Санела Д. АНДРИЋ[1]
Криминалистичко-полицијски универзитет у Београду
Ана С. МУТАВЏИЋ[2]
Криминалистичко-полицијски универзитет у Београду
Весела М. МИЛОВАНОВИЋ[3]
Министарство унутрашњих послова Републике Србије

ДОИ: 10.5937/bezbednost2503143A
УДК: 004.056.5:572.087
174:351.755.62
Прегледни научни рад
Примљен: 7. 8. 2025. године
Ревизија: 9. 10. 2025. године
Датум прихватања: 24. 11. 2025. године

Етички и безбедносни аспекти употребе отисака папиларних линија као биометријске идентификације

***Апстракт**: Поред свеī развоја технике и технолоīије, цртеж папиларних линија и даље представља најрасīрострањенији метод реīистрације и идентификације особа. Јединственост, универзалност, непроменљивост и преносивост чине отиске папиларних линија поузданом научно верификованом биометријском карактеристиком. У криминалистичкој техници (форензици) метод дактилоскопирања користи се за реīистрацију и идентификацију особа у циљу проналаска учиниоца кривичних дела. Међутим, у савременом друштву, под утицајем развоја информационо-комуникационих технолоīија, идентификација помоћу отисака папиларних линија користи се у „цивилном сектору" за откључавање сиīурносних брава, сефова, мобилних телефона, рачунара и слично. У раду је дат преīлед основних карактеристика отисака папиларних линија, са освртом на монода-*

[1] sanela.andric@kpu.edu.rs
[2] ana.mutavdzic@kpu.edu.rs
[3] vesela.milovanovic@mup.gov.rs

ктилоскопирање и акцентом на етичким и безбедносним аспектима њихове (зло)употребе као биометријске карактеристике.

***Кључне речи**: етика, безбедност, полицијска етика, отисци папиларних линија.*

Увод

Савремена криминалистичка техника (форензика) за идентификацију особа користи биометријске карактеристике попут отисака папиларних линија прстију, дланова и табана, очне ретине/ириса, ДНК профила и записа гласа. Раније су се за регистрацију и идентификацију учинилаца кривичних дела користиле различите рудиментарне (застареле) и неетичке методе, попут сакаћења, жигосања, осмуђивања (код мушкараца), али и антропометрија, која представља први покушај научне регистрације и идентификације особа. С развојем наука, нарочито криминалистичке технике (форензике) и информатике (информационо-комуникационих технологија) долази до установљавања и развоја савремених метода за регистрацију и идентификацију особа које се заснивају на научним и етичким принципима и које су олакшале процес проналажења учинилаца кривичних дела. У савременом друштву биометрија је добила ширу употребу у цивилном сектору и користи се свакодневно за идентификацију и верификацију особа. Биометријски системи који се користе за регистрацију и идентификацију особа јесу: АФИС (AFIS – *Automated Fingerprint Identification System*), ДНК, 3Д фотометрија, антропологија и фацијална реконструкција, геометрија лица, геометрија длана, распоред вена, изглед очне ретине и ириса, анализа телесних мириса, одонтолошка идентификација, фоноскопија, анализа рукописа и потписа (Бјеловук, 2022: 27).

Правни основ за форензичку регистрацију[4] у Републици Србији дају следећа правна акта: *Закон о полицији*, који дефинише полицијске послове и послове криминалистичко-форензичке идентификације, *Законик о кривичном поступку*, који уређује процедуру узимања биометријских узорака, односно узорака биолошког порекла, затим *Закон о евиденцијама и обради података у области унутрашњих послова*, који регулише утврђивање идентитета, *Закон о заштити података о личности*, који спречава злоупотребу прикупљених података, док *Закон о националном ДНК регистру* уређује област вођења Националног ДНК регистра. Правилник о криминалистичко-форензичкој регистрацији, узимању других узорака и криминалистичко-форензичким вештачењима и анализама регулише поступање полицијских службеника током форензичке регистрације (Бјеловук, 2022: 29–31). У члану 62 Закона о полицији истакнуто је да су полицијски службеници овлашћени да врше криминалистичко-форензичку регистрацију, док се у члану 64 као врсте полицијских овлашћења наводе провера и утврђивање идентитета лица (Закон о полицији).

Папиласкопија, која је првобитно настала као метод регистрације и верификације особа у циљу проналаска учиниоца кривичних дела, у савременом друштву има ширу употребу. Данас отисци папиларних линија за верификацију особа имају распрострањену (цивилну) употребу и користе се за осигуравање/откључавање сигурносних брава, сефова, мобилних телефона, рачунара и слично. Отисци папиларних линија су јединствени за сваку особу и не мењају се током живота. У поређењу са лозинкама и картицама теже их је копирати и украсти, омогућавају брзу аутентификацију, нарочито на мобилним уређајима, у банкарству и контроли приступа. Међутим, њихова употреба носи и одређене ризике. Биометријске базе могу бити мета хакера и „цурење" ових података је трајни безбедносни ризик, те се могу користити без информисаног пристанка у системима за праћење и масовни надзор.

