

Arben Murtezić^{*1}

OPŠTA UREDBA O ZAŠTITI PODATAKA: ODNOS PRAVA NA PRIVATNOST I ZAŠTITE LIČNIH PODATAKA S OSVRTOM NA BOSNU I HERCEGOVINU

SAŽETAK

U radu se, prije svega, nastoje objasniti principi Opšte uredbe o zaštiti ličnih podatka (EU) 2016/67 od 27. aprila 2016. godine (Uredba). Naročita pažnja je posvećena teritorijalnom važenju, odnosno uticaju na treće zemlje, obzirom da su promjene koje je Uredba donijela među najvažnijim, a ujedno i najkontraverznijim. Svakako, ovaj aspekt Uredbe je posebno važan i za Bosnu i Hercegovinu, obzirom na obaveze koje proizilaze iz Sporazuma o stabilizaciji i pridruživanju, a i uopštenu ekonomsku, političku i bezbjedonosnu upućenost na Evropsku uniju. Pomenuti principi i primjena Uredbe se u radu razmatraju kroz odnos između zaštite ličnih podataka i prava na privatnost, odnosno kroz prizmu odredbi Uredbe i Konvencije o zaštiti ljudskih prava (Konvencija), te Povelje o osnovnim pravima Evropske unije (Povelja). Shodno tome, u vrlo sažetoj formi je predstavljena praksa Evropskog suda za ljudska prava u Strazburu i to isključivo u predmetima koji se odnose za zaštitu ličnih podataka, a indirektno i praksa Suda Evropske unije. Konačno, ovaj članak ukazuje da, iako se Uredba smatra jednom od najvažnijih i najkompleksnijih dijelova legislative Evropske Unije, koji dotiče različite sfere života i društva, a samim tim i prava, poštivanje osnovnih ljudskih prava i dosljedna primjena Konvencije u značajnom dijelu rezultira i poštivanjem osnovnih principa i suštine Uredbe.

35

Ključne riječi: zaštita ličnih podataka, pravo na privatnost, pravo Evropske unije, Opšta uredba o zaštiti ličnih podatka, teritorijalno važenje, horizontalno i vertikalno usklađivanje, primjena u Bosni i Hercegovini, Evropska konvencija o zaštiti ljudskih prava, Povelja o osnovnim pravima Evropske unije

¹ *Dr.sc. direktor Centra za edukaciju sudija i tužilaca u Federaciji Bosne i Hercegovine, Sarajevo, Bosna i Hercegovina

UVOD

Generalno, određivanje nadležnosti po teritorijalnom principu (mjesna nadležnost), postaje sve teža i nejasnija u digitalnom dobu. Kada se radi o obradi podataka, situacija je dramatično izmijenjena. Međusobno povezivanje privatnih, korporativnih i društvenih sistema, lako kopiranje, automatizacija i tehnike jednostavnog sakupljanja i upoređivanja podataka dovode do stalno novih faktičkih i pravnih situacija². Pored toga, proces je višesmjeran, postoje tehnologije i postupci koji su direktno usmjereni na lične podatke ali je, isto tako, svaka aktivnost na internetu na neki način povezana sa ličnim podacima. Ne tako davno, procesuiranje ličnih podataka je i faktički i pravno, bilo jednostavno objasnjivo. Ovo zahvaljujući tome što su podaci, kontrolori podataka, obrađivači podataka i korisnici svi potpadali pod jednu jurisdikciju, tako da problem nadležnost između različitih jurisdikcija praktično nije postojao. Pored toga, broj i kompleksnost pitanja koje je trebalo regulisati u vrijeme bez današnje lakoće dostupnosti svim vrstama podataka, uključujući i lične, je bio manji i jednostavniji. Problem sukoba nadležnosti gotovo da nije postojao obzirom da su pravila o mjesnoj, pa i stvarnoj nadležnosti bila jednostavno primjenjiva.

