Примљено: 16. мај 2023.
Прихваћено: 17. септембар 2023.

УДК 343.982.323:342.7(497.11)
COBISS.SR-ID 151624457
DOI: 10.5937/ssb2401083R

ТЕХНОЛОГИЈА ПРЕПОЗНАВАЊА ЛИЦА И ПРАВА И СЛОБОДЕ ЛИЦА – СЛУЧАЈ РЕПУБЛИКЕ СРБИЈЕ

Невена РУЖИЋ*, докторанткиња
Универзитет у Београду, Факултет безбедности,
Београд

* nevena@privatnost.rs

ТЕХНОЛОГИЈА ПРЕПОЗНАВАЊА ЛИЦА И ПРАВА И СЛОБОДЕ ЛИЦА – СЛУЧАЈ РЕПУБЛИКЕ СРБИЈЕ

Сажетак: *Тема технологије препознавања лица, која укључује обраду биометријских података у великом обиму, а на јавним површинама у Републици Србији, била је предмет интересовања почевши од 2019. године, када је најављена њена примена. Интерес предузимања мера ради спречавања, истраге и откривања кривичних дела, гоњења учинилаца кривичних дела или извршења кривичних санкција, укључујући спречавање и заштиту од претњи јавној безбедности употребом напредне технологије, и интерес остваривања и омогућавања уживања основних права и слободе лица, могу се посматрати као опречни интереси друштва, чак и међусобно искључујући. Ипак, ова два, једнако важна, интереса нису нужно непомирљива. У овом раду дат је приказ појединих истраживања о утицају употребе технологија на понашање појединаца, иницијативе за правно уређење употребе технологије препознавања лица у различитим верзијама нацрта Закона о унутрашњим пословима који су садржали одредбе којима се омогућава употреба ове технологије, као и различите верзије процена утицаја на заштиту података. Такође је указано на релевантне акте Уједињених нација и Европске уније. Иако коначног одговора да ли је и, уколико јесте, у којим случајевима је дозвољен општи надзор јавних површина употребом овако развијене, а са становишта људских права интрузивне, технологије нема, дат је предлог мера које би могле да допринесу остваривању различитих интереса на начин да је задирање у права и слободе лица у мери која је неопходна у демократском друштву.*
Кључне речи: *биометријски надзор, вештачка интелигенција, заштита података о личности, право на приватност.*

Увод

Током 2019. године Министарство унутрашњих послова најавило је спровођење пројекта „Сигурни град" (БЕТА, 2021). Овај пројекат претпостављао је и постављање неколико стотина камера у Србији, на улицама и другим јавним местима, махом у Београду. Важећи

Закон о полицији[1], Закон о евиденцијама и обради података у области унутрашњих послова[2], као и други закони који се односе на рад Министарства унутрашњих послова нису садржавали одредбе које су уређивале питање обраде биометријских података видео-надзором јавних површина. У међувремену, новембра 2018. године, Народна скупштина усвојила је Закон о заштити података о личности[3] (у даљем тексту наведено и као Закон или ЗЗПЛ). који је, по узору на прописе Европске уније усвојене 2016. године у области заштите података, прописао услове обраде података, укључујући и обавезу вршења процене утицаја обраде на заштиту података о личности у оним случајевима за које се сматра да могу проузроковати ризик по права и слободе лица. Између осталих, обрада биометријских података у великом обиму, као и системски надзор над јавним доступним површинама у великој мери овим прописима су препознати као претпостављене ризичне обраде, тако да је израда процене утицаја обавезна (чл. 54. ЗЗПЛ).

Технологија препознавања лица и биометријски подаци

Према значењу израза Закона о заштити података о личности (чл. 4.), истоветан дефиницијама према релевантним прописима Европске уније – Општој уредби о заштити података[4] (чл. 4), као и Полицијској директиви,[5] биометријски податак је податак о личности добијен

[1] („Сл. гласник РС", бр. 6/16, 24/18 и 87/18).

[2] („Сл. гласник РС", бр. 24/18).

[3] („Сл. гласник РС", бр. 87/18).

[4] У преводу: Уредба (ЕУ) 2016/679 Европског парламента и Савета од 27. априла 2016. о заштити лица у вези с обрадом података о личности и о слободном кретању таквих података, те о стављању ван снаге Директиве 95/46/ЕЗ (Општа уредба о заштити података). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), ("Official Journal of the European Union", L 119/1), доступно на: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

[5] У преводу: ДИРЕКТИВА 2016/680 Европског парламента и Савета о заштити појединаца у вези са обрадом података о личности од стране надлежних органа у сврхе спречавања, истраге, откривања или прогона казнених дела или извршавања кривичних санкција (Полицијска директива). Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the

посебном техничком обрадом у вези са физичким обележјима, физиолошким обележјима или обележјима понашања физичког лица, која омогућава или потврђује јединствену идентификацију тог лица, као што је слика његовог лица или његови дактилоскопски подаци. Важно је истаћи да фотографија или видео снимак неког лица, иако су подаци о личности, нису нужно уједно и биометријски подаци, већ само у оним случајевима када је технички начин обраде такав да се на основу фотографије, односно снимка, лице може идентификовати на јединствен начин.