[4] Регистрационе збирке су базе података о личности које садрже биометријске податке и евиденције. Погледати опширније у: Бјеловук, И. (2022). *Криминалистичка техника*. Криминалистичко-полицијски универзитет, Београд.

Трагови папиларних линија као биометријска идентификација

Папиларне линије су рељефне линије на кожи прстију, дланова и табана које формирају цртеже. Представљају идентификационе карактеристике које имају велики значај за криминалистичку технику, односно форензику. С обзиром на то да папиларне линије формирају графички цртеж и садрже отворе/завршетке знојних и лојних жлезда, оне уједно представљају и морфолошку и биолошку идентификациону карактеристику сваке особе. Морфолошки, оне остављају цртеж, односно траг који је јединствен за сваку особу, док биолошки представљају извор ДНК материјала јер су папиларне линије прстију, дланова и табана прекривене знојем и епителним ћелијама које се перманентно љуште са коже (Бјеловук, 2022: 41–42; Бјеловук, Ламовец & Васовић, 2023: 29). Научно верификоване идентификационе карактеристике папиларних линија јесу универзалност, непроменљивост, индивидуалност, могућност груписања и преносивост. То значи следеће: да папиларне линије на прстима, длановима и табанима поседују сви људи на свету; да се оне формирају још у трећем гестацијском месецу и образују цртеж који се не мења током живота већ се сразмерно увећава; да су јединствене код сваког човека, нису исте на прстима једне шаке, не понављају се ни код једнојајчаних близанаца јер постоји разлика у врсти и положају минуција; може се извршити типизација цртежа папиларних линија; остављају латентне површинске трагове јер су константно прекривене знојем (Бјеловук, 2022: 42–43).

За визуелизацију латентних трагова папиларних линија користе се физичке и хемијске методе. Као физичке методе користе се разне врсте дактилоскопских прахова и суспензија које се заснивају на адхезивној сили и које не доводе до физичке реакције између зноја и супстанце која се користи за визуелизацију. Дактилоскопски прахови који се најдуже користе јесу: златни прах, графитни или угљени прах, магнетни прах, прашкови у боји и флуоресцентни прашкови/УВ прашкови (Бјеловук, 2022: 176). Нове мање штетне методе заснивају се на (био)полимерним материјалима, попут декстрана као компоненте праха за визуелизацију латентних трагова. Декстран је биоразградив

и биокомпатибилан, нетоксичан је и спречава штетне ефекте по особе које га користе (Vučković, et al., 2021a: 149–160; Vučković, et al., 2020b: 83–86). Хемијске методе за изазивање латентних трагова папиларних линија подразумевају употребу реагенса који изазивају хемијску реакцију са неком супстанцом из зноја, а примењују се код трагова на порозним подлогама попут хартија и платна. Реагенси који се најчешће користе у хемијским методама јесу сребро-нитрат ($AgNO_3$), нинхидрин, ДФО (DFO), ИНД (IND) и ПД (PD) раствори (Бјеловук, 2022: 180–184). Након изазивања/визуелизације, трагови папиларних линија се фиксирају, фотографишу размерном камером, описују у увиђајном записнику и изузимају са места догађаја дактилоскопским фолијама. Дактилоскопска фолија може бити црна, бела и желатинаста (Бјеловук, 2022: 179).

Дактилоскопија је метод за регистрацију и идентификацију на основу папиларних линија на кожи прстију. Декадактилоскопија је метод за регистрацију и идентификацију особа на основу проучавања папиларних линија на свих десет прстију (*deka* – десет, *dactilo* – прст, *skopein* – гледати, посматрати), док је монодактилоскопија метод за регистрацију и идентификацију особа на основу проучавања папиларних линија на једном прсту (*monos* – један, *dactilo* – прст, *skopein* – гледати, посматрати). У савременој криминалистичкој техници/форензици картотека дактилоскопске збирке дигитализована је и преведена у АФИС систем (Бјеловук, 2022: 46).

