

VEŠTAČKA INTELIGENCIJA U SLUŽBI SPROVOĐENJA ZAKONA U EVROPSKOJ UNIJI I REPUBLICI SRBIJI

Zorančo Vasilkov³³

doi: 10.59864/Oditor72501ZV

Pregledni rad
UDK: 340.134:004.8(497.11)
340.134:004.8(4-6EU)

Apstrakt

Veštačka inteligencija od nedavno intenzivno pomera granice razvoja ljudske civilizacije i tehnološkog razvoja. Kao tehnološko dostignuće, ona se neprimetno „ušunjala“ u život svakog pojedinca i postala sastavni deo svih sfera društvenog života. U primeni veštačke inteligencije danas kao da ne možemo da se otmemo utusku da ono što je u jednom trenutku izgledalo moguće za sto godina, u stvari je postalo realnost u poslednjih desetak godina. Potreba za pravnom regulacijom i zakonskim uređenjem korišćenja veštačke inteligencije se nameće kao važno pitanje za njen budući razvoj u korist ljudske zajednice i celokupnog čovečanstva. Ovo istraživanje je deo šire slike o potencijalnoj upotrebi veštačke inteligencije u pojedinim granama prava, usmereno ka sagledavanju posebnog „interregnuma“ između uspostavljene prakse korišćenja veštačke inteligencije i njene pravne regulacije. U radu se posebno fokusiramo na analizu i istraživanje upotrebe sistema veštačke inteligencije u oblasti sprovođenja zakona. Tačnije, osvetličemo regulatorni proces vezan za veštačku inteligenciju u EU i ukazati na specifičnosti njene upotrebe u bezbednosne i policijske svrhe, pre svega uspostavljanjem ograničenja u korist javnosti i građana, kategorizacijom upotrebe pojedinih sistema veštačke inteligencije kao zabranjeni i visokorizični. Radi se o sistemima veštačke inteligencije koji koriste tehnike predviđanja, biometrijskog nadzora odnosno prepoznavanja lica i izvedenih biometrijskih podataka. Njihov uticaj na ljudska prava je predmet posebnog dubinskog istraživanja van ovog okvira, imajući u vidu da se nekontrolisana upotreba ovih tehnika kao deo sistema veštačke inteligencije danas može poistoveti sa posledicama bacanja „atomske bomba“ na čovekove slobode i prava. Osim regulatornog procesa unutar EU, ukazujemo i na potencijalnu upotrebu veštačke inteligencije u Srbiji od strane službi za sprovođenje zakona kroz analizu pravnog okvira Republike Srbije.

Ključne reči: veštačka inteligencija, sprovođenje zakona, policijsko predviđanje, prepoznavanje lica, biometrijske tehnike

JEL: K33

³³ Docent, dr Zorančo Vasilkov, Poslovni i pravni fakultet, Univerzitet MB, E-mail: vasilkovzoranco@yahoo.com, <https://orcid.org/0000-0001-8282-2777>

Uvod

Veštačka inteligencija je tehnološko dostignuće čija primena u svim oblastima ljudskog delovanja postaje neizbežna, kako globalno, tako regionalno i lokalno. Time na scenu stupa „trka“ za pravnu regulaciju i zakonsko uređenje korišćenja veštačke inteligencije kao ključno pitanje za njen budući razvoj u korist ljudske zajednice i celokupnog čovečanstva. Debate o potrebi, načinu i metodama pravne regulacije se odvijaju na raznim nivoima od međunarodnog, preko regionalnih organizacija i nacionalnog nivoa do privatnog sektora i tehnoloških giganta koji već čine dostupnim pojedine oblike veštačke inteligencije svim građanima na dnevnom nivou. Pravna regulacija se pre svega odnosi na razne aspekte primene veštačke inteligencije i može se posmatrati i kao uspostavljanje „pravne infrastrukture“ za njeno korišćenje, upotrebu, razvoj i monitoring u svim oblastima društvenog života.

Ovim radom autor istražuje pravnu regulaciju i potencijalnu upotrebu veštačke inteligencije u osetljivoj oblasti prava, usmeravajući se na sagledavanje već uspostavljene prakse za korišćenje veštačke inteligencije u sprovođenju zakona. Tačnije, osvetlićemo regulatorni proces vezan za veštačku inteligenciju u EU i fokusirati se na upotrebu veštačke inteligencije u bezbednosne i policijske svrhe, ukazujući na ograničenja uspostavljena u korist javnosti i građana koja se nameću službama za sprovođenje zakona kategorizacijom određenih postupanja kao zabranjena i visokorizična. Polazimo od pravne infrastrukture za veštačku inteligenciju koja se uspostavlja predloženom Uredbom EU o utvrđivanju usklađenih pravila o veštačkoj inteligenciji koja se često naziva i Zakon o veštačkoj inteligenciji ili Akt o veštačkoj inteligenciji.

Bezbednost i policijsko postupanje treba da obezbede ambijent, siguran i lišen bilo kog straha po svakog pojedinca, u kom su ljudska prava i osnovne slobode zaštićeni od maliciozne upotrebe veštačke inteligencije, imajući u vidu da službe za sprovođenje zakona poseduju systemska, diskreciona i javna ovlašćenja sa visokim stepenom rizika za potencijalnu zloupotrebu veštačke inteligencije. Veliki broj istraživanja na globalnom nivou ukazuje na opasnosti po ljudska prava i osnovne slobode u slučaju primene veštačke inteligencije u bezbednosne svrhe, posebno u slučajevima biometriskog prepoznavanja i otkrivanja nepoželjnog ponašanja pojedinaca. Osim regulatornog procesa unutar EU, sagledavamo i upotrebu veštačke inteligenciju u ovoj oblasti u Srbiji kroz analizu pravnog okvira odnosno Strategije Republike Srbije i drugih nacionalnih akata mekog prava o veštačkoj inteligenciji (u daljem tekstu: VI).

Uspostavljanje pravne infrastrukture i definisanje zabranjenih i visokorizičnih sistema VI

Pravna infrastruktura je termin koji se koristi u novijim istraživanjima i označava uspostavljanje pravnog okvira i regulacija određene oblasti društvenog ponašanja

odnosno normiranje i donošenje pravnih akata kao osnova uređenja i stvaranja uslova za dalji razvoj te oblasti. Infrastrukture u običnom govoru se odnose na fizičke ili organizacione aspekte sveta koji su društvima potrebni da bi funkcionisala. Metafora prava kao infrastrukture nastaje u spajanju odnosno ozbiljnog shvatanja prava kao društveno-materijalni oblik, s jedne strane ostvaren kroz društveno delovanje, ali s druge značajno preoblikujući svet oko nas (Byrne, Gammeltoft-Hansen, 2023). Ovaj termin je odvojen i ne treba ga mešati sa stvarnom elektronskom, digitalnom i informatičkom infrastrukturom kao materijalnom bazom razvoja VI. Pravna infrastruktura u konkretnom slučaju naglašava značaj pravne regulacije i razumevanja neophodnosti za normativno uređenje korišćenja VI posebno ako potrebu, način i metode pravne regulacije shvatimo kao „uslov nad uslovima“ za funkcionisanje društva odnosno, kao infrastrukturnu pripremu i radove na definisanju ogromne oblasti koja organizacijski zahteva uspostavljanje savremenog pravnog „auto puta sa velikim dozvoljenim brzinama“. Bezbednost i sprečavanje rizika od ugrožavanja ljudskih života nameće i definisanje striktnih „ograničenja brzine i pojedinih obaveznih pravaca kretanja“ koji su istinski neophodni kako se razvoj i upotreba VI ne bi pretvorile u kaos, pretnju i ugrožavanju opstanka čovečanstva. Balans između mogućnosti daljeg brzog razvoja VI u korist svakog pojedinaca i maksimalnog smanjenja rizika od nekontrolisanog „kretanja ili iskakanja“, danas znači omogućiti, podstaći i usmeriti njen dalji budući razvoj u oblastima ekonomije, medicine, javnog zdravlja, ekologije, proizvodvodnje hrane, snabdevanja, energetike itd. Željom da veštačka inteligencija potpuno poboljša način na koji ljudi razmišljaju, stvaraju i kreću se u stvarnom svetu, govori i o izgradnja jednog budućeg „naučnog auto puta sa mnoštvom traka“(Prlja et al.,2021:96).

Uspostavljanje pravne infrastrukture za VI, odnosno pripremni radovi za njeno definisanje, se ubrzano odvijaju u međunarodnim organizacijama kao i unutar formalnih i neformalnih skupova i koalicija država. Na primer, preispitivanja etičkih dilema korišćenja VI i smernice Ujedinjenih nacija su dati u Uneskovom vodiču (UNESCO, 2022), dok su prve smernice za upotrebu VI u sprovođenju zakona predstavljene od strane Interpola i Međuregionalnog instituta za istraživanje kriminala i pravde UN (Interpol&UNICRI, 2019). Regionalne organizacije, pre svega Savet Evrope i Organizacija za ekonomsku saradnju i razvoj - OECD su uvojile preporuke (OECD, 2022) oko modaliteta, načina i stepena obuhvata korišćenja VI i sa državama članicama pripremaju konvencije (Council of Europe, 2023) ili vodiče za upotrebu VI u različitim sferama društvenog života. Države su takođe uključene u nacionalno definisanje okvira za primenu VI u čemu prednjače SAD (White House Office of Science and Technology Policy, 2022) i Kina The China Academy of Information and Communications Technology, 2022), a u međunarodnim okvirima je otpočelo grupisanje i održavanje samita država koje podstiču inovacije u oblasti VI i zakonski ili kroz nacionalne strategije regulišu razvoj VI. U sve to je uključen

privatni sektor i tehnološki giganti od kojih većina nije oduševljena nametanjem međunarodnog i nacionalnog okvira regulacije, imajući u vidu da su već učinile dostupnim pojedine oblike veštačke inteligencije svim građanima na dnevnom nivou. Ne mali doprinos kako razvoju VI tako i celokupnom postupku pravne regulacije daje i akademska zajednica u okviru koje postoje istraživački instituti kao što je Institut za VI usmerenu na čoveka Univeziteta Stenford koji vodi sveukupni godišnji globalni indeks razvoja, napredka i pravne regulacije VI (Maslej, et al., 2024).

U ovakvoj globalnoj konstelaciji, od svih pokušaja uspostavljanja pravne infrastrukture za korišćenje VI najdalje je otišla EU u okviru koje je u završnoj fazi zakonodavni postupak za usvajanje Uredbe o VI (COM/2021/ 206, u daljem tekstu: Uredba o VI ili Uredba). Naime, Evropski parlament je u okviru redovne zakonodavne procedure usvojio Zakonodavnu rezoluciju (Evropski Parlament, 2024) i čeka se potvrda i njeno usvajanje u Savetu EU. Dogovor institucija EU o ovom aktu je postignut krajem 2023 godine i u prvim reakcijama na vest o usvajanju regulative ističe se da interes građana ipak nije stavljen na prvo mesto i da su uveden dvostruki standardi za policiju i službe bezbednosti, sa dovoljno mogućnosti za kršenje ljudskih prava (Share Fondacija, 2024). Ipak, nisu beznačajne izmene izvršene u poslednjem trenutku uvođenjem obavezne procene uticaja na osnovna prava za visokorizične sisteme VI, obavezujući one koji ih koriste da procene i ublaže predvidive uticaje na osnovna prava onih koji su pogođeni, posebno marginalizovanih i ranjivih grupa. To se odnosi i na uvođenje prava pojedinaca da podnose žalbe nadležnim organima u vezi sa mogućim kršenjem Uredbe o VI (Friedl, Gasiola, 2024.).

