NOVI STANDARDI ZAŠTITE LIČNIH PODATAKA U EU

NEW STANDARDS OF DATA PROTECTION IN EU

Derviša Zahirović, MA prava
Univerzitet u Zenici
Zenica

REZIME
U radu je predstavljen pravni okvir zaštite ličnih podataka u Evropskoj uniji sa posebnim akcentom na Uredbu o zaštiti ličnih podataka (GDPR- General Data Protection Regulation) koja je stupila na snagu u maju 2018. godine i član 8. Povelje o osnovnim pravima Evropske unije. Osim toga u radu su prezentirani najznačajniji slučajevi iz sudske prakse Suda EU (ECJ) Schrems i Google Spain, slučaj Evropskog suda za ljudska prava (ECHR) Big Brother Watch i jedan primjer iz prakse Agencije za zaštitu ličnih podataka Bosne i Hercegovine u pitanju vršenja videonadzora u firmi „ADV PAX Lutec" d.o.o. Maglaj.

Ključne riječi: GDPR, zaštita ličnih podataka, data protection, ECJ, ECHR

ABSTRACT
This paper presents legal frame of data protection in European Union with special focus on General Data Protection Regulation (GDPR) that has come into force in May of 2018 and article 8. of the Charter of Fundamental Rights of the European Union. Additionaly, this paper presents the most significant cases from the court practice of the European Court of Justice (ECJ) like Schrems and Google Spain, case of the European Court of Human Rights (ECHR) Big Brother Watch and an example from Personal Data Protection Agency in Bosnia and Herzegovina in question of video surveillance in „ADV PAX Lutec" Ltd. Maglaj.

Keywords: GDPR, data protection, ECJ, ECHR

1. UVOD

Tehnološkim razvojem i novim načinima obrade ličnih podataka, postalo je neophodno donošenje novog instrumenta koji će osigurati zaštitu prava i osnovnih sloboda pojedinaca u vezi s obradom njihovih ličnih podataka. Internet je kreiran tako da dozvoljava brzi prijenos podataka u svijetu samo jednim klikom miša, te na taj način geografske granice zemalja postaju irelevantne. Na primjer informacije mogu uključivati imena pojedinaca, adrese, rasu, spol, godine, pa čak i neke osjetljive i intimne informacije kao što je informacija da neko očekuje dijete. Stoga je Evropska unija u jednom dugom, sedmogodišnjem procesu kreiranja, sačinila i 2016. godine usvojila Uredbu o zaštiti ličnih podataka.[1]

2. PRAVNI OKVIR ZAŠTITE PODATAKA U EU

2.1. Opća uredba o zaštiti ličnih podataka EU (2016/679)

U modernom društvu, u eri interneta, društvenih mreža i internetskih medija, posebno važne elemenat čine informacije kao sastavni dijelovi slobode i prava na širenje informacija koji u velikoj mjeri ovisi upravo o legitimnosti i mogućnosti upravljanja zbirkama podataka.

25. maja 2018. godine na snagu je stupila Opća uredba o zaštiti ličnih podataka Evropske unije EU – General Data Protection Regulation ili skraćeno GDPR (2016/ 679) koja je zamijenila direktivu 95/46/EC o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka.[2] Uz navedenu Opću uredbu, sastavni dio usvojenog zakonodavnog paketa je i Direktiva o zaštiti pojedinaca pri obradi ličnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona počinilaca krivičnih djela ili izvršavanja krivičnih sankcija i o slobodnom kretanju takvih podataka (2016/680).