Техничка обрада неког податка о личности као биометријског податка може бити изведена у моменту прикупљања података, нпр. приликом фотографисања лица, дакле, у реалном времену, или накнадно, након што је податак прикупљен. Иако се у обе описане ситуације обрађују биометријски подаци који се, према ЗЗПЛ, сматрају посебном врстом података (чл. 17), и иако обе представљају ризик по права и слободе лице, нивои ризика значајно се међусобно разликују. Отуд и њихов различити третман. Ризици по права и слободе лица, услови примене и слично, посебно се разликују када се овај начин обраде примењује у сврху спречавања, истраге и откривања кривичних дела, гоњења учинилаца кривичних дела или извршења кривичних санкција, укључујући спречавање и заштиту од претњи јавној и националној безбедности.

Додатно, ова технологија може да се користи за различите сврхе – верификацију, идентификацију или категоризацију лица (FRA, 2019: 7–8). За разлику од прве две методе, потоња не мора нужно за резултат да има обраду података о личности на начин да се утврди идентитет лица, већ, примера ради, пол, оквирни узраст или чак раса тог лица. Без обзира на бројна етичка питања[6] која се намећу код питања сврсисходности категоризације као методе употребе ове технологије (Najibi, 2020; Buolamwini and Gebru, 2018), питање категоризације лица није предмет овог рада.

Метод верификације уобичајено се користи у затвореном окружењу, као што је то верификација дозволе приступа одређеним деловима објекта по утврђивању идентитета лица. У овом случају упо-

---

prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA ("Official Journal of the European Union", L 119/89 доступно на: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680.

[6] Примера ради, утврђивање „расног порекла" неког лица може бити основ за дискриминацију тог лица.

ређује се податак добијен преко слике лица у физичком присуству са постојећом евиденцијом, или чак подацима који се налазе на картици у поседу самог лица. Поред ових случаја, метод верификације све је чешће у употреби на граничним прелазима и аеродромима (Sachs, 2023).

Метод идентификације служи да се утврди јединствена идентификација одређеног лица тако што се упоређује са затвореном или потпуно отвореном базом података и ова метода се често назива обрадом у реалном времену (Cyphers, B., Schwartz, A., and Sheardeff, N., 2021), и са становишта права и слободе лице ова метода је највише изложена критикама, посебно имајући у виду поузданост (Goldberg, 2021), с једне стране, и обимност обраде (ReclaimYourFace, 2020), с друге.

Утицај технологије на понашање појединаца

Утицају технологије препознавања лица, односно о утицају утиска континуираног надзора над понашањем појединца, посвећена је пажња у научним часописима. Ова технологија превасходно утиче на права на приватност и на заштиту података о личности. Осећај непрестаног праћења кретања и понашања лица утиче на његово понашање, тако утиче и на избор оног кретања или понашања које је прихватљиво, и с тим у вези емпиријски је тешко утврдити ниво, обим или проценат утицаја ове технологије на понашање појединца, будући да је он у домену самоконтроле, односно самоцензуре (Xu et all., 2019).

Додатно, утицај употребе технологије препознавања лица на права на приватност и заштиту података о личности посредно утиче и на остваривање других права и слобода, као што су слобода кретања, слобода удруживања, а од посебног је значаја код грађанских протеста. Субјективан осећај приватности, као одраз стандарда „разумно очекиване приватности", који Европски суд за људска права узима у обзир приликом разматрања представки које се односе на тврдњу повреде права на приватност, не може се занемарити (ECHR, 22: 32, 70 и др). Примера ради, осећај лица у ситуацијама да, иако учествују у неком грађанском протесту на јавном месту, могу лако бити под присмотром органа, те имају бојазан да ће због изражавања својих ставова у оквиру института демократског уређења трпети последице и те како је значајан фактор у процени дозвољености неке мере (Leong, 2019). Поред ових, слобода вероисповести може бити угрожена на

начин да се лица категоришу као припадници појединих религиозних група кроз употребу алгоритама (Wakefield, 2021). Ризик од пристрасности проузроковане аутоматизованом обрадом података кроз употребу технологије вештачке интелигенције може довести до предрасуда и дискриминације према одређеним групама или појединцима (Nesterova, 2020).

Поузданост обраде је значајан предуслов приликом разматрања оправданости мере. Важно је имати у виду да ова технологија није у потпуности поуздана, а посебно није прецизна у односу на одређене групације. Дакле, може се разматрати оправданост употребе ове технологије са становишта остваривања сврхе обраде података, имајући притом у виду и друга начела обраде података – начело тачности – те се ови ризици морају узети у обзир.