Uredba daje definiciju samih sistema VI kao „mašinski sistem dizajniran za rad na različitim nivoima autonomije, koji nakon uvođenja može pokazati prilagodljivost i koji, za eksplicitne ili implicitne ciljeve, iz ulaznih vrednosti koje prima, zaključuje kako generisati izlazne vrednosti kao što su predviđanja, sadržaj, preporuke ili odluke koji mogu uticati na fizička ili virtualna okruženja“ (član 3, tačka 1 Uredbe). U Uredbi je istaknut pristup razvoja i upotrebe VI zasnovan na riziku a sami sistemi VI su kategorisani u različite klase i podležu različitim pravilima u skladu sa stepenom rizika koji se pretpostavlja da predstavlja po pojedince i društvo u celini. Uredba o VI postavlja različita ograničenja za sisteme VI koji bi mogli da se koriste u oblasti sprovođenja zakona. Sistemi za koje se smatra da predstavljaju „neprihvatljiv rizik“, kao što su takozvani sistemi „socijalnog bodovanja“ ili određene vrste biometrijskog nadzora, zabranjeni su u potpunosti (čl. 5 Uredbe). Najveći broj sistema VI koje se koriste od službi za sprovođenje zakona u bezbednosne i policijske svrhe je smešten u neprihvatljivu, odnosno zabranjenu ili strogo kontrolisanu, visokorizičnu praksu. Zabranjenu praksu korišćenja sistema VI čine: manipulativne ili obmanjujuće tehnike, iskorištavanje bilo koje slabosti pojedinaca ili određenih grupa, evaluacija ili klasifikacija fizičkih lica ili grupe lica u određenom periodu na osnovu njihovog

društvenog ponašanja, procena ili predviđanje verovatnoće da će fizičko lice počiniti krivično delo isključivo na osnovu izrade profila fizičkog lica ili procene negovih osobina i obeležja ličnosti, baze podataka za prepoznavanje lica neciljanim prikupljanjem fotografija lica s interneta ili snimaka CCTV-a, izvođenje zaključaka o emocijama fizičkog lica na radnom mestu i u obrazovnim ustanovama, biometrijska kategorizaciju u kojima se fizička lica pojedinačno kategorizuju na osnovu biometrijskih podataka o njihovoj rasi, političkim mišljenjima, članstvu u sindikatu, verskim ili filozofskim uverenjima, seksualnoj orijentaciji kao i biometrijska identifikacija pojedinaca u realnom vremenu. Daljinska biometrijska identifikacija u realnom vremenu može se koristiti samo ako je njena upotreba vremenski i geografski ograničena i ako je prethodno data posebna sudska ili administrativna dozvola. Uredbom su definisana tri izuzetka za daljinsku biometrijsku identifikaciju u svrhu krivičnog gonjenja za krivična dela koja sadrže visok stepen društvene opasnosti i to: 1) ciljane potrage za konkretnim žrtvama otmice, trgovine ljudima ili seksualnog iskorištavanja ljudi, kao i potrage za nestalim osobama; 2) sprečavanja konkretne, značajne i neposredne pretnje životu ili telesnoj bezbednosti fizičkih lica ili stvarne i prisutne ili stvarne i predvidljive pretnje od terorističkog napada; i 3) lociranja ili identifikacije lica osumnjičenog za izvršenje krivičnog dela u svrhu vođenja krivične istrage, progona ili izvršenja krivične sankcije za krivična dela nabrojana u Prilogu 2 a koja su državama članicama kažnjiva kaznom zatvora ili merom oduzimanja slobode u maksimalnom trajanju od najmanje četiri godine (član 5, stav 1, tačka h Uredbe).

Visokorizična praksa ili kategorizacija sistema VI na visokorizične obuhvata ispunjenje strogih zahteva za njihovu upotrebu uvođenjem dopunskih pravila regulacije i kontrole. Razlika između neprihvatljivih ili zabranjenih sistema VI i visokorizičnih je u tome što se drugi ne smatraju toliko opasnim, odnosno ne predstavljaju toliko visok stepen rizika po ljudska prava da ih je neophodno zabraniti. Tu se u najvećem broju nalaze sistemi VI koji se koriste u sprovođenju zakona odnosno, oblasti policije, sudstva i kritične infrastrukture (Prilogu 3 Uredbe).

Zabranjena i visokorizična praksa upotrebe VI u sprovođenju zakona oslanja se pre svega na razvoj i primenu određenih komponenata VI vezane za obradu velike količine podataka, algoritme i naprednu kompjutersku tehnologiju. Ove komponente su ranije podsticane radi promene, primene i preispitivanja tehnika pametnog nadzora, profilisanja, upotreba velikog broja podataka i što šire digitalizacije javnog sektora (Fuster, 2020:21). Generalno, VI se povezuje i klasifikuje po unapređenim grupisanjem algoritama koji se koriste za razvoj tehnologije, prema teorijskim konceptima koji stoje iza njih a koji su prvenstveno nastali u matematici, logici, filozofiji i teoriji informacija (Samoili, 2021:11). Postoje razne teorije koje ističu subjektivnost ljudske percepcije iz perspektive prava, za to šta je autonomno i inteligentno u računskim procedurama

ukazivanjem na jednostranost u upotrebi termina koji će se menjati u budućnosti. Naime, ono što je tokom 80 godina prošlog veka spadalo u te kategorije danas nije ni inteligentno ni autonomno. Zato se Kodagnoneu (Codagnone) VI kao pojam čini neprikladnim za regulaciju zakonskim i podzakonskim aktima, već bi legislativno trebalo urediti algoritame koji su u osnovi sistema VI. Shodno tome, pravni akti koji su već donešeni i uređuju algoritamske procese i donošenje odluka u različitim scenarijima i sa različitim svrhama su povezani sa izgradnjom i sastavni su deo regulatornog okvira za VI u EU (Codagnone et al., 2022:46). Algoritmi su naime, moćni artefakti koji deluju unutar našeg informacionog miljea, vršeći strukturiranje naših podataka, profilisanje, kategorizaciju, i predviđanje ko smo, šta smo, šta želimo, pa i više od toga (Hayes et al., 2020).

Izazovi upotrebe sistema VI u sprovođenju zakona sa aspekta predviđanja i upotrebe posebnih biometrijskih tehnika

Upotreba algoritama u oblasti policijskog postupanja i bezbednosti, je posebno osetljivo pitanje sa velikim potencijalom za unapređenje mera i postupaka u sprovođenju zakona, ali i sa ogromnim rizikom za nanošenje štete i kršenje ljudskih prava (Hayes et al., 2020:1). Jedna od prvih tehnika korišćenja algoritama u oblasti bezbednosti, tančije u policijskom postupanju a koja predhodi upotrebi sistema VI je policijsko predviđanje (inače zabranjeno članom 5, tačka d. Uredbe). Policijsko predviđanje je algoritamska obrada skupova podataka koja otkriva obrasce verovatnih budućih krivičnih dela i ugrožavanja radi njihovog sprečavanja pre samog izvršenja. Ono može da se podeli u četiri šire kategorije kao što su: 1) metodi za predviđanje krivičnih dela ili mesta i vremenski periodi u koje postoji povećani rizik od pojave kriminalnih aktivnosti; 2) metodi predviđanja i otkrivanje mogućih učinilaca krivičnih dela; 3) metodi predviđanja identiteta učinilaca ili kreiranje profila sličnim učiniocima krivičnih dela u prošlosti; i 4) predviđanje žrtava krivičnih dela odnosno identifikovanje grupa i individua za koje postoji verovatnoća da će postati žrtve krivičnog dela (Perry et al., 2013:xiv). Policijsko predviđanje kao nova tehnika za sprečavanje kriminala se pojavljuje u SAD krajem 20. veka, kada se u policijskim upravama pojedinih velikih gradova angažuju profesionalni analitičari kriminala koji eksperimentišu sa obradom velikog broja podataka i korišćenjem novih tehnologija, pokušavajući da predvide događaje, tačnije, vreme, mesto i sama krivična dela koja će biti učinjena kao i potencijalne učinioce. Kasnije je u Velikoj Britaniji razvijen poseban model policijskog predviđanja pod nazivom Matriks nasilja bandi (Gang Violence Matrix) koji je policija Londona počela da koristi 2012 godine. Ovaj model je služio za identifikovanje i procenu rizika članova bandi uključenih u nasilju kao i identifikaciju ranjivih grupa odnosno onih ka kojima je nasilje usmereno. U drugim državama članicama EU pojavljuje se u sprovođenju zakona u oblasti pranja novca i finansiranja terorizma, kada su na nivou EU bankama i drugim pravnim licima nametnute obaveze preduzimanja odgovarajućih korake za

identifikaciju faktora rizika za procenu izvršenja pomenutih krivičnih dela (Fuster, 2020:23).

Prepoznavanje lica je biometrijska tehnika u rapidnom razvoju, koja je u Uredbi uvršćena u dve kategorije, odnosno pominje se kao zabranjena odnosno visokorizična praksa korišćenja VI u oblasti sprovođenja zakona. Tehnologija prepoznavanja lica kao deo sistema VI omogućava automatsku identifikaciju ili potvrdu autentičnosti pojedinca putem upoređivanja i potvrđivanja crta lica sa dve ili više digitalnih slika (EU FRA, 2019:2). To je proces kojim AI softver može da identifikuje ili prepozna osobu koristeći njene biometrijske crte lica izvučene sa fotografije ili video snimka (Gikay, 2023:417). Iako je prepoznavanje lica tehnologija koja postoji već nekoliko decenija, tehnički napredak u poslednjih nekoliko godina je ogroman. Neki od današnjih algoritama za prepoznavanje lica sa najboljim performansama imaju skoro 100% uspeha na izazovnim skupovima podataka. Nacionalni institut za standarde i tehnologiju SAD (National Institute of Standards and Technology (NIST)) je napravio test za prepoznavanja lica (Face Recognition Vendor Test (FRVT)) mereći napredak u prepoznavanju lica i koliko dobro algoritmi izvršavaju različite zadatke vezane za bezbednost i sprovođenja zakona, a odnose se konkretno na prepoznavanje lica sa fotoreporterskih slika, u svrhu identifikacije žrtve trgovine decom, otkrivanja falsifikovanih pasoša i unakrsne provere slike izdate vize. Napredak algoritma u prepoznavanju lica se meri prema lažnoj stopi nepodudaranja ili stopi greške koja predstavlja učestalost sa kojom algoritam ne uspeva da uskladi sliku sa stvarnom osobom. U 2017. najuspešnija prepoznavanja lica su imali stope greške od preko 50,0% dok od 2021. nije registovana stopa greške veća od 3,0%. Model sa najboljim učinkom u svim skupovima podataka u 2021 (fotografije vize) registrovao je stopu greške od 0,1%, što znači da za svakih 1000 lica, model je tačno identifikovao 999. Posebno zabrinjavajuća je upotreba ove tehnologije putem sistema VI, odnosno prepoznavanje lica i detekcija pojedinaca uživo u realnom vremenu. Softver VI upoređuje, u realnom vremenu, biometrijske slike lica snimljene kamerom sa postojećim šablonima osumnjičenog lica u bazi podataka. Stepem rasprostranjenosti upotrebe sistema prepoznavanja lica je indikativan imajući u vidu da u SAD danas, 18 od 24 vladinih agencija za sprovođenje zakona već koriste neku vrstu tehnologije za prepoznavanje lica (Zhang et al., 2022:62). Izveštaji iz SAD još od 2016 ukazuju na rasprostranjenu upotrebu prepoznavanja lica uživo, upozoravajući da je tada nekoliko velikih policijskih uprava aktivno istraživalo prepoznavanje lica u realnom vremenu na video snimcima kamere za nadzor uživo. Od tada je sve češće izričito pozivanje na donošenje zakona koji bi regulisao upotrebu prepoznavanja lica od strane organa za sprovođenje zakona, upozorenjem da je „prepoznavanje lica previše moćno da bi ostalo tajno“ i pravno nedefinisano (Garvie et al., 2016).

