route

847 J. Shute, S. Townsley, "The 'road of death': A treacherous, jungle trafficking route lined with rotting corpses", The Telegraph, 17. oktobar 2022. https://www.telegraph.co.uk/global-health/climate-and-people/darien-gap-migration/

848 E. Guo, "The US wants to use facial recognition to identify migrant children as they age", MIT Technology Review, 14. avgust 2024, https://www.technologyreview.com/2024/08/14/1096534/homeland-security-facial-recognition-immigration-border/

849 Office of the United Nations High Commissioner for Human Rights, "Guiding Principles on Business and Human Rights", 2011. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

850 J. Davidson, "Calls for privacy law reform after Bunnings facial recognition scandal", Financial Review, 20. jun 2022. https://www.afr.com/technology/calls-for-privacy-law-reform-after-bunnings-facial-recognition-scandal-20220617-p5aume

851 J. Blakkarly, "Kmart, Bunnings and The Good Guys using facial recognition technology in stores", CHOICE, 12. juli 2022. https://www.choice.com.au/consumers-and-data/data-collection-and-use/how-your-data-is-used/articles/kmart-bunnings-and-the-good-guys-using-facial-recognition-technology-in-store

852 A. Pereira, "Complaint to OAIC on use of facial recognition in retail stores", CHOICE, jun 2022. https://www.choice.com.au/consumer-advocacy/policy/policy-submissions/2022/june/complaint-oaic-on-use-of-facial-recognition

853 J. Taylor, "Bunnings and Kmart halt use of facial recognition technology in stores as privacy watchdog investigates", The Guardian, 25. juli 2022. https://www.theguardian.com/technology/2022/jul/25/bunnings-and-kmart-halt-use-of-facial-recognition-in-stores-as-australian-privacy-watchdog-investigates

854 J. Nadel, "Bunnings and Kmart facial recognition probe set to finish by July", IT News, 14. februar 2023. https://www.itnews.com.au/news/bunnings-and-kmart-facial-recognition-probe-set-to-finish-by-july-590881

855 J. Taylor, "Bunnings breached privacy of customers by using facial recognition, watchdog finds", The Guardian, 19. novembar 2024. https://www.theguardian.com/australia-news/2024/nov/19/bunnings-facial-recognition-technology-breach-stores-ntwnfb

856 A. Barbaschow, "The Good Guys Says It's No Longer Trialling Facial Recognition Tech", Gizmodo, 1. juli 2022. https://www.gizmodo.com.au/2022/07/the-good-guys-facial-recognition/

857 R. Crozier, "7-Eleven disables facial image capture on customer feedback tablets", IT News, 14. oktobar 2021. https://www.itnews.com.au/news/7-eleven-disables-facial-image-capture-on-customer-feedback-tablets-571272

858 J. Dastin, "Amazon extends moratorium on police use of facial recognition software", Reuters, 18. maj 2021. https://www.reuters.com/technology/exclusive-amazon-extends-moratorium-police-use-facial-recognition-software-2021-05-18/

859 J. Nash, "New Amazon biometric-scan cases in media-saturated NYC could add to tech opposition", Biometric Update, 20. mart 2023. https://www.biometricupdate.com/202303/new-amazon-biometric-scan-cases-in-media-saturated-nyc-could-add-to-tech-opposition

860 C. Douglas Moran, S. Silverstein, "As self-checkout expands in grocery, here are 4 ways the technology is leveling up", Grocery Dive, 14. mart 2022. https://www.grocerydive.com/news/as-self-checkout-expands-in-grocery-here-are-4-ways-the-technology-is-leve/620122/

861 S. Mitchell, "Retailers' blind spot over facial recognition technology", The Australian Financial Review, 29. septembar 2022. https://www.afr.com/companies/retail/retailers-blind-spot-over-facial-recognition-technology-20220927-p5blc8

862 K. Hill, "How Target Figured Out A Teen Girl Was Preagnant Before Her Father Did", Forbes, 16. februar 2012. https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did

863 R. Raj, "Let's Get (Not Too) Personal; When Hyper-personalization Turns From Cool To Creepy", Analytics India Mag, 9. decembar 2019. https://analyticsindiamag.com/lets-get-not-too-personal-when-hyper-personalization-turns-from-cool-to-creepy/

864 S. Clark, "When Hyper-Personalization Becomes Hyper-Creepy", CMSWire, 7. decembar 2021. https://www.cmswire.com/customer-experience/when-hyper-personalization-becomes-hyper-creepy/

