Forenzičke metode za identifikaciju lica: juče, danas, sutra

Snežana Stojičić, Radovan Radovanović, Nataša Petrović i Milesa Srećković

Apstrakt—**Identifikacija lica je bila, jeste i biće izazov za koji se kontinuirano nalaze rešenja koja pružaju tehnološki odgovor u ovoj oblasti, posebno zasnovanih na upotrebi biometrijskih podataka u elektronskom obliku i primene principa i iskustava najbolje prakse elektronskog poslovanja uopšte. Upotreba podataka u elektronskom obliku, smeštenih u određenim bazama podataka, sredstava elektronske komunikacije i elektronske obrade velike količine podataka u obavljanju poslovnih procesa identifikacije lica je evidentno u porastu, kao odgovor na izazove koje elektronsko poslovanje donosi, neophodno je usaglašavanje razvoja normativnog okvira kako u domenu povećanja efikasnosti poslovanja tako i izazova koje digitalna era sa sobom nosi. Izazov, sa forenzičkog aspekta, kao odgovor na potencijalno narušavanje i nepoštovanje pravnih normi, uslovljava razvoj i primenu novih procedura i alata u ovoj oblasti. Danas je evidentna potreba stalnog praćenja razvoja i primene novih metoda za identifikaciju lica, a posebno onih, koje mogu biti vezane za forenzičke aspekte u digitalnom svetu. Predmet razmatranja su upravo ova pitanja, koja se odnose na izazove u identifikaciji lica u digitalnoj eri.**

***Ključne reči*—Forenziče metode; idetifikacija lica; biometrijski podaci.**

I. Uvod

Za sisteme za biometrijsku identifikaciju se može reći da imaju više generacija, koje se zasnivaju na tehnološkim rešenjima, odnosno prate razvoj tehnologije, koja uslovljava i omogućava identifikaciju lica zasnovan na biometrijskim podacima. Savremeno digitalno okruženje, stvara nove izazove i mogućnosti za počinioce krivičnih dela, ali i službe, koje utiču u rasvetljavanju istih. Tako proces digitalizacije i modernizacije poslovnih procesa, neophodno prati i razvoj adekvatnog odgovora sa aspekta primene metoda za identifikaciju lica sa aspekta forenzike.

II. Prve generacije biometrijskih tehnologija

Biometrijske tehnologije prve generacije bile su fokusirane na jaku biometriju i jedinstvenost identifikacija ili autentikacija određenih pojedinaca (fizičkih lica). Prvi slučajevi upotrebe velikih razmera, počeli su kasnih 1990-ih u SAD, sa povećanjem primene posebno posle uvođenja biometrijskih pasoša, koji sadrže otiske prstiju, fotografiju i podatke o licu. Od tada, biometrijske tehnologije su postale robusnije i naprednije, značajno smanjujući stope grešaka uz pomoć razvoja računarske tehnologije i primenjenih rešenja, a naročito u tehnologijama za prepoznavanje lica.

Prve primene biometrije i razvijenih alata za brzu i pouzdanu identifikaciju ili autentikaciju, našle su širok spektar konteksta primene, uključujući potrebe sprovođenja zakona. Primena se zayim proširila i na privatni sektor, uključujući rešenja kao što su ona za otključavanje pametnih telefona ili prepoznavanje VIP-a kupaca. Rešenja zasnovana na biometriji u nekim slučajevima zamenjuju tradicionalne lozinke, posebno imajući u vidu da sa najnovijim tehnologijama za prepoznavanje lica moguća je identifikaciju za manje od jedne sekunde.

Ne manji značaj imaju i takozvane “slabe” biometrijske metode, kao biometrijske metode druge generacije, kao što su motoričke veštine, osobenosti položaja tela, hod i način interakcije sa okruženjem [1]. Ova druga generacija biometrije se naziva i „biometrija ponašanja“, jer je digitalno fizičko i kognitivno ponašanje ljudi analizira, a ne relativno statičke karakteristike, kao što su otisci prstiju. Posebno je od interesa, to što druga generacija biometrijskih sistema, pruža nove mogućnosti automstizacije poslovnih procesa u organima za sprovođenje zakona, vršenju granične kontrole, omogućavajući, na primer, otkrivanje lica sumnjivog ponašanja koje bi moglo da ukaže na nameru da počini krivično delo.