Sa druge strane Vlada Velike Britanije pozvala je policiju da proširi upotrebu tehnologija baziranih na VI i pored činjenice da ovakvi sistemi ugrožavaju

građanske slobode. U jednoj britanskoj nacionalnoj anketi iz 2019., 70% ispitanika je istaklo da policiji treba dozvoliti da koristi prepoznavanje lica u krivičnim istragama, a 71% je podržalo njegovu upotrebu na javnim prostorima, ako pomaže u smanjenju kriminala. Ilustrativan je primer akcije sprečavanja krađa i nasilja u maloprodajnim objektima u Londonu 2023. godine, u kojoj je Metropoliten policija koristila prepoznavanje lica za identifikaciju 149 osumnjičenih za maloprodajne zločine upoređivanjem stotine CCTV fotografija (Gikay, 2023). Trenutno su dostupne samo ograničene informacije o mogućoj upotrebi tehnologija prepoznavanja lica u državama članicama EU. U Nemačkoj je Hamburška policija koristila tehnologije za prepoznavanje lica demonstranata koji su izazvali nered zbog Samita G20 u julu 2017. dok je 2018. sprovedeno testiranje mogućnosti upotrebe ovih sistema na železničkoj stanici u Berlinu (Engel, 2024). Policija u Nici (Francuska) sprovela je test korišćenja tehnologije za prepoznavanje lica uživo na karnevalu 2018. Žandarmerija u Francuskoj koristi tehnologije za prepoznavanje lica za krivične istrage, ali ne koristi tehnologije prepoznavanja lica uživo, zbog nepostojanja pravnog osnova. Austrijske vlasti su kupile softver za prepoznavanje lica 2019. za pretraživanje baze podataka kako bi se identifikovali nepoznati počinioci krivičnih dela čije su slike dostupne sa CCTV-a kamera ili drugih izvora. U Holandiji su takođe počela testiranja za upotrebu tehnologije prepoznavanja lica (EU FRA, 2019:6). Neke studije ukazuju i na buduću upotrebu 3D tehnologije za prepoznavanje lica i to u oblasti kontrole spoljnih granica Unije od strane Fronteksa. Dok se trenutne tehnologije za prepoznavanje lica oslanjaju na „ravnu“ fotografiju lica pojedinca, 3D prepoznavanje lica koristi trodimenzionalne karakteristike ljudskog lica za automatsko prepoznavanje i uparivanje. Kada se stekne 3D geometrija ljudskog lica, onda se izdvajaju značajne karakteristike sa površine lica. To omogućava veću preciznost od klasičnog dvodimenzionalnog prepoznavanja lica (Statewatch, 2023:37).

Suštinski prepoznavanje lica predstavlja samo jedan mozaik šireg korišćenja biometrije u bezbednosne svrhe. Postoje biometrijske tehnike koje uključuju biometrijsku identifikaciju, biometrijsku kategorizaciju, detekciju ponašanja, prepoznavanje emocija, interfejsi mozga i računara i druge slične tehnike koje imaju širok spektar namena. Termin „biometrijske tehnike“ treba shvatiti tako da uključuju bilo koju tehnologiju ili operaciju koja se: 1) oslanja na specifičnu tehničku obradu podataka koji se odnose na fizičke, fiziološke aspekte ili aspekte ponašanja ljudskog tela (uključujući i kada je u pokretu); i 2) za svrhe kao što su autentifikacija ili identifikacija ljudskih individua, kategorizacija ljudskih individua prema trajnim ili dugoročnim karakteristikama (uključujući u cilju predviđanja budućeg ponašanja) ili otkrivanje privremenih ili trajnih stanja ljudske individue (kao što je strah, umor, ili bolest, ili određena namera). Napominje se međutim sve veća upotreba „slabe“ i „meke“ biometrije zajedno sa „jakom“ biometrijom, fokusirajući se na niz obrazaca različitih vrsta ponašanja, i

razvoj ka multimodalnoj biometriji. Zajedno sa poboljšanim senzorskim i računarskim mogućnostima, kao i poboljšanom vezom, ovo utire put za masovno uvođenje biometrijskih tehnologija u širok spektar sektora i za širok spektar namena, čak daleko izvan sprovođenja zakona i graničnih kontrola, pretvarajući biometrijske tehnologije u nešto poput univerzalnih tehnologija. (Wendehorst, Duler, 2021:1).

Druga istraživanja nalaze da se radi o mnoštvu tehnologija prepoznavanja lica kao specifičan tip biometrijskih tehnologija koje se koriste u različite svrhe, u rasponu od jednostavnog otkrivanja prisustva lica na slici, do složenijih verifikacija, identifikacija i kategorizacija ili klasifikacija pojedinaca. **Verifikacija** (poređenje jedan na jedan) omogućava poređenje dva biometrijska šablona, za koje se obično pretpostavlja da pripadaju istoj osobi. **Identifikacija** (poređenje jedan prema više) znači da se šablon slike lica osobe upoređuje sa drugim šablonima uskladištenim u bazi podataka kako bi se otkrilo da li je njihova slika tamo uskladištena. Prepoznavanje lica se takođe koristi za vršenje **kategorizacije** (ili klasifikacije) pojedinaca, na osnovu njihovih ličnih karakteristika. U tom smislu, razvijen je širok spektar softvera za procenu atributa osobe sa njenog lica, u svrhu „klasifikacije atributa lica“ (npr. pol, rasa ili etnička pripadnost) ili za „procenu atributa lica“ (npr. godine). Štaviše, prepoznavanja lica se može koristiti za klasifikaciju izraza lica (kao što je osmeh) ili emocionalnog stanja osobe kao što je srećan, tužan ili ljut (Madiaga, Mildebrath, 2021:1).

Slika 1. Prepoznavanje emocija u realnom vremenu.



Izvor: Article 19. <https://www.article19.org/resources/eu-emotion-misrecognition/>

Ovo poslednje je istraživano na spoljnim granicama EU, tačnije na pojedinim graničnim prelazima Grčke, Mađarske i Letonije u okviru projekta Horizont 2020, pod nazivom Integrirani prenosni sistem kontrole (iBorderCtrl) koji integriše prepoznavanje lica i druge tehnologije za otkrivanje da li pojedinac govori istinu. Ispitivani su i identifikovani tzv. „biomarkeri prevare“, neverbalni mikroizrazi

povezivani sa laganjem kao što su treptanje levog oka, pojačano crvenilo lica, pravci kretanja glave itd. (Sánchez-Monedero, Dencik, 2022). Radi se u stvari o nepreglednom nizu varijacija u korišćenju biometrijskih tehnika, identifikatora i preko njih biometrijski izvedenih podataka. Biometrijski izvedeni podaci su zbir skupova podataka koji su rezultat informacija dobijenih iz biheviornalnih, fizičkih i psiholoških biometrijskih tehnika identifikacije i drugih neverbalnih metoda komunikacije.

Slika 2. Biometrijski izvedeni podaci dobijeni na osnovu analize pogleda.



Izvor XRSI: https://xrsi.org/wp-content/uploads/2020/09/illustrations_XRSI_privacy_framework_20200906_DEF-7-1-1536x1277.png

Ovi izvedeni podaci se dobijaju od glavnih biometrijskih tehnika identifikacije odnosno „jakih“ biometrijskih identifikatora kao što su: prepoznavanje lica, daktiloskopski podaci (provera otisaka prsta), skeniranje šarenice, analiza mrežnjače; prepoznavanje glasa i prepoznavanje oblika uha. Tu su uključeni i analiza tastera, analiza vlastitog potpisa, analiza hoda, analiza pogleda (praćenje očiju) (XRSI, 2024). Za jedinstvenu identifikaciju fizičkih lica, „jake“ biometrijske identifikatore treba uhvatiti, transformisati u digitalne podatke i na kraju u standardizovani u šablon (Wendehorst, Duler, 2021b). Na kraju moramo da pomenemo i „otisak ljudskog pokreta“ kao jedan od biometrijski jakih identifikatora. Otisak ljudskog pokreta može takođe biti idealan za predviđanje aktivnosti, kriminala i bolesti pa samim tim i deo policijskog predviđanja i bezbednosti. Prema pioniru VI Luisu Rozenbergu, postoje stvarne opasnosti „da će sistemi moći da vas identifikuju bez vašeg pristanka i učešća bez uopšte i da znate da ste bili meta identifikacije“. Otisak pokreta za razliku od tehnike prepoznavanja lica može omogućiti identifikaciju otpozadi, bez da se uopšte vidi lice osobe (Kremidas-Courtney, Linderstal, 2023).

Sve opisane biometrijske tehnike su moćan alat za službe bezbednosti što dramatično komplikuje već dovoljno polarizovane strane koje se zalažu za više bezbednosti ili više prava i sloboda građana. Tako, po zaštitnicima ljudskih prava

konačni tekst Uredbe o VI predstavlja propuštenu prilika za zaštitu građanskih sloboda. Usvajanje Uredbe o VI se shvata kao prihvatanje prakse koja je kroz istoriju bila povezana sa „eugenikom“ odnosno naukom o različitim načinima poboljšanja i kontrolisanja ljudske vrste. Konačna verzija Uredbe o VI ide na dušu Francuskoj koja se optužuje da je značajno uticala na njenu sadržinu sa namerom očuvanja i širenja ovlašćenja države da koristi netransparentne i nepouz dane sisteme VI iz bezbednosnih razloga i povećavanje efikasnosti rada policije na sprečavanju kriminala i nasilja na javnim okupljanjima i sve to uoči Olimpijskih i Paraolimpijskih igara u Parizu (Reclaim your face, 2024).

Pravni okvir za upotrebu sistema VI u sprovođenju zakona u Republici Srbiji

Značaj upotrebe VI i njenog prožimanja svih sfera društvenog života u Republici Srbiji je prepoznat sredinom druge decenije 20 veka. Sprovođenje digitalizacije i značajan razvoj IT sektora koji poslednjih godina ima priličan udeo u rastu BDP su bili direktan most ka istraživanjima, inovacijama i uobličavanju primene VI. To je dovelo do usvajanja prve Strategije za razvoj veštačke inteligencije 2019. godine, etabli rajući Srbiju kao prvu zemlju u Jugoistočnoj Evropi i 26. u svetu koja ima ovakav dokument. Takođe, Srbija 2022. godine, postaje deo Globalnog partnerstva za veštačku inteligenciju (u daljem tekstu: GPAI) a 2023. i članica Alijanse za upravljanje veštačkom inteligencijom Svetskog ekonomskog foruma (Euroactiv, 2024).

GPAI je inicijativa koja teži da uspostavi globalne standarde i pravila za razvoj veštačke inteligencije, kao i da ubrza razvoj veštačke inteligencije globalno. Članstvom u GPAI Srbija je stekla brojne benefite na nekoliko različitih polja. Jedan od najznačajnijih je svakako pristup najsavremenijim tokovima u oblasti veštačke inteligencije. Srbija će u naredne tri godine biti predsedavajuća GPAI i to u prvoj i trećoj pomoćna, dok će u drugoj godini biti glavna. Kriterijumi za članstvo bili su napredak razvoja veštačke inteligencije, i posvećenost odgovornom razvoju veštačke inteligencije. Sekretarijat GPAI je pri Organizaciji za ekonomsku saradnju i razvoj (OECD), a ekspertske centri su u Montrealu i Parizu, dok će novi biti otvoren u Japanu (Euroactiv, 2024a).

Republika Srbija ima ukupno 21 politiku i oblasti saradnje i razvoja VI koje su registrovane na OECD-ovoj Observatoriji za VI (OECD AI, 2024). Jedna značajnijih je već pomenuta Strategija za razvoj veštačke inteligencije u Republici Srbiji za period 2020-2025. godine (u daljem tekstu: Strategija).

Strategija u uvodnom delu sadrži ciljeve i mere za razvoj veštačke inteligencije čija implementacija treba da rezultira ekonomskim rastom, unapređenjem javnih usluga, unapređenjem naučnog kadra i razvojem veština za poslove budućnosti (Strategija razvoja veštačke inteligencije u Republici Srbiji za period 2020-2025. godine, "Sl. glasnik RS", br. 96/2019). Usklađena je sa Evropskom inicijativom za VI koja je predhodila Strategiji i Predlogu Uredbe EU o VI kao jedna od obaveza

iz procesa pristupanja Republike Srbije EU i koja treba da omogući njenu potpunu integraciju u Evropski istraživački prostor. Od razloga za usvajanje se u Strategiji naglašava „da je VI tehnologija opšte namene poput parne mašine, železnice i električne struje koja dramatično doprinosi razvoju svih oblasti privrede i društva i u mnogim od njih unosi revolucionarne promene“. Takođe se ističe da VI može unaprediti i efikasnost rada javne uprave i kvalitet usluga koje država pruža građanima i privredi (naslov 2.1 Strategije).

Ukazuje se na prednosti njene upotrebe u raznim društvenim sferama sa mogućim rizicima koji proizlaze iz njene primene. U konkretnim rizicima po na primer lične podatke, unutar naslova „Pojedinaac i društvo“ ističe se da politika i zakonski okvir Republike Srbije u ovoj oblasti prati standarde EU tačnije Opštu uredbu EU o zaštiti podataka obezbeđujući time primenu visokih standarda zaštite podataka o ličnosti. U izazovima se sagledavajući uporednu praksu, naglašava potreba za prevenciju diskriminacije ukazujućim „da se može dogoditi da se uvede sistem koji analizom podataka utvrđuje stepen rizika pojedinaca da počine prekršaj ili zločin. Ukoliko se ne koriste adekvatno podaci, ovakav sistem može da reprodukuje diskriminativni obrazac“ (naslov 4.4 Strategije). Deo koji se odnosi na konkretne ciljeve, posebno delovi koji se odnose na upotrebu VI u javnoj upravi ne sadrže nikakvo pozivanje niti spominje rizike od njene primene u policijske i bezbednosne svrhe.