Грешке у утврђивању идентитета могу се тицати како непрепознавања лица чији је идентитет неопходно утврдити и случајеве који се употребљавају као аргументи у прилог употреби ове технологије (у литератури се називају *False negatives*), тако и оне ситуације у којима се идентификује лице које заправо није тражени субјект (у литератури се називају *False positives*). "False positives" значајно утичу на живот лица који је погрешно уведен у категорију тражених, било да је реч о учиниоцима кривичних дела, или онима за које се сумња да су повезани са терористичким активностима. Случај Роберта Вилијамса из јуна 2020. године у Сједињеним Америчким Државама илустративан је пример могућих последица на права и слободе лица (Hill, 2020).

Обрада биометријских података и Закон о заштити података о личности

Свака обрада података о личности, на коју се примењује Закон о заштити података о личности,[7] мора да буде у складу са начелима обраде података – начело законитости, поштења и транспарентности, начело ограничености сврхе, начело минимизације података, начело тачности података, начело ограниченог чувања података, начело безбедности података и начело одговорности (чл. 12). Правилна примена

[7] ЗЗПЛ се примењује на обраду података о личности која се врши, у целини или делимично, на аутоматизован начин – као што је то случај са сваком применом технологије препознавања лица.

ових начела резултира у конкретним обавезама руковалаца, а за потребе овог рада само укратко ће бити приказана.

Начело законитости, поштења и транспарентности претпоставља постојање адекватног правног основа за обраду података, што у случају употребе технологије препознавања лица у сврхе спречавања, истраге и откривања кривичних дела, гоњења учинилаца кривичних дела или извршења кривичних санкција, укључујући спречавање и заштиту од претњи јавној безбедности, може бити једино да је обрада неопходна у циљу извршења законом прописаних овлашћења руковаоца (чл. 12. ст. 1. т. 5) ЗЗПЛ). Из одредбе Закона који се односи на предмет Закона изузет је део одредбе који се односи на спречавања и заштиту од претњи националној безбедности, будући да ови послови нису у искључивој надлежности Министарства унутрашњих послова, те да и други органи који се сматрају руковаоцима подацима обрађују податке о личности. У односу на ове руковаоце такође је предуслов да је обрада прописана законом.

Сам законодавац наметнуо је додатне услове обраде података када је реч о наведеним сврхама, а нарочито уколико остваривање ових сврха може да резултира обрадом посебних врста података, као што су биометријски подаци. Према члану 14. ЗЗПЛ, обрада коју врше надлежни органи у посебне сврхе је законита само ако је та обрада неопходна за обављање послова надлежних органа и ако је прописана законом, којим се одређују најмање циљеви обраде, подаци о личности који се обрађују и сврхе обраде. Додатно, у случају да је надлежни орган законом овлашћен да обрађује посебне врсте података о личности, они морају да буду неопходни, уз примену одговарајућих мера заштите права лица на које се подаци односе (чл. 18).

Дакле, обрада биометријских података мора бити прописана законом, неопходна за остваривање сврхе и сразмерна правима лица на које се подаци односе. Неопходност се у случају органа сектора безбедности подразумева, како у односу на обраду у целости тако и у односу на појединачни податак о личности који се сматра посебном врстом података.

Поред ових услова, морају бити испуњени општи услови који се односе на задирање у права и слободе лица зајемчених Уставом Републике Србије, као и Европском конвенцијом о људским правима. У складу са чланом 20. Устава РС, људска права и слободе могу законом бити ограничена ако ограничење допушта Устав, у сврхе ради којих га Устав допушта, у обиму неопходном да се уставна сврха ограничења

задовољи у демократском друштву и без задирања у суштину заједмченог права. Додатно, при ограничавању људских и мањинских права, сви државни органи, а нарочито судови, дужни су да воде рачуна о суштини права које се ограничава, важности сврхе ограничења, природи и обиму ограничења, односу ограничења са сврхом ограничења и о томе да ли постоји начин да се сврха ограничења постигне мањим ограничењем права. И према Европској конвенцији (члан 8), јавне власти неће се мешати у вршење права на приватност, али и права на заштиту података о личности), сем ако то није у складу са законом и неопходно у демократском друштву у интересу националне безбедности, јавне безбедности или економске добробити земље, ради спречавања нереда или криминала, заштите здравља или морала, или ради заштите права и слобода других.