Dakle, do stupanja na snagu Opće uredbe pitanje zaštite ličnih podataka u Evropskoj uniji, između ostalog bilo je regulirano Direktivom 95/46/EC što je značilo da je državama članicama ostavljena mogućnost da implementirajući ovu Direktivu, na različite načine obezbijede zaštitu građana kroz nacionalne zakone. Naime, direktive kao sekundarni izvor prava Evropske unije se prije svega moraju implementirati u nacionalno zakonodavstvo zemlje članice Unije kako bi se pravo garantovano direktivom moglo primjeniti, a u zavisnosti od vrste direktive, odnosno da li je to direktiva maksimalne ili minimalne harmonizacije zavisit će i način njene implementacije u nacionalno zakonodavstvo.[3]

Za razliku od prethodne Direktive Uredbu nije potrebno posebno implementirati u nacionalni zakon jer se ona primjenjuje direktno umjesto nacionalnog zakona. Povodom početka primjene nove Uredbe, države članice Unije donose nacionalne provedbene zakone kojima prestaju važiti dosadašnji nacionalni zakoni o zaštiti ličnih podataka

Prema odredbama člana 4. stav (1) lični podaci su svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi, a („ispitanik") pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati direktno ili indirketno, posebno uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više činilaca svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca. Pored toga, članom 4. Uredbe date su i definicije ključnih pojmova na koje se odnosi Uredba, no onaj koji je ipak najvažniji smatramo jeste pojam pristanka. Uredba definira pristanak kao svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose.

Neka od područja koja Uredba želi da regulira su: režim zaštite podataka u online eri, društvenim mrežama, pohrana podataka na tzv. oblacima, te želi da postavi standard minimalne, odnosno maksimalne zaštite, kao i da uspostavi principe zaštite podataka.

Ono što je novo u Uredbi jeste njeno područje primjene. Naime GDPR se primjenjuje i na situacije kada je voditelj ili izvršitelj obrada ima poslovni nastan van Evropske unije, a na njega se može primijeniti pravo članice unije kao međunarodno pravo. Isto tako GDPR se primjenjuje i na situacije kada voditelj ili izvršitelj obrade imaju poslovni nastan u Uniji, bez obzira na to da li se obrada podataka obavlja u Uniji ili van nje. Uredba se primjenjuje na obradu ličnih podataka ispitanika u Uniji koju obavlja voditelj obrade ili izvršitelj obrade bez poslovnog nastana u Uniji, ako su aktivnosti obrade povezane s:

(1) nuđenjem robe ili usluga takvim ispitanicima u Uniji, neovisno o tome treba li ispitanik izvršiti plaćanje; ili

(2) praćenjem njihova ponašanja dokle god se njihovo ponašanje odvija unutar Unije (GDPR, član 3. Stav (2)).

Važno je istaći još nekoliko važnih "novina" koje je Uredba donijela, a to su: pravo na zaborav (right to be forgotten) ili pravo na brisanje, zaštita podataka djece, uspostavljanje obučenih službenika za zaštitu ličnih podataka, osnivanje nadzornih tijela u državama koje će vršiti nadgledanje provođenja zaštite ličnih podataka, propisivanje visokih novčanih kazni za organizacije koje budu kršile prava garantirana Uredbom i na kraju pravna zaštita garantirana kroz pravo na efikasan pravni lijek i pravo na pravično suđenje (Preambula Uredbe). Uredbom su normirane ogromne novčane kazne za prekršioce pa se tako govori i ciframa od najmanje 10 miliona eura odnosno 2% ukupnog godišnjeg prometa, zavisno koji je od ta iznosa veći ukoliko se radi povredema prava djeteta, obrade koja ne zahtijeva identifikaciju, općim odredbama o kontrolama i slično ili 20 miliona eura ili 4% ukupnog godišnjeg prometa, zavisno koji je iznos veći ako se radi po povredama principa obrade podattaka, nezakonite obrade podataka, situacijama bez pristanka, prijenosu podataka u treće zemlje i slično.