Rizici i izazovi kao i kategorizacija ovih sistema su sadržani u Etickim smernicama za razvoj, primenu i upotrebu pouzdane i odgovorne VI iz 2023 ("Sl. glasnik RS", br. 23/2023, u daljem tekstu: Smernice). Smernice slede kategorizaciju sadržanu u predlogu Uredbe o VI Evropske komisije i u kategoriji visoko rizične nabraja sisteme VI:

- biometrijske identifikacije i kategorizacije pojedinca: naročito obuhvataju sisteme namenjene za daljinsku biometrijsku identifikaciju pojedinca u realnom vremenu kao i naknadnu daljinsku biometrijsku identifikaciju;
- krivičnog gonjenja: naročito obuhvata sisteme namenjene organima krivičnog gonjenja koji vrše procenu rizika pojedinaca za izvršenje ili ponovno izvršenje krivičnih dela na osnovu osobina, karakteristika ili prethodnog kriminalnog ponašanja; sisteme koji bi se koristili kao poligrafska sredstva ili sredstva za otkrivanje emocionalnog stanja pojedinca; sisteme koji bi se koristili za ocenu verodostojnosti dokaza tokom predistražnog, istražnog i sudskog postupka; sisteme koji bi se koristili za procenu pojedinca; sisteme namenjene za analitiku krivičnih dela koji se odnose na pojedince i koji omogućavaju pretraživanje složenih povezanih i nepovezanih velikih skupova podataka iz različitih izvora ili u različitim formatima s ciljem uočavanja nepoznatih uzoraka u podacima ili skrivenih veza među podacima;
- upravljanja migracijama ljudi, azilom i nadzora državne granice: naročito obuhvata sisteme koji bi se koristili kao poligrafska sredstva ili sredstva za otkrivanje emocionalnog stanja pojedinca; sisteme namenjene nadležnim

organima/institucijama za procenu rizika (uključujući rizik za sigurnost, rizik od nezakonitih imigracija ili rizik za zdravlje) koji predstavlja pojedinac koji namerava da uđe ili je ušao na teritoriju države Republike Srbije; sisteme namenjene nadležnim organima/institucijama za proveru verodostojnosti putnih isprava, naročito kroz proveru sigurnosnih obeležja tih isprava; sisteme namenjene za pomoć nadležnim organima/institucijama pri razmatranju zahteva za azil, vize, boravišne i radne dozvole i s njima povezanim procesima (povezani procesi obuhvataju proveru krivične i prekršajne osuđivanosti, postojanje i vrstu pritužbi datih u vezi s predmetnim zahtevima i sl.), a u cilju donošenja odluka u vezi sa predmetnim zahtevima (Naslov 2.3 Smernica).

Usvajanje Smernica je iskorak u oblikovanju pravnog okvira za upotrebu VI u Republici Srbiji s tim što Smernice nemaju obaveznú snagu već predstavljaju instrument mekog prava kojim se načelno usmerava budući razvoj VI i njena primena od strane službi za sprovođenje zakona. One nisu u potpunosti usklađene sa Uredbom EU o VI jer ne sadrže listu zabranjene odnosno neprihvatljive prakse upotrebe sistema VI u bezbednosne svrhe. Smernice, u stvari, u visokorizične sisteme ubrajaju zabranjene sisteme u EU kao što je na primer, biometrijska identifikacija i kategorizacija pojedinaca odnosno sisteme namenjene za daljinsku biometrijsku identifikaciju pojedinca u realnom vremenu kao i naknadnu daljinsku biometrijsku identifikaciju.

Postavlja se pitanje da li je upotreba sistema VI u bezbednosne i policijske svrhe definisana Smernicama kao visokorizična, dovoljna za sprečavanje njene maliciozne upotrebe od strane službi za sprovođenje zakona u Republici Srbiji? Da li je Zaključak Vlade kao pravni akt koji definiše Smernice dovoljan da spreči službe u masovnom nadzoru putem sistema VI? Odgovor na ova pitanja je određen posebno imajući u vidu iskustva sa neuspešnim pokušajem donošenja Zakon o unutrašnjim poslovima u periodu 2020-2022. koji je *de facto* trebao da legalizacije upotrebu biometrijskog nadzora. Bilo je predviđeno korišćenje biometrijskog nadzora između ostalog u javnom prostoru odnosno na javnim okupljanjima visokog rizika na osnovu naređenja ministra (Vasilkov, 2023). Nevladine organizacije i civilno društvo su svojim aktivizmom, debatama i kritikama uspele da odlože legislativni proces legalizacije zabranjene i visokorizične prakse biometrijskog nadzora i pored obrazloženja predstavnika MUP-a kao predlagača, da ovi sistemi u mnogome doprinose povećanju bezbednosti građana, i da su već standardna praksa u EU. Naime, civilno društvo ističe da se Srbija se više puta našla na „procurelim“ spiskovima korisnika moćnih softvera za prepoznavanje lica poput *Clearview AI-a* i *Griffeye* kao i da su nabavljeni sistemi VI pomoću kojih je moguće vršiti obradu biometrijskih i drugih podataka, poput „pametnih“ kamera, softvera *Social Links*, *Maltego* i *Mozenga*, kao i programa za napredno prepoznavanje lica (European Western Balkans, 2023).

Zaključak

Bezbednost, policijsko postupanje i rad službi za sprovođenja zakona sa jedne strane i zaštita ljudskih prava i osnovnih sloboda sa druge, su oduvek suprotni polovi, nepomirljive suprotnosti, teme koje razdvajaju i polarizuju javnost posebno zaštitnike ljudskih prava i bezbednosne eksperte i profesionalce. Kada na ovaj većiti antagonizam i debate o tome ko je stariji, bezbednost ili ljudska prava, da li zaštita jedne od ovih vrednosti isključuje zaštitu i poštovanje druge, koliko je dovoljno bezbednosti a kolika je oblast zaštićene privatnosti i nivo poštovanja ljudskih prava, dodamo i primenu sistema VI u bezbednosne svrhe dobijamo veoma izazovnu, rizičnu i prilično tešku jednačinu sa tri nepoznate.

Biometrijski sistemi VI označeni kao zabranjeni i visokorizični u Uredbi o VI će prestati da se primenjuju odnosno početi da se primenjuju na način predviđen Uredbom, 6 meseci od njenog objavljivanja u Službenom glasniku EU sa obavezom potpune implementacije u narednih dve godine što označava uspostavljanje prvog zakonodavnog okvira kojim se uređuje primena sistema VI u oblasti sprovođenja zakona. Države članice će morati da nađu transparentan, odgovoran i proporcionalni način i oblik upotrebe sistema za predviđanje, upotrebe biometrije i drugih tehnika za nadzor granica, krivično gonjenje i borbu protiv terorizma a na čije korišćenje pretenduju službe za sprovođenje zakona.

Regulisanje pojedinih praksi primene VI u oblasti sprovođenja zakona u Republici Srbiji je definisano Strategijom o primeni veštačke inteligencije 2020 - 2025 i Etičkim smernicama iz 2023. Pokušaj zakonskog uvođenja biometrijskog nadzora kroz predloženi Zakon o unutrašnjim poslovima tokom 2022 je uznemirio javnost i razbesneo zastupnike ljudskih prava u Srbiji. Ono što predstoji u narednom periodu posebno do kraja 2024. godine za kada je predviđeno usvajanje Zakona o unutrašnjim poslovima je nastavak „borbe“ između pristalica više bezbednosti sa jedne i pristalca zaštite ljudskih prava, sa druge strane. Jedna vrsta mogućeg rešenja ovog društveno bezbednosnog fenomena kao i preporuka koja proizlazi iz ovog istraživanja može biti povezivanje postojećih politika u oblasti VI sa pojedinim zakonima odnosno parcijalno zakonsko normiranje putem izmene postojeće legislative. Tako, pojedini zakoni bi mogli da regulišu primenu sistema VI, posebno u oblasti sprovođenja zakona kao pomenuti Zakon o unutrašnjim poslovima i Zakon o graničnoj kontoli koji bi regulisao upotrebu sistema VI na graničnim prelazima i nadzoru i zaštiti državne granice. Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala bi sadržao odredbe o zabrani korišćenju sistema VI za radnje koje ugrožavaju visokotehnološku bezbednost. Krivični zakonik i Zakon o krivičnom postupku bi obezbedili dovoljan nivo zaštite ljudskih prava u primeni sistema VI u krivičnopravnoj materiji a Zakon o bezbednosno-informativnoj agenciji bi izmenama onemogućio samovoljnu i neseliktivnu upotrebu sistema VI i omogućio takođe veći stepen zaštite ljudskih prava i sloboda. Ovakav način izgradnje pravne infrastrukture i pravne regulacije bi doprineo ne samo izgradnji standarda i prakse

zakonite upotrebe biometrijskih i drugih visokorizičnih sistema VI u nacionalnom pravnom poretku Republike Srbije već i unapređenju međunarodne bezbednosne saradnje sa službama EU za sprovođenje zakona kao što su Evropol i Fronteks, zatim Interpola i na kraju na bilateralnoj osnovi kada se bezbednosna saradnja sa drugim državama upotrebom sistema VI pokaže kao neophodnost.

Literatura

1. Byrne W. H., T. Gammeltoft-Hansen. 2023. Untangling the Legal Infrastructure of Schengen. MOBILE Working Paper, No. 21. DOI: <https://doi.org/10.31235/osf.io/9h4e3>
2. Prlja D., G. Gasmi., i V. Korać. 2021. Veštačka inteligencija u pravnom sistemu EU. Institut za uporedno pravo. Beograd. ISBN 978-86-80186-73-3
3. UNESCO. 2022. Recommendation on the Ethics of Artificial Intelligence. (dostupno na web sajtu: <https://unesdoc.unesco.org/ark:/48223/pf0000381137>)
4. Interpol&UNICRI. 2019. Artificial Intelligence and Robotics for Law Enforcement. (dostupno na web sajtu: <https://unicri.it/artificial-intelligence-and-robotics-law-enforcement>)
5. OECD. 2022. Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449. (dostupno na web sajtu: <https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449>)
6. Council of Europe. 2023. Draft Framework Convention on artificial intelligence, human rights, democracy and the rule of law. (dostupno na web sajtu: <https://rm.coe.int/-1493-10-1b-committee-on-artificial-intelligence-cai-b-draft-framework/1680aee411>)
7. White House Office of Science and Technology Policy. 2022. The Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People. (dostupno na web sajtu: <https://www.whitehouse.gov/ostp/ai-bill-of-rights>)
8. The China Academy of Information and Communications Technology. 2022. Artificial Intelligence White Paper. (dostupno na web sajtu: https://cset.georgetown.edu/wpcontent/uploads/t0442_AIwhite_paper2022_EN.pdf)
9. Maslej N. et al., 2024. The AI Index 2024 Annual Report. AI Index Steering Committee, Institute for Human-Centered AI. Stanford University, Stanford, CA. (dostupno na web sajtu: <https://aiindex.stanford.edu/report/>)
10. European Commission. 2021. 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. COM/2021/206 final.
11. Evropski Parlament. 2024. Akt o umjetnoj inteligenciji. Zakonodavna rezolucija Evropskog parlamenta od 13. ožujka 2024. o Prijedlogu uredbe Evropskog parlamenta i Vijeća o utvrđivanju usklađenih pravila o umjetnoj inteligenciji (Akt o umjetnoj inteligenciji) i izmjeni određenih zakonodavnih