Da bi se povećala tačnost, biometrijske tehnologije prve generacije se redovno kombinuju u multimodalne sisteme. Ovi sistemi kombinuju nekoliko biometrijskih identifikatora za identifikaciju jedne osobe. Multimodalni sistemi mogu minimizirati rizike od pojave grešaka i pomoći u prevazilaženju poteškoća uzrokovanih lošim kvalitetom podataka ili podacima koji nedostaju, istovremeno povećavajući mogućnosti i u drugim aspektima, kao što je etički.

Tehničko tehnološki napredak omogućava sve veću primenu sistema video nadzora, kojima se omogućava upotreba biometrijskih tehnika i veštačke inteligencije za identifikaciju lica u javnim prostorima, što implicira potrebu da se striktno reguliše upotreba ovih sistema. Napredak tehnologije i potreba za normativnim uređenjem primene savremenih tehnoloških rešenja predstavlja stalni izazov, posebno imajući u vidu komparativnost ovih oblasti korišćanja biometrije, kako na nacionalnom, tako i na međunarodnom planu.

Snežana Stojičić, Ministarstvo unutrašnjih poslova, Kneza Miloša 101, 11000 Beograd, Srbija (e-mail: snezana.stojici@mup.gov.rs),
Radovan Radovanović – Kriminalističko policijski univerzitet, Cara Dušana 196, 11000 Beograd, Srbija (e-mail: radovan.radovanovic@kpu.edu.rs),
Nataša Petrović – Ministarstvo unutrašnjih poslova, Kneza Miloša 101, 11000 Beograd, Srbija (e-mail: natasa.petrovic@mup.gov.rs)
Milesa Srećković – Elektrotehnički fakultet, Univerzitet u Beogradu, Bulevar Kralja Aleksandra 73, 11020 Beograd, Srbija (e-mail: esreckov@etf.bg.ac.rs).

 ISBN 978-86-7466-930-3

Pošto su aktivnosti mozga merljivi biološki signali, one se takođe smatraju biometrijskim. S obzirom na poteškoće u hvatanju elektrohemijskih signala mozga i njihovu složenost, relevantnost moždanih aktivnosti je dugo vremena bila ograničena na medicinski sektor. Međutim, poslednjih godina, elektroencefalografija (EEG), koja snima električne aktivacije mozga postavljanjem elektroda na skalp i takozvani interfejsi mozak-kompjuter (BCI), koji mogu da prevedu aktivnost mozga u mašinski čitljivi unos, postali su pristupačniji [2] i čak su integrisani u proizvodima širo biometrijske autentikacijeke potrošnje[1].

III. Dalji pravci razvoja metoda identifikacije lica

Predlog regulatornog okvira o veštačkoj inteligenciji[2], Evropska komisija je usvojila u prvoj polovini 2021. godine, kao novi pravni okvir za primenu veštačke inteligencije. Predlog uredbe ima za cilj da programerima, onima koji koriste veštačku inteligenciju i korisnicima, pruži jasne zahteve i obaveze u vezi sa specifičnom upotrebom AI[3]. U isto vreme, predlog uredbe obuhvata i aspect usmeren ka smanjenju administrativnih i finansijskih opterećenja za preduzeća, posebno za mala i srednja preduzeća (MSP) [3, 4].

Predlog je deo šireg paketa, koji se odnosi na veštačku inteligenciju, a koji je posvećen jačanju, prihvatanju, ulaganju i inovacijana u oblasti AI u EU.

Zašto su nam potrebna pravila o AI? Predloženi propis o veštačkoj inteligenciji obezbeđuje da se izgradi poverenje u ono što veštačka inteligencija može da ponudi. Dok većina sistema veštačke inteligencije predstavlja ograničen rizik i može doprineti rešavanju mnogih društvenih izazova, određeni sistemi veštačke inteligencije stvaraju rizike, koji se moraju rešavati, kako bi se izbegli neželjeni ishodi.

