UDC: 004.056.4 INFO M: str. 17-22

PRAVNO REGULISANJE ZAŠTITE BIOMETRIJSKIH PODATAKA
LEGAL REGULATION OF BIOMETRIC DATA

Saša Paunović

REZIME: Građani se često neprijatno osećaju znajući da neko prikuplja podatke o njihovoj ličnosti, posebno ako su oni osetljivog karaktera. Da bi se biometrija na najbolji način implementirala u društvu, neophodno je da postoji pozitivan odnos između građana i države, koji treba da bude baziran na principu dobrovoljnosti u primeni biometrije. Međutim, ukoliko bi se građanima na adekvatan način predočile prednosti biometrije, kao i postojanje adekvatnih institucionalizovanih mehanizama kontrole, pravne regulative, koja se odnosi na zaštitu privatnosti i zaštitu podataka, u velikoj meri bi se otklonile barijere u opravdanosti primene biometrije.

KLJUČNE REČI: Biometrija, primena biometrije, privatnost, pravna regulativa

ABSTRACT: Citizens often feel uncomfortable knowing that someone collects information about their personality, especially if they are sensitive character. The best way to implement biometrics in society, it would be essential that there is a positive relationship between citizens and the state, which should be based on the voluntary principle in the application of biometrics. However, if it is adequately explained and present the benefits of biometrics to the citizens, as well as the adequate control of institutionalized mechanisms, legal regulations which is concerning the protection of privacy and data protection in large part the barriers would be removed in favor of the justification of the application of biometrics.

KEY WORDS: Biometrics, application of biometrics, privacy, legislation.

1. UVOD

Danas je sve češća primena biometrijskih metoda, budući da one omogućavaju veću sigurnost u oblasti pristupa određenim podacima, dobra su preventivna mera kod zloupotrebe identiteta, olakšavaju transakcije podataka kod elektronske kupovine i imaju veliki značaj kod identifikovanja kriminalaca. Međutim, ovako široka primena dovodi i do zabrinutosti pojedinaca zbog mogućnosti povrede prava na privatnost, te je iz tog razloga neophodno ovu oblast normativno regulisati i to tako da se sa jedne strane zaštiti poštovanje ovog prava a sa druge strane da se omogući nesmetano primenjivanje biometrijskih metoda. To nije jednostavan zadatak, imajući u vidu da su u pitanju osetljivi lični podaci. U ovom momentu ne postoji zakonska definicija biometrije niti u Evropi, niti na drugim kontinentima [1].

Pravo na privatan život je jedno od osnovnih ljudskih prava zajemčenih Evropskom konvencijom o zaštiti ljudskih prava i osnovnih sloboda [2,3]. Ovo pravo, između ostalog, podrazumeva i zaštitu bilo kojih osetljivih ličnih podataka, kao što je slučaj i sa biometrijskim. Prema tome, zašita biometrijskih podataka je pre svega bazirana na zaštiti privatnosti. Iz to razloga, većina zemalja se oslanja se na zakonsku zaštitu podataka o ličnosti.

Cilj pravnog regulisanja ove materije je da se primena biometrijskih metoda zakonodavno uokviri, odnosno da se nacionalna zakonodavstva usaglase sa međunarodno pravnim principima. Važnost dobre pravne regulative u ovoj oblasti se ogleda i u tome što je neophodno obezbediti i poštovanje načela zabrane diskriminacije. Naime, neke zemlje u kojima se ne poštuje načelo vladavine prava mogu zloupotrebiti ove podatke, odnosno različito postupati u odnosu na određena lica ili grupe.

Biometrijski podaci predstavljaju specifičnu kategoriju ličnih podataka, te iz tog razloga mogu biti korišćeni samo za specifične, jasne i zakonom definisane svrhe uz primenu adekvatnih mera zaštite. Znači, potrebno je pružiti pojedincima zaštitu i sigurnost da njihov identitet neće biti ukraden i zloupotrebljen.

2. BIOMETRISKI PODACI KAO OSETLJIVI LIČNI PODACI

Nedavni izveštaj Saveta Evrope govori o tome da odgovarajuća arhitektura biometrijskog sistema treba da bude izabrana u zavisnosti od svrhe [1]. Ovaj izveštaj preporučuje da kompletne informacije o svrsi ovog sistema moraju biti dostupne osobama čiji se biometrijski podaci i uzimaju. Te osobe moraju imati pravo uvida i ispravke podataka o njima. Neophodna je kompletna transparentnost biometrijskog sistema, posebno u koliko je sistem dizajniran za raznovrsnu upotrebu [4].

Pravo na privatnost, između ostalog, znači „mogućnost da svoj život vodite slobodno, bez instrukcija, autonomno i da kontrolišete pristup vašim ličnim podacima“.

