PROCENA UTICAJA NAMERAVANIH RADNjI OBRADE BIOMETRIJSKIH PODATKA O LIČNOSTI NA ZAŠTITU PODATAKA O LIČNOSTI

I OPIS OBRADE PODATAKA

Na osnovu Zakona o policiji („Službeni glasnik RS”, br. 6/16, 24/18 i 87/18), policija vrši nadzor i snimanje javnog mesta i vrši obradu podataka o ličnosti u skladu sa Zakonom o evidencijama i obradi podataka u oblasti unutrašnjih poslova („Službeni glasnik RS”, br. 24/18).

U prethodnom periodu Ministarstvo unutrašnjih poslova (u daljem tekstu: Ministarstvo) je na osnovu izrađenog profila bezbednosnog problema[1] odnosno na osnovu procene bezbednosno interesantnih događaja, primenom policijsko-obaveštajnog modela, opredelilo lokacije i postavilo kamere za snimanje na javnom mestu. Takođe, u cilju unapređenja stanja javne bezbednosti, prateći razvoj savremenih informacionih tehnologija, u Ministarstvu je u toku uvođenje i eLTE tehnologije, odnosno savremenih radio stanica poslednje generacije opremljenih video kamerama, koja funkcioniše u okviru 4G mreže na *android* platformi. Pored toga, jedan broj „policijskih“ vozila je opremljen kamerama za „video nadzor u pokretu“, a u planu je i opremanje jednog broja policijskih službenika kamerama koje se nose na uniformi.

Takođe, policija ima uvid i u video zapise koji nastaju vršenjem poslova privatnog obezbeđenja. Naime, prema odredbama čl. 32. Zakona o privatnom obezbeđenju („Službeni glasnik RS”, br. 104/13, 42/15 i 87/18) kada se poslovi zaštite objekta ili prostora koji se koriste za javnu upotrebu vrše uz upotrebu uređaja za snimanje slike, korisnik usluga je obavezan da arhivirane snimke, stavi na uvid ovlašćenom policijskom službeniku.

Na osnovu dostupnih video zapisa ili fotografija bez obrade biometrijskih podataka Ministarstvo vrši identifikaciju lica: prepoznavanjem od strane policijskog službenika u toku snimanja ili naknadnim pregledom snimljenog materijala, takođe prepoznavanjem od strane policijskog službenika ili drugog lica kome je radi identifikacije lica sa snimaka ili fotografije, omogućen uvid u video zapis u skladu sa zakonom.

Policijski službenici prilikom ovakavog načina identifikacije lica, moraju da izvrše analizu video nadzora da bi utvrdili lokacije kamera odnosno objekata na kojima postoji video nadzor i koje su sve kamere mogle da zabeleže izvršenje krivičnog dela ili učinioca krivičnog dela, vreme izvršenja krivičnog dela, vreme neposredno pre i nakon izvršenja krivičnog dela. Nakon ovakve analize policijski službenici vrše pregled snimljenog materijala, izdvajaju određene segmente video zapisa radi njihove reprodukcije, a sve u cilju identifikacije određenog lica sa video zapisa.

Kod ovakvog načina identifikacije lica, neophodno je dodatno angažovanje policijskih službenika koji moraju da pregledaju celokupan video materijal, odnosno video zapise čije trajanje često može da traje nekoliko desetina ili stotina sati. S tim u vezi, namera Ministarstva je da unapredi mogućnosti pretraživanja, odnosno obrade video zapisa ili

[1] Скуп података и информација прикупљених у циљу сагледавања, разјашњења и бољег разумевања постојећих и нових појавних облика криминала, како би се иницирала или подржала полицијска активност према њима.- Извор: МУП (2016): Приручник: "Полицијско-обавештајни модел", доступно на сајту: www.mup.gov.rs.

fotografija, uz mogućnost da se identifikacija lica iz video zapisa ili fotografija vrši obradom biometrijskih podataka o ličnosti. Ovakva obrada video zapisa ili fotografija, radi izdvajanja biometrijskih podataka i njihovog poređenja sa biometrijskim podacima koje Ministarstvo već obrađuje u drugim evidencijama bi policijskim službenicima omogućila znatno bržu identifiakciju lica sa video zapisa ili fotografije.

Kod ovakvog načina obrade biometrijskih podataka o ličnosti, mora se imati u vidu da se prema odredbama Zakona o zaštiti podataka o ličnosti („Sl.glasnik RS",87/2018) radi o posebnoj vrsti podataka o ličnosti, čija je obrada u cilju jedinstvene identfikacije lica od strane nadležnih organa u „posebne svrhe“[2] dopuštena ako je to neophodno uz primenu odgovarajućih mera zaštite prava lica na koje se podaci odnose, u slučajevima kada:

1) je nadležni organ zakonom ovlašćen da obrađuje posebne vrste podataka o ličnosti;
2) se obrada posebnih vrsta podataka o ličnosti vrši u cilju zaštite životno važnih interesa lica na koje se podaci odnose ili drugog fizičkog lica;
3) se obrada odnosi na posebne vrste podataka o ličnosti koje je lice na koje se oni odnose očigledno učinilo dostupnim javnosti.

Dakle, neophodno je zakonsko ovlašćenje Ministarstva, kao osnovni preduslov za obradu biometrijskih podataka u posebne svrhe. S tim u vezi, kod ovakve nameravane obrade podataka, neophodno je razmotriti zakonski okvir za obradu biometrijskih podataka.

Sva pitanja koja se odnose na zakonitost obrade biometrijskih podataka o ličnosti od strane Ministarstva kao nadležnog organa u smislu člana. 4. tačka 26) Zakona o zaštiti podataka o ličnosti, moraju se razmatriti u kontekstu člana 8. Evropske konvencije o ljudskim pravima (Konvencija) kojom se jemči pravo na poštovanje privatnog i porodičnog života (pravo na privatnost).

Pravo na poštovanje privatnog i porodičnog života, pripada grupi takozvanih relativnih (kvalifikovanih) prava i sloboda, za koje su propisana legitimna ograničenja u njihovom ostvarivanju: a) u interesu nacionalne bezbednosti; b) u interesu javne bezbednosti ili ekonomske dobrobiti zemlje; c) radi sprečavanja nereda ili kriminala; d) radi zaštite zdravlja ili morala, ili e) radi zaštite prava i sloboda drugih (čl. 8. st. 2. Konvencije)[3].

S tim u vezi, u skladu sa načelima obrade podataka o ličnosti proklamovanih Zakonom o zaštiti podataka o ličnosti, obrada biometrijskih podataka podrazumevala bi obradu podataka o ličnosti u skladu sa zakonskim ovlašćenjima policije i to obradu podataka samo onih lica čiji podaci su neophodni za utvrđivanje identiteta lica u odnosu na konkretnu svrhu obrade, bez nepotrebnog zadržavanja (pohranjiva ili arhiviranja) tih podataka.

U skladu sa odredbama Zakona o zaštiti podataka o ličnosti, Ministarstvo bi imalo ulogu rukovaoca koji samostalno, angažovanjem sopstvenih resursa, obrađuje podatke o ličnosti

[2] Обрада података коју врше надлежни органи у сврхе спречавања, истраге и откривања кривичних дела, гоњења учинилаца кривичних дела или извршења кривичних санкција, укључујући спречавање и заштиту од претњи јавној и националној безбедности

[3] Чл. 8. Право на поштовање приватног и породичног живота: 1. Свако има право на поштовање свог приватног и породичног живота, дома и преписке. 2. Јавне власти неће се мешати у вршење овог права сем ако то није у складу са законом и неопходно у демократском друштву у интересу националне безбедности, јавне безбедности или економске добробити земље, ради спречавања нереда или криминала, заштите здравља или морала, или ради заштите права и слобода других.

uz primenu adekvatnih mera zaštite i mehanizama kontrole svih radnji obrade. Primalac odnosno korisnik ovih podataka bi mogao biti samo drugi nadležni organ i takvi podaci bi se mogli preneti primaocu u drugoj državi, odnosno međunarodnoj organizaciji, u skladu sa zakonom ali samo ako se radi o nadležnom organu za obradu podataka u posebne svrhe.

II PROCENA NEOPHODNOSTI I SRAZMERNOSTI

Režim zaštite obrade podataka o ličnosti koju jemči član 8. Konvencije, se posmatra i u kontekstu člana 17. Konvencije, kojim se zabranjuje zloupotreba prava. Naime, čl. 17. propisuje da se nijedna odredba Konvencije ne može tumačiti tako da podrazumeva pravo bilo koje države ili lica, da se „upuste u neku delatnost ili izvrše neki čin usmeren na poništavanje bilo kog od navedenih prava i sloboda ili na njihovo ograničavanje u većoj meri od one koja je predviđena Konvencijom“.

Takođe, pored zakonskog okvira u pogledu obrade biometrijskih podataka o ličnosti u posebne svrhe, uzimaju se u obzir i činjenice da obrada ove vrste podataka ne može biti opravdana po svaku cenu odnosno bez pažljivog balansiranja potencijalne koristi od njihovog korišćenja i legitimnog interesa pojedinca za zaštitom njegove privatnosti.

U skladu sa važećim Zakonom o policiji, identifikacija lica korišćnjem sistema video nadzora bez obrade biometrijskih podataka vrši se uvidom u video zapis ili fotografiju i to neposerednim prepoznavanjem od strane ovlašćenog policijskog službenika ili od strane drugog lica (oštećenog/žrtve krivčnog dela ili svedoka).

S tim u vezi treba istaći da je proteklih 5 godina, na području 26 područnih policijskih uprava, izvršeno ukupno 7 ubistava, od kojih su 4 kvalifikovana kao teška ubistva, čije izvršenje ili učinioce tih dela su zabeležile kamere video nadzora, a koja još uvek nisu rasvetljena. Policijski službenici Odeljenja kriminalističke policije područnih policijskih uprava po nalogu nadležnog tužilaštva, odnosno po naredbi suda, su preduzimali sve zakonom propisane mere i radnje iz svoje nadležnosti, odnosno iscrpeli su sve raspoložive resurse ali učinioci navedenih krivičnih dela nisu identifikovani.

Analizom preduzetih radnji i primenjenih ovlašćenja od strane policijskih službenika u vezi sa identifikovanjem učinioca samo dva krivična delo ubistva koja su 2017 godine, izvršena u Srbiji, može se oceniti neophodnost nameravane obrade biometrijskih podtaka o ličnosti u cilju unapređenja efikasnosti identifikacije lica.

Naime, krivično delo ubistva koje je 2017. godine, izvršeno u centralnoj Srbiji zabeleženo je kamerama video nadzora sa objekta na kojem su kamere instalirane kao mera tehničke zaštite u skladu sa Zakonom o privatnom obezbeđenju. Pregledom oko 1000 sati video zapisa sa ukupno 17 objekata, policijski službenci nisu uspeli da identifikuju učinioca ovog krivičnog dela.

Drugo krivično delo ubistva izvršeno 2017. godine na jugu Srbije je takođe zabeleženo sigurnosnim kamerama, ali policijski službenici pregledom više stotina sati video zapisa sa sigurnosnih kamera sa oko 20 objekata, takođe nisu uspeli da identifikuju učinioca.

Pored pregleda video zapisa, a u cilju identifikacije učinioca samo ova dva krivična dela, policijski službenici su preduzeli niz policijskih mera i radnji i primenili policijska

ovlašćenja prema velikom broju građana, ali još uvek nisu uspeli da identifikuju učinioca. Naime, policijski službenici su izvršili:

- 60 pretresa stanova i drugih prostorija,
- 64 poligrafska testiranja,
- 55 veštačenja (balistička, DNK veštačenja, zapaljenih vozila i sl),
- 1809 analiza ostvarenog telekomunikacionog saobraćaja sa baznih stanica,
- sačilni 291 službenu belešku o obaveštenju primljenom od građana,
- pregledali više od 80 snimaka video nadzora sa sigurnosnih kamera čije trajanje je duže od 1000 sati.

Neophodnost obrade biometrijskih podataka može se prikazati i kroz druge vidove identifikacije lica od strane policijskih službenika, na primer, analizom korišćenja „Vanrednih obavešenja“. Naime pored pregleda video zapisa ili fotografija, policija u svom radu u cilju identifikacije lica koristi i vanredna obaveštenja (raspis) koja se u papirnoj formi dostavljaju svim područnim policijskim upravama radi upoznavanja svih policijskih službenika koji rade na terenu kako bi pomogli u identifikaciji lica. Ova obaveštenja sadrže kratku informaciju o krivičnim delu i fotografije lica koje treba identifikovati. Takođe, ovakva obaveštenja se neretko javno objavljuju i preko medija ili drugih sredstava javnog obaveštavnja, radi prikupljanja informacija o eventualnim saznanjima koja policiji mogu pomoći u identifikaciji lica. Na isti način se postupa i u situacijama kada policija u cilju identifikacije lica koristi „foto-robot“ odnosno crtež koji je sačinjen na osnovu opisa lica od strane oštećenih ili drugih svedoka.