Иницијативе за увођење биометријског надзора у Републици Србији

Уређивање употребе технологије препознавања лица на јавним местима у Републици Србији, односно покушаји уређивања, могу се, укратко изнето, сагледати како кроз јавне изјаве политичара, као руководилаца надлежног органа, тако и кроз различите верзије нацрта закона о унутрашњим пословима и пропратним актима, као што су процене утицаја на заштиту података о личности. Треба напоменути да није неуобичајено да изјаве политичара не садрже адекватну аргументацију основа и сразмерности увођења неке мере која за последицу има ограничавање права и слободе лице, Ипак, ове изјаве су резултирале реакцијама превасходно удружења грађана и појединих медија (DW, 2021). У поступку који се тицао припреме одредаба различитих верзија нацрта закона о унутрашњих пословима, али и процене утицаја на заштиту података о личности, а које су се односиле на употребу технологије препознавања лица, сучељавање опречних или другачијих мишљења се временом усложњавало (нпр. Centar DPA, 2021; SHARE, 2022; Танјуг, 2022).

Прве вести у вези са увођењем видео-надзора на јавним површинама, које би резултирале у масовној обради биометријских података о личности, потекле су од тадашњег министра унутрашњих послова током септембра 2017. године. Гостујући у једном телевизијском програму, министар је најавио почетак пројекта „Безбедан град", а који се

састоји у примени „више технологија за бољи надзор у циљу препознавање лица, таблица, могућност анализе" (Танјуг, 2017а). У то време на материју обраде података у области послова полиције примењивали су се Закон о полицији, као и Закон о заштити података о личности усвојен 2008. године, а на основу којих обрада биометријских података није била могућа. Убрзо након ове изјаве Министарство је издало саопштење, негирајући да су у питању камере ових могућности, истичући да од постављања камера у сврху утврђивања саобраћаних прекршаја, закључно са 2011. годином, није постављена ниједна нова опрема (Танјуг, 2017б).

Године 2019. тема масовног биометријског видео-надзора поново је била у жижи јавности, када је, након најаве министра унутрашњих послова да ће у главном граду бити постављено на 800 локација камере са уграђеном технологијом препознавања лица, Повереник за информације од јавног значаја и заштиту података о личности спровео надзор (Повереник, 2019а). У поступку надзора Повереник је утврдио да ова технологија није била у употреби. Такође је истакао да недостаје правни основ за овакву обраду података, као и процена утицаја на заштиту података према новом закону о заштити података о личности[8] (*ibid*.).

Прва процена утицаја на заштиту података о личности достављена је Поверенику септембра 2019. године. Ова процена припремана је као засебан документ, без иницијативе за промену законског оквира рада Министарства унутрашњих послова. У мишљењу на процену, коју је Повереник објавио на интернет презентацији овог органа, истиче се да није наведен систем, односно системи видео-надзора на које се процена односи, као ни правни основ и сврха обраде података о личности, нити територијална примена система – територија града Београда или Републике Србије. Примедбе Повереника односиле су се и на утврђивање ризика по права и слободе лица, у погледу њихове јасноће, али и погрешно утврђених ризика на начин да се извор ризика дефинише као ризик, као што је случај са „људским фактором", или опис могућег утицаја ризика на права и слободе лица чији се подаци обрађују, као ни вероватноћа и озбиљности њиховог наступања (Повереник, 2019б).

[8] У време вршења овог надзора није почела примена Закона о заштити података о личности. Он је ступио на снагу новембра 2018. године, док је примена била одложена на 9 месеци, рок који је наступио крајем августа 2019. године.

Током лета 2021. године Министарство унутрашњих послова упутило је Нацрт закона о унутрашњим пословима на јавну расправу, које је садржало одредбе о употреби технологије биометријског видео-надзора. Према члану 71. овог Нацрта, овлашћено службено лице може извршити препознавање на основу биометријских карактеристика лица ради: 1) проналажења извршиоца кривичног дела за које се гоњење предузима по службеној дужности; 2) проналажења лица за које се основано сумња да припрема извршење кривичног дела; или 3) проналажења лица за којим се трага. У вези са овом одредбом треба истаћи да, поред тога што нису јасно одређени биометријски подаци који се обрађују, веома је неодређена категорија лица која би била обухваћена овом обрадом. Након бурних реакција удружења грађана, као и појединих медија, који су указивали и на недавно усвојена документа како Уједињених нација и Европске уније, о којима је више речи у наставку овог чланка, тадашњи министар унутрашњих послова повукао је Нацрт (Еспресо, 2021).