36 Svi koji su bilo kada pročitali neki članak o zaštiti ličnih podataka odnosno o kompjuterskom, ili internet pravu, mogli su primijetiti sličnost između ovakvih uvodnih dijelova koji u svrhu naglašavanja važnosti teme, na različite načine, manje ili više detaljno, opisuju promjene koje je digitalizacija donijela u svakodnevni život, pa slijedom toga i u pravni promet, te u sferu počinjenja krivičnih djela. Stoga, ovdje nema potrebe ponavljati poznato. Međutim, treba naglasiti još jedno shvatanje koje je opšteprihvaćeno u literaturi, a to je da zakoni, odnosno zakonodavaci, ne mogu pratiti razvoj tehnologije. Pomirenost sa ovom činjenicom se može pročitati i od autoriteta koji dolaze iz zemalja sa gotovo savršeno funkcionalnom zakonodavnom i izvršnom vlasti i u kojima je, obzirom na uređenost drugih sfera života i ekonomski prosperitet, regulisanje sfere informacionih tehnologija, prioritet³. Ovo treba imati na umu kada se govori

² D.Samardžić/T.Fischer, *European Integration from a Single to a Digital Single Market*, *Zeitschrift für Europarechtliche Studien*, ZEUS 03/2017, Saarbrücken, Germany, 2018; Zlatan Meškić / Darko Samardžić, *The Strict Necessity Test on Data Protection by the CJEU: A Proportionality Test to Face the Challenges at the Beginning of a New Digital Era in the Midst of Security Concerns*, Croatian Yearbook of European Law & Policy, CYELP 2017, Zagreb, Croatia, 2017.

³ C. Kuner/ F.H. Cate/ C.Millard & Svantesson, *The (data privacy) law hasn't even checked in when technology takes off*, D. J. B. 2014.

o Bosni i Hercegovini sa njenim notornim problemima. Konkretan primjer je potreba usklađivanja Zakona o zaštiti podataka Bosne i Hercegovine sa Opštom uredbom o zaštiti podataka, što je kao i usklađivanje ostalog domaćeg zakonodavstva sa zakonodavstvom Evropske unije, obaveza koja proizilazi iz Sporazuma o stabilizaciji i pridruživanju sa Evropskom unijom. Jasno je da je postupak usklađivanja u većini sfera svakako zahtjevan proces čiji je vremenski okvir i konačan ishod u Bosni i Hercegovini vrlo neizvjestan. Ono što situaciju u vezi sa Uredbom čini specifičnom, jeste potreba njenog poštivanja u Bosni i Hercegovini već od samog stupanja na snagu, 25. maja 2018. godine.

Stoga je ovaj rad usmjeren prenstveno na datu, sadašnju, *de lege lata*, situaciju, i ono što privatni subjekti i javni organi mogu, odnosno moraju uraditi i prije zakonskih izmjena.

U radu se u najkraćem predstavljaju predmet i važnost s fokusom na teritorijalno važenje Uredbe te ukazuje na direktno i indirektno pozivanje na Konvenciju u tekstu Uredbe. Dalje se ukazuje na osnovne karakteristike prava na privatnost u kontekstu Konvencije, te noviju relevantnu praksu Evropskog suda za ljudska prava, a što se u radu koristi kao „alat“ prilikom evaluacije principa Uredbe. U svim dijelovima rada se, gdje god je to moguće, ukazuje na relevantnost i pravi paralela sa situacijom u Bosni i Hercegovini.

Zaključak, osim sumiranja istraživanja i nalaza rada, ukazuje i na pravce budućeg istraživanja u ovoj iznimno važnoj oblasti.

1. Opšta uredba o zaštiti podataka: predmet i važnost

Evropski parlament je 14. aprila 2016. godine usvojio Uredbu koja je stupila na snagu 20 dana nakon što je objavljena u Službenom listu EU 4. maja 2016. godine. Izvršenje i direktna primjena u svim državama članicama počela je dvije godine nakon ovog datuma: 25. maja 2018. godine. Uredba je zamijenila Direktivu o zaštiti podataka 95/46 /EZ⁴, sa kojom dijeli ciljeve i principe, a to su u najkraćem: zaštita temeljnih prava i sloboda pojedinaca u vezi s obradom podataka i usklađivanje ovih prava sa potrebom slobodnog protoka ličnih podataka između država članica. Međutim, preovladavajuće je mišljenje, a koje je svoj odraz dobilo i u ovoj Uredbi (član 9.), da Direktiva o zaštiti podataka 95/46 /EZ nije sprječila pravnu nesigurnost i rascjepkanost, te opšte shvatanje da su rizici internetskih aktivnosti u pogledu zaštite pojedinaca i njihovih podataka