Tokom prethodne tri godine, Služba za suzbijanje kriminala, Uprave kriminalističke policije i područne policijske uprave raspisale su ukupno 234 vanrednih obaveštenja gde je identifikovano samo 35 lica (14,96%). Samo na teritoriji Policijske uprave za grad Beograd je u 2021. godine raspisno 25 vanrednih obaveštenja, a toku 2022. godine, 21 obaveštenje.

Pregledom snimaka ili fotografija, u nekim slučajevima učinioci krivičnih dela se mogu identifikovati na osnovu registarskih oznaka vozila. Identifikacija lica na ovaj način podrazumeva pozivanje svih vlasnika ili korisnika vozila čije registarske oznake se mogu videti na video zapisu ili fotografiji kao i obavljanje razgovora sa njima radi utvrđivanja relevantnih činjenica koje možda mogu dovesti do identifikacije učinioca krivičnog dela. Međutim, otežavajuća okolnost u većem broju slučajeva je činjenica da učinioci krivičnih dela na otvorenom prostoru ne koriste vozila ili u slučajevima da ih koriste oni često prekriju ili uklone registarske oznake vozila ili za izvršenje krivičnog dela koriste ukradena vozila ili registarske tablice.

Primenom drugih policijskih ovlašćenja, mera i radnji, što uključuje i korišćenje odnosno analizu podataka o ostvarenom telekomunikacionom saobraćaju, moguće je u određenim slučajevima identifikovati učinioca krivičnih dela. Međutim, i ovde treba imati u vidu činjenicu da učinioci krivičnih dela uglavnom koriste „pripejd“ SIM kartice za kratkotrajnu upotrebu ili uopšte ne koriste mobilne telefone jer su svesni činjenice da se preko njih mogu identifikovati.

Činjenica je i da učinioci krivičnih dela sve češće za međusobnu komunikaciju koriste nove tehnologije, posebne aplikacije ili specijalizovane kriptovane telefone[4], kako bi

[4] криптовани мобилни телефон „Anonimus“, чија цена се креће око 2.000 евра за период коришћења од шест месеци

onemogućili ili znatno otežali identifikaciju od strane policijskih službenika, te je neophodno da i policija u svom radu koristi moderne tehnologije i da, ako verovatno ne može da bude ispred, onda je nužno da u pogledu upotrebe modernih tehnologija bude na bar približno istom nivou sa kriminalnim strukturama.

Strateški cilj Vlade Republike Srbije i Ministarstva jeste izgradnja savremene, efikasne, funkcionalne i visoko profesionalizovane policije koja doprinosi bezbednosti Republike Srbije, uživa poverenje svih njenih građana i predstavlja pouzdanog partnera u međunarodnoj policijskoj saradnji.

Zadaci Ministarstva su prevashodno usmereni na smanjenje stope kriminala, efikasnije, efektivnije i ekonomičnije obavljanje policijskih poslova, zakonito i moralno postupanje policijskih službenika, poštovanje ljudskih prava i povećanje osećaja sigurnosti građana Republike Srbije.

Strateškom procenom javne bezbednosti Ministarstva unutrašnjih poslova (2022-2025)[5]. definisani su prioriteti rada Ministarstva gde je, pored suprotstavljanja organizovanom kriminalu i korupciji kao najvećim bezbednosnim pretnjama i rizicima, jedan od ključnih prioriteta istaknuto suprotstavljanje „uličnom kriminalu“ odnosno sprečavanje krivičnih dela koja se vrše na javnom prostoru.

Tokom 2021. godine samo na teritoriji grada Beograda izvršeno je ukupno 7.457 krivičnih dela na javnom prostoru (*ulični kriminal*). U istom vremenskom periodu rasvetljeno je 2.606 krivičnh dela (34.94%).

Imajući u vidu sve navedeno, neophodno ja da policija ima mogućnost da obradom biometrijskih podataka o ličnosti brže i jednostavnije identifikacije učinioce krivičnih dela. Svako zadiranje u osnovna prava i slobode lica koje bi ovakva obrada podataka mogla da izazove, bilo bi srazmerno i proporcionalno interesu nacionalne, odnosno javne bezbednosti, imajući u vidu da je pre svega usmereno na sprečavanje, istragu i otkrivanja krivičnih dela, gonjenje učinilaca krivičnih dela uključujući zaštitu prava i sloboda drugih.

Eventualno zadiranje u pravo na privatan život, odnosno slobodu udruživanja, okupljanja, mišljenja i izražavanja, prava na miran protest, slobodu kretanja, slobode misli, savesti, uverenja i veroispovesti, zabrane diskriminacije, obradom biometrijskih podataka o ličnosti kao posebne vrste podatka koje bi se izdvojile iz video zapisa ili fotografija, srazmerno je cilju zaštite interesa javne i nacionalne bezbednosti, sprečavanja nereda (javni red i mir) ili kriminala kao i zaštiti prava i sloboda drugih i u skladu je sa čl. 8 st. 2. Evropske konvencije o ljudskim pravima.

Imajući u vidu da je zakonski okvir osnovni/ključni preduslov za obradu biometrijskih podataka o ličnosti, i da drugi zakoni koji se primenjuju u Republici Srbiji ne uređuju obradu biometrijskih podatka u svrhu „identifikacije lica“, od strane Ministarstva pokrenuta je procedura za donošenje novog zakona o unutrašnjim poslovima kojim bi se pored ostalog uredila i obrada biometrijskih podataka kao posebno ovlašćenje policije. Nakon konsultacija sa zamenicima tužioca Višeg javnog tužilaštva u Beogradu i sudijama za prethodni postupak Višeg suda u Beogradu, zaključeno je da je neophodno uspostaviti

[5] http://www.mup.gov.rs/wps/wcm/connect/98632591-2b0d-4cba-9cd1-e7ff993705a6/Strateska+procena+javne+bezbednosti+MUP.pdf?MOD=AJPERES&CVID=nYH6yro

pravni okvir za primenu ovlašćenja policije da u skladu sa odredbama zakona kojim se uređuje krivični postupak izvrši pretraživanje video zapisa i fotografija radi izdvajanja biometrijskih karakteristika lika i njihovog poređenja sa podacima koji se u posebne svrhe obrađuju u skladu sa zakonom. S tim u vezi, treba razmotriti i neophodnost izmene Zakonika o krivičnom postupku u pogledu ovlašćenja policije.

Ministarstvo od decembra 2021. godine vodi društveni dijalog sa predstavnicima civilnog društva u koji je, u određenoj meri, uključen i Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti. Tokom ovog dijaloga u određenoj meri razmotren je *Predlog Uredbe Evropskog parlamenta i Saveta o utvrđivanju jednoobraznih pravila za veštačku inteligencijju i izmenama određenih propisa Unije*, kojim su pored ostalog definisani i različiti sistemi veštačke inteligencije sa opcijom biometrijske idenetifikacije: 1) sistem za biometrijsku kategorizaciju, 1) sistem za daljinsku biometrijsku identifikaciju, 3) sistem za daljinsku biometrijsku identifikaciju u stvarnom vremenu (uživo) i 4) sistem za naknadnu biometrijsku identifikaciju na daljinu.

Razmotrene su i preporuke *Evropskog odbora za zaštitu podataka o ličnosti, za obradu biometrijskih podataka od značaja za obradu putem video nadzora sa opcijom prepoznavanja lica* kao i brojne primedbe i sugestije civilnog društva u vezi sa rizicima i verovatnoćom uticaja na prava i slobode građana.

III PODACI O LIČNOSTI KOJI SE OBRAĐUJU

Upotrebom video nadzora koji Ministrstvo trenutno koristi, obrađuju se sledeći podaci o ličnosti: video zapis lica i događaja u kojem lice učestvuje, vreme i mesto nastanka video zapisa, lokacija kamere, registarske i druge oznake vozila.

Namera Ministarstva je da upotrebom odgovarajućeg softverskog rešenja vrši naknadnu obradu odnosno pretraživanje video zapisa ili fotografija izdvajanjem biometrijskih karakteristika lika, radi njihovog poređenja sa podacima koji se u posebne svrhe obrađuju u skladu sa zakonom.

IV RADNjE OBRADE

Obrada podataka upotrebom sistema video nadzora podrazumeva sledeće radnje obrade: prikupljanje, razvrstavanje, pretraživanje, izdvajanje upoređivanje, uvid, prenošenje, ograničavanje, čuvanje i brisanje odnosno uništavanje na drugi način.

Video zapisi sa kamera se u skladu sa zakonom pohranjuju na čvrstu memoriju - hard diskovi centralnog sistema za skladištenje podataka (*datacentar*) i čuvaju najmanje 30 dana. Namera Ministarstva je, da se u skladu sa novim Zakonom o obradi podataka u oblasti unutrašnjih poslova, ovi podaci na centralnom sistemu za skladištenje podataka čuvaju najmanje trideset dana, a najduže godinu dana, po sistemu kružnog snimanja.

Prilikom skladištenja na centralnom sistemu, video zapisi se automatski generišu i razvrstavaju po vremenu nastanka video zapisa i po mestu snimanja/lokacija kamere.

Uvid u video zapis (podatke koji se obrađuju) u realnom vremenu u toku snimanja (*live stream*), omogućen je ovlašćenom policijskom službeniku[6] neposrednim posmatranjem, u korisničkom centru. Uvid u video zapis moguće je izvršiti pretraživanjem i izdvajanjem odabranog video zapisa i njegovom reprodukcijom na radnoj stanici[7].

Pretraživanje pohranjenih video zapisa radi njihovog izdvajanja vrši se prema nekom od kriterijuma kao što su: lokacija odnosno naziv kamere/kamernog mesta, datum i vreme nastanka video zapisa, ali je moguće i prema registarskoj ili drugoj oznaci vozila upotrebom kamera za prepoznavanje registarskih oznaka.

Pretraživanje i uvid u pohranjene video zapise omogućeno je samo policijskim službenicima sa posebnom dozvolom odnosno odobrenjem i to u korisnikom centru ili na radnoj stanici van korisničkog centra. Ovo pretraživanje i vršenje uvida ograničeno je na svrhu i ciljeve prikupljanja podataka, a njihova dalja obrada vrši se u skladu sa zakonom odnosno ovlašćenjima policijskih službenika.

Video zapisi ili fotografije se u svrhu propisanu zakonom mogu preneti kopiranjem na nosač podataka (cd/dvd ili eksterni hard disk) ako je to potrebno radi vršenja uvida ili drugih radnji obrade van korisničkog centra. Fotografije izdvojene iz segmenta video zapisa se osim kopiranja i prenošenja na drugi nosač podataka mogu kopirati/umnožavati i štampanjem na papiru (ako je to potrebno na primer radi kreiranja vanrednog obaveštenja).

Nakon umnožavanja/kopiranja izdvojenog video zapisa ili fotografija, oni se u skladu sa zakonom čuvaju u drugim evidencijama Ministarstva i dalje se obrađuju u zavisnosti konkretne svrhe obrade. Kopije se, u pojedinačnim slučajevima, mogu preneti ovlašćenim primaocima kao što su drugi nadležni organi (tužilaštvo, sud) ili lice na koje se podaci odnose i to dostavljanjem na nosaču podataka.

U sistemu video nadzora koji Ministarstvo trenutno koristi, identifikacija lica vrši se neposredno od strane policijskog sužbenika i to pretraživanjem i vršenjem uvida u pohranjene video zapise ili izdvajanjem određenog segmenta video zapisa radi njegove reprodukcije na radnoj stanici van korisničkog centra.

Nameravana radnja obrade biometrijskih podataka upotrebom posebnog softverskog rešenja vršila bi se u slučajevima kada neposrednim uvidom u video zapis od strane policijskog službenika, nije moguće identifikovti lice te je neophodno da se pretraživanjem pohranjenog video zapisa ili fotografija izdvoje biometrijski podaci (biometrijske karakeristike lika) radi njihovog poređenja sa raspoloživim biometrijskim podacima koje Ministarstvo u posebne svrhe obrađuje u skladu sa zakonom. Kod ovakve obrade biometrijskih podataka, potrebno je da radna stanica na kojoj se vrši obrada video zapisa ili fotografija, bude povezana sa određenom evidencijom u kojoj se nalaze

[6] Под овлашћеним полицијским службеником за потребе израде ове процене подразумева се полицијски службеник који је распоређен на радно место чији опис послова подразумева руковање системом видео надзора и обраду видео записа. Ови полицијски службеници су едуковани и одобрена су им разуличита права приступа..Немају сви полицијски службеници исти ниво приступа. Под овлашћеним полицијским службеником се такође подразумева и поступајући полицијски службеник (у конкретном случају задужен за поступање).