Безбедносни аспект биометријских система

Отисци папиларних линија представљају најраспрострањенији метод биометријске идентификације особа и пружају високу прецизност и ефикасност. Регистрација и идентификација на основу отисака папиларних линија комфорна је и неинвазивна, а с развојем технике и технологије, нарочито информационо-комуникационих технологија, њена употреба је знатно олакшана. Међутим, њихова употреба отвара низ етичких питања и могућност злоупотребе, попут нарушавања приватности, крађе идентитета,

неовлашћеног прикупљања, злоупотребе од стране државних органа, „подметања" отисака и слично, иако се сугерише се да су биометријски идентификациони документи имуни на ове злоупотребе или изузетно отпорни на њих, те да су заправо облик заштите од њих (Alterman, 2003: 139). Технологија отисака прстију је тренутно најпоузданија, уз тврдњу да је стопа лажног прихватања (FAR) и стопа лажног одбијања (FRR) 0,01% или мања. То значи да се мање од једне особе од 10.000 људи упари са туђим отисцима прстију (FAR) или се не упари са сопственим отисцима прстију (FRR). Односно, ако неко жели да нас верификује/идентификује, наши отисци прстију ће нас идентификовати у 99,99 случајева од 100. Међутим, да ли је заиста тако?

Недавно је Међународна организација цивилног ваздухопловства (ICAO) усвојила глобални хармонизовани план за интеграцију биометријских идентификационих информација у пасоше и друге машински читљиве путне исправе. Међутим, повезивање биометријских база података може представљати опасност по заштиту података о личности, а масовна употреба биометријских система може довести до социјалне контроле и дискриминације, нарочито у ауторитарним режимима, где се такви системи могу (зло)употребити за праћење и контролу грађана. Биометријске идентификације потенцијално могу нанети штету појединцима, кроз кршење грађанских слобода и права. Чак ни људи са кривичним досијеом тренутно нису нужно криминалци, те органи за спровођење закона немају право да спроводе надзор над општом популацијом без икаквих доказа и основане сумње. (Alterman, 2003; Sutrop & Laas-Mikko, 2012). „Етика биометријске идентификације не може да почива на претпоставци да су подаци апсолутно безбедни" (Alterman, 2003: 142).

Биометријски систем је аутоматски систем за идентификацију и аутентификацију особа који користи јединствене биолошке карактеристике појединца, попут отиска прста, лица, дужице ока, гласа, мрежњаче и слично. Због високе ефикасности биометријског система отисака прстију у верификацији и идентификацији особа, бројне владине и приватне организације користе овај сис-

тем у безбедносне сврхе (Joshi et al., 2018). Биометријски системи данас имају широк опсег примене – од система за евиденцију радног времена малих компанија до система контроле приступа за нуклеарне уређаје; од контроле приступа, контроле граница, војних база, заштите осетљивих података, преко банкомата, кредитних картица, онлајн трансакција до заштите приватних рачунара и мобилних телефона. Међутим, иако употреба биометрије побољшава безбедност, сами биометријски системи су рањиви и подложни спољашњим претњама (хаковање и претња малициозним програмима), тако да је све већа употреба биометрије у безбедносне сврхе наметнула потребу за истраживањем метода напада на биометријске системе (Alaswad et al., 2014).

Напади на биометријске уређаје и системе деле се у четири групе: 1) напади на нивоу обраде и преноса, 2) напади на нивоу улаза (*input*), 3) напади на позадину (*back-end*), 3) напади на (биометријски) упис и 4) напади током процеса пријављивања (Alaswad et al., 2014).

Напади на улазном нивоу (*input*) дешавају се у тренутку прикупљања података, те системи морају имати резервне процесе у случају квара. Најчешћи улазни напади су спуфинг (s*poofing* – имитација отиска прста), пропуштање или саботажа уређаја (*buffer overflow*, прекомерно светло које омета сензор, кратак спој или прекидање улазних података). Напади на позадински систем (*background*) јесу напади на системе за упоређивање узорака или одлучивање. Најчешћи су напади на базу, збирку отисака, при чему може доћи до крађе идентитета. На крају, напади током процеса пријављивања обухватају коришћење лажних докумената за идентификацију, сарадњу са корумпираним службеницима и хаковање електронског система за пријаву. Заштита од свих наведених напада подразумева енкрипцију, заштићену комуникацију и систем за откривање неовлашћених измена података (Alaswad et al., 2014).

Када је реч о биометријском систему отисака прстију, идентификовано је шеснаест тачака напада. Тај систем може бити мета напада администратора система, овлашћеног корисника, лаика који покреће *DoS* напад коришћењем биометријске апликаци-