⁴ Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca glede obrade osobnih podataka i o slobodnom kretanju takvih podataka, Službeni list L 281.

znatni. Razlike između zemalja članica u ovoj domeni su ostale posebno prepreka otvorenom tržištu kao jednoj od temeljnih vrijednosti Evropske unije.

Za osnovno razumijevanje ove Uredbe treba poći od definicije ličnih podataka prema kojoj su to svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi.⁵ Načini identifikacije su, kao i sama definicija, navedeni ekstenzivno, od standardnog imena i prezimena do mrežnog identifikatora. Isto tako, važno je znati da, iako se često razmatra na forumima, te u stručnim i naučnim publikacijama o internet pravu i kompjuterskoj sigurnosti, ovo nije akt dominantno usmjeren na tu oblast.

Niz je atributa koji se koriste u akademskim i stručnim člancima u vezi ove Uredbe. Uredba se naziva revolucionarnom ili "Uredbom koja će promijeniti svijet"⁶ te "kopernikanskom"⁷ itd. Ono što se sa čisto pravnog stanovišta mora primijetiti kao ključno jeste da se sa Direktive (Directive) prešlo na Uredbu (što je uobičajen prevod za Regulation). Podsjecamo da u pravu Evropske Unije to predstavlja značajnu razliku, jer Uredba (Regulation) postaje obavezujuća za sve zemlje članice sa danom stupanja na snagu, dok Direktiva obavezuje članice da domaćim propisima postignu određene ciljeve. Postoje mišljenja da je ova Uredba o zaštiti podataka, iako je formalno uredba (Regulation) suštinski direktiva, obzirom da u mnogim dijelovima ostavlja mogućnost zemljama članicama da uz relativno široku diskreciju prenesu načela Uredbe. Drugim riječima, određene odredbe Uredbe nisu dovoljno jasne, kako bi se očekivalo od akta koji ima snagu zakona i omogućavanje zemljama članicama da same regulišu određena pitanja. Međutim, zaista je riječ limitiranom broju pitanja koja su ostavljena državama članicama da regulišu u skladu sa svojim željama i potrebama. Radi se uglavnom o pitanjima i propisima koji se tiču medija, odbrane i nacionalne sigurnosti koja teško da su mogla i biti detaljnije regulisana u Uredbi, te su ovakve primjedbe, uglavnom neosnovane.

2. Pravo na privatnost: kratko podsjećanje na sadržaj i noviju praksu

Pravo na privatnost je definisano u članu 8. stav 1. Evropske konvencije o ljudskim pravima, jednostavnom formulacijom: "Svako ima pravo na

⁵ Član 4. stav 1. Uredbe

⁶ J.P. Albrecht, *How the GDPR will change the world*, Eur. Data Prot. L. Rev. 2, 287, 2016.

⁷ C. Kuner, *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law (February 6, 2012)*, Bloomberg BNA Privacy and Security Law Report (2012) February 6, 2012.

poštovanje svog privatnog i porodičnog života, doma i prepiske”. Upravo zbog jednostavnosti i uopštenosti ove norme konkretno razumijevanje pojma privatnosti u smislu Konvencije, može se, kao uostalom i kada se radi o bilo kojem drugom institutu Konvencije postići samo kroz poznavanje prakse Evropskog suda za ljudska prava (ESLJP). Sud je ustanovio i više puta podsjetio da je koncept “privatnog života” širok termin koji ne podliježe konačnoj definiciji, odnosno pokriva fizički i psihološki integritet osobe. Dalje, kao temeljna odredba koja je poslužila kao osnov za donošenje ove Uredbe, navodi se Povelja o osnovnim pravima Evropske Unije, odnosno član 8. stav 1., prema kojem svako ima pravo na zaštitu ličnih podataka. Dalje, iako se u preambuli Uredbe ne spominje izričito, može se reći da se Uredbom operacionalizuje stav 2. istog člana: “Lični podaci moraju se obrađivati poštano i koristiti u za to utvrđene svrhe i na osnovu pristanka osobe koje se tiču ili na nekoj drugoj zakonitoj osnovi. Svako ima pravo na pristup prikupljenim podacima o njemu i pravo na njihovo ispravljanje”. Interesantno je primijetiti da Uredba ne sadrži pozivanje na član 7. Povelje (Pravo na privatnost), koji je istovjetan gore citiranom članu 8. stav 1. Konvencije.