865 T. Claburn, "Apple Sued in Nightmare Case Involving Teen Wrongly Accused of Shoplifting, Driver's Permit Used By Impostor, and Unreliable Facial-Rec Tech", The Register, 29. maj 2021. https://www.theregister.com/2021/05/29/apple_sis_lawsuit/

866 United States District Court of Massachusetts, "Bah v. Apple Inc. and Security Industry Specialists, Inc.", 1:21-cv-10897-RGS, 2021. https://regmedia.co.uk/2021/05/29/pacer_bah_apple.pdf

867 J. Grierson, "Facial recognition cameras in UK retail chain challenged by privacy group", The Guardian, 26. juli 2022. https://www.theguardian.com/world/2022/jul/26/facial-recognition-cameras-in-uk-retail-chain-challenged-by-privacy-group

868 Vision Labs, "Luna Platform", https://visionlabs.ai/solutions/luna-platform/

869 Fight for the Future, "Ban Facial Recognition In Stores", https://www.banfacialrecognition.com/stores/#scorecard

870 C. Burt, “Facial recognition deployed in convenience stores in Mexico, England, Singapore”, Biometric Update, 14. decembar 2020. https://www.biometricupdate.com/202012/facial-recognition-deployed-in-convenience-stores-in-mexico-england-singapore

871 Asian Banking and Finance, “Thailand embraces facial recognition tech for e-KYC”, 10. maj 2019. https://asianbankingandfinance.net/retail-banking/news/thailand-embraces-facial-recognition-tech-e-kyc

872 NDID, “Services”, https://www.ndid.co.th/service/

873 F. Hersey, “Thailand’s NDID partners with Mastercard to connect digital IDs internationally”, Biometric Update, 10. mart 2022. https://www.biometricupdate.com/202203/thailands-ndid-partners-with-mastercard-to-connect-digital-ids-internationally

874 Bangkok Post, “Thailand’s digital GDP skyrockets to B2tn in 2021”, 3. novembar 2022. https://www.bangkokpost.com/tech/2428640/thailands-digital-gdp-skyrockets-to-b2tn-in-2021

875 ЦБТ, “Единая биометрическая система”, https://bio.rt.ru/about/

876 M. N. Zakirov, “Application of biometric face identification technologies in financial institutions”, Biometric Update, 5. februar 2023. https://www.biometricupdate.com/202302/application-of-biometric-face-identification-technologies-in-financial-institutions

877 A. Mascellino, “Russia pushing Unified Biometric System to enter secure facilities”, Biometric Update, 8. avgust 2022. https://www.biometricupdate.com/202208/russia-pushing-unified-biometric-system-to-enter-secure-facilities

878 A. Macdonald, “Russian pols OK bill to make banks share client biometrics with government”, Biometric Update, 7. juli 2022. https://www.biometricupdate.com/202207/russian-pols-ok-bill-to-make-banks-share-client-biometrics-with-government

879 J. Nash, “Russia offers carrots to consolidate biometrics systems under government control”, Biometric Update, 20. januar 2022. https://www.biometricupdate.com/202201/russia-offers-carrots-to-consolidate-biometrics-systems-under-government-control

880 L. Matsakis, “Scraping the Web Is a Powerful Tool. Clearview AI Abused It”, Wired, 25. januar 2020. https://www.wired.com/story/clearview-ai-scraping-web/

881 NOYB, “€20 Mio fine for Clearview AI in Italy”, 10. mart 2022. https://noyb.eu/en/eu-20-mio-fine-clearview-ai-italy

882 NOYB, “Second €20 Mio fine for Clearview AI”, 13. juli 2022. https://noyb.eu/en/second-eu-20-mio-fine-clearview-ai

883 CNIL, “Facial recognition: 20 million euros penalty against Clearview AI”, 20. oktobar 2022. https://www.cnil.fr/en/facial-recognition-20-million-euros-penalty-against-clearview-ai

884 Privacy International, “Get out our faces, Clearview AI”, https://privacyinternational.org/campaigns/get-out-our-face-clearview

885 CNIL, “Facial recognition: the CNIL imposes a penalty payment to Clearview AI”, 10. maj 2023. https://web.archive.org/web/20230614161044/https://www.cnil.fr/en/facial-recognition-cnil-imposes-penalty-payment-clearview-ai

886 NOYB, “Clearview AI data use deemed illegal in Austria, however no fine issued”, 10. maj 2023. https://noyb.eu/en/clearview-ai-data-use-deemed-illegal-austria-however-no-fine-issued