је попут банкомата или противника (хакера) који поседује знање о биометријском систему. Напади који долазе од администратора система називају се инсајдерским нападима или административним преварама. Тачке напада на биометријски систем су следеће: 1) директни и индиректни напад – директни напад се врши приказивањем биометријских карактеристика регистроване особе циљањем улазног уређаја или апликације како би се приступило систему, док се код индиректног напада подразумевају стручност и познавање биометријских система како би се пресреле информације. Овде ћемо нагласити да су поједини аутори извршили процену рањивости система за верификацију отисака прстију која је показала да је преко 75% покушаја директног напада било успешно, док су други аутори доказали да 11 различитих система за препознавање отисака прстију прихвата вештачки створене лепљиве (желатинске) прсте; 2) одбацивање – искоришћавање ограничења биометријског система феноменом лажног прихватања; 3) контаминација или прикривена аквизација (преузимање) – несвесно остављање отисака папиларних линија у свакодневној рутини које нападач користи за генерисање лажних отисака тако што врши визуелизацију и подизање латентних трагова и прављење калупа (мулажирање); 4) присила – нападач може употребом силе натерати особу да унесе своје биометријске податке, а могућност ових инцидената постоји на недовољно обезбеђеним банкоматима; 5) немар – овакви напади се дешавају уколико особа заборави да се одјави са биометријске апликације; 6) администратор система или овлашћено лице могу покренути напад; 7) напади на сензоре манипулисањем биометријским подацима – напад лажним отиском, креирањем лажног прста или мењањем отиска регистроване особе и слично; 8) напади помоћу екстракције карактеристика – циљање модула за екстракцију карактеристика тако да он постане неспособан да генерише стварну карактеристику која одговара достављеном отиску прста; 9) напад на модул техничке заштите шаблона – нападач циља информације у вези са кључем у алгоритму који се користи за шифровање (енкрипцију); 10) напади на модул за подударање, хардверску или софтверску компоненту која је одговорна за извршавање подударања током фазе аутентификације; 11) напад на базу података шаблона/збирке отисака – циљање на

базу података директно или индиректно путем споља компромитованог система како би се поново употребили или изменили шаблони/збирке отисака; 12) напад типа „човек у средини" – нападач пресреће комуникациони канал како би прикупио биометријске податке легитимне особе; 13) измена права приступа – уписивање корисника са различитим привилегијама или правима приступа у биометријски контролисану апликацију; 14) поништавање одлуке – нападач користи тзв. тројанског коња (компјутерски вирус) да поништи модул за одлучивање и окрене резултат верификације у своју корист; 15) напад ускраћивања услуге (DoS) – убацивање мноштва лажних захтева за приступ („бомбардовање система") до тачке у којој рачунарски сервер није више у могућности да обради валидне захтеве; 16) упад – нападач продаљује у складиште шаблона преко екстерног система. На крају, постоје и напади без напора услед системских ограничења. Овде се мисли на нетачну аутентификацију и одбијање услед лажног неподударања (Joshi et al., 2018: 4–10).

Поред наведених тачака напада на биометријске системе постоје четири модела претњи које представљају начин да се идентификују различите могућности напада или потенцијалне претње и рањивости у биометријском систему (Joshi, 2018). Први модел дали су Рата и сарадници (*Ratha et al. model*). Овај модел на основу приступне тачке информација у биометријском систему идентификује осам слабости (рањивости) које доводе до специфичног типа напада – напад на сензоре, односно, лажна биометријска презентација на сензору; напад пресретањем комуникационог канала између сензора и екстрактора карактеристика; напад заобилажењем модула за екстракцију карактеристика помоћу тројанског коња; напад на комуникациони канал између екстрактора карактеристика и упаривача; напад на модул за подударање и поништавање резултата помоћу тројанског коња, како би генерисао висок резултат подударања и послао позитиван одговор биометријски контролисаној апликацији и потпуно заобишао процес аутентификације; напад који помаже уљезу да истражи начине за цурење података, што омогућава прикупљање шаблона и њихову модификацију; напад на комуникациони канал између базе пода-

така шаблона и модула за подударање како би нападач прикупио шаблоне и директно их репродуковао или изменио да би приступио систему са идентитетом различитих корисника; напад који омогућава заобилажење свих компоненти система и директно манипулисање одлуком система у своју корист како би се поништиле карактеристике перформанси биометријске апликације. Други модел претњи је модел „рибље кости" (*The fishbone model*) који приказује пет узрока рањивости биометријских система: унутрашњи квар, администрација, инфраструктура, небезбедна обрада и патент или биометријска отворености. Овај модел наглашава опште грешке које треба избегавати и безбедносне технике које треба имплементирати у биометријске системе. Најједноставнији начин за обезбеђивање биометријског система јесте чување шаблона и системских модула (компоненти) на паметним картицама. Трећи модел дали су Нагар и сарадници (*The Nagar et al. model*). Овај модел се наслања на модел „рибље кости" при одређивању узрока рањивости биометријских система – небезбедна инфраструктура, очигледност биометрије и унутрашњи квар. Четврти модел су направили Бартлоу и Цукић (*Bartlow and Cukic framework*) и разложен је на неколико модула и подсистема – модул административног посматрања односно управљања системом, подсистем ИТ окружења и биометријски подсистем. Овај модел се може користити само као референтна вредност за тестирање и валидацију постојећих и предложених безбедносних техника (Joshi et al., 2018: 10–14). Међутим, биометријска аутентификација је последњих година заменила лозинке и постала најпопуларнији модел аутентификације па заштита биометријских података постаје приоритет. (Lovisotto, et al., 2020)