Министарство унутрашњих послова је, по повлачењу Нацрта, организовало неколико састанака са представницима заинтересованих страна, удружења грађана, синдиката и др, и разматрало поједине институте, укључујући и употребне технологије препознавања лица. Децембра 2022. године изнет је нови Нацрт закона о унутрашњим пословима, заједно са нацртима закона или нацртима измена и допуна закона у домену рада Министарства унутрашњих послова, као и нова процена утицаја на заштиту података о личности. Иако је јавна расправа о нацрту била продужена и током новогодишњих празника, удружења грађана су измене садржане у новом документу оценили као „козметичке" (Настевски, 2022). Министарство унутрашњих послова је, на налог председнице Владе Републике Србије, повукло и овај Нацрт закона о унутрашњим пословима из процедуре усвајања, а у циљу, како је наведено у саопштењу, „да се разјасне све недоумице у јавности и да свако разуме интенцију закона који је од посебне важности за безбедност свих грађана" (Влада, 2022). За разлику од претходних верзија процена утицаја на заштиту података о личности, акт који је припреман уз Нацрт закона садржао је идентификацију појединих значајних ризика, укључујући и делимичну процену истих.[9]

[9] Акт о процени утицаја на заштиту података доступан је на интернет презентацији SHARE фондације. Преузето 29.2.2024. године са: https://www.sharefoundation.info/wp-content/uploads/Procena-uticaja-novembar-2022.pdf.

До закључења писања овог рада Министарство није објавило вест о даљем раду на Нацрту закона, односно нову верзију закона.

Међународни документи о биометријском надзору

Бројни су међународни документи којима се истиче висока ризичност излагања готово неодредивог броја лица обради по правилу непромењивих података о личности, као што су биометријски подаци који служе за јединствену идентификацију појединца, као што су физичке карактеристике лица, ход лица, или чак глас, те је у овом чланку приказана само неколица.

У Извештају „Право на приватност у дигиталном добу" Високе комесарке УН за људска права, усвојеном септембра 2021. године, наводи се да је последњих година значајно порасла доступност различитих програма за обраду података употребом технологија за препознавање лица (лика), уз једновремену приуштивост и доступност у виду висине трошкова набавке, односно поједностављене употребе. Тиме је ова обрада постала предмет свеобухватног разматрања, и нарочито критике, како у научним круговима тако и у политичком, и то како са становишта етике и људских права тако и са становишта потребе заштите јавне или националне безбедности (УН, 2021). Истичући ризике, посебно уколико употреба ове технологије подразумева и примену вештачке интелигенције, Висока комесарка предложила је државама листу активности у погледу уређења, митигације ризика, ограничене примене вештачке интелигенције, као и неопходност учешћа свих заинтересованих страна у разматрању увођења и примене ових технологија (УН, 2021: пасуси 37–56). У погледу изазова, посебно су истакнута основна начела, а посебно начела једнакости и недискриминације, учешће, као и одговорности, затим постојања, али и квалитета закона који се не односе само на оне законе непосредно у вези са употребом оваквих технологија, већ и оних којима се гарантују механизми заштите права. Даље је истакнута неопходност одговорно спроведене процене на људска права, осетљивост везе између државе и бизниса, посебно код развоја технологија, као и значаја транспарентног поступања.

Поред УН, и друге, за креирање прописа у Србији значајне, организације истакле су ризике употребе технологије препознавања лица,

посебно на начин да је таква обрада неомеђена како простором тако и временом, категоријом лица на које се може применити, начином/техником обраде и слично.

Савет Европе усвојио је Приручник о технологији препознавања лица којим је посебно истакао неопходност укључивања надзорних органа за заштиту података о личности, дакле, у случају Републике Србије, укључивање Повереника за информације од јавног значаја и заштиту података о личности (Савет Европе, 2021: 12). Даље, документом се истичу ризици употребе технологије, од идентификације података који ће бити коришћени за унос података, поузданости система и сл. (исто: 14–17).

Европски одбор за заштиту података, као тело ЕУ формирано и од представника надзорних органа за заштиту података у ЕУ и државама чланицама, са циљем уједначавања примене прописа који се односе на заштиту података, и Европски супервизор за заштиту података, као надзорни орган за примену заштите података у органима Европске уније, усвојили су заједничко мишљење у уређењу вештачке интелигенције, а које се тицало и употребе технологије препознавања лица (EDPB-EDPS, 2021). Истичући бројне ризике, штетне последице по појединца, али и друштво, с једне стране, као и непоузданост саме технологије, али и њене употребе, с друге, ова тела позвала су на општу забрану употребе вештачке интелигенције, односно технологија за аутоматизовану обраду биометријских података на јавним местима и просторима (EDPB-EDPS, 2021: пасус 32).

Употреба технологије препознавања лица, посебно када је реч о оној у реалном времену, по правилу се ставља у контекст употребе вештачке интелигенције, односно алгоритама који су дизајнирани на начин да могу независно да раде, или се чак унапређују. Вештачка интелигенција као појам, чија је употреба за законодавним процесима постала готово неизбежна, сагледава се како са становишта добробити за човека и друштво, од чега предњачи њена употребна вредност у медицини, а посебно дијагностици, тако и са становишта ризика. За сада већина земаља још увек нема националне законе, па чак ни стратешка документа којима се адресира развој и употреба система вештачке интелигенције, а Србија је једина у региону која је усвојила стратешки документ развоја вештачке интелигенције за период од 2020. до 2025. године (Стратегија, 2019).