887 A. Robertson, “Clearview AI agrees to permanent ban on selling facial recognition to private companies”, The Verge, 9. maj 2022. https://www.theverge.com/2022/5/9/23063952/clearview-ai-aclu-settlement-illinois-bipa-injunction-private-companies

888 J. Axelrod, “Government Relies on Industry for Facial Recognition Technology”, Bloomberg Law, 19. jul 2022. https://news.bloomberglaw.com/privacy-and-data-security/government-relies-on-industry-for-facial-recognition-technology

889 C. Burt, “Clearview facial recognition searches double, database reaches 50B images”, Biometric update, 26. juni 2024. https://www.biometricupdate.com/202406/clearview-facial-recognition-searches-double-database-reaches-50b-images

890 D. Temple-Raston, S. Powers, “At war with facial recognition: Clearview AI in Ukraine”, The Record, 17. maj 2022. https://therecord.media/at-war-with-facial-recognition-clearview-ai-in-ukraine

891 K. Zidan, “The Qatar World Cup Ushers in a New Era of Digital Authoritarianism in Sports”, The Nation, 8. decembar 2022. https://www.thenation.com/article/society/qatar-world-cup-surveillance/

892 L. Foroudi, “France looks to AI-powered surveillance to secure Olympics”, Reuters, 23. mart 2023. https://www.reuters.com/technology/france-looks-ai-powered-surveillance-secure-olympics-2023-03-23/

893 A. Holland Michel, “Stadiums Have Gotten Downright Dystopian”, The Atlantic, 27. februar 2023. https://www.theatlantic.com/technology/archive/2023/02/sports-stadiums-security-facial-recognition-surveillance-technology/673215/

894 France 24, “Qatar’s ground control on alert for World Cup disasters”, 12. avgust 2022. https://www.france24.com/en/live-news/20220812-qatar-s-ground-control-on-alert-for-world-cup-disasters

895 C. J. Bennett, K. Haggerty (eds.), Security Games: Surveillance and Control at Mega-Events, Routledge, 2011, str. 5.

896 M. Wesfreid, “Paris 2024 : pas de reconnaissance faciale aux JO”, Le Parisien, 23. novembar 2022. https://www.leparisien.fr/politique/paris-2024-pas-de-reconnaissance-faciale-aux-jo-23-11-2022-4E3FP2XBWZC4LBY3B4UMPA3QPE.php

897 N. Lomas, “French parliament votes for biometric surveillance at Paris Olympics”, TechCrunch, 24. mart 2023. https://techcrunch.com/2023/03/24/paris-olympics-biometrics-surveillance/

898 MEP Patrick Breyer, “Vote to stop a future of biometric mass surveillance in Europe!”, Patrick-Breyer.de, 17. mart 2023. https://www.patrick-breyer.de/wp-content/uploads/2023/03/MEP-letter-to-FR-MPs-about-biometric-mass-surveillance-in-2024-Olympic-law.pdf

899 La Quadrature du Net, “France Becomes The First European Country To Legalize

Biometric Surveillance", 29. mart 2023. https://www.laquadrature.net/en/2023/03/29/france-becomes-the-first-european-country-to-legalize-biometric-surveillance/

900 A. Lodie, S. Celis Juarez, "Ai-Assisted Security At The Paris 2024 Olympic Games: From Facial Recognition To Smart Video", AI Regulation, 27. januar 2023. https://ai-regulation.com/ai-driven-systems-paris-olympics/

901 C. Whelan, "Surveillance, security and sporting mega events: Toward a research agenda on the organisation of security networks", Surveillance and Society 11(4): Surveillance and Sport, 392-404, 2014. http://dx.doi.org/10.24908/ss.v11i4.4722, str. 393.

902 M. Viegas Ferrari, "Test, swarm, normalize: how surveillance technologies have infiltrated Paris 2024 Olympic Games", Cadernos Metrópole 25(56), 75- 96, 2023. http://dx.doi.org/10.1590/2236-9996.2023-5603, str. 83.