Када је у питању Република Србија, биометријски подаци (фотографија, отисци прстију и потпис) који се прикупљају приликом издавања путних и личних исправа користе се искључиво за ту сврху, односно само за израду и проверу идентитета у вези са личним и путним исправама. Обрада биометријских података строго је ограничена *Законом о заштити података о личности* и *Законом о путним исправама*, податке обрађује искључиво Минис-

тарство унутрашњих послова (МУП) ради издавања докумената и вођења евиденција, те се узети подаци не смеју користити у друге сврхе без изричите законске основе. Међутим, у оквиру кривичног поступка или међународне сарадње, уз судски налог или на основу међународног уговора, могућа је употреба биометрије за идентификацију лица. Министарство унутрашњих послова, као надлежни орган који прикупља биометријске податке приликом издавања личних и путних исправа, има право приступа тим подацима за издавање докумената, искључиво за проверу идентитета, у оквиру истрага (ако се трага за особом), у сарадњи са другим државним органима у складу са законом (тужилаштво, суд). МУП не може давати те податке трећим лицима без јасног законског основа. Тако, на пример, здравствене установе немају приступ биометријским подацима из система за путне исправе. Те податке могу користити искључиво у специфичним случајевима, као што су вештачења у судским поступцима, одлуке суда (у кривичном поступку) и хитне мере по одобрењу надлежног органа. У редовним здравственим поступцима (пријем, лечење, дијагноза) нема основа за коришћење података као што су отисци прстију или дигитални потпис из пасоша. Такође, установе образовног система (школе, факултети) немају никакво законско овлашћење да приступају или користе биометријске податке из система МУПРС. Чак и ако се ради о идентификацији ученика (нпр. за испите или евиденцију присуства), она се може спроводити само на основу података које ове установе прикупљају саме, уз сагласност ученика или њихових родитеља.[5]

На крају је неопходно да се осврнемо на могућности смањења безбедносних ризика употребе отисака папиларних линија као биометријске идентификације, односно, биометријских подата-

[5] Информисати се опширније у: *Закон о полицији*, Службени гласник Републике Србије, бр. 6/2016, 24/2018 и 87/2018, *Закон о путним исправама*, Службени гласник Републике Србије, бр. 90/2007, 116/2008, 104/2009, 76/2010, 62/2014 и 81/2019, и *Закон о заштити података о личности*, Службени гласник Републике Србије, бр. 87/2018.

ка уопштено. Непроменљивост отисака прстију уједно представља и предност иману. Предност је брза и једноставна идентификација, а мана је то што биометријски подаци не могу бити замењени уколико су угрожени. На пример, уколико су лозинка или број кредитне картице на мети хакера, они се могу заменити, док код отисака прстију та опција не постоји. Да би се безбедносни ризик умањио, уводи се концепт поништиве биометрије (*cancelable biometrics*), који су предложили Рата и сарадници (Ratha, et al., 2001). Поништива биометрија представља концепт у којем се оригинални биометријски податак (нпр. отисак прста) намерно трансформише (деформише) математичком функцијом у нови, изведени шаблон, који се користи за идентификацију и аутентификацију, док се оригинал никада не чува. Ако тај шаблон буде компромитован, може се једноставно „поништити" и заменити новим, применом другачије трансформације над истим биометријским узорком – слично као промена лозинке. На тај начин, поништива биометрија омогућава ревокацију и поновно издавање биометријских података, чиме се смањује ризик неповратног губитка приватности који постоји код традиционалних биометријских система, где се једном откривени отисак не може променити (Ratha, et al., 2001, 628–633).

Етички аспект и могућност злоупотребе биометријских података

Претпоставке о неовлашћеном приступу и коришћењу биометријских података могуће су као и са свим другим подацима о личности. С развојем информационо-комуникационих технологија и вештачке интелигенције (*AI*) наши подаци се налазе свуда и потенцијално су свима доступни. Свакодневно остављамо шифре на разним серверима, користимо отисак прста за приступ паметним телефонима и рачунарима, а сви ти подаци остају похрањени у „неком делу интернета". Стога је легитимно поставити питање о безбедности личних података. Међутим, прецизних истраживања и података о злоупотреби биометријских података у нашој држави још увек нема.