Praksa ESLJP po pitanju prava na privatnost je bogata i pokriva široku sferu, te zaista obuhvata brojne aspekte fizičkog i društvenog identiteta osobe, između ostalog: rodne identifikacije, seksualne orijentacije, informacije o zdravlju i sl...

Ova lista je duga i gotovo da svako pitanje zahtijeva posebnu pažnju. Međutim, za predmet ovog razmatranja važno je napomenuti i da je sud proširio pitanje privatnosti, i izvan onoga što bi se moglo nazvati intimnost, na sferu “javne privatnosti”, odnosno odlučio i da neki javni događaji i dešavanja mogu ući u sferu privatnog te stoga i biti zaštićeni. Tako je u predmetu *Peck protiv Velike Britanije* (28. januar 2003. godine)⁸ Sud uvažio aplikaciju podnosioca koji je tužio državne organe zbog toga što su objavili njegove snimke sačinjene neposredno nakon njegovog pokušaja samoubistva. Iako su nadzorne kamere bile na javnom mjestu, a snimci tih kamera službeno zavedeni kao neka vrsta javnog podatka, Sud je odlučio da je objavljivanje tih podataka neopravdano, te da pojedinci imaju pravo na uživanje određenog stepena privatnosti i u javnosti.

Do gotovo istog zaključka u sličnoj situaciji je došao i ESLJP u relativno novijem predmetu, koji je utoliko interesantniji obzirom da se radi o predmetu iz regionala, *Antović i Mirković protiv Crne Gore* a u kojem je presuda donesena 28. novembra 2017. godine.⁹ Predmet se odnosio na apelaciju dvojice fakultetskih profesora sa Univerziteta u Podgorici, koji su se žalili na narušavanje prava na privatnost obzirom da je video

39

⁸ *Peck v United Kingdom*. Reference (2003) 36 EHRR 41; [2003] EMLR 287.

⁹ *Antović and Mirković v Montenegro* br. 70838/13 [2017] ECHR 1068.

nadzor instaliran na fakultetu, odnosno u prostorijama u kojima su držali predavanja. Podnosioci žalbe su istakli i da nisu imali bilo kakvu kontrolu, odnosno saznanja o tome kako se koriste informacije koje su prikupljene video nadzorom te da je sam video nadzor nezakonit. Svi postupci koje su profesori pokrenuli pred domaćim sudovima bili su bezuspješni, uz obrazloženje da privatnost ne može biti ugrožena, obzirom da je video snimanje bilo vršeno isključivo u javnim prostorima, odnosno u salama gdje se vrše predavanja. Međutim, ESLJP je ustanovio da je došlo do narušavanja prava na privatnost, prvenstveno zbog toga što snimanje nije bilo regulisano zakonom, a ni drugim propisom. Osnovi argument tužene vlade bio je da predmet ne može biti razmatran sa aspekta narušavanja prava na privatnost obzirom da se radilo o nadzoru nad javnim i to radnim prostorom. U tom kontekstu, Sud je podsjetio da privatnost može uključivati i profesionalni život pojedinca, što je slučaj i u ovom predmetu, te je član 8. primjenjiv. Prilikom meritornog odlučivanja, Sud je ustanovio da je do narušavanje prava na privatnost došlo upravo zbog narušavanja principa da svaki ovakav postupak mora biti regulisan zakonom, što ovdje nije ispoštovano. Interesantno je u predmetu koji se odnosi na video nadzor odlučivao i Sud Bosne i Hercegovine, o čemu će više riječi biti niže u tekstu.