[7] Радна станица се за потребе израде овог документа посматра као посебан рачунар који је смештен у издвојену просторију ван корисничког центра и која је обезбеђена посебним мерама физичкок техничке заштите. Улазак и боравак у просторију као и приступ овом рачунару омогућен је само одређени полицијским службеницима са посебним одобрењем.

biometrijski podaci, a koje Ministarstvo u posebne svrhe obrađuje u skladu sa zakonom (“ forenzički registrovana lica“).

Obrada biometrijskih podataka o ličnosti na ovaj način podrazumevala bi obradu pohranjenih video zapisa koja bi bila ograničena, odnosno trajala bi samo tokom poređenja. Obrada podataka odnosila bi se samo na lica iz određenog video zapisa, samo sa određenih kamera, a koji su sačinjeni u određenom vremenskom periodu. Biometrijski podaci bi se poredili samo sa podacima određene grupe lica (forenzički registrovana lica).

Ukolko bi softver pronašao podudarne biometrijske podatke, na radnoj stanici bi se kreirao izveštaj koji bi trebalo da sadrži podatke lica čiji su biometrijski podaci najpribližniji biometrijskim podacima iz obrađenog video zapisa sa iskazanim stepenom podudarnosti ili bi se prikazao izveštaj da nema podudarnih podataka. Ovakav izveštaj bi se dostavio postupajućem policijskom službeniku koji bi dalje preduzimao druge neophodne aktivnisti radi pronalaska lica sa video zapisa ili fotografije. Dakle postupajući policijski službenik bi donosio odluku o preduzimanju drugih radnji, odnosno primeni drugih policijskih ovlašćenja u cilju pronalaska lica, jer se identitet lice ne može potvrditi samo na osnovu softverskog rezultata poređenja.

Izveštaj o rezultatu poređenja bi trebalo da sadrži i sledeće podatke o ličnosti: broj i datum naredbe i naziv suda, broj izveštaja, ime i prezime policijskog službenika i naziv organizacione jedinice u kojoj on radi, jedinstvenu oznaku radne stanice na kojoj je vršena obrada video zapisa ili fotografije, datum i vreme obrade, jedinstvenu oznaku video zapisa ili fotografije koji su obrađeni, fotografiju, ime i prezime, delovodni broj i naziv evidencije u kojoj su evidentirana lica čije biometrijske karakteristike lika su podudarne sa biometrijskim karakteristikama lika izdvojenih iz obrađenog video zapisa ili fotografije.

Izdvojeni biometrijski podaci iz obrađenog video zapisa ili fotografije se nakon poređenja ne bi čuvali, a rezultat poređenja bi se kreirao na radnoj stanici.
U slučaju potrebe za ponovnim poređenjem biometrijskih podataka ceo postupak bi trebalo ponoviti.

Sistemski žurnal treba da beleži datum i vreme izdvajanja i obrade video zapisa, oznaku video zapisa, informacije o korisniku radne stanice i pristup podacima svih lica iz evidencije čiji su podaci najpribližniji biometrijskim podacima lica iz obrađenog video zapisa.

V PROCENA RIZIKA PO PRAVA I SLOBODE LICA

Razmatrajući različite sisteme veštačke inteligencije koje prepoznaje *Predlog Uredbe Evropskog parlamenta i Saveta o utvrđivanju jednoobraznih pravila za veštačku inteligencijju i izmenama određenih propisa Unije,* Ministarstvo nalazi da bi upotreba softvera za „naknadnu biometrijsku identifikaciju“, bila najprihvatljivija, pre svega imajući u vidu nadležnosti i ovlašćenja za obradu podataka o ličnosti i svrhe obrade podataka o ličnosti od strane Ministarstva s jedne strane, odnosno potencijalne rizike koje takva obrada može imati na zajemčena prava i slobode lica kao i očuvanje demokratskog karaktera društva, s druge strane.

Zakonitost upotrebe softvera, uz čiju pomoć bi se mogla vršiti „naknadna identifikacija“ od strane Ministarstva, može se posmatrati kroz nekoliko kumulativnih elemenata:

(a) priroda slučaja koji opravdava upotrebu softvera, a naročito težina krivičnog dela, verovatnoća i obim štete i posledica koje bi nastale nekorišćenjem sistema;
(b) posledice njegove upotrebe na prava i slobode svih lica čiji podaci bi se obrađivali a posebno težina, verovatnoća i obim tih posledica.
(v) ostvarivanje usko definisanih zakonitih ciljeva (pronalazak lica za koje postoje osnovi sumnje da je učinilo krivično delo za koje se goni po službenoj dužnosti), mora biti u skladu s neophodnim i srazmernim zaštitnim merama i uslovima korišćenja, naročito kada je reč o vremenskim i prostornim ograničenjima za korišćenje.

U okviru ovako definisanih uslova Ministarstvo nalazi da je za svaku pojedinačnu upotrebu softvera neophodno prethodno odobrenje-naredba nadležnog suda odnosno sudije za prethodni postupak, a koje se izdaje na obrazložen predlog nadležnog tužioca, kao i da je u konkretnom slučaju upotreba softvera nužna i srazmerna za postizanje propisanih legitimnih ciljeva.

Nakon analize opisanih radnji obrade podataka, nephodnosti, srazmernosti odnosno opravdanosti eventualne upotrebe ovakvog softvera, identifikovani su i ocenjeni rizici po prava i slobode lica, do kojih može dovesti obrada biometrijskih podataka o ličnosti. Definisane su mere za kontrolu i smanjenje rizika nakon čega je ocenjen rezidualni rizik, a Ministarstvo će kao rukovalac podataka o ličnosti periodično ažurirati analizu rizika u skladu sa pojavljivanjem pretnji.

Rangiranje rizika je izvršeno ukrštanjem uticaja i verovatnoće, a za merenje rizika korišćena je matrica rizika 5x5.

Stepen ugroženosti/ ozbiljnost posledica	Visok	5	10	15	20	25
	Pretežno visok	4	8	12	16	20
	Srednji	3	6	9	12	15
	Pretežno nizak	2	4	6	8	10
	Nizak	1	2	3	4	5
Procena rizika		Mala	Pretežno mala	srednja	Pretežno velika	velika
		Verovatnoća ostvarivanja pretnje				

1-3…..**NEZNATNA** (ne zahteva se nikakva aktivnost)
4-6…. **DOPUSTIVA** (nema potrebe za dodatnim aktivnostima, potrebno je pratiti situaciju)
7-11…**UMERENA** (potrebno je u naredenom periodu planirati i druge mere, pratiti pojedine aktivnosti i definisati način kontrole)
12-15 **ZNATNA** (potrebni su efikasni mehanizmi kontrole primene mera za smanjenja rizika)
16-25. **NEDOPUSTIVA** (obradu podataka ne bi trebalo vršiti dok se rizik ne umanji)

PREPOZNATI RIZICI:

1. **<u>Obrada podataka neodređenog broja lica</u>**

Ovaj rizik kod upotrebe sistema video vezuje se za prikupljanje i čuvanje podataka neodređenog broja lica odnosno svih lica koja se zateknu u zoni snimanja, a čiji podaci se mogu obrađivati naknadnom obradom video zapisa.

Takođe, ovakvom obradom podataka nije moguće napraviti neophodnu razliku između pojedinih vrsta lica (čl. 9. Zakona o zaštiti podataka o ličnosti) odnosno sistem video nadzora prikuplja podatke svakog lica koje se zatekne u zoni snimanja.

Ovakav način obrade podataka svakog „prolaznika“ ozbiljno utiče na razumna očekivanja lica da budu anonimna na javnom prostoru što je preduslov za mnoge aspekte demokratskog procesa, kao što su na primer: slobodna odluka o udruživanju sa drugima, posećivanje skupova i upoznavanje ljudi iz drugih društvenih i kulturnih sredina, učestvovanju u političkom protestu i slično.

Prilikom vršenja nadzora na javnom prostoru uz mogućnost naknadne identifikacije, kod lica se stvara osećaj da su podvrgnuti konstantnom nadzoru, a da pritom nisu ni sigurni da li je stvarno tako, odnosno da li će i kada odnosno u kojim sve okolnostima biti identifikovani od strane policije. Ovakav osećaj može uticati na ponašanje pojedinaca, što dalje utiče i na karakter društva. Dodatni aspekt ovakvog osećaja kod pojedinaca je i odvraćanje od susreta ili viđanja u javnosti sa određenim licima (rođacima, prijateljima) za koje se pretpostavlja da su imali ili mogu imati „problem“ sa policijom.

Kod video nadzora na javnom prostoru nemoguće je ograničiti njegovu primenu na način da se obezbedi poverljiv kontakt sa određenim licima (kao što je naprimer kontakt sa novinarima, advokatima, sveštenstvom, lekarima i sl.). Takođe, od upotrebe ovog sistema nemoguće je na javnom prostoru „zaštiti“ posebno osetljive grupe lica kao što su na primer deca. Ovakva neselektivna upotreba sistema za nadzor na javnom prostoru gde sva lica koja se zateknu na određenom prostoru mogu biti predmet obrade odnosno naknadne identifikacije, pored pomenutih prava ugrožava i pravo na pretpostavku nevinosti.

Stepen ugroženosti/ozbiljnost posledica:visok (5)
Verovatnoća ostvarivanja pretnje:srednji (4)
Izloženost riziku povreda prava i slobode je: nedopustiva (20)

Umanjenje ovog rizika moguće je pre svega primenom zakonskih ograničenja i efikasnom kontrolom, upravljanjem rizikom, primenom organizacionih i tehničkih mera zaštite.

Naime, na osnovu Zakona o policiji Ministarstvo vrši nadzor i snimanje javnog mesta, radi obavljanja policijskih poslova, korišćenjem opreme za video akustičke snimke i fotografisanje i vrši obradu podataka o ličnosti u skladu sa Zakonom o evidencijama i obradi podataka u oblasti unutrašnjih poslova. Pravilnikom o načinu snimanja na javnom mestu i načinu saopštavanja namere o tom snimanju („Sl. glasnik RS“, broj 111/20) predviđeno je da će Ministarstvo putem medija, drugih sredstava javnog obaveštavanja (sredstvo javnog informisanja, internet prezentacije i sl.) obavestiti javnost, a samim tim i sva lica koja mogu biti obuhvaćena video nadzorom.

Ministarstvo je na osnovu izrađenog profila bezbednosnog problema odnosno na osnovu procene bezbednosno interesantnih događaja, primenom policijsko-obaveštajnog modela opredelilo lokacije kamera za snimanje na javnom mestu, a obrada biometrijskih

podataka vršila bi se naknadnom obradom video zapisa i fotografija i to samo kada je takva obrada neophodna u cilju pronalaska lica za koje postoje osnovi sumnje da je učinilo krivično delo za koje se goni po službenoj dužnosti, samo ukoliko primenom drugih policijskih ovlašćenja nije izvršena identifikacija lica i to na osnovu naredbe sudije za prethodni postupak, a na predlog nadležnog tužioca.

Obrada biometrijskih podataka o ličnosti na ovaj način podrazumevala bi obradu pohranjenih video zapisa koja bi bila ograničena odnosno trajala bi samo tokom poređenja. Obrada podataka odnosila bi se samo na određene lica iz određenog video zapisa, samo sa određenih kamera, u određenom vremenskom periodu, a biometrijski podaci bi se poredili samo sa podacima određenih lica koje ovo Ministarstvo obrađuje u posebne svrhe.

Obrada biometrijskih podataka vrši se samo u toku poređenja, dakle bez zadržavanja (čuvanja) biometrijskih podataka, a rezultat podudarnosti biometrijskih podataka usmeravao bi policijske službenike na druge aktivnosti odnosno primenu drugih mera i radnji u cilju pronalaska lica i provere odnosno utvrđivanje njegovog identiteta. Dakle ni jedno lice se ne identifikuje automatski, odnosno ne primenjuje se tzv.automatsko prepoznavanje lica, već je u svakom konkretnom slučaju neophodna uloga policijskog službenika.