903 La Quadrature du Net, "General Mobilisation Against The Legalisation Of Algorithmic Video Surveillance!", 16. februar 2023. https://www.laquadrature.net/en/2023/02/16/general-mobilisation-against-the-legalisation-of-automatic-video-surveillance/

904 M. Borak, "French top court OKs AI surveillance at Olympics but no biometrics", Biometric Update, 19. maj 2023. https://www.biometricupdate.com/202305/french-top-court-oks-ai-surveillance-at-olympics-but-no-biometrics

905 A. Carpentier, "How algorithmic video surveillance was used during the Paris Olympics", Le Monde, 16. avgust 2024, https://www.lemonde.fr/en/france/article/2024/08/16/how-algorithmic-video-surveillance-was-used-during-the-paris-olympics_6716745_7.html

906 P. Caddle, "Paris Olympics' AI mass-surveillance system 'to be made permanent', media reports", Brussels Signal, 2. oktobar 2024. https://brusselssignal.eu/2024/10/paris-olympics-ai-mass-surveillance-system-to-be-made-permanent-media-reports/

907 Privacy International, "King's Cross has been watching you - and the police helped", 25. jun 2020. https://privacyinternational.org/case-study/3973/kings-cross-has-been-watching-you-and-police-helped

908 Liberty, "Legal Challenge: Ed Bridges V South Wales Police", https://www.libertyhumanrights.org.uk/issue/legal-challenge-ed-bridges-v-south-wales-police/

909 L. Dearden, "Police stop people for covering their faces from facial recognition camera then fine man £90 after he protested", The Independent, 31. januar 2019. https://www.independent.co.uk/news/uk/crime/facial-recognition-cameras-technology-london-trial-met-police-face-cover-man-fined-a8756936.html

910 Big Brother Watch, "Face off: The lawless growth of facial recognition in UK policing", maj 2018. https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/report/

911 V. Dodd, "Met police found to be institutionally racist, misogynistic and homophobic", The Guardian, 21. mart 2023. https://www.theguardian.com/uk-news/2023/mar/21/metropolitan-police-institutionally-racist-misogynistic-homophobic-louise-casey-report

912 Liberty, "Facial Recognition", https://www.libertyhumanrights.org.uk/fundamental/facial-recognition/; Big Brother Watch, "Stop Facial Recognition", https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/

913 P. Fussey, D. Murray, "Impact: Report on the police use of facial recognition technology identifies significant concerns", University of Essex, https://www.essex.ac.uk/research/showcase/report-on-the-police-use-of-facial-recognition-technology-identifies-significant-concerns

914 University of Essex, "Impact: Viewing the risks of Artificial Intelligence through a human rights lens", https://www.essex.ac.uk/research/showcase/viewing-the-risks-of-advanced-ai-through-a-human-rights-lens

915 M. Burgess, "Co-op is using facial recognition tech to scan and track shoppers", Wired, 10. decembar 2020. https://www.wired.co.uk/article/coop-facial-recognition

916 R. Williams, "Supermarkets in talks to trial age estimation technology for buying alcohol later this year", inews, 13. april, 2021. https://inews.co.uk/news/technology/age-estimation-trials-supermarket-alcohol-953540; M. Prendergast, "Yoti digital age verification trialled at supermarkets", techUK, 6. januar 2023. https://www.techuk.org/resource/yoti-digital-age-verification-trialled-at-supermarkets.html

917 Meta, "Introducing New Ways to Verify Age on Instagram", 23. jun 2022. https://about.fb.com/news/2022/06/new-ways-to-verify-age-on-instagram/

918 Privacy International, "The Identity Gatekeepers and the Future of Digital Identity", 10. oktobar 2019. https://privacyinternational.org/long-read/3254/identity-gatekeepers-and-future-digital-identity

919 Biometrics Institute, "Home", https://www.biometricsinstitute.org/

920 IBIS World, "Biometrics Scan Technology Development in the UK - Market Size 2011–2029", 16. mart 2023. https://www.ibisworld.com/united-kingdom/market-size/biometrics-scan-technology-development/

921 HR News, "Number of CCTV Cameras in the UK reaches 5.2 million", 19. novembar 2020. https://hrnews.co.uk/number-of-cctv-cameras-in-the-uk-reaches-5-2-million/

922 Aljazeera, "Head of UK anti-monarchy group arrested at coronation protest", 6. maj 2023. https://www.aljazeera.com/news/2023/5/6/head-of-uk-anti-monarchy-group-arrested-at-coronation-protest

923 I. Kottasová, "'It's not a good look.' As cost of living crisis bites, some Brits are questioning spending money on glitzy coronation", CNN, 2. maj 2023. https://www.cnn.com/2023/05/02/business/cost-of-living-doncaster-coronation-gbr-cmd-intl/index.html