Крајем јануара 2024. окончане су завршне консултације надлежних тела Европске уније у вези са Законом о вештачкој интелигенцији, а

чији се коначни изглед очекује и ишчекује, а затим и тумачење појединачних одредби, усвојен је принцип такозваних недопуштених ризика, односно оних случајева када је употреба вештачке интелигенције забрањена (Proposal AI Act, 2021). Како се залагао Европски парламент, али и наведена тела Европске уније, један од тих недопуштених ризика је употреба система за идентификацију лица, као што је технологија за препознавање лика у реалном времену или на даљину (Европски парламент, 2023).

Ипак, у вести о Закону о вештачкој интелигенције, објављеној са презентације Европског савета, истиче се изузетак од забране употребе ове технологије када је реч о органима надлежним за полицијске послове, под условом да су испуњене додатне гаранције (Европски савет, 2024). Оваква решења представљају компромис и балансирања остваривања заштите основних права, с једне, и остваривања интереса безбедности, посебно борбе против криминала, с друге стране.

У Анализи усаглашеног текста, објављеног крајем јануара 2024. године, образлажу се разлози и услови када је могуће да ови органи могу користити ову напредну технологију и у реалном времену (Савет ЕУ, 2024.). Треба напоменути да национална безбедност није адресирана у овим документима Европске уније, како је то случај са питањима као што је јавна безбедност и борба против криминала, имајући у виду ограничење надлежности ЕУ, односно разграничење између надлежности ове организације и њених држава чланица.

Дакле, употреба система за идентификацију лица на основу биометријских података у реалном времену на даљину може се користити на изричито одређене појединце, у ограниченом временском трајању, као и ограниченом географском подручју, посебно имајући у виду доказе или наводе који се односе на претње, жртве или учиниоце. Предуслов за примену овог изузетка јесте претходно извршена процена утицаја на основна права, као и, уколико није изузето, регистрација таквог система у базу података која је прописана овим законом (Савет ЕУ, 2024: пасус 20).

Закључак

Употреба технологије препознавања лица на основу биометријских података о лицу представља радњу обраде података која се сматра високоризичном по права и слободе лица. Отуда овај вид обраде може

бити оправдан само у изузетним случајевима уз испуњење услова који се односе како на процену ризика тако и на примену додатних гаранција. Процену ризика треба вршити на начин не само да се узму у обзир сви ризици по сва права и слободе неког лица, већ и на начин да оправда основаност одлуке за примену овакве мере у ограниченом времену, простору, као и опсегу. Оваква мера не сме да буде дозвољена на начин који омогућава примену дискреционих овлашћења, а истовремено се мора обезбедити поштовање начела одговорности. Процена ризика треба да се врши како на припрему законског основа за могуће успостављање технологије препознавања лица тако и на доношење одлуке о примени у конкретној ситуацији, односно у неком конкретном окружењу. Одлука о евентуалној потреби усвајања новог закона о дозвољености примене технологије у ограниченом обиму треба да буде донета уз укључивање свих заинтересованих страна.

Литература

Buolamwini J. and Gebru T. (2018.), Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Proceedings of Machine Learning Research 81:1–15, 2018. Conference on Fairness, Accountability, and Transparency. Retrieved 29.2.2024; https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

БЕТА (1.10.2019), „Стефановић: Систем видео-надзора у Београду омогућиће лакше расветљавање кривичних дела", Данас онлајн. Преузето 29.2.2024. https://www.danas.rs/vesti/drustvo/stefanovic-sistem-video-nadzora-u-beogradu-omogucice-lakse-rasvteljavanje-krivicnih-dela/

Влада Републике Србије (22.12.2022), „Повлачи се Нацрт закона о унутрашњим пословима из процедуре усвајања", преузето 29.2.2024. https://www.srbija.gov.rs/vest/674074/povlaci-se-nacrt-zakona-o-unutrasnjim-poslovima-iz-procedure-usvajanja.php.

Goldberg, R. D. (12.4.2021), You Can See My Face, Why Can't I? Facial Recognition and Brady, HRLR Online, Columbia Human Rights Law Review. Retrieved 29.2.2024; https://hrlr.law.columbia.edu/hrlr-online/you-can-see-my-face-why-cant-i-facial-recognition-and-brady/.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA ("Official Journal of the European Union", L 119/89; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680.