40

3. Direktna i indirektna veza između Konvencije i Uredbe

Član 4. Uredbe uspostavlja generalan princip da bi «Obrada osobnih podataka trebala bi biti osmišljena tako da bude u službi čovječanstva». Nastavak istog člana kojim se nastoji pobliže objasniti značenje ovog principa, praktično parafrazira različite članove Konvencije i to: član 8. stav 1. (Pravo na privatnost), član 9. (Sloboda misli, savjesti i vjeroispovjeti), član 6. (Pravo na pravično suđenje) i član 13. (Pravo na djelotvoran pravni lijek).

Inače, u Uredbi se Konvencija samo jednom direktno spominje. Međutim, radi se vrlo važnoj odredbi koja se odnosi na mogućnost ograničenja prava koja se daju Uredbom. Ova mogućnost ograničenja se daje državama članicama ili samoj Evropskoj Uniji, i uključuje praktično sve oblasti koje se regulišu Uredbom, između ostalog: pristup i ispravak ili brisanje ličnih podataka te ograničenja prava na prenosivost podataka, prava na prigovor, odluka koje se temelje na izradi profila, kao i ograničenja obavještavanja ispitanika o povredi ličnih podataka te ograničenja određenih povezanih obveza voditelja obrade.

Kao razloge za ova ograničavanja navode se praktično isti razlozi kao i članu 8. stav 2. Konvencije, s tim što se ovi razlozi navode kroz primjere.

Tako se kao primjer ugrožavanja, odnosno interesa javne bezbjednosti, navode: prirodne katastrofe, sprečavanje kriminala i nereda, istraga i progon kaznenih djela ili izvršavanje kaznenopravnih sankcija; ekonomski dobrobit zemlje odnosno posebno važan gospodarski ili finansijski interes Unije ili države članice. Pored toga se uopšteno, gotovo identično kao u Konvenciji, navode razlozi javnog zdravlja i zaštite prava i sloboda drugih. Posebno interesantan primjer, koji je očigledno uvršten zbog konkretnih predmeta od kojih su neki završili i pred Sudom u Strazburu, jeste predviđanje izuzetka u slučajevima obrada arhiviranih ličnih podataka za potrebe pružanja posebnih informacija u vezi s političkim ponašanjem za vrijeme bivših totalitarnih državnih režima.

Princip proporcionalnosti.¹⁰ kojim se zahtjeva da se sva ova ograničenja koriste u mjeri u kojoj je to nužno i proporcionalno u demokratskom društvu, je dobro poznat iz Konvencije.

Na kraju, donosioci Uredbe su i pored ovog očiglednog ključnog uticaja Konvencije na definisanje ove odredbe željni otkloniti svaku dilemu te kao neku vrsta “osiguranja” naveli da bi sva ograničenja trebala biti u skladu sa zahtjevima utvrđenima u Povelji i Evropskoj konvenciji za zaštitu ljudskih prava i temeljnih sloboda.¹¹

Što tiče Bosne i Hercegovine, Zakon o zaštiti ličnih podataka „Službeni glasnik BiH“, br. 49/06, ne sadrži pozivanje na Konvenciju, ali već u članu 1. stav 1. definiše sam cilj zakona, a to je da se “.....na teritoriji Bosne i Hercegovine svim licima, bez obzira na njihovo državljanstvo ili prebivalište, osigura zaštita ljudskih prava i osnovnih sloboda, a naročito pravo na privatnost i zaštitu podataka u pogledu obrade ličnih podataka koji se na njih odnose”. Na ovaj način se zaštita podataka stavlja isključivo u kontekst prava na privatnost, odnosno ne pravi se posebna distinkcija, već se samo u svrhu zakona naglašava važnost u pogledu obrade ličnih podataka.