Važno je istaći da iako postojeće zakonodavstvo pruža određeni okvir, procenjuje se da je nedovoljno da se odgovori na specifične izazove, koje donose sistemi veštačke inteligencije.

Predložena pravila će se baviti rizicima, koje posebno stvaraju AI aplikacije, predložiti listu visokorizičnih aplikacija, postaviti jasne zahteve za AI sisteme za aplikacije visokog rizika; definisati posebne obaveze za korisnike veštačke inteligencije i provajdere visokorizičnih aplikacija; predložiti ocenu usaglašenosti, pre nego što se sistem veštačke inteligencije stavi u upotrebu ili stavi na tržište; predložiti način praćenja pošto se takav AI sistem stavi na tržište; i predložiti strukturu upravljanja na evropskom i nacionalnom nivou [4].

Opis stanja biometrijskih tehnologija sa aspekta EDPS[4] (European Data Protection Supervisor), indukuje da broj uređaja koji se primenjuju za obradu biometrijskih podataka raste neverovatnom brzinom. Mnogi pametni telefoni koriste slike lica i otiske prstiju za autentikaciju svojih korisnika. Virtuelni glasovni asistenti obrađuju glasovne podatke kao odgovore na zahteve korisnika. Sistemi video nadzora mogu se koristiti za identifikaciju ili klasifikaciju pojedinaca/lica. Pametni satovi i fitnes narukvice mogu pratiti i obrađivati podatke o fiziološkom statusu (kao što su otkucaji srca i navike spavanja). Sistemi video nadzora su imali značajnu ulogu i sa aspekta pandemije COVID-19, podrška korišćenju prepoznavanja lica i veštačke inteligencije za praćenje socijalnog distanciranja ili pravilne upotrebe maski za lice, kao i upotrebe osetljivih termovizijskih kamera i prepoznavanja lica, koja se mogu na osnovu povišene temperature identifikovati, kao potencijalno zaražen, korona virusom.

Poseban domen primene i korišćenja biomtrijskih podataka čine informacioni sistemi velikih razmera, kao što su tri velika IT sistema u oblastima azila i migracija, koji su trenutno operativni i uključuju korišćenje biometrijskih podataka: Vizni informacioni sistem (VIS), Šengenski informacioni sistem (SIS II) i EURODAC (European Asylum Dactyloscopy Database), sistem koji obrađuje podatke o tražiocima azila.

Pored toga u pripremi su, još tri nova evropske informaciona sistema, velikih razmera, od kojih će dva obrađivati biometrijske podatke: Ulazno-izlazni sistem (EES) i Evropski informacioni sistem krivičnih evidencija za državljane trećih zemlja (ECRIS-TCN). Iako su ovi informacioni sistemi razvijeni nezavisno, nova regulativa interoperabilnosti[5], definiše četiri osnovne komponente interoperabilnosti koje bi trebalo da omogućavaju međusobnu interakciju. Među njima, i rešenje za zajedničko upoređivanje biometrije - (sBMS) odnosno otisaka i slika lica kroz različite sisteme [5].

Međutim, uz očekivan porast primene, važno je paralelno sprovoditi i aktivnosti na podizanju svest o izazovima koje biometrijske tehnologije donose, a posebno sa aspekta izgradnje poverenja u tehnološka rešenja [6].

Takođe, javljaju se izazovi i nove mogućnosti zloupotreba novih tehnologija, kao što je kompanija koja se bavi obradom fotorgafija lica, Clearview AI, koja je preuzela oko 3 milijarde slika, prikupljenih sa miliona web lokacija, uključujući Fejsbuk, Tviter i Jutjub, i prodaje svoje usluge organima za sprovođenje zakona, ili poljska platforma PimEyes, koja je na sličan način došla do podataka i koristi ih za sticanje dobiti [7,8]. Povećana upotreba biometrijskih podataka uz nemogućnost promene fizioloških osobina, donosi povećanu zabrinutost za bezbednost biometrijskih podataka.