EDPB-EDPS (18.6.2021), Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Retrieved 29.2.2024; https://www.edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf

Европски парламент (последње измене 19.12.2023), EU AI Act: first regulation on artificial intelligence. Retrieved 29.2.2024; https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

Европски савет (последње измене 2.2.2024), Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world. Retrieved 29.2.2024; https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/

Еспресо (23.9.2021), Повучен Нацрт закона о унутрашњим пословима: огласио се министар Вулин. Преузето 29.2.2024; https://www.espreso.co.rs/vesti/politika/877643/povucen-nacrt-zakona-o-unutrasnjim-poslovima-aleksandar-vulin

DW (2021), China's gateway to Europe – the New Silk Road (2/2), DW Documentary. Retrieved 29.2.2024; https://www.youtube.com/watch?v=V2C0sMXyD80

Proposal for 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, Brussels, 21.4.2021, COM(2021) 206 final, 2021/0106(COD). Retrieved 29.2.2024; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

European Court of Human Rights (31.8.2022), Guide on Article 8 of the European Convention on Human Rights – Right to respect for private and family life, Council of Europe/European Court of Human Rights, home and correspondence. Retrieved 29.2.2024; https://www.echr.coe.int/documents/d/echr/Guide_Art_8_ENG

Cyphers, B., Schwartz, A., and Sheardeff, N., (7.10.2021), Face Recognition Isn't Just Face Identification and Verification: It's Also Photo Clustering, Race Analysis, Real-time Tracking, and More, EFF. Retrieved 29.2.2024; https://www.eff.org/deeplinks/2021/10/face-recognition-isnt-just-face-identification-and-verification

Закон о евиденцијама и обради података у области унутрашњих послова („Сл. гласник РС", бр. 24/18).

Закон о заштити података о личности („Сл. гласник РС", бр. 87/18).

Закон о полицији („Сл. гласник РС", бр. 6/16, 24/18 и 87/18).

(„Сл. гласник РС", бр. 6/16, 24/18 и 87/18)

Leong, B. (2019). Facial recognition and the future of privacy: I always feel like ... somebody's watching me. Bulletin of the Atomic Scientists, 75(3), 109–115. Преузето 29.2.2024. године са: https://doi.org/10.1080/00963402.2019.1604886.

Najibi, A. (2020), Racial Discrimination in Face Recognition Technology, Science in the News, Harvard Graduate School of the Arts and Science. Retrieved 29.2.2024; https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/

Настевски, А. (16.12.2022), „МУП продужио јавну расправу о спорном нацрту Закона о полицији", Нова. Преузето 29.2.2024; https://nova.rs/vesti/politika/mup-produzio-javnu-raspravu-o-nacrtu-novog-zakona-o-policiji/

Nesterova, I. (2020), Mass data gathering and surveillance: the fight against facial recognition technology in the globalized world. *SHS Web of Conferences*. Vol. 74. EDP Sciences.

Повереник за информације од јавног значаја и заштиту података о личности (12.11.2019), Мишљење Повереника на акт Министарства унутрашњих послова – Процена утицаја обраде на заштиту података о личности коришћењем система видео-надзора 073-15-1741/2019-02. Преузето 29.2.2024; https://praksa.poverenik.rs/predmet/detalji/FB967E2A-AE57-4B2C-8F11-D2739FD85A9B

Повереник за информације од јавног значаја и заштиту података о личности (22.3.2019), Повереник је спровео поступак надзора у вези са најавом постављања видео-камера од стране Министарства унутрашњих послова. Преузето 29.2.2024; https://www.poverenik.rs/sr/%D1%81%D0%B0%D0%BE%D0%BF%D1%88%D1%82%D0%B5%D1%9A%D0%B0/3071-%D0%BF%D0%BE%D0%B2%D0%B5%D1%80%D0%B5%D0%BD%D0%B8%D0%BA-%D1%98%D0%B5-%D1%81%D0%BF%D1%80%D0%BE%D0%B2%D0%B5%D0%BE-%D0%BF%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%B0%D0%BA-%D0%BD%D0%B0%D0%B4%D0%B7%D0%BE%D1%80%D0%B0-%D1%83-%D0%B2%D0%B5%D0%B7%D0%B8-%D1%81%D0%B0-%D0%BD%D0%B0%D1%98%D0%B0%D0%B2%D0%BE%D0%BC-%D0%BF%D0%BE%D1%81%D1%82%D0%B0%D0%B2%D1%99%D0%B0%D1%9A%D0%B0-%D0%B2%D0%B8%D0%B4%D0%B5%D0%BE-%D0%BA%D0%B0%D0%BC%D0%B5%D1%80%D0%B0-%D0%BE%D0%B4-%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B5-%D0%BC%D0%B8%D0%BD%D0%B8%D1%81%D1%82%D0%B0%D1%80%D1%81%D1%82%D0%B2%D0%B0-%D1%83%D0%BD%D1%83%D1%82%D1%80%D0%B0%D1%88%D1%9A%D0%B8%D1%85-%D0%BF%D0%BE%D1%81%D0%BB%D0%BE%D0%B2%D0%B0.html.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ("Official Journal of the European Union", L 119/1). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