2.2. Univerzalna deklaracija o ljudskim pravima

Pravo na zaštitu ličnih podataka možemo smatrati kao dijelom prava na privatnost garantiranim članom 12. Univerzalne deklaracije o ljudskim pravima usvojene od strane Generalne skupštine Ujedinjenih nacija 1948. godine - Niko se ne smije izložiti proizvoljnom miješanju u privatni život, porodicu, stan ili prepisku, niti napadima na čast i ugled. Svako ima pravo na zaštitu zakona protiv ovakvog miješanja ili napada. (No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks).[4]

2.3. Evropska konvencija o ljudskim pravima (EKLJP)

Evropska Konvencija o zaštiti ljudskih prava i osnovnih sloboda u članu 8. garantira pravo na privatan život, odnosno da svako ima pravo na poštivanje svog privatnog i porodičnog života, doma i prepiske.[5] Javna vlast se ne miješa u vršenje ovog prava, osim ako je takvo miješanje predviđeno zakonom i ako je to neophodna mjera u demokratskom društvu u interesu nacionalne sigurnosti, javne sigurnosti, ekonomske dobrobiti zemlje, sprječavanja nereda ili sprječavanja zločina, zaštite zdravlja i morala ili zaštite prava i sloboda drugih.
Bitna razlika između Univerzalne deklaracije i Evropske konvencije o ljudskim pravima jeste u tekstu na engleskom jeziku prema kojem u Univerzalnoj deklaraciji se koristi riječ "privacy", dok se u Evropskoj konvenciji koristi termin "private life". No vremenom Evropski sud za ljudska prava u svojoj praksi ustanovio je termin privatnost (privacy) kada se radilo o slučajevima kršenja člana 8. Konvencije. Posebno su značajne presuda Evropskog suda za ljudska prava (ESLJP) u slučajevima Leander, Gaskin.
Također, važno je spomenuti i Konvenciju Vijeća Evrope o zaštiti lica u pogledu automatske obrade ličnih podataka usvojenu 1981. godine, poznatiju kao Konvencija 108.

2.4. Povelja o osnovnim pravima Evropske unije (POP)

Još 2000. godine u Nici, Evropski parlament, Savjet i Komisija proglasili su Povelju o osnovnim pravima Evropske unije (POP), koja je stupila na snagu tek donošenjem Lisabonskog ugovora 2009. godine. Prema Preambuli cilj Povelje jeste jačanje osnovnih prava u svjetlu promjena u društvu, sociajlnog napretka naučnog i tehničkog razvoja.[6]
Poveljom se pravo na zaštitu ličnih podataka uspostavlja kao osnovno pravo. Naime, član 8. Povelje normira da svaka osoba ima pravo na zaštitu ličnih podataka koji se na nju odnose. Lični podaci moraju se obrađivati pošteno i koristiti u za to utvrđene svrhe i na osnovu pristanka osobe koje se tiču ili na nekoj drugoj zakonitoj osnovi, a svako ima pravo na pristup

prikupljenim podacima o njemu i pravo na njihovo ispravljanje. Nadzor nad poštovanjem ovih pravila vrši nezavisni organ.[7]
Također, Povelja u članu 7. garantira i pravo na privatni i porodični život poput naprijed pomenutih međunarodnih dokumenata, što predstavlja jedan vid kompromisa između različitih rješenja koja su već postojala u državama članicama. Ovo je prvi put da se uspostavlja supranacionalni instrument koji štiti posebno pravo na zaštitu ličnih podataka i posebno pravo na privatni i porodični život.

3. SUDSKA PRAKSA

Evropski sud pravde (ECJ) prvi put je u slučaju Promusicae ustanovio postojanje prava na zaštitu ličnih podataka. Neke od značajnih presuda ECJ-a su u slučajevima Huber, Rijkeboe, Deutsche Telekom, Schrems, Wirtschaftsakademie Schleswig Holstein. U radu ćemo predstaviti presude Schrems i Google Spain. I Evropski sud za ljudska prava odlučivao je u pitanju zaštite ličnih podataka, posebno „masovnog nadzora", a ovdje ćemo ukratko prikazati presudu iz 2018. godine Big Brother Watch.