Obradu biometrijskih podataka iz pohranjenog video zapisa i njihovo upoređivanje vrši samo ovlašćeni policijski službenik po posebnoj dozvoli odnosno odobrenju. Postupanje svih policijskih službenika kod obrade biometrijskih podataka mora biti zasnovano na organizacionoj strukturi u sistemu podeljenih uloga u pogledu vršenja pojedinačnih radnji obrade i odlučivanja o potrebi pojedinačne identifikacije lica, čime će se omogućiti identifikacija samo onih lica bez čije obrade podataka nije moguće ostvariti konkretnu svrhu obrade podataka.

Korisnici podataka su samo policijski službenici koji moraju biti edukovani o zakonskim uslovima i načinu primene policijskih ovlašćenja, o utvrđenim standardima policijskog rada i o pravnom režimu zaštite podataka o ličnosti. Svi dodeljeni nalozi za pristup sistemu se pri promeni poslova ili prestanka radnog odnosa ukidaju, odnosno nivoi pristupa se ažuriraju. Dakle, postoje ograničenja u pogledu lica čiji podaci se obrađuju kao i svhe obrade, ograničenja čuvanja i prenosa. Takođe uspostavljen je i mehanizam kontrole obrade podataka i primenjenih mera zaštite. Svaki pristup sistemu se automatski beleži (sistemski žurnal).

Primenom organizacionih i tehničkih mera i efikasnim mehanizmima kontrole obrade podataka, može se efikasno upravljati rizikom te se rezidualni rizik odnosno izloženost riziku povrede prava i slobode može efikasno kontrolisati i umanjiti.

Stepen ugroženosti/ozbiljnost posledica:visok(5)
Verovatnoća ostvarivanja pretnje:pretežno mala(2)
Izloženost riziku povreda prava i slobode je: umerena (10)

2. Rizik nedovoljne transparetnosti

Rizik nedovoljne transparentnosti se vezuje za način ostvarivanja prava na informisanost lica čiji se podaci obrađuju, odnosno za nedovoljnu informisanost lica o tome da li su se i

u kojim sve situacijama obrađivali ili se i dalje obrađuju njihovi podaci o ličnosti i da li će i kakvom sve obradom i kojih podataka biti identifikovani.

Upotrebom sistema video nadzora na javnom prostoru, a posebno kod uvođenja u upotrebu video nadzora u pokretu odnosno upotrebom video nadzora koji je postavljen na policijskim vozilima ili upotrebom kamera koje policijski službenici mogu da nose na uniformi, kod lica se stvara osećaj da su podvrgnuti konstantnom nadzoru, a da pri tom nisu sigurni da li je stvarno tako i da li će i kada, odnosno u kojim sve okolnostima i na kojim lokacijama biti snimnjeni ili identifikovani, usled čega se kod njih može javiti osećaj nesigurnosti, odnosno neizvesnosti ostvarivanja ljudskih prava i sloboda i to ne samo prava koja su im zajemčena propisima o zaštiti podataka o ličnosti.

Ovakav osećaj se dodatno produbljuje zbog činjenice da policija na javnom mestu ne postavlja obaveštenje o upotrebi sistema video nadzora niti javno saopštava nameru snimanja u slučaju kada primenjuju posebne dokazne radnje odnosno tajno praćenje i snimanje kao ni u slučaju sprovođenja testa integriteta,

Izostanak ili nedovoljna informisanost lica o obradi podatka dodatno produbljuje osećaj nesigurnosti, odnosno nelagodnosti.

Stepen ugroženosti/ozbiljnost posledica: srednji (3)
Verovatnoća ostvarivanja pretnje: srednja (3)
Izloženost riziku povreda prava i slobode je: umerena (9)

Kontrola rizika vrši se primenom predviđenih organizacionih i tehničkih mera.

Transparentnom upotrebom video nadzora umanjuje se subjektivni osećaj ugroženosti prava na privatnost lica, čime se podiže i svest građana o visini rizika po ovo njihovo pravo. U skladu sa Pravilnikom o načinu snimanja na javnom mestu i načinu saopštavanja namere o tom snimanju, Ministarstvo će putem medija, drugih sredstava javnog obaveštavanja (sredstvo javnog informisanja, internet prezentacije i sl.) obavestiti javnost, a samim tim i sva lica koja mogu biti obuhvaćena video nadzorom.

Lokacije kamera na javnom mestu moraju biti jasno obeležene kao i policijska vozila koja su opremljena video nadzorom kako bi se svim licima koji se zateknu na toj lokaciji omogućilo da se upoznaju sa činjenicom da će dolaskom na određenu lokaciju zapravo biti pod nadzorom. Spisak lokacija kamera se objavljuje na internet sajtu ministarastva[8]. Kod upotrebe kamera koje policijski službenici nose na uniformama neophodno je da policijski službenici uvek obaveste lica da će snimati svoje, odnosno postupanje lica prema kojem primenjuju policijska ovlašćenja.

Licima se pored ovakvog opšteg informisanja mora omogućiti i konkretno ostvarivanje prava u vezi sa obradom podataka o ličnosti (pravo na uvid, kopiju, brisanje ili druga prava, u skadu sa zakonom). Informisanje bez obzrira na način mora da sadrži i obaveštavanje o načinu ostvarivanja prava kod rukovaoca (npr. podnošenjem zahteva Ministarstvu, teritorijalno nadležnoj policijskoj upravi, po mestu odnosno lokaciji kamera, lokaciji snimanja i sl.).

[8] http://www.mup.gov.rs/wps/wcm/connect/b152c15f-16eb-47b3-b9a4-c7f32c2cc1ba/%D0%A0%D0%B5%D0%B4.pdf?MOD=AJPERES&CVID=oqjaLo7

Uz primenu mera za umanjenje rizika umanjuje se i verovatnoća povrede prava i slobode lica, ali se mora imati u vidu da će i pored svih preduzetih mera uvek postojati lica koja neće biti obaveštena ili neće dovoljno jasno razumeti obaveštenje koje im je pruženo, ili da će policijski službenici propustiti da ih o tome obaveste, te je rezidualni rizik, odnosno izloženost riziku smanjena do nivoa dopustivog i može se kontrolisati efikasnim postupanjem po zahtevima građana za ostvarivanje prava u vezi sa obradom podataka o ličnosti kao i edukacijom odnosno kontrolom rada policijskih službenika.

Stepen ugroženosti/ozbiljnost posledica: srednji (3)
Verovatnoća ostvarivanja pretnje:pretežno mala (2)
Izloženost riziku povreda prava i slobode je: dopustiva (6)

3. Profilisanje lica

Rizik po prava i slobode lica vezuje se za mogućnost profilisanja lica što podrazumeva da se svaki oblik automatizovane obrade podataka, može koristiti da bi se ocenilo određeno svojstvo ličnosti, posebno u cilju analize ili predviđanja ponašanja, lokacija, kretanja ili ličnih sklonosti (na osnovu stvarne ili pretpostavljene pripadnosti udruženju, odnosno verskoj zajednici, političkog ili drugog mišljenja, seksualnog opredeljenja ili drugog stvarnog ili pretpostavljenog ličnog svojstva). Obaveza je rukovaoca je da lice na koje se podaci odnose informiše o mogućnosti profilisanja i pruži mu dodatne informacije kako bi se obezbedila poštena i transparentna obrada.

Zabranjeno je donošenje odluke isključivo na osnovu automatizovane obrade koju Ministarstvo vrši kao nadležni organi u posebne svrhe, uključujući i profilisanje, ako takva odluka može da proizvede štetne pravne posledice po lice na koje se podaci odnose ili značajno utiču na položaj tog lica, osim ako je donošenje te odluke zasnovano na zakonu i ako su tim zakonom propisane odgovarajuće mere zaštite prava i sloboda lica na koje se podaci odnose, a najmanje pravo da se obezbedi učešće fizičkog lica pod kontrolom rukovaoca u donošenju odluke. Zabranjeno je profilisanje koje dovodi do diskriminacije fizičkih lica na osnovu posebnih vrsta podataka o ličnosti.

Rizik po prava i slobode lica upotrebom video nadzora i obradom video zapisa i fotografija predstavljao bi nedozvoljeno profilisanje koje bi podrazumevalo donošenje odluke na osnovu automatizovane obrade bez primene odgovarajućih mera zaštite prava i sloboda lica, odnosno do bilo kakvog oblika diskriminacije na osnovu posebnih vrsta podataka koje nema za cilj analizu ili predviđanje ponašanja, lokacije, kretanje lica za koje se postoji osnovi sumnje da je učinilo krivino delo za koje se gonjenje preduzima po službenoj dužnosti.

Stepen ugroženosti/ozbiljnost posledica:pretežno visok (4)
Verovatnoća ostvarivanja pretnje:pretežno visoka (4)
Izloženost riziku povreda prava i slobode je: nedopustiva (16)

Kontrola rizika vrši se upotrebom predviđenih organizacionih i tehničkih mera.

Uz primenu odgovarajućih mera zaštite prava, sloboda i legitimnih interesa lica na koje se podaci odnose dopušteno je donošenje odluke na osnovu automatizovane obrade koju vrše nadležni organi u posebne svrhe, koja uključuje i profilisanje ali takva obrada, odnosno profilisanje mora biti zasnovano na zakonu. Zabranjeno je profilisanje koje

dovodi do diskriminacije fizičkih lica, a lice na koje se podaci odnose ima pravo da podnese prigovor na obradu podataka.

Donošenje bilo kakve odluke koja proizvodi pravne posledice, odnosno koja utiče na položaj lica na koje se podaci odnose, mora biti zasnovano na zakonu, obrada podataka se mora vršiti na osnovu naredbe sudije za prethodni postupak koja se izdaje na predlog nadležnog tužioca i pri svakoj obradi podataka moraju se preduzeti odgovarajuće mere zaštite prava i sloboda lica a najmanje prava da se obezbedi učešće fizičkog lica (ovlašćenog policijskog službenika) u donošenju odluke.

Ovlašćeni policijski službenik dužan je da za svako lice ponaosob na osnovu rezultata automatizovane obrade, donose odluku o preduzimanju mera i radnji ili primene policijskih ovlašćenja u cilju identifikacije tog lica. Dakle, u svakom konkretnom slučaju neophodna je uloga policijskog službenika kod određivanja svrhe i načina primene konkretne radnje obrade. Samo na osnovu obrade podataka koje je izvršena uz učešće čoveka-policijskog službenika, mogu se preduzeti određene radnje ili doneti odluke koje proizvode pravne posledice po to lice, odnosno koje utiču na položaj lica.

Postupanje policijskih službenika kod obrade video zapisa i fotografija, odnosno obrade biometrijskih podataka o ličnosti u vidu profilisanja, zasnovano je na organizacionoj strukturi u sistemu podeljenih uloga i to u pogledu vršenja pojedinačnih radnji obrade i odlučivanja o neophodnosti analize sklonosti, ponašanja i kretanja lica, čime je umanjena mogućnost nedozvoljenog profilisanja.

Ovakvo dozvoljeno profilisanje mora se vršiti uz primenu adekvatnih organizacionih mera zaštite podataka kao što su upravljanje korisničkim nalozima, softversko generisanje naloga za pretragu, dvostruki pristup sistemu.
Obrada biometrijskih podataka može se vršiti samo uz primenu odgovarajućih tehničkih mera zaštite podataka kao što su: kontrola pristupa opremi, kontrola nosača podataka, kontrola čuvanja odnosno brisanja podataka, kontrola korisnika, kontrola pristupa podacima, kontrola prenosa, kontrola transporta, oporavak sistema, obezbeđivanje integriteta sistema, upravljanje korisničkim nalozima, sistemski žurnal, fizička i tehnička zaštita objekata i opreme, zaštita od oštećenja i krađe sredstava koja čine sistem video nadzora.

Policijski službenici koji vrše obradu podataka moraju biti edukovani o zakonskim uslovima za eventualno profilisanje kao i načinu primene policijskih ovlašćenja, mera i radnji, o utvrđenim standardima policijskog rada i o pravnom režimu zaštite podataka o ličnosti. Dodatna mera zaštite od rizika koji nastaju pri promeni poslova ili prestanka radnog odnosa policijskih službenika je ukidanje naloga za pristup sistemu i ažuriranje odobrenih nivoa pristupa. Mehanizam utvrđivanja disciplinske odgovornosti je istovremeno preventivna i reaktivna mera zaštite podataka koja se mora primenjivati.

Uz primenu navedenih mera za umanjenje rizika kao i činjenice da su radnje automatizovane obrade podataka svedene na minimum i da se vrše na osnovu naredbe suda i to naknadnom obradom pohranjenih video zapisa, rezidualni rizik je znatno umanjen ali izloženost riziku i dalje postoji, te da bi se adekvatno upravljalo ovim rizikom, neophodni su efikasni mehanizmi kontrole.