Ukoliko se u razvoju Sistema yasnovanih na biometrijskim podacima ne primenjuju odgovarajuće mere zaštite, posledice povrede ličnih podataka mogle bi biti veoma ozbiljne. Upravo iz tog razloga, nastali su međunarodni standardi, kao što su ISO/IEC 24745 ISO/IEC 24745:2011 Information technology — Security techniques — Biometric information protection i standard u oblasti mehanizama zaštite biometrijskih šablona (BTP), a aktuelnost potvrđuje ISO/IEC 24745:2022, Information security, cybersecurity and privacy protection — Biometric information protection, revizija koja pokriva zaštitu biometrijskih informacija pod različitim zahtevima za

[1] Technology | Unicorn Hybrid Black (unicorn-bi.com)
[2] EUR-Lex - 52021PC0206 - EN - EUR-Lex (europa.eu)
[3] AI – Artificisl Intelligence
[4] 20-10-07_edps_biometrics_speech_en.pdf (europa.eu)
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0817

 ISBN 978-86-7466-930-3

poverljivost, integritet i obnovljivost/opoziv, tokom skladištenja i prenosa. Standard identifikuje zahteve i daje preporuke za bezbedno upravljanje i obradu biometrijskih informacija u skladu sa pravilima privatnosti[6].

Međutim, neizvesno je u kojoj meri, se pri razvoju biometrijskih sistema prate i primenjuju standard. S obzirom da je otkriveno da je postojao pristup preko 27,8 miliona zapisa nezaštićenih i uglavnom nešifrovanih[7], a da za razliku od kompromitovanja lozinki, kada se to dogodi sa otiscima prstiju, ne postoji mogućnost da promenite otisak prsta. Baza podataka se odnosila na Biostar 2, system, koji je razvila kompanija za obezbeđenje Suprema [8, 9].

Početkom marta 2022. godine objavljeno je da je Samsung potvrdio kršenje bezbednosti pošto što su hakeri pristupili i preuzeli skoro 200 gigabajta poverljivih podataka, uključujući izvorni kod za različite tehnologije i algoritme za operacije biometrijskog otključavanja. Hakerska grupa Lapsus, preuzela je odgovornost i objavila da su preuzeli izvorni kod koji Samsung telefoni koriste za obavljanje osetljivih operacija, algoritme za sve otključavanje na osnovu biometrije [10].

Osetljiva priroda biometrijskih podataka prepoznata je i u okviru pravnog okvira EU, kao i u okviru Modernizovane konvencije Saveta Evrope 108+, podleže posebnoj zaštiti i može se reći da je obrada biometrijskih podataka zabranjena u principu i postoji samo ograničen broj uslova pod kojima takva obrada je zakonita, tako da u okviru svojih zadataka nadzora i sprovođenja, EDPS sprovodi između ostalog i redovne revizije velikih IT sistema EU.

Svakako, prethodno pitanje pre svake primene, treba da bude vezano za procenu neophodnosti i proporcionalnosti. Ne treba da koristimo savršen system, koji nam nije potreban ili koji obrađuje biometrijske podatke na nesrazmeran način. Obrada biometrijskih podataka treba striktno da se pridržava principa ograničenja svrhe. Ograničenje svrhe je posebno relevantno u ovom kontekstu, zbog tipova biometrijskih podataka, koji omogućavaju zaključivanje o drugim ličnim podacima.

Prilokom obrade biometrijskih podataka preporučljivo je u potpunosti primenjivati princip minimalizacije prikupljanja podataka. Prilikom procene koje biometrijske tehnologije koristiti, potrebno je ograničiti obradu biometrijskih podatka, na ono što je neophodno za ostvarivanje određenog zadatka. Uvažavajući činjenicu da bi multimodalni biometrijski sistemi mogli biti sigurniji i tačniji od običnih biometrijskih sistema, takva vrsta obrade koja uključuje više biometrijskih podataka donosi i veće rizike za osnovna prava pojedinaca. Kada se razmatra obrada više od jedne vrste biometrijskih podataka, potrebno je, proceniti njihovu neophodnost i proporcionalnost, balansirajući očekivane koristi sa rizicima.