3.1. Slučaj Schrems

Student prava Maximilian Schrems, inače državljanjin Austrije i korisnik Facebooka od 2018. godine, podnio je prigovor irskom nadzornom tijelu smatrajući da, s obzirom na otkrića Edwarda Snowdena u 2013. godine u vezi s aktivnostima obavještajnih službi SAD-a (posebno u vezi sa National Security Agency ili NSA), pravo i praksa u SAD-u ne nude adekvatnu zaštitu od nadzora javnih tijela podataka prenesenih u tu zemlju. Irsko nadzorno tijelo odbilo je navedeni prigovor iz razloga jer je već postojala odluka Komisije kojom se povtrđuje da je u skladu sa sporazumom „Safe Harbour" osigurana odgovarajuća zaštita prenesenih podataka. [8]
Naime bitno je istaći ovdje još nekoliko činjenica, a to su da je Facebook u Irskoj formirao podružnicu koja je podatke prenosila u SAD, te da je postojao potpisani sporazum o sigurnom prijenosu podataka građana EU u SAD, tzv. „Safe Harbour Arrangement", a koji su potpisali Evropska komisija i Vlada SAD-a. Direktivom EU bio je principijelno zabranjen prijenos podataka građana EU u treće zemlje, osim ukoliko ne postoji garancija te zemlje da će obezbijediti adekvatnu zaštitu podataka. U julu 2000, godine Komisija je usvojila Odluku kojom se izjavljuje da SAD- obezbjeđuju adekvatnu zaštitu podataka.
Nakon što su irske vlasti odbile prigovor, slučaj je završio na sudu. Postupajući u predmetu irski Visoki sud (High Court of Ireland) upućuje sljedeće pitanje Evropskom sudu pravde: onemogućava li odluka Komisije nacionalno nadzorno tijelo da ispita prigovor kojim se navodi da treća zemlja ne osigurava odgovarajuću razinu zaštite te da po potrebi prekine prijenos spornih podataka?
Sud pravde EU je odlučio da nacionalna tijela za zaštitu podataka imaju pravo da istražuju adekvatnost prijenosa podataka zaštićenih SAD-EU sporazumom "Safe Harbour" ili bilo kojim drugim sporazumom sklopljenim u skladu s Odlukom Komisije 2000/520, ali da sporazum "Safe Harbour" bi trebao biti nevažeći zbog nedostatka adekvatnosti, što je za Facebook, Google i slične kompanije značilo obustavu prijenosa podataka iz EU u SAD. Kada je u pitanju adekvatnost to znači da treća država u koju se prenose podaci mora osigurati zaštitu podataka kroz svoje nacionalno zakonodavstvo, a koja će biti jednaka pravnoj zaštiti u EU.
No, prestanak prijenosa podataka iz EU u SAD- nije zadugo potrajao, te su već u februaru 2016. godine Evropska komisija i Obamina administracija usaglasile, a u julu iste godine i usvojile tekst novog sporazuma tzv. "Privacy Shield EU-US Data Transfer Arrangement", kojim je omogućen prijenos podataka ali pod "strožijim" uvijetima.

3.2. Slučaj Google Spain

M. Costeja González, španski državljanin s prebivalištem u Španiji, podnio je AEPD-u prigovor protiv La Vanguardia Ediciones SL, izdavača visokotiražnih dnevnih novina, posebno u Kataloniji (Catalonia) kao i protiv Googlea Spain i Googlea Inc. Prigovor je bio utemeljen na činjenici da bi korisnici interneta prilikom unošenja imena M. Costeje Gonzáleza u internetski pretraživač grupe Google dobivali poveznice prema dvjema stranicama dnevnika La Vanguardia od 19. januara i 9. marta 1998. na kojima se nalazio oglas s imenom M. Costeje Gonzáleza za licitacijsku prodaju nekretnina povezanu s izršenjem radi naplate dugova iz područja socijalnog osiguranja. Slučaj je završio pred Sudom pravde EU koji je odlučio da građani imaju pravo zahtijevati od kompanija koje omogućavaju pretraživanje kao što je Google, odnosno koje prikupljaju lične podatke radi profita, da uklone veze na privatne informacije, ali pod uslovom da su te informacije irelevantne. [10]