Такође, када је реч о етичком аспекту (зло)употребе отисака прста као биометријске идентификације, домаћих истраживања нема. С развојем информационо-комуникационих технологија појавила се и нова врста криминала – високотехнолошки криминал – и требало би истраживања окренути у том смеру. Засад нам примери злоупотребе биометријских података долазе из Индије, Кине и Сједињених Америчких Држава (САД). Индијски национални биометријски систем складишти отиске прстију од више милијарди грађана. У октобру 2023. године дошло је до „цурења" података када се десио безбедносни пропуст на систему за документа Вест Бенгал (*West Bengal*). Фотографије и отисци прстију корисника били доступни јавности пре него што је грешка уочена и отклоњена. Полицији су стизале пријаве да су криминалне групе клонирале отиске прстију из регистара, правиле силиконске отиске и вршиле аутентификације, чинећи кривично дело неовлашћене банковне трансакције. Наводи се да је 500 GB података „процурело" са сервера фирме Зелена мисао (*ThoughtGreen*), а грешка је омогућила нападачу на систем (хакеру) да погоди шеснаестоцифрене шифре за издавање власничких права (Biometric update.com, 2023).[6] Затим је у Кини забележен случај масовног кршења људских слобода и права неетичним и присилним узимањем биометријских података. Хјуман рајтс воч (*Human Rights Watch*) утврдио је да су кинеске власти систематски прикупљале биометријске податке становника Ујгурског региона – отисак прста, глас, ДНК, ирис – формирајући централизовани надзор и профилисање локалног становништва. Биометријски подаци коришћени су за надзор кретања, детекцију „неповерења" и друге облике контроле мањинске заједнице. Становници су без пристанка подвргнути биометријској идентификацији и присилној интервенцији кампова за преваспитавање (*re-education*). Од краја 2016. године, кинеска влада је подвргла 13 милиона етничких Ујгура и других муслимана у Син-

[6] Цео текст погледати на: *State government fixes bug exposing Aadhaar biometric records*, Biometric.com, Oct 13, 2023, 1:09 pm EDT | Chris Burt, https://www.biometricupdate.com/202310/state-government-fixes-bug-exposing-aadhaar-biometric-records?utm_source=chatgpt.com, доступан 29. 7. 2025.

ђангу масовном произвољном притварању, присилној политичкој индоктринацији, ограничењу кретања и верском угњетавању. Процене указују да се под овом појачаном репресијом скоро милион људи држи у камповима за „политичко образовање". Владина „Кампања снажног удара против насилног тероризма" претворила је Синђанг у један од главних кинеских центара за коришћење иновативних технологија у сврху друштвене контроле. Извештај који је поднео Хјуман рајтс воч пружа детаљан опис и анализу мобилне апликације коју полиција и други званичници користе за комуникацију са Интегрисаном платформом за заједничке операције (IJOP, 一体化联合作战平台), једним од главних система које кинеске власти користе за масовни надзор у Синђангу. Хјуман рајтс воч је први пут известио о тој платформи у фебруару 2018. године, напомињући да полицијски програм прикупља податке о људима и пријављује званичницима оне које сматра „потенцијалном претњом". Поједине особе су притворене и послате у кампове за политичко образовање и друге установе. „Обрнутим инжењерингом" ове мобилне апликације тачно је утврђено које врсте понашања и људи циља овај систем масовног надзора (*Human Rights Watch*, 2019).[7] Трећи случај долази из САД, где је тексашки тужилац 2022. године поднео пријаву против компаније Мета (Фејсбук – *Facebook*) због наводног складиштења отисака прстију и гласовних записа без информисаног пристанка корисника како захтева државни закон. Компанија Мета је претходно платила 650 милиона америчких долара (USD) за тужбу због незаконите употребе биометријских података у држави Илионоис. Речима државног тужиоца Тексаса Кена Пакстона, Мета је 2022. године пристала да плати 1,4 милијарде долара тужбу државе Тексас због неовлашћеног прикупљања биометријских података корисника. То је други највећи споразум компаније Мета са савезним или државним законодавцима, након споразума од пет милијарди долара са Феде-

[7] Цео извештај погледати на: *Human Rights Watch*, China's Alorithms of Repression, Reverse Engineering a Xinjiang Police Mass Surveillance App, https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass?utm_source=chatgpt.com, доступан 29. 7. 2025.

ралном трговинском комисијом из 2019. године због кршења приватности потрошача (*Axios*, 2022).[8] На основу наведених примера индикативне су могућности етичке злоупотребе биометријских података, било да су у питању државне службе или приватне компаније. „Цурење" и злоупотреба података могуће су услед грешке на серверима и злоупотребе службеног положаја, а последице се крећу од кривичних дела која врше криминалне групе до државне контроле коју спроводе владине институције.