Stepen ugroženosti/ozbiljnost posledica:visok (5)
Verovatnoća ostvarivanja pretnje: pretežno mala (2)

Izloženost riziku povreda prava i slobode je: umerena (10)

4. Biometrijski podaci iz evidencija za upoređivanje nisu tačni

Upoređivanjem biometrijskih podataka iz pohranjenog video zapisa ili fotografije sa biometrijskim podacima koje Ministarstvo u skladu sa zakonom u posebne svrhe obrađuje u svojim evidencijama, proverava se podudarnost, odnosno traže se biometrijski podaci sa najvećim stepenom podudarnosti.

Rizik po slobode i prava lica vezuje se za obradu biometrijskih podataka sadržanih u evidencijama Ministarstva, a koji nisu tačni. Obrada takvih netačnih podataka dovela bi do pogrešnog usmeravanja policijskih službenika na preduzimanje određenih mera i radnji odnosno primenu policijskih ovlašćenja prema pogrešnom licu. Ovakva obrada bi za posledicu mogla imati neosnovano identifikovanje lica odnosno neosnovano postupanje policijskih službenika prema „pogrešnom“ licu jer se za njega vezuju netačni biometrijski podaci iz evidencija Ministarstva, čime bi se povredilo njegovo pravo na privatnost i dostojanstvo.

Nivo verovatnoće povrede prava i sloboda lica određen je obradom netačnih podataka kojom se mogu ugroziti pravo na privatnost i dostojanstvo lica čiji se podaci obrađuju. Mogućnost da nisu tačni biometrijski podaci koji su pohranjeni u evidencijama Ministarstva se ne može zanemariti, pre svega iz razloga što su biometrijski podaci u prethodnom periodu prikupljani i obrađivani upotrebom drugačije tehnologije. Takođe, postoje mogućnosti da je na primer fotografija jednog lica povezana sa podacima drugog lica jer je načinjena greška prilikom ručnog unosa podataka u evidencije (prilikom prenosa podataka iz evidencija koje su se ranije vodile u papirnoj formi).

Stepen ugroženosti/ozbiljnost posledica: pretežno nizak (2)
Verovatnoća ostvarivanja pretnje:mala (1)
Izloženost riziku povreda prava i slobode je: neznatna (2)

Kontrola rizika vrši se preduzimanjem organizacionih i tehničkih mera zaštite podataka o ličnosti.

Primena policijskih ovlašćenja mera i radnji povezanih sa obradom biometrijskih podataka mora se vršiti profesionalno i u skladu sa utvrđenim standardima policijskog rada, što podrazumeva da policijski službenik u slučaju očigledne netačnosti podatka mora izvršiti dodatne provere pre donošenja odluke o daljem postupanju. Sprovođenjem kontinuirane edukacije i kontrolno-instruktivne delatnosti omogućiće se i efikasan mehanizam upravljanja podacima koji podrazumeva uređen način prikupljanja podataka i vođenja evidencija kao i uvid u postupanje policijskih službenika.

Postupanje policijskih službenika prilikom vođenja evidencija mora biti zasnovano na organizacionoj strukturi u sistemu podeljenih uloga u pogledu vršenja pojedinačnih radnji obrade, čime je umanjena mogućnost greške odnosno netačnog ili neažurnog vođenja evidencija što podrazumeva proveru unosa, ažuriranja, izmena ili ispravljanje podataka sadržanih u evidencijama.

Primenom određenih tehničkih mera zaštite podataka kao što su: kontrola pristupa opremi, kontrola nosača podataka, kontrola unosa, čuvanja podataka, kontrola korisnika, kontrola pristupa podacima, kontrola prenosa, kontrola transporta, oporavak sistema,

obezbeđivanje integriteta sistema, upravljanje korisničkim nalozima, sistemski žurnal, obezbeđuje se efikasan mehanizam upravljanja podacima.

Kod izloženosti ovom riziku mora se imati u vidu da je „čovek“ karika koja predstvlja najveću pretnju za netačno ili neažurno vođenje evidencija kada je u pitanju ručni unos podataka. Međutim, ne može se zanemariti ni činjenica da nije uvek ljudska greška ili nesavestan rad razlog za netačno unete podatke u evidencije, jer postoji mogućnost da na primer podaci koji su od drugog rukovaoca dostavljeni Ministarstvu radi unosa u evidecije nisu tačni ili da je podatak izmenjen prilikom prenosa. Primenom efikasnih kontrolnih mehanizama može se obezbediti visok nivo tačnosti podataka, te se i rezidualni rizk može uspešno kontrolisati.

Stepen ugroženosti/ozbiljnost posledica: pretežno nizak (2)
Verovatnoća ostvarivanja pretnje: mala (1)
Izloženost riziku povreda prava i slobode je: neznatna (2)

5. Snimanje lica u privatnom prostoru

Rizik po prava i slobode lica postoji u situacijama kada se snimanje na javnom prostoru vrši kamerama koje snimaju i deo privatnog prostora. Snimanjem, pohranjivanjem i drugim radnjama obrade podataka o aktivnosti lica koja se nalaze u privatnom prostoru može se ugroziti pravo na privatnost lica. Ovaj rizik se znatno uvećava očekivnim uvođenjem u upotrebu kamera koje policijski službenici nose na uniformi.

Lice opravdano očekuje da su aktivnosti koje preduzima u privatnom prostoru zaštićene od pogleda drugih ljudi i da ih niko bez njihove dozvole odnosno saglasnosti neće snimati dok borave u privatnom prostoru.
Transparentnom upotrebom video nadzora, i obaveštavanjem o snimanju umanjuje se subjektivni osećaj ugroženosti prava na privatnost lica, čime se podiže svest građana o visini rizika po ovo njihovo pravo.

Upotreba sistema video nadzora ima za cilj snimanje javnog prostora, ali postoji mogućnost da se snimi i privatni ili poslovni prostor na onim mestima na kojim ne postoje fizičke prepreke ili ako policijski službenik koji nosi kameru na uniformi uđe u privatni ili poslovni prostor i uključi kameru, čime se ugrožava pravo na privatnost.

Ukoliko je kamera veoma udaljena od privatnog ili poslovnog prostora, odnosno ukoliko se u odnosu na privatni prostor nalazi pod neodgovarajućim uglom, ili je takav prostor zaklonjen drvećem, zavesama, roletnama, ogradama i sl., kvalitet prikupljenih podataka je loš, a mogućnost povrede prava je pretežno mala. Mogućnost povrede prava snimanjem od strane policijskog službenika kamerom koju nosi na uniformi se može umanjiti samo ukoliko policijski službenik uvek proverava da li je kamera koju nosi na uniformi uključena ili ne.

Stepen ugroženosti/ozbiljnost posledica:visok (5)
Verovatnoća ostvarivanja pretnje: pretežno mala (2)
Izloženost riziku povreda prava i slobode je: umerena (10)

Kontrola rizika vrši se sprovođenjem organizacionih i tehničkih mera.

Uz periodično preispitivanje vidnog polja kamera, kao i sprovođenjem kontrolno-instruktivne delatnosti i edukacijom policijskih službenika omogućen je uvid u način rukovanja kamerama i postupanja policijskih službenika. Korisnici sistema su policijski službenici koji moraju biti osposobljeni i edukovani za rukovanje kamerama kao i o zakonskim uslovima i načinu upotrebe sistema video nadzora bez obzira na vrstu uređaja i opreme koja se koristi za snimanje. Postupanje policijskih službenika prilikom rukovanja kamerama zasnovano je na organizacionoj strukturi u sistemu podeljenih uloga.

Obrada snimnjenog materijala vršila bi se na osnovu sudske naredbe i podrazumevala bi obradu pohranjenih video zapisa koja bi bila ograničena odnosno trajala bi samo tokom poređenja. Obrada podataka odnosila bi se samo na lica iz određenog video zapisa, samo sa određenih kamera a koji su sačinjeni u određenom vremenskom periodu a biometrijski podaci bi se poredili samo sa podacima određenih lica koje ovo ministarstvo obrađuje u posebne svrhe.

Takođe, uz primenu tehničkih mera zaštite kao što su: kontrola pristupa opremi, kontrola nosača podataka, kontrola snimanja, čuvanja podataka, kontrola korisnika, kontrola pristupa podacima, kontrola prenosa, kontrola transporta, obezbeđivanje integriteta sistema, upravljanje korisničkim nalozima, sistemski žurnal obezbeđuje se efikasan mehanizam upravljanja podacima.

Javni prostor koji se snima upotrebom video nadzora podrazumeva i veliki broj stambenih, poslovnih i drugih objekata u kojima lica borave, te je nemoguće vršiti video nadzor na način da se ne posmatraju i ovi objekti odnosno lica koja u njima borave. Projektovanje sistema video nadzora mora biti usklađeno sa postojećom ili planirnanom infrastrukturom, ali treba imati u vidu da je gotovo nemoguće da video nadzor ne obuhvata i određene objekte koji nisu predmet nadzora. Upotrebom odgovarajućih filtera, video nadzor se može koristiti na način da se ne ugrožava privatnost nečijeg doma ili poslovnog prostora, odnosno na način da ne izaziva nelagodnost kod građana zbog bojazni da su predmet nadzora dok borave u tom prostoru. Primenom adekvatnih mera zaštite i mehanizama kontrole njihove primene, može se obezbediti da nivo rezidualnog rizika bude dopustiv.

Stepen ugroženosti/ozbiljnost posledica:visok (5)
Verovatnoća ostvarivanja pretnje: mala (1)
Izloženost riziku povreda prava i slobode je: dopustiva (5)

6. Greška softvera

Postojanje rizika vezuje se za činjenicu da se obrada biometrijskih karakteristika (pretraživanje, upoređivanje) ne može posmatrati kao stopostotno tačna tehnologija, već da se zasniva na „podešavanju nivoa osetljivosti“ u odnosu na „lažne negativne“ i „lažne pozitivne rezultate“. Lažni rezultati (negativni ili pozitivni) nose značajne rizike za pojedinca (lice može biti pogrešno označeno kao izvršilac krivičnog dela ili obrnuto, da softver za obradu biometrijskih video zapisa uopšte ne detektuje lik izvršioca krivičnog dela ili se izvršiocu krivičnog dela usled greške softvera obezbeđuje alibi).

Verovatnoća greške mora se posmatrati u odnosu na kvalitet video zapisa ili fotografija koje se obrađuju radi obrade biometrijskih podataka. Za razliku od uslovno rečeno

„kontrolisanih okruženja“ ili okruženja koja su u potpunosti pokrivena video nadzorom, gde se obezbeđuje visok kvalitet video zapisa i gde verovatnoća greške mala ali svakako da procenat greške raste kada se koristi video zapis sa kamera gde je kvalitet video zapisa lošiji usled različitih okolnosti (osvetljenje, vremenske prilike, udaljenost kamere, korišćenje različitih sredstava za izbegavanje video nadzora poput naočara za sunce, kape, šala ili maske preko lica) povećava se i rizik od greške.

Tačnost i pouzdanost obrade biometrijskih podataka određuje se na osnovu podatka proizvođača ali mora postojati i nezavisno ocenjivanje uz periodično preispitivanje nivoa tačnosti.

Ni jedna odluka koja na bilo koji način može da utiče na prava lica se ne sme donositi samo na osnovu automatizovane obrade odnosno na osnovu rezultata rada softvera odnosno rezultata upoređivanja podataka. Nivo uticaja greške softvera na povrede prava na privatnost i dostojanstvo lica kod obrade biometrijskih podataka o ličnosti određen je primenom policijskih ovlašćenja, mera i radnji kojima se ugrožavaju prava tog lica. Nivo verovatnoće povrede prava na privatnost i dostojanstvo lica, određen je na način što ovlašćeni policijski službenik u cilju identifikacije lica na osnovu obrade biometrijskih podataka uvek dodatno proverava rezultat njihovog upoređivanja i donosi odluku o preduzimanju drugih mera i radnji prema licu. Izostanak potrebne provere rezultata upoređivanja biometrijskih podataka povećava se i rizik povrede prava na privatnost i dostojanstvo lica.