3.3. Slučaj Big Brother Watch

Pred Evropskim sudom za ljuska prava u Strasbourgu našao se i slučaj Big Brother Watch i drugi protiv Velike Britanije.[11] Ovaj predmet je privukao ogromnu pažnju evropske javnosti. Naime aplikanti su svi redom naveli da sumnjaju, a na bazi Snowdenovih podataka da su zbog prirode njihovih poslova njihove elektroničke komunikacije bile nadzirane od strane obavještajnih službi Velike Britanije ili ih su ih pribavile obavještajne službe Velike Britanije presretanjem prisluškivanja stranih vlada ili razmjenom ili su ih obavještajne službe pribavile od britanskih komunikacijskih tijela odnosno provajdera. Dakle, slučaj se bavio trima vrstama nadzora: skupnim presretanjem komunikacija, razmjenom obavještajnih podataka sa stranim vladama i pribavljanjem podataka od pružalaca komunikacijskih usluga.
Presuda je obimna i obrazložena na 212 strana, tako da je zaista teško sve sumirati u nekoliko rečenica. No, ono što je najbitnije jeste da je Sud u ovom slučaju utvrdio povredu člana 8. (pravo na privatni i porodični život) i člana 10. EKLJP (sloboda izražavanja) zbog masovnih presretanja komunikacije. Sud navodi da režim presretanja komunikacija krši član 8. EKLJP iz razloga jer nije bilo dovoljno nadzora nad selekcijom odabira internetskih nositelja za presretanje i filtriranje, pretraživanje i odabir presretnutih komunikacija, te da su i zaštitne mjere za odabir komunikacija za presretanje bile neadekvatne. Dalje, sud je utvrdio da preuzimanje podataka od pružalaca komunikacijskih usluga, kao i sam režim presretanja komunikacija krše član 10. EKLJP iz razloga jer nije bilo dovoljne zaštite povjerljivih novinarskih podataka. I na kraju Sud je utvrdio da u slučaju razmjene podataka između obavještajnih službi Velike Britanije i drugih država nije bilo kršenja niti člana 8. niti člana 10. EKLJP.

3.4. Slučaj iz prakse Agencije za zaštitu ličnih podataka Bosne i Hercegovine

U Bosni i Hercegovini trenutno je na snazi Zakon o zaštiti ličnih podataka Bosne i Hercegovine iz 2006. godine koji je djelimično izmijenjen i dopunjen 2011. godine. Potrebno je napomenuti da je Bosna i Hercegovina odredbama Sporazuma o stabilizaciji i pridruživanju EU obavezna svoje zakonodavstvo uskladiti sa pravom Evropske unije, te stoga zakonodavna vlast ima zadatak donijeti novi zakon koji će biti usklađen sa Općom uredbom o zaštiti podataka EU. Još je važno istaći da se odredbe Uredbe ne odnose na teritorij i građane Bosne i Hercegovine, osim u slučajevima kako je navedeno ranije u radu.
Pred Agencijom za zaštitu ličnih podataka našla se prijava kojom se tražilo pokretanje postupka protiv „ADV PAX Lutec“ d.o.o. Maglaj zbog obrade podataka putem video-nadzora uspostavljenog nad poslovnim prostorijama navedenog pravnog lica. U prijavi je navedeno da je ADV postavio kamere za video nadzor u kancelarijama administrativnih radnika, kantini, kao i u kancelariji rukovodioca proizvodnje u kojoj je pored kamera postavljen i mikrofon za tonsko snimanje. Pored toga u prijavi je navedeno da se prikupljeni snimci prenose putem