- akata Unije (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)). P9_TA(2024)0138.
12. Share Fondacija. 2024. Usvojen AI Akt: Ljudska prava ostala u drugom planu. (dostupno na web sajtu: <https://www.sharefoundation.info/sr/usvojen-ai-akt-ljudska-prava-ostala-u-drugom-planu/>)
 13. Friedl P., G.G. Gasiola. 2024. Examining the EU's Artificial Intelligence Act. VerfBlog. DOI: 10.59704/789d6ad759d0a40b (dostupno na web sajtu: <https://verfassungsblog.de/examining-the-eus-artificial-intelligence-act/>)
 14. Fuster G.G. 2020. Artificial Intelligence and Law Enforcemen - Impact on Fundamental Rights. Study requested by the LIBE committee. doi:10.2861/880024
 15. Samoili S. et al., 2021. AI Watch. Defining Artificial Intelligence 2.0. Towards an operational definition and taxonomy for the AI landscape. Publications Office of the European Union. European Parliament, Luxembourg, doi:10.2760/019901.
 16. Codagnone C. et al., 2022. Identification and assessment of existing and draft EU legislation in the digital field. Study for the special committee on Artificial Intelligence in a Digital Age (AIDA). Policy Department for Economic, Scientific and Quality of Life Policies. European Parliament, Luxembourg, doi: 10.2861/73141.
 17. Hayes P. et al., 2020. Algorithms and values in justice and security. AI & SOCIETY 35: 533–555. <https://doi.org/10.1007/s00146-019-00932-9>
 18. Perry L.W. et al., 2013. Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations. Rand Corporation. ISBN: 978-0-8330-8148-3. (dostupno na web sajtu: https://www.rand.org/pubs/research_reports/RR233.html)
 19. European Union Agency for Fundamental Rights (EU FRA). 2019. Facial recognition technology: fundamental rights considerations in the context of law enforcement. (dostupno na web sajtu: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf)
 20. Gikay A.A. 2023. REGULATING USE BY LAW ENFORCEMENT AUTHORITIES OF LIVE FACIAL RECOGNITION TECHNOLOGY IN PUBLIC SPACES: AN INCREMENTAL APPROACH.” The Cambridge Law Journal 82, no. 3 (2023): 414–49. <https://doi.org/10.1017/S0008197323000454>
 21. Zhang D. et al., 2022. The AI Index 2022 Annual Report. AI Index Steering Committee, Stanford Institute for Human-Centered AI, Stanford University. (dostupno na web sajtu: <https://aiindex.stanford.edu/ai-index-report-2022/>)
 22. Garvie C., et al., 2016. The Perpetual Line-Up. Unregulated Police Face Recognition, Georgetown Law Center on Privacy & Technology. (dostupno na web sajtu: <https://www.perpetuallineup.org/>)
 23. Engel A. 2024. Facial Recognition Technologies in the Public Sector: Observations from Germany. Chapter. In The Cambridge Handbook of Facial

Recognition in the Modern State, edited by Rita Matulionyte and Monika Zalnieriute, 186–97. Cambridge Law Handbooks. Cambridge: Cambridge University Press.

24. Gikay A.A. 2023. Live Facial Recognition for Law Enforcement: The European Union’s Regulatory Approach Should be Informed by UK Police’s Practice. (dostupno na web sajtu: <https://eulawanalysis.blogspot.com/2023/11/live-facial-recognition-for-law.html>)
25. Statewatch. 2023. Europe’s techno borders. EuroMed Rights & Statewatch. (dostupno na web sajtu: <https://www.statewatch.org/publications/reports-and-books/europe-s-techno-borders/>).
26. Wendehorst C., Y. Duler. 2021a. Biometric Recognition and Behavioural Detection Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces. BRIEFING Requested by the JURI AND PETI committees Policy Department for Citizens' Rights and Constitutional Affairs. Directorate-General for Internal Policies PE 697.131 (dostupno na web sajtu: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/697131/IPOL_BRI\(2021\)697131_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/697131/IPOL_BRI(2021)697131_EN.pdf))
27. Madiega T., H. Mildebrath. 2021. Regulating facial recognition in the EU. European Parliamentary Research Services (EPRS). Brussels. DOI:10.2861/140928. (dostupno na web sajtu: [https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA\(2021\)698021_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf))
28. Sánchez-Monedero J., L. Dencik. 2022. The politics of deceptive borders: ‘biomarkers of deceit’ and the case of iBorderCtrl. Information, Communication & Society. 25:3, 413-430. (dostupno na web sajtu: <https://www.tandfonline.com/doi/full/10.1080/1369118X.2020.1792530>)
29. XReality Safety Intelligence (XRSI).2024. Biometrically-Inferred Data (BID). (dostupno na web sajtu: <https://xrsi.org/definition/biometrically-inferred-data-bid>).
30. Wendehorst C., Y. Duler. 2021b. Biometric Recognition and Behavioural Detection Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces. European Parliament Study requested by the JURI AND PETI committees Policy Department for Citizens' Rights and Constitutional Affairs. Directorate-General for Internal Policies. doi: 10.2861/982599
31. Kremidas-Courtney C., H. Linderstal. 2023.The convergence of new technologies endangering human agency. Friends of Europe. (dostupno na web sajtu: <https://www.friendsofeurope.org/insights/the-convergence-of-new-technologies-endangering-human-agency/>)
32. Reclaim your face. 2024. EU AI Act will fail commitment to ban biometric mass surveillance (Deutsche Version unten). (dostupno na web sajtu: <https://reclaimyourface.eu/eu-ai-act-will-fail-commitment-to-ban-biometric-mass-surveillance/>)

33. Euroactiv. 2024. Da li smo spremni za Veštačku inteligenciju? Indeks pokazuje da smo na 57. mestu, Srbija će uložiti 100 miliona evra. (dostupno na web sajtu: <https://euractiv.mondo.rs/tehnologija/a6320/Da-li-je-Srbija-spremna-za-vestacku-inteligenciju.htm>)
34. Euroactiv. 2024a. ŠTA JE "ORGANIZACIJA GLOBALNO PARTNERSTVO ZA VEŠTAČKU INTELIGENCIJU"? Srbiji donosi brojne benefite i razvoj tehnologije (dostupno na web sajtu: <https://euractiv.mondo.rs/tehnologija/a6482/Sta-je-organizacija-Globalno-partnerstvo-za-vestacku-inteligenciju-i-sta-znaci-za-Srbiju.html>)
35. OECD 2024. OECD AI Policy Observatory. AI in Serbia (dostupno na web sajtu: <https://oecd.ai/en/dashboards/countries/Serbia>)
36. Strategija razvoja veštačke inteligencije u Republici Srbiji za period 2020-2025. godine. "Sl. glasnik RS", br. 96/2019.
37. Zaključak o usvajanju Etičkih smernica za razvoj, primenu i upotrebu pouzdane i odgovorne veštačke inteligencije. "Sl. glasnik RS", br. 23/2023.
38. Vasilkov Z. 2023. Unutrašnji poslovi i bezbednost u pravu Evropske unije nakon Lisabonskog ugovora. Zadužbina Andrejević: Beograd. ISBN 978-86-525-0429-9
39. European Western Balkans. 2023. Akt EU o veštačkoj inteligenciji će onemogućiti nekontrolisan biometrijski nadzor u Srbiji. (dostupno na web sajtu: <https://europeanwesternbalkans.rs/akt-eu-o-vestackoj-inteligenciji-ce-onemoguciti-nekontrolisan-biometrijski-nadzor-u-srbiji/>)

Datum prijema (Date received): 23.11.2024.

Datum prihvatanja (Date accepted): 20.03.2025.

ARTIFICIAL INTELLIGENCE IN SERVICE LAW ENFORCEMENT IN THE EUROPEAN UNION AND THE REPUBLIC OF SERBIA

Zorančo Vasilkov³⁴

Abstract

Artificial intelligence has recently been intensively pushing the boundaries of human civilization and technological development. As a technological achievement, it imperceptibly "sneaked" into the life of every individual and became an integral part of all spheres of social life. In the application of artificial intelligence today, it seems that we cannot shake the impression that what at one point seemed possible in 100 years, has in fact become a reality in the last 10 or so years. The need for legal regulation and legal regulation of the use of artificial intelligence arises as an important issue for its future development for the benefit of the human community and the entire humanity. This research is part of a broader picture of the potential use of artificial intelligence in certain branches of law, aimed at looking at the special "interregnum" between the established practice of using artificial intelligence and its legal regulation. In the work, we focus in particular on the analysis and research of the use of artificial intelligence systems in the field of law enforcement. More precisely, we will shed light on the regulatory process related to artificial intelligence in the EU and point out the specifics of its use for security and police purposes, primarily by establishing restrictions for the benefit of the public and citizens, by categorizing the use of certain artificial intelligence systems as prohibited and high-risk. These are artificial intelligence systems that use prediction techniques, biometric surveillance, i.e. face recognition and derived biometric data. Their impact on human rights is the subject of special in-depth research outside this framework, bearing in mind that the uncontrolled use of these techniques as part of the artificial intelligence system today can be equated with the consequences of dropping an "atomic bomb" on human freedoms and rights. Apart from the regulatory process within the EU, we also point out the potential use of artificial intelligence in Serbia by law enforcement services through the analysis of the legal framework of the Republic of Serbia.

Keywords: artificial intelligence, law enforcement, police forecasting, facial recognition, biometric techniques

JEL: K33

³⁴ Assistant professor, PhD Zorančo Vasilkov, MB University, Faculty of Business and Law, E-mail: vasilkovzoranco@yahoo.com, <https://orcid.org/0000-0001-8282-2777>

Introduction

Artificial intelligence is a technological achievement whose application in all areas of human activity is becoming inevitable, both globally, regionally and locally. Thus, the "race" for legal regulation and legal regulation of the use of artificial intelligence enters the scene as a key issue for its future development for the benefit of the human community and the entire humanity. Debates on the need, manner and methods of legal regulation take place at various levels, from international, through regional organizations and national level to the private sector and technological giants who already make certain forms of artificial intelligence available to all citizens on a daily basis. Legal regulation primarily refers to various aspects of the application of artificial intelligence and can be seen as the establishment of a "legal infrastructure" for its use, use, development and monitoring in all areas of social life.

With this work, the author investigates the legal regulation and potential use of artificial intelligence in the sensitive area of law, focusing on the review of already established practice for the use of artificial intelligence in law enforcement. More specifically, we will shed light on the regulatory process related to artificial intelligence in the EU and focus on the use of artificial intelligence for security and policing purposes, pointing out the limitations established for the benefit of the public and citizens that are imposed on law enforcement services by categorizing certain actions as prohibited and high risk. We start from the legal infrastructure for artificial intelligence that is established by the proposed EU Regulation establishing harmonized rules on artificial intelligence, often referred to as the Artificial Intelligence Law or the Artificial Intelligence Act.

Security and policing should provide an environment, safe and devoid of any fear for each individual, in which human rights and basic freedoms are protected from the malicious use of artificial intelligence, bearing in mind that law enforcement services possess systemic, discretionary and public powers with high degree of risk for potential abuse of artificial intelligence. A large number of studies at the global level point to the dangers to human rights and basic freedoms in the case of the application of artificial intelligence for security purposes, especially in cases of biometric recognition and detection of undesirable behavior of individuals. Apart from the regulatory process within the EU, we also look at the use of artificial intelligence in this area in Serbia through the analysis of the legal framework, i.e. the Strategy of the Republic of Serbia and other national soft law acts on artificial intelligence (hereinafter: AI).

Establishing legal infrastructure and defining prohibited and high-risk AI systems

Legal infrastructure is a term used in recent research and denotes the establishment of the right framework and regulation of a certain area of social behavior, that is, the standardization and adoption of legal acts as the basis of regulation and creation of conditions for the further development of that area. Infrastructures in common parlance refer to the physical or organizational aspects of the world that societies need to function. The metaphor of law as an infrastructure arises in the merging, that is, of a serious understanding of law as a socio-material form, on the one hand realized through social action, but on the other significantly reshaping the world around us (Byrne, Gammeltoft-Hansen, 2023). This term is separate and should not be confused with the actual electronic, digital and information infrastructure as the material base of AI development. The legal infrastructure in the specific case emphasizes the importance of legal regulation and understanding the necessity for normative regulation of the use of AI, especially if we understand the need, method and methods of legal regulation as a "condition above the conditions" for the functioning of society, that is, as infrastructural preparation and work on defining a huge area that organizationally requires the establishment of a modern legal "high speed highway". Security and prevention of the risk of endangering human lives also imposes the definition of strict "speed limits and certain mandatory directions of movement" which are truly necessary so that the development and use of AI does not turn into chaos, a threat and a threat to the survival of humanity. The balance between the possibility of further rapid development of AI for the benefit of each individual and the maximum reduction of the risk of uncontrolled "movement or popping" today means enabling, encouraging and directing its further future development in the fields of economy, medicine, public health, ecology, food production, supply, energy etc. The desire for AI to completely improve the way people think, create and move in the real world also speaks of the construction of a future "scientific highway with many lanes" (Prlja et al., 2021:96).