Етички аспект (зло)употребе отисака папиларних линија као биометријске идентификације односи се пре свега на заштиту приватности и аутономије појединца, као и на одговорност институција које те податке прикупљају и користе. Да би се спречиле злоупотребе, неопходно је увести низ техничких, правних и организационих мера које ће осигурати да се биометријски подаци користе искључиво у сврху за коју су прикупљени и омогућити да корисник има контролу над својим подацима. Пре свега, прикупљање биометријских података мора бити засновано на информисаном и добровољном пристанку, уз јасно објашњење где, на који начин и колико дуго ће се прикупљени подаци чувати. Институције треба да се придржавају начела минимизације података (прикупљање само онога што је неопходно) и да обезбеде строгу контролу приступа и шифровање шаблона. Неопходна је и законска регулатива, односно, прописивање санкција за неовлашћено прикупљање (без информисаног пристанка), обраду и/или дистрибуцију биометријских података, као и надзор независних тела. Поред тога, треба промовисати етичку одговорност и транспарентност. Тачније, корисници морају знати како се њихови подаци користе и имати право на приступ, кориговање или брисање својих биометријских података. Комбинација технолошке заштите, правне контроле и (про)етичке свести представља најделотворнији начин за спречавање злоупотреба.

[8] Цео текст погледати на: *Texas AG sues Meta for allegedly exploiting users' biometric data*, Axios.com, https://www.axios.com/2022/02/15/texas-facebook-meta-biometric-data?utm_source=chatgpt.com, доступан 29. 7. 2025.

На крају можемо поставити филозофско-етичко питање: ако се узимање биометријских података заснива на добровољности и неприсилности, а њихово похрањивање у базе података је обавезно ради утврђивања идентитета и уређено законом, да ли се онда заиста заснива на добровољности? И да ли се заиста безбедност особа и података о личности може гарантовати вулнерабилним биометријским системима? Бројна етичка и безбедносна питања се отварају, те је неопходно да се спроведу домаћа истраживања и да се покуша дати одговор на егзистенцијалистичко питање – колико смо заиста безбедни?

Закључак

Трагови папиларних линија, као јединствено и непроменљиво морфолошко обележје сваког појединца, представљају један од кључних елемената у области криминалистичке технике и форензичке идентификације. Њихова универзалност, индивидуалност и могућност типизације омогућавају ефикасно повезивање физичких трагова са конкретним лицима, што значајно доприноси откривању и расветљавању кривичних дела и идентификацији учиниоца. Посебан значај у криминалистичкој пракси има монодактилоскопија, која омогућава идентификацију на основу отисака само једног прста, што је од пресудне важности у случајевима када се на месту кривичног догађаја налазе само делимични трагови. Међутим, у савременом друштву је дошло до ширења употребе метода биометријске идентификације помоћу отисака папиларних линија и на цивилни сектор, те се он свакодневно користи за откључавање личних рачунара и мобилних телефона, сигурносних брава и сефова, за верификацију и одобрење приступа објектима и слично.

Развој савремених технологија, посебно информационо-комуникационих технологија и биометријских система као што је АФИС, значајно је унапредио брзину и ефикасност идентификације, али истовремено отворио и бројна етичка и правна питања. Биометријски подаци, укључујући трагове папиларних линија,

представљају осетљиву категорију личних података чија заштита захтева изузетну пажњу. Могућности њихове злоупотребе, посебно у контексту неовлашћеног надзора, профилисања и нарушавања приватности, намећу потребу за јасним и прецизним нормативним оквирима који ће регулисати прикупљање, обраду и чување ових података. Рањивост биометријских података, нарочито биометрије отисака папиларних линија, произилази из њихове широке употребе у верификацији и идентификацији особа, од система за евиденцију радног времена, система контроле приступа, контроле граница, војних база, заштите осетљивих података, преко банкомата, кредитних картица, онлајн трансакција до заштите приватних рачунара и мобилних телефона. У Републици Србији, правни основ за формирање и коришћење регистрационих збирк представљају *Закон о полицији*, *Законик о кривичном поступку*, *Закон о евиденцијама и обради података у области унутрашњих послова*, *Закон о заштити података о личности* и *Закон о националном ДНК регистру* који уређује област вођења Националног ДНК регистра, док *Правилник о криминалистичко-форензичкој идентификацији* регулише поступање полицијских службеника током форензичке регистрације.

Упркос очигледним предностима, верификација и идентификација особа на основу отисака папиларних линија као биометријска метода није лишена недостатака, а услед тога ни бројних изазова. Биометријски системи су подложни бројним врстама напада, попут хаковања, крађе идентитета и манипулације подацима, али и злоупотреби од овлашћених лица и државних органа. Поред тога, етичке дилеме у вези са приватношћу, добровољношћу и транспарентношћу обраде, складиштења и чувања података остају нерешене. Иако национални закони, попут *Закона о заштити података о личности*, штите грађане од злоупотребе, технолошки развој и недовољна информисаност јавности остављају простор за потенцијалне злоупотребе. Чињеница да су биометријски подаци све заступљенији у свакодневној употреби, а да притом нема довољно домаћих истраживања о њиховој безбедности, указује на потребу за критичким преиспитивањем, едукацијом јавности и сталним

унапређењем правне регулативе и технолошке заштите. У светлу тога, поставља се суштинско питање – да ли смо заиста безбедни у друштву које све више зависи од система који, иако ефикасни, нису непогрешиви.