servera u Republiku Njemačku. Podnosilac prijave je smatrao da ovakva obrada podataka ugrožava osnovna prava radnika.[12]
Nakon zaprimanja prijave inspektori Agencije za zaštitu ličnih podataka su izvršili inspekcijski uvid i tom prilikom u navedenim prostorijama zabilježili postojanje nadzornog sistema od 15 kamera od čega su 3 kamere bile vanjske, a ostalih 12 kamera bile su raspoređene unutar poslovnih prostorija. Prilikom inspekcijskog uvida nisu pronađeni video snimci, odnosno svi podaci su izbrisani, a kamere nisu pohranjivale snimke nego su samo nadzirale u realnom vremenu, dok je praćenje bilo omogućeno odgovornoj osobi putem aplikacije na mobitelu. Osim toga u skladu sa Zakonom o zaštiti ličnih podataka odgovorno lice trebalo je donijeti odluku o vršenju video-nadzora i njome detaljno propisati načine na koji će se isti realizovati. Odgovorno lice tvrdilo je da su kamere postavljene radi zaštite lica i imovine, a nikako radi nadgledanja radnika. No, s obzirom da su kamere bile usmjerene na radnike, te da su se isti jasno mogli identifikovati, postojala je bojazan da se takvim video-nadzorom ipak prikupljaju podaci o ponašanju radnika. Agencija za zaštitu ličnih podataka je svojim rješenjem zabranila „ADV PAX Lutec“ d.o.o. Maglaj da vrši video-nadzor u kancelarijama radnika, u Sali za sastanke i kantini, te naložila da izbriše sve snimke nastale upotrebom video-nadzora. Također, naredila je donošenje odluke o vršenju video-nadzora sa jasno propisanim procedurama.

4. ZAKLJUČAK

Od samog usvanja Opće uredbe o zaštiti podataka EU do njenog stupanja na snagu u maju prošle godine, pisalo se mnogo o mogućim problemima sa kojima će biti suočeni građani EU, ali i osobe koje imaju svoj poslovni nastan u EU. Skoro godinu dana nakon stupanja na snagu još uvijek nije jasno koliko je zaista pozitivnih efekata donijela i šta je to negativno u cijeloj ovoj priči oko zaštite podataka. Naime, cilj EU jeste da nastavi svoju pravnu tradiciju u kojoj je zaštita ljudskih prava iznad svega, no postavlja se pitanje da li je moguće sve nuspojave koje je već izazvala Uredba u primjeni i koje će u budućnosti izazvati opravdati zaštitiom ljudskih prava, a posebno ukoliko uzmemo u obzir masovnu pojavu korištenja društvenih mreža Facebooka, Instagrama i Twitera putem kojih korisnici doslovno i konstantno iznose svoje privatne podatke.
Jedan od problema koji je već primjećen, a jako je značajan za razvoj pravne nauke ali i transparentnost rada pravosudnih institucija jeste da su neki sudovi npr. sudovi na Cipru ali i Evropski sud za ljudska prava razmatrali ili već uveli zabranu objavljivanja imena u presudama, pa čak i inicijala osoba. Naime predloženo je da se u objavljenim presudama navode nasumično izabrani inicijali. Za razvoj pravne nauke smatramo da je takvo nešto neodrživo iz čisto praktičnih razloga. Sam ovaj rad ne bi imao smisao ukoliko bi umjesto naziva ključnih presuda u praksi sudova stajali nasumični inicijali stranaka, pa tako bi teško zamislivo bilo razumjeti presudu Schrems ukoliko ne bi smo znali da je cijeli slučaj koncipiran oko Facebooka.
Dalje, Uredbom se dosta zadire u pitanje objavljivanja i snimanja fotografija. Prilikom svake objave fotografije na društvenim mrežama ili korištenja fotografija radi obavljanja poslovne djelatnosti neophodno je pribaviti pristanak osoba koje se nalaze na fotografiji, ali i pored kojeg postoji mogućnost da neka osoba zatraži brisanje fotografije.
Pored toga, smatra se da će ovako strogom zaštitom podataka doći do povećanja cyber kriminala, jer npr. u transakcijskim rješenjima, zakonodavstvo u nekim zemljama zahtijeva „sljedivost“ za radnje koje izvršavaju pojedini korisnici.Uredba nalaže kompanijama da brišu sve podatke koji se odnose na pojedinačne radnje, što znači da je pojedinačna sljedivost izgubljena i da mogućnost revizije toka poduzeća postaje nemoguća.