The establishment of the legal infrastructure for the AI, that is, the preparatory work for its definition, is rapidly taking place in international organizations as well as within formal and informal gatherings and coalitions of states. For example, reviews of the ethical dilemmas of the use of AI and United Nations guidelines are provided in a UNESCO guide (UNESCO, 2022), while the first guidelines for the use of AI in law enforcement were presented by Interpol and the UN Interregional Institute for Crime and Justice Research (Interpol&UNICRI, 2019). Regional organizations, primarily the Council of Europe and the Organization for Economic Co-operation and Development - OECD have introduced recommendations (OECD, 2022) regarding the modalities, ways and degree of coverage of the use of AI and are preparing conventions (Council of Europe, 2023) or guides for use with the member states AI in different spheres of

social life. States are also involved in the national definition of the framework for the implementation of AI, in which the USA is leading (White House Office of Science and Technology Policy, 2022) and China The China Academy of Information and Communications Technology, 2022), and in international frameworks grouping and holding summits have begun states that encourage innovation in the field of AI and regulate the development of AI by law or through national strategies. All this includes the private sector and technological giants, most of which are not enthusiastic about the imposition of an international and national regulatory framework, bearing in mind that they have already made certain forms of artificial intelligence available to all citizens on a daily basis. Not a small contribution to both the development of AI and the entire process of legal regulation is made by the academic community, within which there are research institutes such as the Institute for Human-Centered AI at Stanford University, which leads the overall annual global index of the development, progress and legal regulation of AI (Masley, at al., 2024).

In this global constellation, of all attempts to establish a legal infrastructure for the use of AI, the EU has gone the furthest, within which the legislative procedure for the adoption of the Regulation on AI (COM/2021/206, hereinafter: Regulation on AI or Regulation) is in the final stage. Namely, within the regular legislative procedure, the European Parliament adopted the Legislative Resolution (European Parliament, 2024) and its confirmation and adoption by the Council of the EU is awaited. The agreement of the EU institutions on this act was reached at the end of 2023, and in the first reactions to the news about the adoption of the regulation, it is emphasized that the interests of citizens were not put first and that double standards were introduced for the police and security services, with enough opportunities for human rights violations (Share Foundation, 2024). However, last-minute changes are not insignificant, introducing a mandatory fundamental rights impact assessment for high-risk AI systems, obliging those who use them to assess and mitigate foreseeable impacts on the fundamental rights of those affected, especially marginalized and vulnerable groups. This also refers to the introduction of the right of individuals to submit complaints to competent authorities regarding possible violations of the AI Regulation (Friedl, Gasiola, 2024).

The regulation defines the AI systems themselves as "a machine system designed to work at different levels of autonomy, which after introduction can show adaptability and which, for explicit or implicit goals, infers from the input values it receives how to generate output values such as predictions, content, recommendations or decisions that may affect physical or virtual environments" (Article 3, Point 1 of the Regulation). In the Regulation, a risk-based approach to the development and use of AI is highlighted, and the AI systems themselves are categorized into different classes and subject to different rules in accordance with the degree of risk assumed to represent individuals and society as a whole. The AI

Regulation places various restrictions on the AI systems that could be used in law enforcement. The majority of AI systems used by law enforcement agencies for security and policing purposes are placed in unacceptable, i.e. prohibited or strictly controlled, high-risk practices. The prohibited practice of using AI systems consists of: **manipulative** or misleading techniques, exploiting any weakness of individuals or certain groups, **evaluating or classifying natural persons** or a group of persons in a certain period based on their social behavior, **estimating or predicting** the probability that a natural person will commit a criminal offense exclusively based on the creation of a profile of a natural person or assessment of his characteristics and personality traits, **databases for facial recognition** by untargeted collection of face photos from the Internet or CCTV recordings, **drawing conclusions about the emotions** of a natural person in the workplace and in educational institutions, **biometric categorization** in which natural persons are individually categorized based on biometric data about their race, political opinions, union membership, religious or philosophical beliefs, sexual orientation, as well as **biometric identification** of individuals in real time.

Real-time remote biometric identification may only be used if its use is limited in time and geographically and if special judicial or administrative permission has been previously granted. The regulation defines three exceptions for remote biometric identification for the purpose of criminal prosecution for criminal offenses involving a high degree of social danger, namely: 1) targeted searches for specific victims of kidnapping, human trafficking or sexual exploitation of people, as well as searches for missing persons; 2) prevention of a concrete, significant and immediate threat to the life or physical safety of natural persons or a real and present or real and foreseeable threat of a terrorist attack; ; and 3) locating or identifying a person suspected of committing a criminal offense for the purpose of conducting a criminal investigation, prosecution or execution of a criminal sanction for the criminal offenses listed in Annex 2, which are punishable by imprisonment or deprivation of liberty for a maximum period of at least four years (Article 5, paragraph 1, point h of the Regulation).

High-risk practice or the categorization of AI systems as high-risk includes the fulfillment of strict requirements for their use by introducing additional rules of regulation and control. The difference between unacceptable or prohibited AI systems and high-risk ones is that others are not considered so dangerous, that is, they do not pose such a high degree of risk to human rights that it is necessary to ban them. This is where the largest number of AI systems are found, which are used in law enforcement, that is, in the areas of the police, the judiciary and critical infrastructure (Annex 3 of the Regulation).

The prohibited and high-risk practice of using AI in law enforcement relies primarily on the development and application of certain AI components related to the processing of large amounts of data, algorithms and advanced computer

technology. These components were previously encouraged in order to change, apply and review the technique of smart surveillance, profiling, the use of a large amount of data and, as widely as possible, the digitalization of the public sector (Fuster, 2020:21). In general, AI is linked and classified by the advanced grouping of algorithms used for technology development, according to the theoretical concepts behind them, which primarily originated in mathematics, logic, philosophy and information theory (Samoili, 2021:11).

There are various theories that emphasize the subjectivity of human perception from the perspective of law, for what is autonomous and intelligent in computational procedures by pointing to the one-sidedness in the use of terms that will change in the future. Namely, what fell into those categories during the 80s of the last century is neither intelligent nor autonomous today. That is why Kodagnone (Codagnone) AI as a term seems unsuitable for regulation by legal and by-laws, but the algorithms that are the basis of the AI system should be legislated. Accordingly, the legal acts that have already been adopted and regulate algorithmic processes and decision-making in different scenarios and with different purposes are related to the construction and are an integral part of the regulatory framework for AI in the EU (Codagnone et al., 2022:46). Namely, algorithms are powerful artifacts that operate within our information milieu, structuring our data, profiling, categorizing, and predicting who we are, what we are, what we want, and more (Hayes et al., 2020).

Challenges of using the AI system in law enforcement from the aspect of predicting and using special biometric techniques

The use of algorithms in the field of policing and security is a particularly sensitive issue with great potential for improving law enforcement measures and procedures, but also with a huge risk of causing harm and violating human rights (Hayes et al., 2020:1). One of the first techniques of using algorithms in the field of security, more specifically in police action, which precedes the use of the AI system, is police prediction (otherwise prohibited by Article 5, point d of the Regulation). Police predicting is the algorithmic processing of data sets that reveals patterns of likely future crimes and threats in order to prevent them before they actually occur. It can be divided into four broad categories such as: 1) methods for predicting criminal acts or places and time periods in which there is an increased risk of criminal activity; 2) methods of prediction and detection of possible perpetrators of criminal acts; 3) methods of predicting the identity of perpetrators or creating profiles similar to perpetrators of criminal acts in the past; and 4) predicting crime victims, that is, identifying groups and individuals who are likely to become victims of crime (Perry et al., 2013:xiv). Police predicting as a new technique for crime prevention appeared in the USA at the end of the 20th century, when the police departments of some large cities hired professional crime analysts who experimented with the processing of large amounts of data and the

use of new technologies, trying to predict events, more precisely, the time, the place and the criminal acts that will be committed as well as the potential perpetrators. Later, a special police prediction model called the Gang Violence Matrix was developed in Great Britain, which the London police began to use in 2012. This model was used to identify and assess the risk of gang members involved in violence, as well as to identify vulnerable groups, that is, those towards whom violence is directed. In other EU member states, it appears in the law enforcement in the area of money laundering and terrorist financing, when at the EU level, banks and other legal entities are required to take appropriate steps to identify risk factors for the assessment of the execution of the mentioned criminal acts (Fuster, 2020:23).

Facial recognition is a biometric technique in rapid development, which is included in two categories in the Regulation, that is, it is mentioned as a prohibited and high-risk practice of using AI in the field of law enforcement. Facial recognition technology as part of the AI system enables the automatic identification or authentication of an individual by comparing and confirming facial features with two or more digital images (EU FRA, 2019:2). It is the process by which AI software can identify or recognize a person using their biometric facial features extracted from a photo or video (Gikay, 2023:417). Although facial recognition is a technology that has been around for several decades, the technical advances in the last few years have been enormous. Some of today's best-performing face recognition algorithms have nearly 100% success on challenging datasets. The US National Institute of Standards and Technology (NIST) has created a Face Recognition Vendor Test (FRVT) measuring advances in facial recognition and how well algorithms perform various security and law enforcement tasks of the law, and refer specifically to the recognition of faces from photojournalist images, for the purpose of identifying victims of child trafficking, detecting forged passports and cross-checking the image of the issued visa. An algorithm's progress in facial recognition is measured by the false mismatch rate, or error rate, which represents the frequency with which the algorithm fails to match an image to a real person. In 2017, the most successful face recognitions had an error rate of over 50.0%, while as of 2021, no error rate higher than 3.0% was registered. The best-performing model across all datasets in 2021 (visa photos) registered an error rate of 0.1%, meaning that for every 1000 faces, the model correctly identified 999. Of particular concern is the use of this technology through system AI, i.e. recognition faces and detection of individuals live in real time. The AI software compares, in real time, the biometric facial images captured by the camera with the existing patterns of the suspect in the database. The extent of the use of facial recognition systems is indicative given that in the US today, 18 out of 24 government law enforcement agencies already use some form of facial recognition technology (Zhang et al., 2022:62). Reports from the US as far back as 2016 indicate widespread use of live facial recognition,

noting that at the time several major police departments were actively exploring real-time facial recognition on live surveillance camera footage. Since then, there have been increasingly explicit calls for legislation to regulate the use of facial recognition by law enforcement, warning that “facial recognition is too powerful to remain secret” and legally undefined (Garvie et al., 2016).

On the other hand, the UK government has called on the police to expand the use of AI-based technologies despite the fact that such systems threaten civil liberties. In a 2019 British national poll, 70% of respondents said the police should be allowed to use facial recognition in criminal investigations, and 71% supported its use in public spaces if it helped reduce crime. An illustrative example is the operation to prevent theft and violence in retail stores in London in 2023, in which the Metropolitan Police used facial recognition to identify 149 retail crime suspects by comparing hundreds of CCTV images (Gikay, 2023). Currently, only limited information is available on the possible use of facial recognition technologies in EU member states. In Germany, the Hamburg police used facial recognition technologies on protesters who caused riots over the G20 Summit in July 2017, while in 2018 the feasibility of using these systems was tested at a train station in Berlin (Engel, 2024). Police in Nice (France) conducted a test of the use of live facial recognition technology at Carnival 2018. The Gendarmerie in France uses facial recognition technologies for criminal investigations, but does not use live facial recognition technologies, due to the lack of a legal basis. Austrian authorities bought facial recognition software in 2019 to search a database to identify unknown criminals whose images are available from CCTV cameras or other sources. Testing for the use of facial recognition technology has also begun in the Netherlands (EU FRA, 2019:6). Some studies point to the future use of 3D facial recognition technology in the area of control of the Union's external borders by Frontex. While current facial recognition technologies rely on a "flat" photograph of an individual's face, 3D facial recognition uses three-dimensional features of the human face for automatic recognition and matching. Once the 3D geometry of the human face is acquired, significant features from the surface of the face are extracted. This enables greater precision than classic two-dimensional face recognition (Statewatch, 2023:37).