Međunarodna biometrijska grupa je podelila rizik za privatnost na dve osnovne kategorije: ličnu privatnost, koja se odnosi na to da biometrijski postupci mogu ljudima biti neprijatni, i informacionu privatnost, koja podrazumeva mogućnost zloupotreba (neovlašćeno prikupljanje, upotreba, zadržavanje i otkrivanje) biometrijskih podataka.

Činjenica da se za vreme biometrijske transakcije koristi deo nečega što je ljudsko biće za vreme transakcije može da se shvati kao “davanje informacija o sebi“. Pored toga, biometrijska tehnologija je nova i prilično nepoznata širem krugu ljudi i zato ljudi mogu imati unapred negativan stav u pogledu, pa njenom uvođenju prilaze sa rezervom.

Priliv novih tehnologija uvek zahteva i novu zakonsku regulativu. Zaista, sa pojavom novih tehnologija postojeći zakonski okvir biva prevaziđen i javlja se potreba da se osmisli

drugi, usklađen sa novom stvarnošću, i da se postave društveno prihvatljive granice za njegovu upotrebu. To je upravo ono što se danas dešava sa uvođenjem biometrije u svakodnevne aktivnosti i njene implementacije u identifikacione dokumente. Pravni stručnjaci treba da istraže sa svog aspekta „šta je neophodno da se zaštiti javni interes i obezbede optimalni rezultati za društvo“, jer postoji potencijalna opasnost od zloupotreba [4]. Glavna opasnost je u tome što se biometrijske informacije, bilo da se koriste sa ili bez dozvole, mogu zloupotrebi, na primer, radi nedozvoljenog pristupa određenim podacima ili aplikacijima. Ono što posebno zabrinjava u pogledu korišćenja biometrije je sledeće [1]:

– biometrijski podaci se mogu skupljaju bez dozvole
– biometrijski podaci se koriste u druge svrhe
– biometrijski podaci se mogu prenositi bez dozvole
– biometrijski podaci se mogu kombinovati sa drugim podacima o ličnosti radi dobijanja potpunije predstave o ličnosti
– biometrijski podaci omogućavaju stvarni nadzor i profilisanje.

Zabrinutost je opravdana tim više jer je većina računarski sistema, koji sadrže prikupljene biometrijske podatke, međusobno umrežena, pa se prikupljeni biometrijski podaci mogu jednostavno transferovati i agregirati. Treba imati u vidu da računarski sistemi pored biometrijskih podataka nužno moraju imati i druge podatke o ličnosti kako bi se na osnovu biometrijskih podataka mogla identifikovati ličnost, a Konvencija 108 Saveta Evrope smatra da povezanost biometrije sa bilo kojom informacijom iz baze jeste lični podatak. Može se tvrditi da prikladno i pametno korišćenje biometrije je jedan od najsigurnijih načina za dokazivanje identiteta, ali možemo se zapitati da li jačanje sigurnosti u pogledu dokazivanja identiteta korišćenjem biometrijskih sistema nanosi štetu ljudskoj slobodi i da li treba menjati slobodu za sigurnost. Korišćenje ovog sistema zahteva primenu pravila proporcionalnosti u odnosu na ishod. Zaista, upotreba ovog sistema i opasnost koja proizilazi iz stvaranja baze podataka i samim tim mogućnosti njene zloupotrebe moraju biti proporcionalni, moraju biti bar propocionalni.

3. MEĐUNARODNA PRAVNA REGULATIVA

Na 25. Međunarodnoj konferenciji o zaštiti podataka i poverenicima za zaštititu privatnosti održanoj u Sidneju septembra 2003. godine, usvojeno je pet rezolucija koje su tretirale problematiku zaštite privatnosti i jačanje zaštite podataka, od kojih se neke mogu primeniti i na slučajeve biometrijskog dokumentovanja identiteta, to su [1]:

– Rezolucija o unapređenju veze između zaštite podataka i razmene ličnih podataka. Cilj je da se postigne saglasnost o potrebi, kako privatnog, tako i javnog sektora, o boljoj razmeni informacija o načinu prikupljanja i obrade ličnih podataka. Treba imati u vidu da uprkos trenda rasta broja različitih evidencija o ljudima, pojedinci nisu dobro informisani o tome kako mogu imati uvid u te podatke, u kojoj formi i sa kojim sadržajem.
– Rezolucija o transferu podataka o putnicima (u svetlu borbe protiv terorizma i organizovanog kriminala uz poštovanje određenih principa zaštite podataka o ličnosti).
– Rezolucija o zaštiti podataka i međunarodnim organizacijama.Mnoge međunarodne organizacije i njihova tela su inicirale uvođenje novih standarda u oblasti zaštite ličnih podataka pri njihovoj razmeni na međunarodnom nivou. Na primer, inicijativa za dodavanje biometrijskih podataka u pasoše je potekla od Međunarodne organizacije za civilno vazduhoplovsto.
– Predlog rezolucije o softveru za automatsko ažuriranje podataka sa ciljem da ohrabri razvoj i implementaciju tehnologija za ažuriranje softvera na način koji poštuje privatnost i autonomiju korisnika računara.
– Rezolucija o radiofrekvencijskim (RF) tehnologijama s obzriom da ova tehnologija može omogućiti praćenje lica i povezivanje prikupljenih informacija sa postojećim bazama podataka.