Poverenje u biometrijske sisteme, zahteva tačnost, jasanoću i direktan pristup u saopštavanju prednosti i ograničenja svake biometrije tehnologije, predstavljanje mogućnosti i rizika. Percepcija javnosti o rizicima je razlog zašto milioni korisnika dobrovoljno odlučuje da koriste biometrijske podatke za autentikaciju kada koriste svoje pametne telefone, dok je sve veće protivljenje upotrebi biometrijske identifikacije u javnim prostorima.

Podaci, kao što su otisci prstiju i DNK, generalno su jedinstveni za pojedinca i tako mogu potvrditi nečiji identitet i prisustvo na mestu zločina, odnosno imati forenzički značaj. Takođe, može pomoći da se dokaže nevinost osumnjičenog. Posebno na međunarodnom nivou, forenzički podaci mogu se koristiti i za povezivanje niza transnacionalnih krivičnih dela, imajući u vidu da se otisci prstiju mogu brzo proveriti, naročito, ako osumnjičeni prelazi granicu. Ne manji značaj, imaju ovi podaci, sa aspekta korišćenja za identifikaciju žrtava velikih katastrofa.

Najbrži razvoj, ostvaren je u oblasti identifikacije na osnovu prepoznavanja fotografije lica i time otvara mnoge nove mogućnosti, za identifikaciju pojedinaca i pronalaženje počinioca krivičnih dela. U ovom smislu forenzička ekspertiza i podaci su od vitalnog značaja za sprovođenje istraga na nacionalnom nivou, kao i ostvarivanje učešća u međunarodnim istragama u skladu sa normativnim okvirom i nadležnoatima [9].

Posebna oblast primene su biometrijske autentikacije, kao siguran i praktičan alternativni način autentikacije putem lozinki. Međutim, i u ovom, slučaju, pojavljuju se izazovi, koje je potrebno imati u vidu, kao što je očuvanje privatnosti lica, obezbeđivanje bezbednosti i poverljivosti biometriskih podataka pri prenosu i skladištenju, kao i činjenica da se za razliku od lozinki biometrijske osobine ne mogu poništiti i ponovo je izdati. Ukoliko dođe do kompromitovanja, korišćenog biometrijskog podatka, s obzirom da se ne može promeniti, isti se ne može dalje korisititi u svrhu autentikacije [11]. U ovom smislu Cloud tehnologija može da iskoristi prednosti biometrijske tehnologije i obrnuto. Biometrija sa svojim jakim svojstvima autentikacije, može da se iskoristi da poboljša bezbednost Cloud sistema i ponudi novi modeli usluga (tj. biometrijska autentikacija kao jedna od usluga u Cloud-u. S druge strane, Cloud omogućava svojim resursima fleksibilnosti, skalabilnost i smanjenje troškova za rad biometrijskih Sistema (tj. procesorsku snagu ili skladištenje podataka), kao i da omogući poboljšanje performansi biometrijskih sistema [11].

Standardi omogućavaju efikasan razvoj biometrijskih sistema, uspostavljanjem zajedničkih kriterijuma i postavljanjem smernica za zaštitu privatnosti (Eversheds Sutherland, 2022). Sporazumi o formatima podataka i interfejsima aplikativnog softvera mogu pomoći će da se smanje troškovi razvoja sistema. Razvoj standarda za primenu biometrije i za testiranje tačnosti, doprinosi razjašnjavanju ranjivosti i usmerava ka pronalaženju rešenja.

Imajući u vidu da ljudska faktor i slabe lozinke, prema proceni iz Imageware analize, čine 52% narušavanja bezbednosti podataka, što se može smatrati indikatorom potrebe da se tradicionalne metode autentikacije zamene novijom biometrijskom tehnologijom, kao što su specijalizovani hardverski senzori u mobilnim telefonima, skeneri otiska prsta, kamere za prepoznavanje lica (2D/3D) ili

[6] https://www.iso.org/

[7] https://www.securitymagazine.com/articles/90731-more-than-27-million-biometric-records-exposed-in-a-public-database

 ISBN 978-86-7466-930-3

prepoznavanje irisa oka [11]. Biometrijske tehnologije postaju sve popularnije, posebno sa pojavom dvofaktorske autentikacije za *online* usluge. Pregled prednosti i nedostataka multifaktorske autentikacije dat je u Tabeli 1. Na osnovu analiza tržišta procenjuje se da će se u narednim godinama tržište biometrijskih tehnologija dostići 55,42 milijarde dolara do 2027. godine, tržište kamera za video nadzor sa procenama predviđanja rasta na 44 milijarde dolara do 2025. godine [11].