Essentially, facial recognition represents only one mosaic of the wider use of biometrics for security purposes. There are biometric techniques that include biometric identification, biometric categorization, behavior detection, emotion recognition, brain-computer interfaces, and other similar techniques that have a wide range of uses. The term "biometric techniques" should be understood to include any technology or operation that: 1) relies on the specific technical processing of data relating to the physical, physiological or behavioral aspects of the human body (including when it is in motion); and 2) for purposes such as authentication or identification of human individuals, categorization of human individuals according to permanent or long-term characteristics (including for the

purpose of predicting future behavior) or detection of temporary or permanent conditions of a human individual (such as fear, fatigue, or illness, or certain intention). However, the increasing use of "weak" and "soft" biometrics together with "strong" biometrics, focusing on a range of patterns of different types of behavior, and the development towards multimodal biometrics are noted. Together with improved sensing and computing capabilities, as well as improved connectivity, this paves the way for the mass adoption of biometric technologies in a wide range of sectors and for a wide range of purposes, even far beyond law enforcement and border controls, making biometric technologies something of a universal technology. (Wendehorst, Duler, 2021:1).

Other research finds that it is a multitude of facial recognition technologies as a specific type of biometric technologies that are used for different purposes, ranging from simple detection of the presence of a face in an image, to more complex verification, identification and categorization or classification of individuals. **Verification** (one-to-one comparison) allows the comparison of two biometric templates, which are usually assumed to belong to the same person. **Identification** (one-to-many comparison) means that a person's face image template is compared to other templates stored in the database to find out if their image is stored there. Facial recognition is also used to **categorize** (or classify) individuals, based on their personal characteristics. In this sense, a wide range of software has been developed to estimate a person's attributes from their face, for the purpose of "classifying facial attributes" (eg gender, race or ethnicity) or "estimating facial attributes" (eg age). Furthermore, facial recognition can be used to classify facial expressions (such as a smile) or a person's emotional state such as happy, sad or angry (Madiaga, Mildebrath, 2021:1).

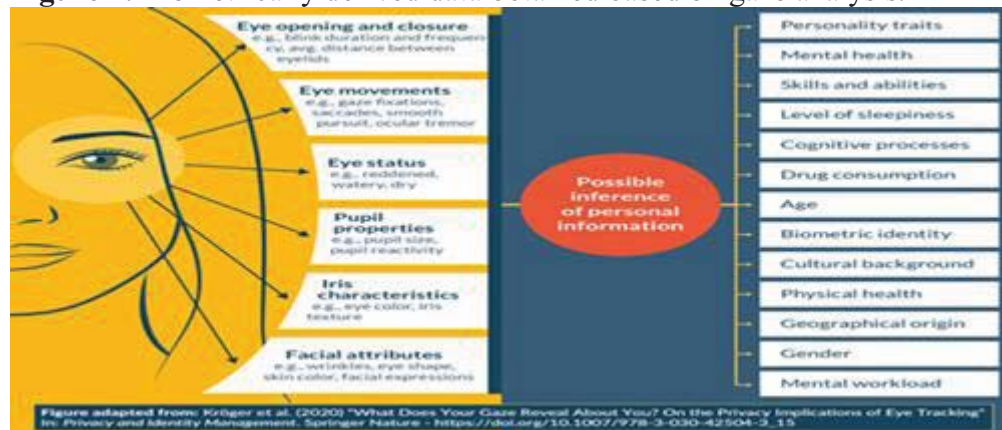
Figure 1. Real-time emotion recognition.



Source: Article 19. <https://www.article19.org/resources/eu-emotion-misrecognition/>

The latter was investigated at the external borders of the EU, more precisely at certain border crossings of Greece, Hungary and Latvia within the Horizon 2020 project, called the Integrated Transfer Control System (iBorderCtrl) which integrates facial recognition and other technologies to detect whether an individual is telling the truth. The so-called were examined and identified. "deception biomarkers", non-verbal micro-expressions associated with lying such as blinking of the left eye, increased redness of the face, directions of head movement, etc. (Sánchez-Monedero, Dencik, 2022). It is, in fact, an inexhaustible series of variations in the use of biometric techniques, identifiers and biometrically derived data through them. Biometrically derived data is a collection of data sets that are the result of information obtained from behavioral, physical and psychological biometric identification techniques and other non-verbal communication methods.

Figure 2. Biometrically derived data obtained based on gaze analysis.



Source XRSI: https://xrsi.org/wp-content/uploads/2020/09/illustrations_XRSI_privacy_framework_20200906_DEF-7-1-1536x1277.png

These derived data are obtained from the main biometric identification techniques, i.e., "strong" biometric identifiers such as: facial recognition, dactyloscopic data (fingerprint verification), iris scanning, retina analysis; voice recognition and ear shape recognition. Key analysis, signature analysis, gait analysis, gaze analysis (eye tracking) are also included (XRSI, 2024). For the unique identification of natural persons, "strong" biometric identifiers should be captured, transformed into digital data and finally standardized into a template (Wendehorst, Duler, 2021b). Finally, we have to mention the "print of human movement" as one of the biometrically strong identifiers. Human movement fingerprinting can also be ideal for predicting activity, crime and disease and therefore part of police prediction and security. According to AI pioneer Louis Rosenberg, there are real dangers "that systems will be able to identify you without your consent and participation without you even knowing that you have been targeted." Gesture printing, unlike

face recognition techniques, can enable identification from behind, without seeing the person's face at all (Kremidas-Courtney, Lindersthal, 2023).

All the described biometric techniques are a powerful tool for the security services, which dramatically complicates the already sufficiently polarized parties that advocate for more security or more rights and freedoms of citizens. Thus, according to defenders of human rights, the final text of Regulation AI represents a missed opportunity for the protection of civil liberties. The adoption of the AI Regulation is understood as the acceptance of a practice that throughout history has been associated with "eugenics", that is, the science of various ways of improving and controlling the human species. The final version of the AI Regulation goes to the soul of France, which is accused of significantly influencing its content with the intention of preserving and expanding the state's authority to use non-transparent and unreliable AI systems for security reasons and increasing the effectiveness of police work to prevent crime and violence in public gatherings and all this on the eve of the Olympic and Paralympic Games in Paris (Reclaim your face, 2024).

Legal framework for the use of the AI system in law enforcement in the Republic of Serbia

The importance of the use of AI and its permeation of all spheres of social life in the Republic of Serbia was recognized in the middle of the second decade of the 20th century. The implementation of digitalization and the significant development of the IT sector, which in recent years has had a considerable share in GDP growth, were a direct bridge to research, innovation and shaping the implementation of AI. This led to the adoption of the first Strategy for the Development of Artificial Intelligence in 2019, establishing Serbia as the first country in Southeast Europe and the 26th in the world to have such a document. Also, in 2022, Serbia will become part of the Global Partnership for Artificial Intelligence (hereinafter: GPAI) and in 2023, a member of the Alliance for Artificial Intelligence Management of the World Economic Forum (Euroactiv, 2024).

GPAI is an initiative that aims to establish global standards and rules for the development of artificial intelligence, as well as to accelerate the development of artificial intelligence globally. Membership in GPAI Serbia has gained numerous benefits in several different fields. One of the most important is certainly access to the most modern trends in the field of artificial intelligence. In the next three years, Serbia will be the chairman of the GPAI, and in the first and third years it will be the assistant chair, while in the second year it will be the main chair. The criteria for membership were progress in the development of artificial intelligence, and commitment to responsible development of artificial intelligence. The GPAI secretariat is at the Organization for Economic Cooperation and Development

(OECD), and the expert centers are in Montreal and Paris, while a new one will be opened in Japan (Euroactiv, 2024a). The Republic of Serbia has a total of 21 policies and areas of cooperation and development of AI that are registered on the OECD Observatory for AI (OECD AI, 2024). One of the more significant ones is the already mentioned Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the period 2020-2025. (hereinafter: Strategy).

The Strategy in the introductory part contains goals and measures for the development of artificial intelligence, the implementation of which should result in economic growth, improvement of public services, improvement of scientific staff and development of skills for the jobs of the future (Strategy for the development of artificial intelligence in the Republic of Serbia for the period 2020-2025, " Official Gazette of RS", No. 96/2019). It is harmonized with the European Initiative for AI, which preceded the Strategy and Proposal of the EU Regulation on AI as one of the obligations from the accession process of the Republic of Serbia to the EU and which should enable its complete integration into the European Research Area. The reason for its adoption is emphasized in the Strategy, "that AI is a general-purpose technology such as the steam engine, railways and electricity, which dramatically contributes to the development of all areas of the economy and society and brings revolutionary changes in many of them". It is also emphasized that AI can improve the efficiency of public administration work and the quality of services provided by the state to citizens and the economy (heading 2.1 of the Strategy).

It points out the advantages of its use in various social spheres with the possible risks arising from its application. In specific risks for example personal data, under the title "Individual and society" it is emphasized that the policy and legal framework of the Republic of Serbia in this area follows EU standards, more precisely the EU General Data Protection Regulation, thereby ensuring the application of high standards of personal data protection. In the challenges, looking at the comparative practice, he emphasizes the need for the prevention of discrimination by pointing out that "it may happen to introduce a system that, through data analysis, determines the level of risk of individuals to commit a misdemeanor or crime." If the data is not used adequately, such a system can reproduce a discriminatory pattern" (heading 4.4 of the Strategy). The part that refers to specific objectives, especially the parts that refer to the use of AI in public administration, does not contain any reference or mention the risks of its application for police and security purposes.

The risks and challenges as well as the categorization of these systems are contained in the Ethical Guidelines for the Development, Implementation and Use of a Reliable and Responsible AI from 2023 ("Official Gazette of RS", No. 23/2023, hereinafter: Guidelines). The Guidelines follow the categorization contained in the proposal of the Regulation on AI of the European Commission and in the category of high risk lists AI systems:

- biometric identification and categorization of an individual: in particular, they include systems intended for remote biometric identification of an individual in real time as well as subsequent remote biometric identification;
- criminal prosecution: in particular, it includes systems intended for criminal prosecution bodies that assess the risk of individuals for committing or re-committing criminal acts based on characteristics, characteristics or previous criminal behavior; systems that would be used as polygraph devices or devices to detect an individual's emotional state; systems that would be used to assess the credibility of evidence during pre-investigation, investigation and court proceedings; systems that would be used to assess the individual; systems intended for the analysis of crimes related to individuals and which enable the search of complex linked and unlinked large data sets from different sources or in different formats with the aim of spotting unknown patterns in data or hidden connections between data;
- management of human migration, asylum and state border surveillance: in particular, it includes systems that would be used as polygraph means or means to reveal the emotional state of an individual; systems intended for competent authorities/institutions for risk assessment (including security risk, illegal immigration risk or health risk) represented by an individual who intends to enter or has entered the territory of the Republic of Serbia; systems intended for competent authorities/institutions for checking the authenticity of travel documents, especially through checking the security features of those documents; systems intended to assist competent authorities/institutions in considering applications for asylum, visas, residence and work permits and related processes (related processes include checking criminal and misdemeanor convictions, the existence and type of complaints made in connection with the relevant applications, etc.), and in for the purpose of making decisions regarding the subject requests (Title 2.3 of the Guidelines).

The adoption of the Guidelines is a step forward in shaping the legal framework for the use of AI in the Republic of Serbia, with the fact that the Guidelines do not have mandatory force, but rather represent a soft law instrument that in principle guides the future development of AI and its application by law enforcement services. They are not fully aligned with the EU Regulation on AI because they do not contain a list of prohibited or unacceptable practices of using the AI system for security purposes. The guidelines, in fact, include systems prohibited in the EU as high-risk systems, such as, for example, biometric identification and categorization of individuals, that is, systems intended for remote biometric identification of an individual in real time as well as subsequent remote biometric identification.

The question arises whether the use of the AI system for security and police purposes is defined by the Guidelines as high-risk, sufficient to prevent its malicious use by law enforcement services in the Republic of Serbia? Is the

Government's Conclusion as a legal act defining the Guidelines sufficient to prevent services from mass surveillance through the AI systems? The answer to these questions is denied, especially considering the experience with the unsuccessful attempt to pass the Law on Internal Affairs in the period 2020-2022, which was supposed to de facto legalize the use of biometric surveillance. The use of biometric surveillance was foreseen, among other things, in public space, that is, at high-risk public gatherings based on the minister's order (Vasilkov, 2023). Non-governmental organizations and civil society, with their activism, debates and criticisms, managed to postpone the legislative process of legalizing the prohibited and high-risk practice of biometric surveillance, despite the explanation of the MUP representative as the proposer, that these systems greatly contribute to increasing the security of citizens, and that they are already a standard practice in EU. Namely, the civil society points out that Serbia has repeatedly been on the "leaked" lists of users of powerful face recognition software such as *Clearview AI* and *Griffeye*, as well as that AI systems have been acquired with which it is possible to process biometric and other data, such as "smart" cameras, *Social Links*, *Maltego* and *Mozenga* software, as well as programs for advanced facial recognition (European Western Balkans, 2023).