Stavovi iz navedenih rezolucija služe nacionalnim zakonodavnim telima da definišu nacionalnu politiku u oblasti zaštite privatnosti podataka o ljudima. Na primer, u Švajcarskoj, poverenik za zaštitu podataka još nije zauzeo stav po pitanju biometrije za identifikaciona dokumenta, ali se očekuje da to uskoro učini. Međutim, zuzeo je stav da je uzimanja otisaka prsta u cilju identifikacije pri dolasku i odlasku sa posla, pohranjen u smart karticu, u skladu sa zakonskim propisima o zaštiti podataka.

Na 26. međunarodnoj konferenciji o zaštiti podataka o ličnosti, održanoj septembra 2004. godine u Poljskoj, istaknuto je da prikupljanje i obrada biometrijskih podataka mora da zadovolji nekoliko osnovnih principa, i to [1]:

Princip zakonitosti – u privatnom sektoru, biometrijski podaci, u principu, mogu biti korišćeni samo uz odobrenje osobe na koju se odnose a odobrenje mora biti dato slobodno, mora biti određeno i pojedinac mora biti upoznat sa razlogom davanja ličnih podataka.

Princip „dobre vere“ – proces prikupljanja i obrade biometrijskih podataka mora biti transparentan i ne sme biti sproveden bez znanja osobe na koju se odnose.

Princip svrhe – ukoliko se isti cilj (kontrola pristupa) može ostvariti na manje osetljiv način u smislu zadiranja u privatnost, kao što je verifikacija umesto identifikacije, onda ta tehnika treba da bude upotrebljena.

Princip proporcionalnosti – lični podaci se mogu prikupljati samo ako je to neophodno uz uvažavanje svrhe za koju se inače mogu prikupljati i obrađivati.

Princip zaštite – sigurnost biometrijskih podataka je primarna, pa mere obezbeđenja treba uključiti već u procesu akvizicije.

Najvažniji evropski i međunarodno prihvaćeni standardi značajni za normativno regulisanje ove oblasti su [5]:

- **Evropska konvencija za zaštitu ljudskih prava i osnovnih sloboda** (1950), koja u članu 8. garantuje pravo na poštovanje privatnog i porodičnog života;
- **Evropska konvencija o zaštiti lica u pogledu automatske obrade ličnih podataka Saveta Evrope**, broj 108, usvojena 28. januara 1981. u Strazburu i **Dodatni protokol uz Konvenciju o zaštiti lica u odnosu na automatsku obradu ličnih podataka**, u vezi sa nadzornim organima i prekograničnim protokom podataka, usvojen u Strazburu 2001. godine;
- **Konvencija o sprovođenju Šengenskog sporazuma** od 14. juna 1985. između vlada Privredne unije Beneluks, Savezne Republike Nemačke i Francuske Republike o postupnom uklanjanju kontrole na zajedničkim granicama (koju moraju poštovati sve države članice šengenskog graničnog režima). Podneti podaci se mogu koristiti samo za svrhu koja je predviđena Konvencijom Saveta Evrope iz 1981.godine i to samo od strane ovlašćenih organa [6]. Upotreba u druge svrhe se može odobriti samo ukoliko nacionalni propisi država članica koje su podatak poslale to odobravaju. Konvencija takođe, propisuje da je država članica koja je poslala podatak odgovorna za njegovu tačnost i da strana koja prenosi netačne podatke može biti obavezana da naknadi eventualnu štetu. Istom Konvencijom regulisano je i uspostavljanje nezavisnog organa od strane ugovornica, koji je nadležan za sprovođenje nadzora nad zbirkom podataka nacionalnog dela šengenskog informacionog sistema kao i za proveru zakonitosti obrade podataka koji su uneti u šengenski informacioni sistem;
- **Direktiva Evropskog parlamenta i Saveta, o zaštiti građana u vezi sa obradom ličnih podataka i slobodnom kretanju tih podataka** (95/46 od 24. oktobra 1995);
- **Direktiva Evropskog parlamenta i Saveta, u vezi obrade ličnih podataka i zaštite privatnosti u elektronskom komunikacionom sektoru** (2002/58 FC od 12. jula 2002);
- **Direktiva Evropskog parlamenta i Saveta o zadržavanju generisanih ili obrađenih podataka u vezi sa odredbom u javnosti raspoloživih elektronskih komunikacionih servisa ili javne komunikacione mreže i dopune** (2002/58/ES) i (2006/24) EU od 15. marta 2006;
- **Direktiva 99/93/EC** od 13.XII 99.godine koja reguliše standarde za digitalni potpis;
- **Direktiva 00/31/EC** od 08. VI 00. koja reguliše pravne okvire za elektronsku trgovinu;
- **Direktiva 01/45/EC** koja reguliše standarde za elektronsku administraciju, odnosno elektronske transakcije sa državnim institucijama i organima;
- **Odluka 01/497/EC** koja reguliše standarde za zaštitu ličnih podataka u transakcijama van EU.