924 V. Dodd, "Police accused over use of facial recognition at King Charles's coronation", The Guardian, 3. maj 2023. https://www.theguardian.com/uk-news/2023/may/03/metropolitan-police-live-facial-recognition-in-crowds-at-king-charles-coronation

925 Ibid.

926 ECHR, "Guide on the case-law of the European Convention on Human Rights: Mass Protests", 31. avgust 2022. https://www.echr.coe.int/Documents/Guide_Mass_protests_ENG.pdf

927 European Digital Rights (EDRi), “Ban Biometric Mass Surveillance Explainer”, https://edri.org/wp-content/uploads/2020/05/Explainer-Ban-Biometric-Mass-Surveillance.pdf

928 Metropolitan Police, @metpoliceuk, “Our tolerance for any disruption, whether through protest or otherwise, will be low. We will deal robustly with anyone intent on undermining this celebration.”, Twitter, 3. maj 2023. https://twitter.com/metpoliceuk/status/1653745710724968448

929 College of Policing, “Changes to legislation for policing protests”, 2. juli 2023. https://www.college.police.uk/article/changes-legislation-policing-protests

930 Liberty, “How Does The New Policing Act Affect My Protest Rights?”, https://www.libertyhumanrights.org.uk/advice_information/pcsc-policing-act-protest-rights/

931 B. Quinn, R. Sya, V. Dodd, “Anti-monarchists receive ‘intimidatory’ Home Office letter on new protest laws”, The Guardian, 2. maj 2023. https://www.theguardian.com/politics/2023/may/02/anti-monarchists-receive-intimidatory-home-office-letter-on-new-protest-laws-coronation

932 M. Hyde, “Yes, the Met police threw royal protesters into cells for no good reason – but at least they regret it”, The Guardian, 9. maj 2023. https://www.theguardian.com/commentisfree/2023/may/09/met-police-royal-protesters-cells-force

933 UK Surveillance Camera Commissioner’s Office, “The Commissioner discusses the new era for live facial recognition after the Coronation”, 17. maj 2023. https://videosurveillance.blog.gov.uk/2023/05/17/the-commissioner-discusses-the-new-era-for-live-facial-recognition-after-the-coronation/

934 UK Biometrics and Surveillance Camera Commissioner, “Letter from the Biometrics and Surveillance Camera Commissioner to Lucy Allan MP about cameras around MPs’ home addresses (accessible)”, 12. maj 2023. https://www.gov.uk/government/publications/letter-to-lucy-allan-mp-about-cameras-around-mps-home-addresses; UK Biometrics and Surveillance Camera Commissioner, “Biometrics and Surveillance Camera Commissioner: report 2021 to 2022”, 9. februar 2023. https://www.gov.uk/government/publications/biometrics-and-surveillance-camera-commissioner-report-2021-to-2022

FOTOGRAFIJE

str. 17, 232 Autor Andrew Heald / Unsplash
str. 21 Autor Steve Johnson / Unsplash
str. 35 Autor Nathaniel Sison / Unsplash
str. 69, 274 Autor Rob Curran / Unsplash
str. 74 Autor Seb / Unsplash
str. 82 Autor Alev Takil / Unsplash
str. 96 Autor Atharva Tulsi / Unsplash
str. 106 Autor Jacques Nel / Unsplash
str. 114 Autor Justin Main / Unsplash
str. 124 Autor Amani Nation / Unsplash
str. 132 Autor Nuno Alberto / Unsplash
str. 146 Autor Fabio Alves / Unsplash
str. 154 Autor Ryan Miglinczy / Unsplash
str. 156 Autor Stephan Cassara / Unsplash
str. 198 Autorka Mavis CW / Unsplash
str. 208 Autor Tatenda Mapigoti / Unsplash
str. 215, 266 Autor Maxim Hopman / Unsplash
str. 234 Autor Saw Wunna / Unsplash
str. 237 Autor Jack Finnigan / Unsplash
str. 248 Autorka Barbara Zandoval / Unsplash
str. 251 EPA/Dimitris Todoris
str. 254 Autorka Sophia Goodfriend za Foreign Policy
str. 257 Autor Greg Bulla / Unsplash
str. 260 Autor Egor Litvinov / Unsplash
str. 262 Autor Bernard Hermant / Unsplash
str. 272 Autor Enrique Alarcon / Unsplash
str. 277 Autor Adrian Raudaschl / Unsplash

S ONE STRANE LICA: BIOMETRIJA I DRUŠTVO
BELEŠKE