Conclusion

Security, police action and the work of law enforcement services on the one hand and the protection of human rights and fundamental freedoms on the other have always been opposite poles, irreconcilable opposites, topics that divide and polarize the public, especially human rights defenders and security experts and professionals. When we add to this antagonism and debates about who is older, security or human rights, whether the protection of one of these values excludes the protection and respect of the other, how much security is enough and what is the area of protected privacy and the level of respect for human rights, we add the application system AI for security purposes we get a very challenging, risky and rather difficult equation with three unknowns.

AI biometric systems marked as prohibited and high-risk in the Regulation on AI will cease to be applied, that is, they will begin to be applied in the manner provided by the Regulation, 6 months after its publication in the Official Gazette of the EU with the obligation of full implementation in the next two years, which marks the establishment of the first legislative framework which regulates the application of the AI system in the field of law enforcement. Member States will have to find a transparent, responsible and proportionate way and form of using prediction systems, using biometrics and other techniques for border surveillance, criminal prosecution and the fight against terrorism, which law enforcement services intend to use.

The regulation of certain practices of the application of AI in the field of law enforcement in the Republic of Serbia is defined by the Strategy on the

Application of Artificial Intelligence 2020 - 2025 and the Ethical Guidelines from 2023. The attempt to legally introduce biometric surveillance through the proposed Law on Internal Affairs in 2022 disturbed the public and enraged human rights representatives in Serbia. What lies ahead in the coming period, especially until the end of 2024, when the Law on Internal Affairs is expected to be adopted, is the continuation of the "struggle" between supporters of more security on the one hand and supporters of human rights protection on the other. One type of possible solution to this social security phenomenon, as well as the recommendation that emerges from this research, can be the connection of existing policies in the area of AI with individual laws, that is, partial legal regulation through the amendment of existing legislation. Thus, certain laws could regulate the application of the AI system, especially in the field of law enforcement, such as the aforementioned Law on Internal Affairs and the Law on Border Control, which would regulate the use of the AI system at border crossings and the supervision and protection of the state border. The Law on the Organization and Competence of State Authorities for Combating High-Tech Crime would contain provisions prohibiting the use of the AI system for actions that threaten high-tech security. The Criminal Code and the Law on Criminal Procedure would ensure a sufficient level of human rights protection in the application of the AI system in criminal law matters, and the Law on the Security and Information Agency would, with amendments, prevent the arbitrary and indiscriminate use of the AI system and also enable a greater degree of protection of human rights and freedoms. This way of building legal infrastructure and legal regulation would contribute not only to building standards and practices of legal use of biometric and other high-risk AI systems in the national legal order of the Republic of Serbia, but also to the improvement of international security cooperation with EU law enforcement services such as Europol and Frontex, then Interpol and finally on a bilateral basis when security cooperation with other countries using the AI system proves to be a necessity.

References

1. Byrne W. H., T. Gammeltoft-Hansen. 2023. Untangling the Legal Infrastructure of Schengen. MOBILE Working Paper, No. 21. DOI: <https://doi.org/10.31235/osf.io/9h4e3>
2. Codagnone C. et al., 2022. Identification and assessment of existing and draft EU legislation in the digital field. Study for the special committee on Artificial Intelligence in a Digital Age (AIDA). Policy Department for Economic, Scientific and Quality of Life Policies. European Parliament, Luxembourg, doi: 10.2861/73141.
3. Council of Europe. 2023. Draft Framework Convention on artificial intelligence, human rights, democracy and the rule of law. (dostupno na web

- sajtu: <https://rm.coe.int/-1493-10-1b-committee-on-artificial-intelligence-cai-b-draft-framework/1680aee411>)
4. Engel A. 2024. Facial Recognition Technologies in the Public Sector: Observations from Germany. Chapter. In *The Cambridge Handbook of Facial Recognition in the Modern State*, edited by Rita Matulionyte and Monika Zalnieriute, 186–97. Cambridge Law Handbooks. Cambridge: Cambridge University Press.
 5. Euroactiv. 2024. Da li smo spremni za Veštačku inteligenciju? Indeks pokazuje da smo na 57. mestu, Srbija će uložiti 100 miliona evra. (dostupno na web sajtu: <https://euractiv.mondo.rs/tehnologija/a6320/Da-li-je-Srbija-spremna-za-vestacku-inteligenciju.htm>)
 6. Euroactiv. 2024a. Šta je "organizacija globalno partnerstvo za veštačku inteligenciju"? Srbiji donosi brojne benefite i razvoj tehnologije (dostupno na web sajtu: <https://euractiv.mondo.rs/tehnologija/a6482/Sta-je-organizacija-Globalno-partnerstvo-za-vestacku-inteligenciju-i-sta-znaci-za-Srbiju.html>)
 7. European Commission. 2021. 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. COM/2021/206 final.
 8. European Union Agency for Fundamental Rights (EU FRA). 2019. Facial recognition technology: fundamental rights considerations in the context of law enforcement. (dostupno na web sajtu: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf)
 9. European Western Balkans. 2023. Akt EU o veštačkoj inteligenciji će onemogućiti nekontrolisan biometrijski nadzor u Srbiji. (dostupno na web sajtu: <https://europeanwesternbalkans.rs/akt-eu-o-vestackoj-inteligenciji-ce-onemoguciti-nekontrolisan-biometrijski-nadzor-u-srbiji/>)
 10. Evropski Parlament. 2024. Akt o umjetnoj inteligenciji. Zakonodavna rezolucija Evropskog parlamenta od 13. ožujka 2024. o Prijedlogu uredbe Evropskog parlamenta i Vijeća o utvrđivanju usklađenih pravila o umjetnoj inteligenciji (Akt o umjetnoj inteligenciji) i izmjeni određenih zakonodavnih akata Unije (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)). P9_TA(2024)0138.
 11. Friedl P., G.G. Gasiola. 2024. Examining the EU’s Artificial Intelligence Act. VerfBlog. DOI: 10.59704/789d6ad759d0a40b (dostupno na web sajtu: <https://verfassungsblog.de/examining-the-eus-artificial-intelligence-act/>)
 12. Fuster G.G. 2020. Artificial Intelligence and Law Enforcemen - Impact on Fundamental Rights. Study requested by the LIBE committee. doi:10.2861/880024
 13. Garvie C., et al., 2016. The Perpetual Line-Up. Unregulated Police Face Recognition, Georgetown Law Center on Privacy & Technology. (dostupno na web sajtu: <https://www.perpetuallineup.org/>)

14. Gikay A.A. 2023. Live Facial Recognition for Law Enforcement: The European Union's Regulatory Approach Should be Informed by UK Police's Practice. (dostupno na web sajtu: <https://eulawanalysis.blogspot.com/2023/11/live-facial-recognition-for-law.html>)
15. Gikay A.A. 2023. Regulating use by law enforcement authorities of live facial recognition technology in public spaces: an incremental approach." The Cambridge Law Journal 82, no. 3 (2023): 414–49. <https://doi.org/10.1017/S0008197323000454>
16. Hayes P. et al., 2020. Algorithms and values in justice and security. AI & SOCIETY 35: 533–555. <https://doi.org/10.1007/s00146-019-00932-9>
17. Interpol&UNICRI. 2019. Artificial Intelligence and Robotics for Law Enforcement. (dostupno na web sajtu: <https://unicri.it/artificial-intelligence-and-robotics-law-enforcement>)
18. Kremidas-Courtney C., H. Linderstal. 2023. The convergence of new technologies endangering human agency. Friends of Europe. (dostupno na web sajtu: <https://www.friendsofeurope.org/insights/the-convergence-of-new-technologies-endangering-human-agency/>)
19. Madiega T., H. Mildebrath. 2021. Regulating facial recognition in the EU. European Parliamentary Research Services (EPRS). Brussels. DOI:10.2861/140928. (dostupno na web sajtu: [https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA\(2021\)698021_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf))
20. Maslej N. et al., 2024. The AI Index 2024 Annual Report. AI Index Steering Committee, Institute for Human-Centered AI. Stanford University, Stanford, CA. (dostupno na web sajtu: <https://aiindex.stanford.edu/report/>)
21. OECD 2024. OECD AI Policy Observatory. AI in Serbia (dostupno na web sajtu: <https://oecd.ai/en/dashboards/countries/Serbia>)
22. OECD. 2022. Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449. (dostupno na web sajtu: <https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449>)
23. Perry L.W. et al., 2013. Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations. Rand Corporation. ISBN: 978-0-8330-8148-3. (dostupno na web sajtu: https://www.rand.org/pubs/research_reports/RR233.html)
24. Prlja D., G. Gasmi., i V. Korać. 2021. Veštačka inteligencija u pravnom sistemu EU. Institut za uporedno pravo. Beograd. ISBN 978-86-80186-73-3
25. Reclaim your face. 2024. EU AI Act will fail commitment to ban biometric mass surveillance (Deutsche Version unten). (dostupno na web sajtu: <https://reclaimyourface.eu/eu-ai-act-will-fail-commitment-to-ban-biometric-mass-surveillance/>)
26. Samoili S. et al., 2021. AI Watch. Defining Artificial Intelligence 2.0. Towards an operational definition and taxonomy for the AI landscape. Publications Office of the European Union. European Parliament, Luxembourg, doi:10.2760/019901.

27. Sánchez-Monedero J., L. Dencik. 2022. The politics of deceptive borders: 'biomarkers of deceit' and the case of iBorderCtrl. *Information, Communication & Society*. 25:3, 413-430. (dostupno na web sajtu: <https://www.tandfonline.com/doi/full/10.1080/1369118X.2020.1792530>)
28. Share Fondacija. 2024. Usvojen AI Akt: Ljudska prava ostala u drugom planu. (dostupno na web sajtu: <https://www.sharefoundation.info/sr/usvojen-ai-akt-ljudska-prava-ostala-u-drugom-planu/>)
29. Statewatch. 2023. Europe's techno borders. *EuroMed Rights & Statewatch*. (dostupno na web sajtu: <https://www.statewatch.org/publications/reports-and-books/europe-s-techno-borders/>).
30. Strategy for the development of artificial intelligence in the Republic of Serbia for the period 2020-2025., "Official Gazette of RS", no. 96/2019.
31. The China Academy of Information and Communications Technology. 2022. Artificial Intelligence White Paper. (dostupno na web sajtu: https://cset.georgetown.edu/wp-content/uploads/t0442_AI_white_paper_2022_EN.pdf)
32. UNESCO. 2022. Recommendation on the Ethics of Artificial Intelligence. (dostupno na web sajtu: <https://unesdoc.unesco.org/ark:/48223/pf0000381137>)
33. Vasilkov Z. 2023. Unutrašnji poslovi i bezbednost u pravu Evropske unije nakon Lisabonskog ugovora. Zadužbina Andrejević: Beograd. ISBN 978-86-525-0429-9
34. Wendehorst C., Y. Duler. 2021a. Biometric Recognition and Behavioural Detection Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces. BRIEFING Requested by the JURI AND PETI committees Policy Department for Citizens' Rights and Constitutional Affairs. Directorate-General for Internal Policies PE 697.131 (dostupno na web sajtu: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/697131/IPOL_BRI\(2021\)697131_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/697131/IPOL_BRI(2021)697131_EN.pdf))
35. Wendehorst C., Y. Duler. 2021b. Biometric Recognition and Behavioural Detection Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces. European Parliament Study requested by the JURI AND PETI committees Policy Department for Citizens' Rights and Constitutional Affairs. Directorate-General for Internal Policies. doi: 10.2861/982599
36. White House Office of Science and Technology Policy. 2022. The Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People. (dostupno na web sajtu: <https://www.whitehouse.gov/ostp/ai-bill-of-rights>)
37. XReality Safety Intelligence (XRSI).2024. Biometrically-Inferred Data (BID). (dostupno na web sajtu: <https://xrsi.org/definition/biometrically-inferred-data-bid>).

38. Conclusion on the adoption of Ethical guidelines for the development, application and use of reliable and responsible artificial intelligence. Official Gazette of RS", No. 23/2023.
39. Zhang D. et al., 2022. The AI Index 2022 Annual Report. AI Index Steering Committee, Stanford Institute for Human-Centered AI, Stanford University. (dostupno na web sajtu: <https://aiindex.stanford.edu/ai-index-report-2022/>)