TABELA I
MULTIFAKTORSKA AUTENTIKACIJA ZA I PROTIV (PRATT, 2021)

Prednosti	**Nedostaci**	**Mere**
Teško se hakuju ili repliciraju	Nepovratna neopozivost u slučaju kompromitovanja	Više faktora je dostupno za MFA
Konformno za korisnike	Povećan rizik od zloupotrebe	Zahteva povećane mere zaštite
Manja zavisnost od medija	Značajne investicije za velike sisteme	Minimalizacija podataka
Manja zavisnost od mrežne povezanosti	Novo i nedovoljno dokazano u praksi	Raspodela rizika
Proširivost novim elementima	Pristrasnost, greške, lažno pozitivni rezultati	Edukacija i uključenost korisnika

Svedoci smo porasta upotrebe biometrijskih tehnologija za različite oblasti primene, ovakav napredak otvara i nove mogućnosti za dalja istraživanja i razvoj. Posebno imaju se u vidu niz fundamentalnih otvorenih pitanja i izazova kojima će se baviti istraživanja u oblasti primene biometrije u svim sverama savremenog života [12-15].

To svakako prati i aspekt bezbednosti, pošto je sve više podataka u opticaju, u digitalnom obliku, uključujući biometrijske podatke, koje pojedinci ostavljaju na web-u i u ličnim elektronskim uređajima, kao što su pametni telefoni i drugi mobilni uređaji. Posebno, imajući u vidu dostupnost digitalnih senzora i kapacitet uređaja za skladištenje podataka, i tu je i činjenica da se identifikacije osoba sve više zasnivaju na digitalnim procesima [16].

IV. ZAKLJUČAK

Osim što su univerzalne i jedinstvene, biometrijske karakteristike treba da budu relativno trajne i lake za prikupljanje i korišćenje. Biometrijski sistem treba da bude u mogućnosti da pruži što tačnije rezultate u različitim okolnostima i uslovima. Svakako važan, a možda i najvažniji aspekt biometrijskog sistema je prihvatanje od strane javnosti. Iako se DNK smatra konačnom biometrijom za identifikaciju osobe (osim jednojajčanih blizanaca), podudaranje DNK je previše invazivno za široku upotrebu u autentikaciji identiteta. Termografija lica, koja otkriva toplotne obrasce, koje stvaraju krvni sudovi i emituju iz kože, nije invazivna metoda, ali je cena previse visoka. Među biometrijskim podacima koji se trenutno razmatraju za buduću primenu su puls, miris tela, sastav kože, šara noktiju, hod i oblik uha. Potrebno je više istraživanja za dalju ocenu prihvatljivosti za širu upotrebu.

Sistem, koji se koristi, treba da bude siguran, obezbeđuje privatnost i daje tačne rezultate. Sistem koji je nesiguran, nepouzdan ili invazivan, s druge strane, može doprineti narušavanju poverenja javnosti, što na kraju može dovesti do otpora u prihvatanju tehnika biometrijskog prepoznavanja. Ključna strategija u garantovanju odgovarajućeg izbora i upotrebe biometrijskih metoda je razvoj međunarodnih standarda. Tokom poslednje decenije, napravljen je ogroman napredak u poboljšanju biometrijskih senzora, algoritama i procedura, ali i dalje, postoje slabosti i ranjivosti, koje treba rešavati. Potreba za zaštitom privatnosti i čuvanjem osetljivih biometrijskih podataka, ostaje i dalje fundamentalna.

ZAHVALNICA

Aurori se zahvaljuju organizacionom odboru konferencije ETRAN 2022 na prepoznatom značaju oblasti forenzike, prostoru i vremenu datom za izlaganje i diskusiju.