Evropska konvencija o zaštiti lica u pogledu automatske obrade ličnih podataka Saveta Evrope ima veliki značaj, ne samo za države članice EU, veći i za ostale države Evrope. Ona predstavlja osnov za mnoge druge kako međunarodne, tako i nacionalne propise koji regulišu pitanje ove zaštite. Cilj ove Konvencije je da dovede u sklad vrednosti kao što su poštovanje privatosti, s jedne strane i potreba slobode protoka informacija među narodima, sa druge strane.

Nakon toga Evropski savet je doneo **Direktivu za zaštitu podataka 95/46/ EC**. Pomenuta Direktiva reguliše zaštitu lica u odnosu na obradu ličnih podataka i njihovo slobodno korišćenje. Osnovni principi ove direktive su sledeći:

- Svođenje prikupljanja ličnih podataka na neophodnu (optimalnu) meru;
- Održavanje transparentnosti na najvišem nivou;
- Institucionalna i individualna kontrola obrade ličnih podataka na što efikasnijem nivou.

Cilj Direktive je usklađivanje zakonodavstva država članica i omogućavanje slobodne cirkulacije podataka i informacija unutar EZ. Domen njene primene je širi od Konvencije jer se odnosi, kako na javne tako i na privatne sektore. Ovom Direktivom takođe, je uspostavljena ravnoteža između osiguranja zaštite, sa jedne strane i slobodnog prometa podataka o ličnosti, sa druge strane. Ona utvrđuje granice prikupljanja i rukovanja ličnim podacima na taj način što zahteva od država članica da uspostave jedno ili više nadzornih tela čiji ce zadatak biti zaštita podataka i praćenje primene zakonskih odredbi.

Nakon toga, doneta je i nova Direktiva o privatnosti i elektronskim komunikacijama kojom je regulisana zaštita osnovnih prava i sloboda pojedinaca, a posebno pravo na privatnost, kao i zaštita legitimnih interesa pravnih lica u vezi sa obradom podataka o ličnosti u sektoru elektronskih komunikacija. Pojedina udruženja, kako u Evropi, tako i u Americi, takođe su izradila kodekse ponašanja koja, zapravo, predstavljaju samoregulativu (*self-regulation*). S tim u vezi, treba pomenuti i Deklaraciju o prekograničnim tokovima podataka, koja je vrlo kratka – sadrži samo četiri tačke osnovnih principa i tri tačke koje se odnose na dalje oblike rada vezane za određene kategorije prekograničnih tokova podataka [1,3].

U Švajcarskoj, iako nije donet poseban zakon koji bi se bavio problematikom biometrije, švajcarski Ustav štiti pravo na privatnost i od zloupotreba ličnih podataka. Takođe, švajcarski Zakon o zaštiti podataka za osnovni zaštitni objekat ima zaštitu ličnosti i osnovnih prava ličnosti čiji se podaci obrađuju. Švajcarski poverenik za zaštitu podataka je upozorio na potencijane probleme uvođenjem biometrijskog sistema. On je istakao da implementacija tog sistema mora da prati, između ostalog, poštovanje principa proporcionalosti i konkretna primena propisa koji uređuju tu oblast[1,3].

U Francuskoj korišćenje biometrije je dozvoljeno u skladu sa Zakonom o zaštiti podataka. Važnu ulogu u regulisanju ove oblasti ima Savet za zaštitu podataka Francuske, koji je dao preporuke za zaštitu privatnosti prilikom korišćenja biometrijske tehnologije, kao što su: korišćenje decentralizovanih baza podataka, uvažavanje pricipa proporcionalnosti i poštovanje pocedure.

Prvi poseban zakon u oblasti zaštite podataka donet je u Nemačkoj 1970 godine. To je Savezni zakon o zaštiti podataka

koji štiti pojedinca i njegovo pravo na privatnost. Međutim, kao i ostale evropske zemlje i Nemačka treba da implementira u svoj federalni zakon Direktivu o zaštiti podataka 95/46 EU. Takođe, u domenu zaštite podataka značajnu ulogu ima i Nemački ured za sigurnost informacija.