Uredba je također, smatraju analitičari, ugrozila poslovanje malih poduzeća koja nisu u mogućnosti uložiti u infrastrukturu i ljudske resurse kojima bi se obezbijedila adekvatna zaštita ličnih podataka. Za građane EU posebno je otežavajuća okolnost da oni više nemaju pristup određenim internetskim stranicama trećih zemalja, jer one nemaju propisanu proceduru zaštite ličnih podataka koja bi bila u skladu sa principa koji važe u EU.
No, nije ipak ni sve tako negativno kada je u pitanju GDPR. Naime, Uredba se implementira direktno u zakonodavstvo država članica EU, što znači da svi građani EU imaju ista prava u svim državama članicama, te da ukoliko postoji bilo kakav problem nije potrebno da poznaju zakonodavstvo konkretne države članice. Dalje, Uredbom je poboljšana zaštita samih građana EU, samih pojedinica, na način da se za svaki podatak koji neko prikuplja treba tražiti pristanak uz objašnjenje zbog čega se određeni podaci prikupljaju i ko će da kontroliše upotrebu tih podataka. Također, građanima sada stoji na raspolaganju i mogućnost pozivanja na „pravo na zaborav".
Svakako je očekivati da će sudska praksa i Suda pravde EU i Evropskog suda za ljudska prava iznjedriti neke nove standarde i da će se tumačenjem odredbi Uredbe doći do sasvim novih rješenja.
Ovaj zaključak je sažetak onih negativnih i pozitivnih efekata Uredbe koje je autor rada zamijetio u kratkom vremenskom periodu i na osnovu ličnih iskustava, a njih je svakako mnogo više. Tema o zaštiti ličnih podataka je zaista kompleksna i zanimljiva da bi mogla biti napisana u kratkim crtama na nekoliko stranica.

LITERATURA

[1] J. Čizmić, M. Boban, Učinak nove EU Uredbe 2016/679 (GDPR) na zaštitu osobnih podataka u Republici Hrvatskoj, Zbornik Pravnog fakulteta Sveučilišta u Rijeci, vol. 39, br. 1, 377-410 (2018)
[2] Opća uredba o zaštiti ličnih podataka EU 2016/679 - The EU General Data Protection Regulation 2016/679 (GDPR)
[3] Z. Meškić, D. Samardžić, Pravo Evropske unije I, TDP Sarajevo, 2012.
[4] Univerzalna deklaracija o ljudskim pravima UN-a usvojena i proglašena rezolucijom UN –a 217/III 10.decembra 1948. godine
[5] Evropsla konvencija o ljudskim pravima, Rim, 04. novembar 1950. godine
[6] Z.Meškić, D. Samardžć, Pravo Evropske unije II- Povelja Evropske unije o osnovnim pravima, Pravni fakultet Zenica, 2017. godine
[7] Povelja o osnovnim pravima Evropske unije, Rim, 2000. godine
[8] Slučaj C-362/14 Maximillian Schrems v Data Protection Commissioner, Odluka Suda pravde EU od 06.oktobra 2015. godine
[9] S. Darcy, Battling for the Rights to Privacy and Data Protection in the Irish Courts, (2015) 31(80) Utrecht Journal of International and European Law 131
[10] Slučaj C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Odluka Suda pravde EU od 13.maja 2014. godine
[11] Slučaj Big Brother Watch i drugi protiv Velike Britanije (Aplikacija broj 58170/13, 62322/14 i 24960/15) od 13. septembra 2018. Godine
[12] Rješenje Agencije za zaštitu ličnih podataka Bosne i Hercegovine, Obrada ličnih podataka upotrebom videonadzora u poslovnim prostorijama „ADV PAX Lutec" d.o.o. Maglaj od 29.08.2018. godine