LITERATURA

[1] C. Wendehorst, & Y. Duller, "Biometric Recognition and Behavioural Detection, Study requested by the JURI and PETI committees", 2021, EU. 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 (europa.eu)

[2] V.H. de Albuquerque, R. Damaševilius, J. M. Tavares & R. Pinheiro, "EEG-Based Biometrics: Challenges And Applications, Computational Intelligence and Neuroscience", Hindawi, 2018. https://doi.org/10.1155/2018/5483921

[3] M. Anzini, "The Artificial Intelligence Act Proposal and its implications for Member States", EIPA Briefing 2021/5, EIPA-Briefing-2021-5-The-Artificial-Intelligence-Act-Proposal-and-its-implications-for-Member-States.pdf

[4] *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, European Comision Brussels, 21.4.2021.

[5] *Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa.* European Comision 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0817

[6] Agencia Española de Protección de Datos (AEPD), and the European Data Protection Supervisor (EDPS) (2020). "14 misunderstandings with regard to biometric identification and authentication", 14 misunderstandings with regard to biometric identification and authentication | European Data Protection Supervisor (europa.eu)

[7] W. Wiewiórowski, *W. "The State of Biometrics, European Data Protection Supervisor (EDPS)".* 2020. 20-10-07_edps_biometrics_speech_en.pdf (europa.eu)

[8] N. Rotem & R. Locar, *"Data Breach in Biometric Security Platform, vpnMentor"*, (2019). Report: Data Breach in Biometric Security Platform Affecting Millions of Users (vpnmentor.com)

[9] *Interpol Report*, (2022). Forensics (interpol.int)

[10] Techcrunch site, Samsung confirms data breach after hackers leak internal source code | TechCrunch, Pristupljeno 13.04.2022.

 ISBN 978-86-7466-930-3

[11] Imageware Report, “Biometric Trends and Statistics to Keep an Eye on in 2022”, Biometric Trends and Statistics to Keep an Eye on in 2022 (imageware.io)
[12] A. A. Ross, S. Banerjee, C. Chen, A. Chowdhury, V. Mirjalili, R. Sharma, T. Swearingen & S. Yadav, “Some Research Problems in Biometrics: The Future Beckons”. 2019 International Conference on Biometrics (ICB), 1-8. 2019.
[13] A. A. Albahdal & T. E. Boult, "Problems and Promises of Using the Cloud and Biometrics," 11th International Conference on Information Technology: New Generations, 2014, 293-300, https://doi.org/10.1109/ITNG.2014.112
[14] Sutherland Global Biometrics Guide 2022, A multi-jurisdictional look at the laws governing the use of biometric technology, (2022). Global_Biometrics_Guide_2022.pdf (eversheds-sutherland.com)
[15] National Research Council (US) Whither Biometrics Committee; Pato JN, Millett LI, editors. “Biometric Recognition: Challenges and Opportunities”. Washington (DC): National Academies Press (US); 2010. 5, Research Opportunities and the Future of Biometrics. Available from: https://www.ncbi.nlm.nih.gov/books/NBK219897/
[16] K.M. Pratt, “Biometric security technology could see growth in 2021”, Biometric security technology could see growth in 2021 (techtarget.com)

ABSTRACT

Identification of persons has been, is and will be a challenge for conductiong, as question which solutions best fit to the purpose and is it provided technological response on adequate level. Especially this one based on the use of biometric data in electronic form and application of principles and experiences of best e-business practice in general. The use of data in electronic form stored in certain databases, issues of electronic communication and electronic processing of large amounts of data in performing business identification processes is evidently increasing, in response to the challenges of e-business, it is necessary to harmonize the development of normative framework as well the business efficiency are the challenges that the digital age brings. Challenges from the forensic aspect in response to potential violations and non-compliance with legal norms, which requires the development and application of new procedures and tools in this area. There is also an evident need for constant monitoring of the development and application of new methods for personal identification, especially those that may be related to forensic aspects in the digital world. The subject of consideration are precisely these issues that relate to the challenges in identifying persons in the digital age.

Title in English

Snežana Stojičić, Nataša Petrović, Radovan Radovanović i Milesa Srećković

 ISBN 978-86-7466-930-3