Закључно, трагови папиларних линија задржавају свој статус једног од најпоузданијих извора идентификације у криминалистичкој пракси. Међутим, њихова примена мора бити заснована на начелима законитости, пропорционалности и поштовања основних људских права, како би се обезбедила равнотежа између безбедносних потреба друштва и заштите индивидуалне слободе.

Литература

1. Alaswad, A. O., Montaser, A. H., Mohamad, F. E. (2014). Vulnerabilities of biometric authentication threats and countermeasures. *International Journal of Information & Computation Technology*, *4*(10): 947–58.
2. Alterman, A. (2003). "A piece of yourself": Ethical issues in biometric identification. *Ethics and information technology*, *5*(3): 139–150.
3. Бјеловук, И. (2022). *Криминалистичка техника*. Криминалистичко-полицијски универзитет, Београд.
4. Бјеловук, И., Ламовец, Ј., Васовић, Р. (2023). Визуелизација латентних трагова папиларних линија на бакарним површинама таложењем метала. *Безбедност*, *65*(3): 29–45.
5. Vučković, N., Glođović, N., Radovanović, Ž., Janaćković, Đ., Milašinović, N. (2020a). A novel chitosan/tripolyphosphate/L-lysine conjugates for latent fingerprints detection and enhancement. *Journal of Forensic Sciences*, *66*(1): 149–160.
6. Vučković, N., Dimitrijević, S. D., Milašinović, N. (2020b). Visualization of Latent Fingerprints Using Dextran-based Micropowders Obtained From Anthocyanin Solution. *Adli Bilimler ve Suç Araştırmaları*, *2*(2): 83–133.
7. Joshi, M., Mazumdar, B., Dey, S. (2018). Security vulnerabilities against fingerprint biometric system. *arXiv preprint arXiv:1805.07116*.

8. Lovisotto, G., Eberz, S., Martinovic, I. (2020, September). Biometric backdoors: A poisoning attack against unsupervised template updating. In *2020 IEEE European Symposium on Security and Privacy (EuroS&P)*, pp. 184–197.
9. Ratha, N. K., Connell, J. H., Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM systems Journal*, *40*(3): 614–634.
10. *Закон о полицији*, Службени гласник Републике Србије, бр. 6/2016, 24/2018 и 87/2018.
11. *Закон о путним исправама*, Службени гласник Републике Србије, бр. 90/2007, 116/2008, 104/2009, 76/2010, 62/2014 и 81/2019.
12. *Закон о заштити података о личности*, Службени гласник Републике Србије, бр. 87/2018.
13. Sutrop, M., Laas-Mikko, K. (2012). From identity verification to behavior prediction: Ethical implications of second generation biometrics. *Review of policy research*, *29*(1): 21–36.

Електронски извори

1. *Human Rights Watch*, China's Alorithms of Repression, Reverse Engineering a Xinjiang Police Mass Surveillance App, https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass?utm_source=chatgpt.com, доступан 29. 7. 2025.
2. *State government fixes bug exposing Aadhaar biometric records*, Biometric.com, Oct 13, 2023, 1:09 pm EDT | Chris Burt, https://www.biometricupdate.com/202310/state-government-fixes-bug-exposing-aadhaar-biometric-records?utm_source=chatgpt.com, доступан 29. 7. 2025.
3. *Texas AG sues Meta for allegedly exploiting users' biometric data*, Axios.com, https://www.axios.com/2022/02/15/texas-facebook-meta-biometric-data?utm_source=chatgpt.com, доступан 29. 7. 2025.

Ethical and Security Aspects of the Use of Papillary Line Imprints as Biometric Identification

***Abstract**: Despite the development of technics and technology, the drawing of papillary lines still represents the most widespread method of registration and identification of persons. The uniqueness, universality, immutability and transferability of papillary line prints make them a reliable, scientifically verified biometric characteristic. However, due to the widespread use of fingerprints for verification the question of the security of the use of this biometric feature arises. There are assumptions about possible unauthorized access and use of biometric data, along with all other personal data. With the advancement of technology, especially information and communication technologies and artificial intelligence (AI), our data is everywhere and is potentially accessible to everyone. Every day we leave passwords on various servers, we use our fingerprints to access smartphones and computers, and all this data remains stored in "some part of the Internet". Therefore, it is legitimate to ask about the security of personal data, yet there is still no precise research on the misuse of biometric data in our country. Biometric systems are susceptible to numerous types of attacks, such as hacking, identity theft, data manipulation, and misuse by authorized persons and government agencies. In addition, ethical dilemmas regarding privacy, voluntariness, and transparency of data processing, storage, and retention remain unresolved.*

***Keywords**: ethics, security, police ethics, fingerprints.*