Stepen ugroženosti/ozbiljnost posledica:srednji(3)
Verovatnoća ostvarivanja pretnje: srednja (3)
Izloženost riziku povreda prava i slobode je: umerena (9)

Kontrola rizika vrši se sprovođenjem predviđenih organizacionih i tehničkih mera. Postupanje policijskih službenika prilikom obrade video zapisa zasnovano je na organizacionoj strukturi u sistemu podeljenih uloga u pogledu vršenja neophodnih provera rezultata upoređivanja biometrijskih podataka, čime je umanjena mogućnost preduzimanja bilo kakvih mera i radnji prema licu, bez vršenja neophodne provere. Obrada video zapisa ili fotografija i upoređivanje biometrijskih podataka vrši se profesionalno i u skladu sa utvrđenim standardima policijskog rada. Preduzimaju se mere zaštite od rizika koji nastaju pri promeni poslova ili prestanka radnog odnosa. Zaposleni u Ministarstvu su edukovani o pravnom režimu zaštite podataka o ličnosti. Utvrđivanje disciplinske odgovornosti je preventivna i reaktivna mera koja u velikoj meri umanjuje ovaj rizik. Nezavisno ocenjivanje i periodično preispitivanje nivoa tačnosti softvera je neophodno kako bi se cenila njegova pouzdanost.

Primenom tehničkih i organizacionih mera kao što su: kontrola korisnika, kontrola pristupa podacima, kontrola obrade, kontrola čuvanja, kontrola brisanja, kontrola prenosa, kontrola transporta, oporavak sistema, obezbeđivanje integriteta softvera i operativnih sistema, sistemski žurnal, zaštita od zlonamernog softvera, obezbeđivanje ispravnog i bezbednog funkcionisanja sistema, čuvanje podataka o događajima koji mogu biti od značaja za bezbednost sistema, obezbeđivanje da aktivnosti na reviziji sistema imaju što manji uticaj na njegovo funkcionisanje i obezbeđivanje kontinuiteta obavljanja poslova u vanrednim okolnostima, obezbeđuju se neophodni preduslovi za pouzdanu obradu podataka o ličnosti.

Mora se imati u vidu i činjenica da se uprkos ubrzanom razvoju softvera, razvoju veštačke inteligencije i primenom predviđenh mera zaštite, rezidualni rizik ne može umanjiti i on će ostati na nivou umerenog.

Stepen ugroženosti/ozbiljnost posledica:srednji(3)
Verovatnoća ostvarivanja pretnje: srednja (3)
Izloženost riziku povreda prava i slobode je: umerena (9)

7. Rizik od pristupanja podacima od strane neovlašćenih lica

Postojanje ovog rizika vezuje se za pristup odnosno mogućnost pristupa podacima od strane neovlašćenih lica.

Različiti nivoi pristupa odobravaju se policijskim službencima u odnosu na organizacionu strukturu u sistemu podeljenih uloga i to u pogledu vršenja pojedinačnih radnji obrade. Nivo uticaja na povrede prava na privatnost i dostojanstvo lica, određen je upotrebom sistema video nadzora i softvera za obradu biometrijskih podataka od strane ovlašćenih lica/ovlašćenih policijskih službenika, gde nivo uticaja povrede prava raste ukoliko postoji bilo kakva mogućnost za pristup neovlašćenih lica.

Nivo verovatnoće povrede prava na privatnost i dostojanstvo lica određen je u odnosu na mogućnost pristupa podacima od strane neovlašćenih lica i to neovlašćenim pristupom opremi ili nosačima podataka. Sama činjenica da takva mogućnost postoji izaziva dodatni osećaj nesigurnosti kod građana te se ona primenom mera zaštite mora u potpunosti eliminisati ili makar svesti na najmanju moguću meru.

Stepen ugroženosti/ozbiljnost posledica:srednji(3)
Verovatnoća ostvarivanja pretnje: pretežno mala (2)
Izloženost riziku povreda prava i slobode je: dopustiva (6)

Kontrola rizika vrši se sprovođenjem organizacionih i tehničkih mera.

Uređaji i oprema za obradu podataka i nosači informacija (CD, DVD, eksterni hard diskovi) na koje su podaci pohranjeni, kopirani ili preneti, moraju biti obezbeđeni, čuvani u posebnim prostorijama koje se zaključavaju, obezbeđene sistemom kontrole pristupa, video-nadzorom, uz primenu mera zaštite od požara, poplava, strujnog udara i drugih incidenata, enkriptovani. Nosači informacija se ne smeju iznositi iz prostorija osim za jasno definisane potrebe, kao što je recimo izrada rezevnih kopija ili oporavak sistema iz rezervnih kopija. U slučaju incidenta mora se obezbediti integritet podataka u okviru sistema i obnova funkcionalnosti sistema, što se postiže redovnom izradom rezervnih kopija podataka (dnevni, mesečni, godišnji nivo) kojima mogu pristupati samo ovlašćeni zaposleni (sistem administratori) i samo u slučaju incidenta kada je neophodno izvršiti oporavak sistema. Primenom tehničkih i organizacionih mera kao što su kontrola nosača podataka, kontrola čuvanja podataka, kontrola korisnika, kontrola pristupa podacima, kontrola prenosa, kontrola transporta, oporavak sistema, obezbeđivanje integriteta softvera i operativnih sistema, sistemski žurnal, zaštita od zlonamernog softvera, obezbeđivanje ispravnog i bezbednog funkcionisanja sistema, čuvanje podataka o događajima koji mogu biti od značaja za bezbednost sistema, obezbeđivanje da aktivnosti na reviziji sistema imaju što manji uticaj na njegovo funkcionisanje i obezbeđivanje kontinuiteta obavljanja poslova u vanrednim okolnostima zabrana kopiranja, umnožavanja i prenosa podataka bez pohranjivanja obezbeđuje pouzdan sistem

upravljanja podacima. Pored navedenih mera, rizik se može kontrolisati ukidanjem ili ažuriranjem prava pristupa pri promeni poslova ili prestanka radnog odnosa, kao i kontinuiranom edukacijom zaposlenih u vezi sa izveštavanjem i reagovanjem u slučaju incidenata.

Gotovo je nemoguće u potpunosti eliminisati rizik neovlašćenog pristupa podacima ali se efikasnom primenom mera zašite rezidualni rizik može značajno umanjiti.

Stepen ugroženosti/ozbiljnost posledica:srednji(3)
Verovatnoća ostvarivanja pretnje: mala (1)
Izloženost riziku povreda prava i slobode je: neznatna (3)

8. **<u>Rizik od zloupotreba koje mogu izvršiti ovlašćena lica.</u>**

Postojanje ovog rizika odnosi se na mogućnosti zloupotrebe podatka od strane ovlašćenih lica/policijskih službenika kojima je odobren pristup podacima. Zlopotrebe su moguće u trenutku prikupljanja podataka ili tokom njihove dalje obrade (ovlašćeni policijski službenik može ivršiti obradu podataka bez pravog osnova, bez prethodno izdate naredbe sudije za prethodni postupak, odnosno koristiti uređaje i opremu u svrhe za koje nisu namenjeni gde je najčešće ovaj rizik motivisan razlozima lične prirode).

Ovlašćeni policijski službenik može snimati, vršiti uvid u pohranjene podatke bez pravnog osnova ili pohranjene podatke može izdvojiti, kopirati i preneti neovlašćenom licu radi dalje upotrebe što može podrazumevati i nedopušteno objavljivanje podataka. Ovlašćeni policijski službenik može bez sudske naredbe izvršiti obradu biometrijskih podataka ili profilisanje. Takođe, ovaj rizik se vezuje i za mogućnost da ovlašćeni policijski službenik propusti da dodatno proveri rezultat podudarnosti upoređivanja biometrijskih podataka usled čega može doneti pogrešnu odluku o preduzimanju drugih mera i radnji prema licu i na taj način ugroziti njegova prava.

Stepen ugroženosti/ozbiljnost posledica:srednji(3)
Verovatnoća ostvarivanja pretnje: pretežno mala (2)
Izloženost riziku povreda prava i slobode je: dopustiva (6)

Kontrola rizika vrši se sprovođenjem organizacionih i tehničkih mera.

Radi pravilne i zakonite obrade biometrijskih podataka neophodno je obezbediti da se prilikom svakog pristupa snimljenom materijalu beleži digitalni zapis o tom pristupu koji bi trebalo da sadrži najmanje sledeće informacije: ime i prezime policijskog službenika, broj službene legitimacije ili matični broj policijskog službenika, jedinstvenu oznaku uređaja sa koga je pristupljeno, podatke o trajanju svake sesije, kao i podatke o aktivnostima. Digitalni zapisi o pristupu se čuvaju u sistemskom žurnalu. Prilikom upotrebe softvera za obradu biometrijskih podataka obrađuje se određeni pohranjeni video zapis ili fotografija lica koji je označen jedinstvenom oznakom zabeleženog video zapisa ili fotografije vremenom i mestom nastanka video zapisa ili fotografije, lokacijom kamere, a rezultat obrade, odnosno poređenja, se u formi izveštaja kreira na radnoj stanici za obradu video zapisa ili fotografija. Izveštaj o rezultatu poređenja pored ostalih podataka sadrži i: broj i datum naredbe i naziv suda, broj izveštaja, ime i prezime policijskog službenika, naziv organizacione jedinice u kojoj radi policijski službenik, jedinstvenu oznaku radne stanice na kojoj je vršena obrada video zapisa ili fotografije, datum i vreme obrade, a pristup i sve aktivnosti preduzete na radnoj stanici za obradu

video zapisa ili fotografija čuva se u sistemskom žurnalu. Sistemski žurnal beleži i pristup podacima svih lica iz evidencije čiji su podaci najpribližniji biometrijskim podacima lica iz obrađenog video zapisa. Na osnovu ovako upostavljene evidencije uvek je moguće nedvosmisleno utvrditi koji policijski službenik je vršio obradu podataka i na kojoj radnoj stanici kao i kakav je bio rezultat obrade. Ova evidencija se može staviti na uvid Povereniku za inforamcije od javnog značaja i zaštitu podataka o ličnosti radi vršenja poslova iz njegove nadležnosti.

Prilikom pristupanja sistemu, za sve dodeljene korisničke naloge mora biti podešena dodatna (dvostruka) autentifikacija prilikom pristupa snimljenim materijalima, koja bi se ostvarivala npr. putem službene legitimacije.

Preporuka je da se prilikom pristupa sistemu u prostorije ne unose bilo kakvi uređaji sa mogućnošću snimanja audio ili video zapisa, kao što su mobilni telefoni, kamere, diktafoni i slično kao i da se ograniči mogućnost prenosa podataka na nosače podataka (USB ili CD). Takođe predviđena je zabrana odnosno nemogućnost čuvanja/pohranjivanja, kopiranja, umnožavanja ili prenosa biometrijskih podataka.

Definisanjem privilegija za svakog policijskog službenika sa ovlašćenjem da pristupa snimljenom materijalu neophodno je utvrditi odgovarajući nivo pristupa u skladu sa radnim mestom, tj. pozicijom u okviru organizacione jedinice. Na primer, samo određeni službenici (sistem administratori) imaju administratorski pristup informacionom sistemu, koji omogućava naprednije opcije poput kreiranja i brisanja naloga za druge službenike. Samo određeni policijski službenici mogu dobiti ulogu koja im omogućava da pregledaju snimke, bez mogućnosti preuzimanja, izmene ili brisanja materijala, dok drugi policijski službenici imaju mogućnost preuzimanja podataka i njihovu dalju obradu. Svako preuzimanje podataka se evidentira uz označavanje broja izrađenih kopija, razloga izuzimanja i sl. Potrebno je obezbediti da se softverski definiše odgovarajući pristupni zahtev, kako bi prilikom svakog pristupa bilo evidentirano na osnovu kog zahteva se postupa.

Nakon prestanka radnog odnosa ili premeštaja na drugo radno mesto u okviru Ministarstva, korisnički nalozi za pristup sistemu kojima je isteklo ovlašćenje moraju biti deaktivirani i arhivirani, tj. mora biti onemogućen pristup sistemu sa tih naloga u najkraćem mogućem roku.

Uz primenu efikasnih mera za umanjenje rizika mora se imati u vidu činjenica da se „čovek“ uvek pojavljuje kao najslabija karika te da mogućnost zloupotrebe uvek postoji i ona uvek za sobom povlači i određene posledice za lice na koje se podaci odnose ali se efikasnom primenom mera rezidualni rizik može kontrolisati.

Stepen ugroženosti/ozbiljnost posledica:srednji(3)
Verovatnoća ostvarivanja pretnje: pretežno mala (2))
Izloženost riziku povreda prava i slobode je: dopustiva (6)

9. Rizik od gubitka, uništenja ili izmene podataka ili izostanak nadzora

Postojanje ovog rizika vezuje se za gubitak, uništenje i izmenu podataka od strane ovlašćenih ili neovlašćenih lica. Postojanje ovog rizika vezuje se i za izostanak adekvatnog nadzora i obaveštavanja i reakcije u slučaju incidenata koji mogu dovesti do gubitka izmene ili uništenja podataka. Nastupanje rizika je moguće kako u trenutku

prikupljanja podataka, tako i prilikom njihove dalje obrade. Ovlašćeni policijski službenik može izvršiti izmenu ili uništenje podataka bez pravnog osnova (zlouopotrebom ovlašćenja ili odobrenog nivoa pristupa). Neodgovorno postupanje sa podacima dovodi do gubitka podataka (npr. prilikom prenosa, transporta nosača podatka, neadekvatno čuvanje podataka takođe dovodi do gubitka podataka).