Što se Slovenije tiče, slovenački zakon o zaštiti podaka o ličnosti reguliše pitanje biometrijskih podataka. Iz odredaba čl.79 i čl.80 ovog zakona proizilazi da je odvojeno regulisana upotreba biometrijskih podataka u privatnom i javnom sektoru [6]. Naime, biometrijske mere u javnom sektoru se mogu predvideti zakonom ukoliko su neophodne radi bezbednosti ljudi i imovine kao i radi zaštite poverljivih podataka i poslovnih tajni, odnosno kada se ovi ciljevi ne mogu ostvariti manje nametljivim sredstvima (čl.79). Iz čl.80 istog zakona proizilazi da privatni sektor može koristiti biometrijske postupke samo ukoliko su neophodne radi sprovođenja svojih aktivnosti, zaštite lica i imovine ili zaštite poverljivih podataka i poslovnih tajni. Takođe, iz istog člana proizilazi da lice koje prikuplja i radi sa biometrijskim podacima zaposlenih može da podnese pismeni zahtev nadzornom organu kojim zahteva uvođenje biometrijskih mera iz nekog drugog razloga.

U nekim zemljama kao što je Japan, ne postoji Zakon o zaštiti podataka već zaštitu sprovodi svako ministarstvo.

U anglosaksonskim zemljama (SAD, Kanada), regulisanje pravne regulative polazi od " privatnopravne" zaštite ličnih prava i sloboda pojedinaca. To znači da se zaštita prava ostvaruje preko sudova na osnovu lične inicijative .

SAD nemaju zakon o zaštiti podataka, već samo preporuke a termin „privatnost" ne postoji u Ustavu SAD. Još od 2001. godine SAD teže normativnom regulisanju ove oblasti sa ciljem da se ojača kontrola građana i zaštiti teritorija, posebno su značajni sledeći zakoni [7]:

US Patriot Act ima za cilj, između ostalog, da odvrati i kazni terorističke akte u SAD i širom sveta i da ojača zakonske mehanizme istrage,

The US Public Law 107-71 (Zakon o zaštiti avionskog saobraćaja i transporta) reguliše upotrebu novih tehnologija u zaštiti avio saobraćaja, kao što je sistem za kontrolu pristupa zaposlenih na aerodromima,

The US Public Law 107-173 ima za cilj jačanje zaštite granica SAD, kao što je uvođenje biometrijskih informacija u putne isprave,

US national Intelligence Reform Act (Nacionalni zakon o reformi obaveštajnog rada iz 2004). U ovom propisu upotreba biometrijske tehnologije se pominje kao način da se poveća bezbednost SAD; upotreba biometrijskog ulaznog i izlaznog sistema za verifikaciju identiteta putnika na aerodromima i za prikupljanje biometrijskih podataka pri izlazu iz SAD; razvoj integrisanog biometrijskog sistema proveravanja; upotreba biometrije za unapređenje zaštite putnih isprava i pilotskih licenci; uspostavljanje odgovarajućeg centra u nacionalnoj laboratoriji za biometriju i promociju istraživanja i razvoja biometrijskih tehnologija primenljivih u zaštiti avio saobraćaja,

US-VISIT program pripada merama zaštite za jačanje kontrole USA granica i isti treba da obezbedi verifikaciju identiteta posetilaca sa vizama i to prikupljanjem biometrijskih informacija, otiska dva prsta i fotografija lica,

The US Real Act, iz februara 2005. godine, ima za cilj uspostavljanje i ubrzanu primenu regulative o vozačkim dozvolama i standardima zaštite identifikacionih dokumenata. Saglasno ovom pravnom aktu koristiće se tehnologija za mašinsko čitanje svih vrsta, kako vozačkih dozvola, tako i ostalih kartice za identifikaciju. Iz napred navedenog akta proizilazi da se elektronski otisak prsta i fotografije uzimaju i čuvaju u elektronskim bazama za sve vozače, a takođe i za sve primaoce socijalne pomoći u SAD. Pored toga, FBI poseduje baze podataka otisaka prstiju svih osuđenih lica i svih prijavljenih za krivična dela.

Zakon o zaštiti podataka u Velikoj Britaniji predviđa registar za zaštitu podataka i nadležnog registratora za vođenje evidencija o zaštiti podataka. U Velikoj Britaniji je predložen projekat stvaranja baze DNK profila cele populacije. Današnja britanska baza je najveća na svetu i sadrži preko 4,5 miliona uzoraka, kako osuđenih, tako i osumnjičenih za izvršenje krivičnih dela. Takođe, britanski pravni sistem dozvoljava čuvanje uzoraka DNK lica koja su optužena i oslobođena krivice za određeno krivično delo.