41

3.1. Principi Uredbe u svjetlu Konvencije i prakse

Principi Uredbe su predstavljeni u 6 tačaka, člana 5. stav 1. Uredbe. Polazi se od generalnog principa da podaci moraju biti procesuirani na

¹⁰ D.Samardžić, *The Principle of Proportionality as Justification Test on the Grounds of Art. 52 I CFR*, Revija za Evropsko Pravo 01/2017, Kragujevac, Serbia, 2017; Zlatan Meškić / Darko Samardžić, *From unrelated to cooperative triple protection of human rights in the EU*, Promotion of Scientific Research and Education in European Integration and Policy-Conference Proceedings, Skopje, Macedonia, 2014.

¹¹ Član 80. Uredbe

zakonit, pošten i transparentan način.¹² Službeno objašnjenje ove svakako uopštene odredbe nudi dodatno pojašnjenje samo u odnosu na zahtjev transparentnosti, te se ukazuje na to da se transparentnost prije svega ogleda u informisanju fizičkog ili pravnog lica čiji se podaci obrađuju, o samom postupku te o svrsi obrade.

Odgovor na pitanje šta predstavlja „pošten“ i „zakonit“ postupak obrade se ne nudi, te se može zaključiti da je primjena tumačenja ovih termina koje u smislu Konvencije, nudi Evropski sud za ljudska prava (ESLJP), adekvatna i dostatna, a što važi i za drugi princip koji je u uskoj vezi sa prethodnim: «Lični podaci se mogu prikupljati u određene, obrazložene i legitimne svrhe i ne mogu biti dalje procesuirani na način koji nije u skladu sa ovim principima».¹³

Treći princip se može nazvati principom minimalizacije.¹⁴ Lični podaci moraju biti procesuirani na način koji je adekvatan svrsi, a obim podataka može biti samo nephodan za svrhu zbog koje se procesuiraju, te se podaci mogu procesuirati samo u slučajevima u kojima se svrha ne može postići na drugi način. Ovaj zahtjev jasno upućuje na zahtjeve proporcionalnosti i neophodnosti iz člana 8. stav 2. Konvencije.

42 Princip tačnosti¹⁵ zahtijeva da podaci moraju biti tačni i kada je to moguće i primjenjivo, ažurirani, te se mora obezbijediti mogućnost da svi netačni podaci budu izbrisani ili ispravljeni. Vremensko ograničenje je princip prema kojem podaci moraju biti čuvani, odnosno pohranjeni na način da identifikacija osobe kojoj podaci pripadaju ne može biti omogućena duže nego što svrha zbog koje su podaci prikupljeni neophodno zahtjeva. I ovo pitanje, odnosno pitanje dužine čuvanja i korištenja ličnih podataka je bilo predmet razmatranja ESLJP u više navrata, u slučajevima, između ostalog, vezanim za čuvanje DNK¹⁶ ili otiska prstiju.¹⁷ Bez obzira na ishode različitih odluka, kriteriji koje je ESLJP primjenio zaista se mogu sažeti u formulaciju ovdje citirane odredbe Uredbe.¹⁸

Princip bezbjednosti je definisan kao zahtjev da: «Procesuiranje i pohranjivanje podataka mora omogućiti sigurnost podataka, odnosno sigurnost od nezakonitog pristupa, mijenjanja oštećenja ili gubitka, i u tu

¹² Ibid., Član 5, stav 1, tačka a).

¹³ Ibid., Član 5, stav 1, tačka b).

¹⁴ Ibid., član 5, stav 1, tačka c).

¹⁵ Ibid., član 5, stav 1, tačka d).

¹⁶ *S and Marper v United Kingdom* br. 30562/04 i 30566/04 [2008] ECHR 1581.

¹⁷ *M.K. v. France* br.19522/09, 18 April 2013 ECHR 120 (2013).

¹⁸ Član 5. Stav 1. tačka e.), Uredbe

svrhu treba obezbjediti sve tehničke uslove».¹⁹ Ova odredba na prvi pogled pokriva isključivo tehnički aspekt i ne asocira na pitanje koje bi se moglo razmatrati pred ESLJP. Zaista je tačno da je suština člana 8. Konvencije u ograničavanju miješanja države u privatni život pojedinca. Međutim, praksa ESLJP, naročito novija ukazuje i na pozitivnu obligaciju države,²⁰ u smislu poduzimanja aktivnosti i mjera da ne dođe do ugrožavanja privatnosti i u sferi odnosa, ne samo između države i pojedinaca, već i fizičkih i pravnih lica međusobno. Ovo se naročito odnosi na odnos između korisnika i pružaoca internet usluga.²¹

Za poštivanje ovih principa odgovoran je kontrolor podataka²².