ReclaimYourFace (1.10.2020), Biometric mass surveillance as general monitoring. Retrieved 29.2.2024; https://reclaimyourface.eu/what-is-general-monitoring-or-how-we-are-all-now-suspects-under-bms/

Савет Европе (2021), Guidelines on facial recognition. Retrieved 29.2.2024; https://rm.coe.int/guidelines-facial-recognition-web-a5-2750-3427-6868-1/1680a31751

Савет Европске уније (26.1.2024), 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 – Analysis of the final compromise text with a view to agreement. Retrieved

29.2.2024; https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf

Sachs, A. (31.1.2023), Goodbye passport stamps, hello biometrics: Customs is getting faster, The Washington Post. Retrieved 29.2.2024; https://www.washingtonpost.com/travel/2023/01/31/clear-customs-fast-airports/.

Стратегија развоја вештачке интелигенције у Републици Србији за период 2020–2025. година („Сл. гласник РС", бр. 96/19).

Share fondacija (2022), Биометрија поново у Нацрту закона о унутрашњим пословима. Преузето 29.2.2024; https://www.sharefoundation.info/sr/biometrija-ponovo-u-nacrtu-zakona-o-unutrasnjim-poslovima/

Танјуг, (16.9.2017), „Стефановић: Србија безбеднија, полиција озбиљно радила за то", Новости. Преузето 29.2.2024; https: Стефановић: Србија безбеднија, полиција озбиљно радила за то | Новости (novosti.rs)

Танјуг (27.12.2017), „МУП: Стефановић говорио само о замени старих камера, РТС". Преузето 29.2.2024; https://www.rts.rs/vesti/drustvo/2984640/mup-stefanovic-govorio-samo-o-zameni-starih-kamera.html

Танјуг (20.12.2022), „Мрежа жена у МУП: Недопустива политизација новог Закона о унутрашњим пословима", Дневник. Преузето 29.2.2024; https://www.dnevnik.rs/hronika/mreza-zena-u-mup-nedopustiva-politizacija-novog-zakona-o-unutrasnim-poslovima-20-12-2022

УН високи комесар за људска права (13.9.2021), The right to privacy in the digital age, Report of the United Nations High Commissioner for Human Rights. Retrieved 29.2.2024; https://documents.un.org/doc/undoc/gen/g21/249/21/pdf/g2124921.pdf?token=g0lZuptPNUyThT8CuN&fe=true

FRA, 2019, Facial recognition technology: fundamental rights considerations in the context of law enforcement. Retrieved 29.2.2024; https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf, 7–8.

Hill, K. (3.8.2020), Wrongfully Accused by an Algorithm, NY Times. Retrieved 29.2.2024; https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html?unlocked_article_code=1.U00.gjYH.yAa1W42Xh62v&smid=nytcore-android-share

Центар ДВА (30.9.2021), Radni sastanak o povučenom nacrtu Zakona o unutrašnjim poslovima. Преузето 29.2.2024; https://www.centarzabezbednost.org/radni-sastanak-o-povucenom-nacrtu-zakona-o-unutrasnjim-poslovima/

Wakefield, J. (26.5.2021), AI emotion-detection software tested on Uyghurs, BBC. Retrieved 29.2.2024; https://www.bbc.com/news/technology-57101248

Xu, K., Stoycheff, E., Wibowo, K., & Liu, J. (2019), Privacy and the Panopticon: Online mass surveillance's deterrence and chilling effects. New Media & Society, 21(3), 602–619. Retrieved 29.2.2024; https://doi.org/10.1177/1461444818801317

FACIAL RECOGNITION TECHNOLOGY, AND THE RIGHTS AND FREEDOMS – CASE OF THE REPUBLIC OF SERBIA

Nevena RUŽIĆ, PHD student,
University of Belgrade, Faculty of Security Studies, Belgrade

Summary

The issue of the use of facial recognition technology, which includes the processing of biometric data on a large scale, and in public areas in the Republic of Serbia, has been debated since 2019, when the deployment of these technologies was announced. The use of technology for the purpose of improving security and its impact on the rights and freedoms of persons may be viewed as conflicting interests, even mutually exclusive. Yet these two, equally important, interests are not necessarily incompatible. This paper presents an overview of the impact of the use of facial recognition technology on the behaviour of individuals, processes of drafting different versions of interior affairs bills containing provisions enabling the use of this technology and different versions of data protection impact assessments, as well as relevant acts of the United Nations and the European Union. Although the final answer whether the use of such technology to process biometric data in public areas should be permitted and, if so, when and under what conditions, is still pending, a proposal is given vis-à-vis measures that could contribute to the accommodation of different interests without interfering with the rights and freedoms of persons in a way that is not excessive in a democratic society.

Keywords: *biometric surveillance, artificial intelligence, personal data protection, privacy.*