Na međunarodnoj konferenciji komesara za informacije i zaštitu podataka koja je održana u Madridu 5.novembra 2009.godine usvojena je Madridska konvencija koja sadrži zajednički predlog Nacrta međunarodnih standarda zaštite privatnosti u pogledu obrade podataka o ličnosti. Rezolucija sadrži principe, prava, obaveze i postupke koje bi svaki sisteme zaštite podataka i privatnosti u savremenom svetu trebalo da obuhvati [6].

3. PRAVNA REGULATIVA U REPUBLICI SRBIJI

U Srbiji faktički sve do pred kraj 2008. godine i nije postojao zakon koji je definisao i određivao način prikupljanja, korišćenja, obrade i čuvanja podataka o ličnosti. Primarni uslov da se ostvari odgovarajuća zaštita podataka o ličnosti u Republici Srbiji je da nacionalno zakonodavstvo bude u potpunosti usaglašeno sa odredbama Direktive 95/46/EZ [5].

Pod pravnim okvirom koji reguliše zaštitu ličnih podataka podrazumevamo ratifikovane međunarodne ugovore i opšte prihvaćena pravila međunarodnog prava koja su deo unutrašnjeg pravnog poretka, kao i domaće zakonodavstvo.

Ustav Republike Srbije članom 42. garantuje zaštitu ličnih podataka. Iz napred pomenutog člana proizilazi da se njihovo prikupljanje, držanje, obrada i korišćenje ličnih podataka uređuje zakonom. Zabranjena je i kažnjiva upotreba ličnih podataka izvan svrhe za koju su prikupljeni. Svako ima pravo da bude obavešten o prikupljenim podacima o svojoj ličnosti u skladu sa zakonom kao i pravo na sudsku zaštitu u slučaju zloupotrebe.

Republika Srbija je potpisala i ratifikovala Konvenciju Saveta Evrope broj 108 o zaštiti lica u odnosu na automatsku

obradu podataka o ličnosti, koja je stupila na snagu 1. januara 2006. godine. U oktobru 2008. godine, usvojen je Zakon o potvrđivanju Dodatnog protokola uz Konvenciju o zaštiti lica u odnosu na automatsku obradu ličnih podataka u vezi sa nadzornim organima i prekograničnim protokom podataka.

Tokom procesa evropskih integracija Srbija je zaključila Sporazum o stabilizaciji i pridruživanju sa EU, a koji između ostalog, sadrži i obavezu da usaglasi svoje zakonodavstvo o zaštiti podataka o ličnosti sa pravom EU i drugim relevantnim evropskim i međunarodnim standardima.

U oblasti zaštite podataka o ličnosti prvi korak je učinjen 2008. godine kada je donet danas važeći Zakon o zaštiti podataka o ličnosti, a koji je počeo da se primenjuje od 01.01.2009.godine. Međutim, ni on nije u celosti usklađen sa Direktivom 95/46/EZ [8, 9].

Važno je napomenuti da je Vlada R.Srbije avgusta 2010. godine usvojila Strategiju zaštite podataka o ličnosti, a kojom su utvrđeni ciljevi, mere i aktivnosti, uloga i odgovornost izvršne vlasti, nadzornog organa i drugih subjekata u ostvarivanju ovog prava [5,8,9].

Zakon o zaštiti podataka o ličnosti je opšti zakon koji reguliše prikupljanje, obradu i prenošenje podataka o ličnosti.

Cilj zakona je da u vezi sa obradom podataka o ličnosti, svakom fizičkom licu obezbedi ostvarivanje i zaštitu prava na privatnost i ostalih prava i sloboda.

Ovaj zakon se primenjuje na svaku automatizovanu obradu, kao i na obradu sadržanu u zbirci podataka koja se ne vodi automatizovano.

Jedno od važnih načela ovog zakona je načelo zabrane diskriminacije što znači da zakon obezbeđuje zaštitu podataka o ličnosti svakom fizičkom licu, bez obzira na državljanstvo i prebivalište, rasu, godine života, pol, jezik, veroispovest, političko i drugo uverenje, nacionalnu pripadnost, socijalno poreklo i status, imovinsko stanje, rođenje, obrazovanje, društveni položaj ili druga lična svojstva.

U smislu načela tačnosti i ažurnosti, obrada podataka o ličnosti nije dozvoljena ako je podatak neistinit ili nepotpun, odnosno kada nije zasnovan na verodostojnom izvoru ili kada je zastareo. To znači da obrađeni podaci o ličnosti moraju odgovarati stvarnim, najnovijim podacima i da su tačni. Zakonodavac je pojedincu dao mogućnost da se uveri da li su prikupljeni podaci tačni i ažurni, te u slučaju da nisu, pokrene odgovarajuće postupke predviđene ovim zakonom.