Stepen ugroženosti/ozbiljnost posledica:srednji(3)
Verovatnoća ostvarivanja pretnje: pretežno mala (2)
Izloženost riziku povreda prava i slobode je: dopustiva (6)

Kontrola rizika vrši se sprovođenjem organizacionih i tehničkih mera.

Kontrola nosača podataka, kontrola čuvanja podataka, kontrola pristupa podacima, kontrola prenosa, kontrola transporta, sistemski žurnal, zaštita od zlonamernog softvera, obezbeđivanje ispravnog i bezbednog funkcionisanja sistema, čuvanje podataka o događajima koji mogu biti od značaja za bezbednost sistema, je neophodna radi uspostavljanja efikasnog mehanizma upravljanja podacima.

Prilikom svakog pristupa podacima neophodno je beležiti digitalni zapis o tom pristupu (sistemski žurnal). Prilikom pristupanja informacionom sistemu, za sve dodeljene korisničke naloge mora biti podešena dodatna/dvostruka autentifikacija i definisanje privilegija i rola za svakog policijskog službenika.

Obrada podataka upotrebom sistema video nadzora mora se vršiti profesionalno i u skladu sa utvrđenim standardima policijskog rada ali je nemoguće eliminisati rizik kad se ima u vidu da je ovlašćeno lice-policijski službenik ipak samo „čovek“ koji je kao što je više puta već konstatovano najslabija karika i nemoguće je dopreti do svesti svakog pojedinca, ali se efikasnom primenom preventivnih i reaktivnih mera rezidualni rizk može umanjiti.

Efikasnom primenom navedenih mera rezidualni rizik se može umanjiti da postane neznatan.

Stepen ugroženosti/ozbiljnost posledica:srednji(3)
Verovatnoća ostvarivanja pretnje: mala (1)
Izloženost riziku povreda prava i slobode je: neznatna (3)

10. Nedopušteno objavljivanje podataka

Postojanje ovog rizika odnosi se na mogućnosti zloupotrebe od strane ovlašćenih lica/policijskih službenika kojima je odobren pristup podacima. Zloupotrebe su moguće u trenutku prikupljanja podataka ili tokom njihove dalje obrade gde je ovaj rizik najčešće motivisan razlozima lične prirode. Ne isključuje se mogućnost i da ovlašćeni policijski službenik može vršiti uvid u pohranjene podatke, izdvojiti, obraditi, kopirati i preneti podatke neovlašćenom licu samoinicijativno ili na osnovu naloga nadređenog. Mora se imati u vidu da se ovaj rizik posmatra samo u odnosu na nedopušteno objavljivanje podataka i tom smislu je neophodno napraviti jasnu razliku od objavljivanja koje je dopušteno.

Nedopušteno objavljivanje podataka prikupljenih sistemom video nadzora, putem medija, društvenih mreža ili korišćenjem drugih sredstava komunikacije ugroziće prava i slobode lica čiji se podaci obrađuju.

Uvidom u aktivnosti lica koje je obuhvaćeno video nadzorom od strane javnosti, odnosno primaoca informacija koje se objavljuju u medijima, u okviru društvenih mreža ili putem drugih sredstava komunikacije ugroziće se pravo na privatan život.Objavljivanjem informacije koja se odnosi na privatan život lica ugroziće se ugled, čast, dostojanstvo, lični i moralni integritet lica čiji se podaci obrađuju video nadzorom. Nedopušteno objavljivanje podataka prikupljenih video nadzorom, putem medija, društvenih mreža ili korišćenjem drugih sredstava komunikacije povrediće prava i slobode lica čiji se podaci obrađuju.

Stepen ugroženosti/ozbiljnost posledica:visok(5)
Verovatnoća ostvarivanja pretnje: srednja (3)
Izloženost riziku povreda prava i slobode je: znatna (15)

Kontrola rizika vrši se sprovođenjem organizacionih i tehničkih mera.

Radi pravilne i zakonite obrade podataka prikupljenih sistemom video nadzora neophodno je obezbediti da se prilikom svakog pristupa snimljenom materijalu beleži digitalni zapis o tom pristupu koji bi trebalo da sadrži najmanje sledeće informacije: ime i prezime policijskog službenika, broj službene legitimacije ili matični broj policijskog službenika, ID uređaja sa koga je pristupljeno (radne stanice), podatke o trajanju svake sesije, kao i podatke o aktivnostima. Digitalni zapisi o pristupu se čuvaju u sistemskom žurnalu.

Prilikom pristupanja informacionom sistemu, za sve dodeljene korisničke naloge mora biti podešena dodatna (dvostruka) autentifikacija prilikom pristupa snimljenim materijalima koja bi se ostvarivala npr. putem službene legitimacije.

Preporuka je da se prilikom pristupa sistemu u prostorije ne unose bilo kakvi uređaji sa mogućnošću snimanja audio ili video zapisa, kao što su mobilni telefoni, kamere, diktafoni i slično kao i da se ograniči mogućnost prenosa podataka na nosače podataka (USB ili CD). Takođe, predviđena je zabrana odnosno nemogućnost kopiranja, umnožavanja i prenosa podataka.

Definisanjem privilegija za svakog policijskog službenika sa ovlašćenjem da pristupa snimljenom materijalu neophodno je utvrditi odgovarajući nivo pristupa u skladu sa radnim mestom, tj. pozicijom u okviru organizacione jedinice. Na primer, samo određeni službenici (sistem administratori) imaju administratorski pristup informacionom sistemu, koji omogućava naprednije opcije poput kreiranja i brisanja naloga za druge službenike. Samo određeni policijski službenici mogu dobiti ulogu koja im omogućava da pregledaju snimke, bez mogućnosti preuzimanja, izmene ili brisanja materijala, dok drugi policijski službenici imaju mogućnost preuzimanja i dalje obrade podataka. Svako preuzimanje podataka se mora evidentirati uz označavanje broja izrađenih kopija, razloge i sl. Neophodno je obezbediti da se softverski definiše odgovarajući pristupni zahtev, kako bi prilikom svakog pristupa bilo evidentirano na osnovu kog zahteva se postupa. Nakon prestanka radnog odnosa ili premeštaja na drugo radno mesto u okviru Ministarstva, korisnički nalozi za pristup sistemu moraju biti deaktivirani i arhivirani, tj. mora biti onemogućen pristup sistemu sa tih naloga u najkraćem mogućem roku.

Mere zaštite kao što su kontrola pristupa opremi, kontrola nosača podataka, kontrola čuvanja podataka, kontrola brisanja podataka, kontrola korisnika, kontrola pristupa podacima, kontrola obrade, kontrola prenosa, kontrola transporta, oporavak sistema, obezbeđivanje integriteta sistema, upravljanje korisničkim nalozima, sistemski žurnal, zaštita od zlonamernog softvera, fizička i tehnička zaštita objekata i opreme, zaštita od oštećenja i krađe sredstava koja čine sistem video nadzora, obezbeđuju efikasan i pouzdan mehanizam upravljanja podacima.

Postupanje policijskih službenika prilikom upotrebe video nadzora zasnovano je na organizacionoj strukturi u sistemu podeljenih uloga u pogledu vršenja pojedinačnih radnji obrade, čime je umanjena mogućnost nedopuštenog objavljivanja podataka i omogućeno je utvrđivanje individualne odgovornosti policijskih službenika.

Uz primenu efikasnih mera za umanjenje rizika mora se imati u vidu činjenica da je i ovde „čovek“ najslabija karika te mogućnost zloupotrebe u vidu nedopuštenog objavljivanja podataka, uvek postoji, koja kao takva gotovo uvek za sobom povlači i određene posledice za lice na koje se podaci odnose. Primena policijskih ovlašćenja, mera i radnji, upotrebom sistema video nadzora, vrše se profesionalno i u skladu sa utvrđenim standardima policijskog rada, a utvrđivanje disciplinske odgovornosti i iniciranje postupka za utvrđivanje krivične odgovornosti od strane nadležnog organa takođe su neophodni elementi efikasnog mehanizma upravljanja podacima kojim se rezidualni rizik može umanjiti do umerenog.

Stepen ugroženosti/ozbiljnost posledica: visok(5)
Verovatnoća ostvarivanja pretnje: pretežno mala (2)
Izloženost riziku povreda prava i slobode je: umerena (10)

VI OPIS MERA I MEHANIZAMA ZAŠTITE U ODNOSU NA RIZIK PO PRAVA I SLOBODE LICA

Mere zaštite bezbednosti podataka i mehanizmi zaštite prava lica

Bezbednost podataka se osigurava primenom propisa o dopuštenoj obradi podataka, kao i odredbi koje se odnose na prava lica, kao i primenom tehničkih, organizacionih i kadrovskih mera u skladu sa zakonom.

Predstavljeni rizici po prava i slobode lica efikasno se uklanjaju, odnosno svode na najmanju meru primenom opštih organizacionih, kadrovskih i tehničkih mera zaštite bezbednosti podataka, odnosno mehanizama zaštite prava i sloboda lica u vezi sa obradom podataka o ličnosti. Mere i mehanizmi zaštite propisani su Zakonom o zaštiti podataka o ličnosti i drugim propisima, kao što je Zakon o informacionoj bezbednosti, Zakon o policiji, Zakon o evidencijama i obradi podataka u oblasti unutrašnjih poslova i podzakonskim aktima donetim od strane ministarstva.

Mere zaštite bezbednosti podataka i mehanizmi zaštite prava lica u sistemu video nadzora primenjuju se na specifičan način. Pojedine od ovih mera i mehanizama primenjuju se u odnosu na više različitih rizika i to na isti ili različit način, dok se druge mere i mehanizmi primenjuju samo u odnosu na pojedinačno određen rizik.

Primena tehničkih mera zaštite podataka i opreme u sistemu video nadzora, i sa njima povezanih organizacionih mera zaštite, uređuje se Zakonom o evidencijama i obradi podataka u oblasti unutrašnjih poslova, Uputstvom o merama informacione bezbednosti u informaciono-komunikacionom sistemu Ministarstva unutrašnjih poslova, Uputstvom o uslovima izgradnje, korišćenja i održavanja sistema video nadzora u Ministarstvu unutrašnjih poslova i Uputstvom o načinu vođenja evidencija u oblasti video-akustičkog snimanja.

Obrada biometrijskih podataka podrazumevala bi i uspostavljanje novih evidencija na osnovu kojih se uvek može utrditi ko je i kada, na kojoj radnoj stanici vršio obradu podataka. Za uspostavljanje ovakve evidencije kao i za utvrđivanje procedura postupanja policijskih službenika, mehanizama kontrole i druge neophodne mere zaštite podatka neophodno je donošenje odgovarajućih podzakonskih odnosno instruktivnih akata od strane Ministarstva. Donošenje ovih akata proističe iz odredbi Zakona o unutrašnjim poslovima i Zakona o obradi podataka u oblasti unutrašnjih poslova koji su trenutno u fazi nacrta, a čije donošenje je preduslov za obradu biometrijskih podataka u svrhu identifikacije lica od strane Ministarstva.

Sistem video nadzora kojim rukuje Ministarstvo, čini skup fiksnih i mobilnih kamera, kao i drugih uređaja i opreme koji su namenjeni za nadzor i snimanje. Izgradnja sistema video nadzora vrši se na obrazloženi predlog Direkcije policije, a na osnovu odluke ministra, odnosno lica koje on ovlasti za donošenje ove odluke. U svrhu donošenja odluke o izgradnji sistema video nadzora vrši se analiza potreba postavljanja kamera na pojedinim kamernim mestima, a prema ranije pomenutoj metodologiji i kriterijumima. Pri tome se u kontekstu procene nivoa izvesnosti nastupanja rizika, posebno vodi računa o ostvarenju svrhe video nadzora, odnosno o tome da se postavljanjem kamera na adekvatne položaje u najvećoj meri onemogući snimanje privatnog prostora.