Obrada podataka nije dozvoljena ukoliko nema odgovarajućeg pravnog osnova, a to može biti zakon ili pojedinac koji daje saglasnost. Ovde je važno naglasiti da se pristanak može opozvati pismeno ili usmeno na zapisniku. Naime, fizička lica imaju pravo na daju ili odbiju pristanak za obradu podataka, pravo na obaveštenje o obradi, pravo na uvid, kopiju kao i pravo povodom izvršenog uvida. Zakonodavac je takođe predvideo i slučajeve kada se može vršiti obrada ličnih podataka i bez pristanka lica na koje se ti podaci odnose, s tim što se prema ovim izuzecima treba odnositi restriktivno. Kada je u pitanju obrada podataka osetljivog karakteta ti podaci moraju biti posebno označeni i moraju biti obezbeđene odgovarajuće mere zaštite. Poverenik ima pravo uvida u ove podatke i pravo provere zakonitosti obrade po službenoj dužnosti ili po zahtevu lica na kojeg se ti podaci i odnose.

Saglasno načelu srazmernosti dozvoljeno je obrađivati samo one podatke koji su očigledno potrebni i primereni za postizanje zakonske namene. Svrha mora biti precizno opredeljena, nepromenjena i dozvoljena. Zabranjena je i kažnjiva upotreba podataka o ličnosti izvan svrhe za koju su prikupljeni, osim za potrebe vođenja krivičnog postupka ili zaštite bezbednosti Republike Srbije.

Zakonom je takođe propisano da lice čiji se podaci obrađuju mora biti obavešteno o obradi i da ima pravo da traži ispravku ili brisanje nezakonitih ili pogrešno unetih podataka. Takođe, Zakonom je regulisano i pravo na žalbu u slučaju povrede prava na zakonitu obradu podataka. Naime, u slučaju nepoštovanja prava na obaveštenje, uvid, kopiju, ispravku ili brisanje podataka, pojedinac ima pravo na žalbu.

Saglasno načelu zaštite podaci moraju biti odgovarajuće zaštićeni od zloupotreba, uništenja, gubitka, neovlašćenih promena ili pristupa. Rukovalac i obrađivač dužni su da preduzmu tehničke, kadrovske i organizacione mere zaštite podataka, u skladu sa utvrđenim standardima i postupcima, a koje su potrebne da bi se podaci zaštitili od gubitka, uništenja, nedopuštenog pristupa, promene, objavljivanja i svake druge zloupotrebe, kao i da utvrde obavezu lica, koja su zaposlena na obradi, da čuvaju tajnost podataka. Obezbeđenje podataka je jedan od ključnih elemenata zaštite podataka o ličnosti. Naime, obezbeđenje podataka je deo šireg pojma zaštite podataka.

Poslove zaštite podataka o ličnosti obavlja Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti. On je samostalan i nezavisni organ koji vrši nadzor nad sprovođenjem zaštite i obezbeđenja podataka o ličnosti, odlučuje po žalbi u slučajevima koji su ovim zakonom predviđeni i daje mišljenja o propisima.

Poseban akcenat treba staviti na odredbe Zakona, kojima je regulisano pitanje zaštite zbirki podataka, imajući u vidu da su sve češće pojave krađe identiteta. Zbirka podataka je skup podataka koji se automatizovano ili neautomatizovano vode i dostupni su po ličnom, predmetnom ili drugom osnovu. Centralni registar omogućava da se zaintetresovano lice upozna sa zbirkama podataka o ličnosti te lakše dođe do informacija o podacima koji su mu potrebni [9].

Takođe, doneti su i propisi koji se neposredno ili posredno odnose na zaštitu podataka o ličnosti. Takvi su na primer propisi koji regulišu: slobodan pristup informacijama od javnog značaja, bankarski sektor, sektor penzijsko-invalidskog i zdravstvenog osiguranja, medicinsku dokumentaciju, sektor bezbednosti, sektor telekomunikacija, evidencije u oblasti rada, sektor oglašavanja i reklamiranja, arhivske građe, sektor tržišta hartija od vrednosti itd. Usvojeni su veoma značajni zakoni koji su u neposrednoj vezi sa zaštitom podataka o ličnosti, kao npr. Zakon o ličnim kartama i Zakon o putnim ispravama. Znači,

pored osnovnog zakona, a radi potpunog regulisanja ove materije celishodno je donošenje i specijalnih zakona u određenim oblastima a koji su usaglašeni sa osnovnim [5].

Brojni aspekti zaštite trenutno se uređuju i podzakonskim aktima. Što se podzakonskih akata tiče, njima se mogu urediti samo tehnički aspekti obrade podataka. Tu spadaju Uredba o obrascu za vođenje evidencije i načinu vođenja evidencije o obradi podataka o ličnosti (2009), Pravilnik o načinu prethodne provere radnji obrade podataka o ličnosti (2009) i Pravilnik o obrascu legitimacije ovlašćenog lica za vršenje nadzora po Zakonu o zaštiti podataka (2009). U pripremi je nacrt Uredbe o načinu arhiviranja i merama zaštite naročto osetljivih podataka. Imajući u vidu da je tek 2008.godine u R.Srbiji započelo normativno regulisanje oblasti zaštite podataka o ličnosti, nije začuđujuće što trenutno postoje veoma važne oblasti (marketing, video nadzor, upotreba biometrijskih podataka i dr.) u kojima još uvek nisu doneti odgovarajući pravni propisi [5].

4. ZAKLJUČAK

Nove informacione i komunikacione tehnologije su pored brojnih koristi, donele i nove izazove, od kojih treba posebno istaknuti one koji se odnosi na korišćenje i upotrebu ličnih podataka. Brzina primena novih tehnologija, kakve su na primer Internet tehnologije, je predstavljalo poseban problem u domenu prava, koje zahteva pažljivo i svestrano proučavanje oblasti primene pre donešenja odgovarajuće pravne regulative. To se posebno odnosi na pravnu regulativu zaštite podataka, a koja se neprekidno izgrađuje širenjem biometrijskih tehnologija u idetifikaciji i verifikaciji ličnosti. Regulisanje biometrije u jednom pravnom okviru predstavllja veliki izazov i nimalo jednostavan zadatak, budući da je neophodno uspostaviti ravnotežu između slobodnog protoka podataka i zaštite privatnosti. Danas sve češće dolazi do zloupotrebe ličnih podataka, tako da je zbog toga neophodno obezbediti adekvatne mere zaštite i informisati građane u vezi njihovih prava i interesa.

Što se tiče evropskog zakonodavstva može se zaključiti da su sve članice EU i države kandidati uspostavile sisteme zaštite ličnih podataka, koji čine jedinstveni zakonski i institucionalni mehanizmi. Zakon o zaštiti ličnih podataka R. Srbije iz 2008. godine većim delom je usaglašen sa pravom Evropske Unije.

Novom strategijom zaštite podataka o ličnosti koju je usvojila Vlada R.Srbije dat je predlog da se nastavi usklađiavnje domaće pravne regulative u oblasti zaštite ličnih podataka u skladu sa Evropskom pravnom regulativom. Pored toga, dat je predlog da se razgraniči upotreba biometrijskih podataka u javnom i privatnom sektoru po uzoru na čl.79 i čl.80 slovenačkog zakona.

Treba imati u vidu da se biometrijske tehnologije stalno unapređuju i usavršavaju, pa je potrebno neprekidno pratiti postojeću pravnu regulativu u ovoj oblasti i po potrebi je menjati i dopunjavati kako bi se obezbedila sigurnost prikupljenih podataka i ostvarila zaštita prava na privatnost.

REFERENCE

[1] K. Jain, Patrick D. Dessimoz, J. Richiardi, Ch. Champod, A. Drygajlo, Multimodal biometrics for identity documents, Forensic Science International 167 (2007) 43–47

[2] Evropska konvencija o zaštiti ljudskih prava i osnovnih sloboda, Rim, 4.novembar 1950.godine

[3] Drakulić M., Drakulić R., Evropska perspektiva regulisanja Internet usluga: izazov tradicionalnog evropskom pravu, časopis Telekomunikacije, Br. 6/2010.

[4] Paunović S., Starčević D., Milenković I, Menadžment identiteta i pitanja privatnosti, Zbornik konferencije INFOTECH 2011, Vrnjačka Banja, (2011)

[5] Strategija zaštite podataka o ličnosti, "Službeni glasnik RS", br. 58/2010 od 20. 08. 2010.

[6] Miletić E., Lilić S., Vitkauskas D. "Podrška instituciji poverenika za informacije od javnog znacaja i Zaštitu podataka o licnosti „IBF International Consulting, 2010

[7] Flynn, a. A. Ross, eds., „Handbook of Biometrics", Springer, (2008)

[8] Zakon o zaštiti podataka o ličnosti, "Službeni glasnik RS", br. 97/2008, 104/2009

[9] Nataša Pirc Musar, Vodič kroz Zakon o zaštiti podataka o ličnosti, Beograd, 2009

Saša Paunović

Kontakt: sasa.sale.paunovic@gmail.com

Oblasti interesovanja: biometrija, biometrijski sistemi, bezbednost, zaštita