Tehničke mere zaštite

Kontrola pristupa opremi, kontrola korisnika, kontrola pristupa podacima i sistemski žurnal, kao tehničke mere, podrazumevaju da je prilikom svakog pristupa snimljenom materijalu, neophodno beležiti digitalni zapis o tom pristupu koji bi trebalo da sadrži najmanje sledeće informacije: ime i prezime policijskog službenika, broj službene legitimacije ili značke policijskog službenika, matični broj, ID uređaja sa koga je pristupljeno (radna stanica), podatke o trajanju sesije, kao i podatke o aktivnostima (sve operacije koje su vršene, pretrage koje su rađene itd.). Digitalni zapisi o pristupu (logovi) se moraju čuvati u sistemskom žurnalu.

Obavezna dvostruka potvrda identiteta (2FA) podrazumeva da prilikom pristupanja sistemu, za sve dodeljene korisničke naloge mora biti podešena dodatna autentifikacija prilikom pristupa snimljenim materijalima, koja se ostvaruje putem službene legitimacije policijskog službenika/korisnika sistema.

Kontrola nosača podataka, kontrola čuvanja podataka, fizička i tehnička zaštita objekata i opreme, zaštita od oštećenja i krađe sredstava koja čine sistem video nadzora kao tehničke mere zaštite podrazumeva da uređaj i nosači informacija na koje su podaci u okviru sistema snimljeni moraju biti čuvani u posebnim prostorijama koje se zaključavaju i koje su obezbeđene zaštitom od požara, poplave, strujnog udara i drugih incidenata, kao i video-nadzorom. Za pristup nosačima informacija neophodan je isti nivo pristupa kao za pristupanje sistemu. Nosači informacija se ne smeju iznositi iz prostorija osim za jasno

definisane potrebe, kao što je izrada kopija ili oporavak sistema iz rezervnih kopija. Prilikom pristupa sistemu u prostorije se ne smeju unositi bilo kakvi uređaji sa mogućnošću snimanja audio ili video zapisa kao što su mobilni telefoni, kamere, diktafoni itd.

Oporavak sistema i obezbeđivanje integriteta sistema podrazumeva da se u slučaju incidenta moraju obezbediti integritet podataka u okviru sistema i obnova funkcionalnosti sistema, što se postiže redovnom izradom rezervnih kopija podataka (dnevni, mesečni, godišnji nivo) kojima mogu pristupati samo ovlašćeni zaposleni (sistem administratori) i samo u slučaju incidenta kada je neophodno izvršiti oporavak sistema.

Unapređenje softvera podrazumeva redovno ažuriranje softvera radi poboljšanja performansi sistema i primenom veštačke inteligencije (mašinsko učenje).

Organizacione mere zaštite

Upravljanje korisničkim nalozima podrazumeva definisanje privilegija za svakog policijskog službenika sa ovlašćenjem da pristupa snimljenom materijalu i neophodno je utvrditi/propisati odgovarajući nivo pristupa u skladu sa radnim mestom, tj. pozicijom u okviru organizacione jedinice. Na primer, samo određeni službenici (sistem administratori) bi trebalo da imaju administratorski pristup sistemu koji omogućava naprednije opcije, poput kreiranja i brisanja naloga za druge službenike, dok ostali mogu dobiti ulogu koja im omogućava da samo pregledaju snimke, odnosno naloge bez mogućnosti preuzimanja, izmene ili brisanja materijala. Nadređenim službenicima se mora omogućiti softversko generisanje korisničkih naloga za pretragu ili kreiranje naloga za pretragu.

Softversko generisanje naloga za pretragu podrazumeva softverski definisan pristupni zahtev, kako bi prilikom svakog pristupa bilo vidljivo/jasno na osnovu kog ili čijeg zahteva, odnosno naloga se postupa.

Mere zaštite od rizika koji nastaju pri promeni poslova ili prestanka radnog odnosa podrazumevaju da nakon prestanka radnog odnosa ili premeštanja na drugo radno mesto u okviru Ministarstva, korisnički nalozi za pristup sistemu kojima je isteklo ovlašćenje moraju biti deaktivirani i arhivirani, tj.mora biti onemogućen pristup sistemu sa tih naloga u najkraćem mogućem roku.

Sistem podeljenih uloga u obradi podataka o ličnosti podrazumeva da jedan policijski službenik ne može samostalno, bez učešća drugih ovlašćenih službenih lica, da preduzme radnje obrade biometrijskih podataka, čime se u velikoj meri smanjuje mogućnost zloupotrebe i verovatnoća nastupanja rizika. Prikupljanje podataka obavlja lice koje je raspoređeno u okviru jedne organizacione jedinice, a dalju obradu podataka vrše druga službena lica koja su raspoređena u drugim organizacionim jedinica. Sistem podeljenih uloga kao organizaciona mera podrazumeva da sistem video nadzora bude kreiran tako da može da bude funkcionalan samo u sistemu podeljenih uloga. To znači da u prikupljanju i daljoj obradi podataka u kontekstu procene nivoa izvesnosti nastupanja rizika, jednostavno nije moguće organizaciono, tehnički i pravno zamisliti situaciju u kojoj se izvan sistema podeljenih uloga donosi odluka o preduzimanju radnji obrade.

Primenom ove organizacione mere efikasno se sprečava eventualni individualni pokušaj zloupotrebe policijskih ovlašćenja, i to zbog toga što jedno ovlašćeno lice nikada ne može

samo, bez učešća drugih ovlašćenih lica, da preduzme sve radnje obrade na koje upućuju rizici navedeni u prethodnom poglavlju. Na taj način se u najvećoj meri minimizuje verovatnoća nastupanja rizika.

Sistem podele uloga u sistemu video nadzora zasniva se na Pravilniku o unutrašnjem uređenju i sistematizaciji radnih mesta u Ministarstvu unutrašnjih poslova. Ovim aktom uređuje se nadležnost pojedinih organizacionih jedinica Ministarstva, kao i opis poslova i zadataka za pojedinačno radno mesto, što uključuje i propisivanje opštih i posebnih uslova za raspoređivanje na radno mesto.

Zaposleni, raspoređeni na pojedinim radnim mestima, u sistemu video nadzora sa ovlašćenjima da prikupljaju i dalje obrađuju podatke, imaju status ovlašćenih službenih lica. U vršenju svojih poslova i zadataka oni su raspoređeni po organizacionim jedinicama Ministarstva.

U svakoj od organizacionih jedinica Ministarstva, svakom ovlašćenom licu dodeljuje se unapred određeni nivo odlučivanja, odnosno ovlašćenje za preduzimanje pojedinih radnji obrade. Tako pojedina ovlašćena lica imaju i ulogu kontrole izvršavanja poslova i zadataka.

U sistemu video nadzora kojim rukuje Ministarstvo, svaku radnju obrade vrši lice koje je ovlašćeno za preduzimanje te radnje. Pri tome, ni jedno od angažovanih lica nema ovlašćenje za preduzimanje svih radnji obrade. Tako, na primer, ovlašćenje za prikupljanje podataka ima samo lice koje je raspoređeno u okviru jedne organizacione jedinice, dok ovlašćenja za obradu i korišćenje biometrijskih podataka kao i za odlučivanje o neophodnosti preduzimanja drugih mera i radnji koje treba da dovedu do identifikacije jednog lica, imaju druga službena lica koja su raspoređena u više različitih organizacionih jedinica.

Kontrolu zakonitosti, odnosno pravilnosti vršenja ovlašćenja, neposredno vrše ovlašćena lica koja rukovode pojedinim organizacionim jedinicama, Sektor unutrašnje kontrole, kao i organizacione jedinice nadležne za poslove kontrole zakonitosti rada. Ovakva kontrola, između ostalog, obezbeđena je evidentiranjem svake radnje obrade, odnosno tehničkim omogućavanjem utvrđivanja činjenica koje se odnose na korišćenje sistema u svakom konkretnom slučaju (sistemski žurnal).

Praćenje primene zakona i drugih propisa koji se odnose na zaštitu podataka o ličnosti u okviru Ministarstva i kontrolu primenjenih mera zaštite vrši lice za zaštitu podataka o ličnosti u Ministarstvu, u saradnji sa drugim policijskim službenicima, koje odredi ministar.

Primena tehničkih mera zaštite takođe je zasnovana na sistemu podeljenih uloga i to prema nadležnostima različitih organizacionih jedinica.

Informisanje građana podrazumeva da se licima, pored informisanja, mora omogućiti i konkretno ostvarivanje prava u vezi sa obradom podataka o ličnosti (pravo na uvid, kopiju, brisanje ili druga prava u skadu sa zakonom). Informisanje mora da sadrži i obaveštavanje o načinu ostvarivanja prava kod rukovaoca (npr. podnošenjem zahteva Ministarstvu, teritorijalno nadležnoj policijskoj upravi, po mestu lokacije kamera, odnosno mestu snimanja).

Disciplinovanost i savesnost policijskih službenika zakonito i profesionalno postupanje policijskih službenika obezbeđuje se primenom proaktivnih i reaktivnih mera zaštite kojima se podiže nivo svesti o neophodnosti zaštite bezbednosti podataka i poštovanja prava i sloboda lica, što u najvećoj meri umanjuje verovatnoću nastupanja rizika.

Preventivne mere podrazumevaju bezbednosne provere kandidata za prijem u radni odnos i zaposlenih u Ministarstvu, kontinuiranu edukaciju ovlašćenih policijskih službenika i to u vezi sa primenom odredbi zakona i drugih propisa koji se odnose na zaštitu podataka o ličnosti.

Poslovi edukacije vrše se u skladu sa Uredbom o stručnom osposobljavanju i usavršavanju u Ministarstvu, na osnovu Programa stručnog usavršavanja policijskih službenika Ministarstva i Direktive o načinu obavljanja poslova u vezi sa zaštitom podataka o ličnosti u Ministarstvu.

Reaktivne mere se primenjuju u slučaju povrede bezbednosti podataka, odnosno prava lica. Prva grupa ovih mera odnosi se na povredu bezbednosti podataka, i to bez obzira na to da li je u konkretnom slučaju na povredu bezbednosti reagovano drugim mehanizmom zaštite. Primena mera iz ove grupe propisana je zakonom i Uputstvom o načinu vođenja evidencije i obaveštavanja o povredama podataka o ličnosti u Ministarstvu. Druga grupa ovih mera jesu disciplinske mere i one su propisane Zakonom o policiji. Treću grupu mera koje su propisane Zakonom o zaštiti podataka o ličnosti i Krivičnim zakonikom primenjuje Ministarstvo, tužilaštvo i sud. Četvrtu grupu čine mere koje primenjuje Poverenik za slobodan pristup informacijama od javnog značaja i zaštitu podataka o ličnosti, u skladu sa zakonom.

Mehanizmi zaštite prava lica podrazumevaju da svako lice čije podatke obrađuje Ministarstvo, može da se obrati zahtevom za ostvarivanje, odnosno zaštitu prava u skladu sa zakonom. Mehanizam kontrole postupanja po zahtevima lica čiji se podaci obrađuju takođe se poverava licu za zaštitu podataka o ličnosti u ministarstvu.

VII MIŠLjENjE LICA ZA ZAŠTITU PODATAKA O LIČNOSTI

U skladu sa članom 54. i članom 58. Zakona o zaštiti podataka o ličnosti, u Ministarstvu je sačinjen ovaj dokument, a od strane Lica za zaštitu podataka o ličnosti data preporuka da se dokument dostavi na mišljenje Povereniku za informacije od javnog značaja i zaštitu podataka o ličnosti kao i da se u celini ili skraćenom obliku javno objavi na internet stranici Ministarstva ili se na drugi prigodan način učini dostupnim javnosti.

Takođe, data je preporuka je da se ovaj dokument prezentuje prilikom nastavka javne rasprave na Nacrt zakona o unutrašnjim poslovima i na Nacrt zakona o obradi podataka u oblasti unutrašnjih poslova.

Imajući u vidu da je procena uticaja nameravanih radnji obrade biometrijskih podatka o ličnosti na zaštitu podataka o ličnosti, izvršena u postupku za donošenje zakona, preporuka je da se dokument, nakon sprovedene procedure pribavljanja mišljenja drugih organa, dostavi i Vladi Republike Srbije prilikom dostavljanja predloga pomenutih Nacrta zakona.

Na kraju, Lice za zaštitu podataka o ličnosti, napominje da je nakon donošenja zakona, a pre početka obrade biometrijskih podataka potrebno izvršiti ažuranje ove procene uticaja, imajući u vidu da nameravane radnje obrade biometrijskih podataka o ličnosti podrazumevaju upotrebu novih tehnologija eventualno formiranje novih zbirki podataka.

U Beogradu
27.04.2023. godine
Broj: 07-7-117/23

v.d. SEKRETARA MINISTARSTVA

Miroslav Panić