4. Teritorijalno važenje: EU i treće zemlje

Jedna od ključnih novina koje ova Uredba donosi jeste uspostavljanje onoga što se naziva “one-stop-shop” sistem, koji bi pomogao izbjegavanju konflikta zakona ili izbjegavanju posljedica kada do takvog sukoba dođe. “Kupovina na jednom mjestu” ili “jedna tačka za obavljanje svih poslova”, kako bi mogli pokušati da prevedemo, termin “one-stop-shop” koji se udomaćio i u našem jeziku, u ovom slučaju ne znači da postoji jedna EU institucija ili tijelo koje će riješiti probleme bilo koje kompanije. Uredba u stvari predviđa koncept kojem je suština da se kroz koordinaciju i konzistentnost kontrolnih tijela u zemljama članicama, omogući kompanijama iz jedne zemlje članice koja posluje u drugoj, da sve svoje poslove i provjere obavi u zemlji u kojoj ima sjedište. Naime, nadzorno tijelo koje ima jurisdikciju nad kompanijom može odlučiti da samo riješi predmet ili u koordinaciji sa tijelom druge zemlje članice, sa kojom kompanija želi da posluje. U svakom slučaju, pitanje nadležnosti, sukoba zakona i usklađenosti sa Uredbom ili zakonodavstvom druge države članice, jeste posao i zadatak kontrolnog odnosno nadzornog tijela matične države kompanije koja želi da posluje u drugim zemljama EU i to kontrolno tijelo je u stvari ta jedinstvena kontakt tačka.

43

Međutim, to nas dovodi do nove poteškoće za zemlje koje nisu članice Evropske unije, odnosno za subjekte koji nemaju sjedište u EU, obzirom da se ovaj koncept ne odnosi na njih, već će i dalje morati da posluju u skladu sa različitim jurisdikcijama na području EU. Konkretno, kompanija iz Bosne i Hercegovine se ne može za pomoć obratiti Agenciji za zaštitu

¹⁹ Ibid., član 5, stav 1, tačka f). Uredbe

²⁰ Roche v. the United Kingdom (application no. 32555/96). ECHR 19 Oct 2005

²¹ K.U. v. Finland br. 2872/02, § 43, 2 December 2008, 48 Eur. H.R. Rep. 52 (2009).

²² Član 5, stav 2. Uredbe

ličnih podataka Bosne i Hercegovine, u vezi sa poslom koji želi da obavi u Njemačkoj ili Holandiji, već mora posebno se obraćati odgovarajućim institucijama zemalja članica.

Već nepunu godinu od početka primjene se može konstatovati da Uredba nema samo značaj kroz zakonodavne izmjene, odnosno da, kao što je gore navedeno, zakonodavci ne mogu, a nužno i ne moraju donositi nove zakone, ili izmjene i dopune postojećih dovoljno brzo da bi kompanije koje djeluju na njihovim teritorijama uskladile svoj rad i interne propise sa Uredbom. Usklađivanje sa Uredbom se globalno vrši na dva načina: vertikalni, kada multinacionalne kompanije, usklađuju svoje aktivnosti u EU sa Uredbom a kroz ovlaštenja i instrukcije koje dolaze iz sjedišta koje je izvan EU. Drugi način je horizontalan, prema kojem se kompanija prilagođava drugoj kompaniji. Ovaj način prilagođavanja nezakonskim putem, se u literaturi spominje kao poseban, teško prevodiv fenomen “GDPR – creep”, dakle “šunjanje” ili “prikradanje” Uredbi²³. Mi bismo ovo mogli nazvati tihom prilagodbom, odnosno tihim prilagođavanjem. Naravno, vertikalno i horizontalno prilagođavanje propisima EU postoji i kada se radi o državama odnosno državnim institucijama, i to i unutar i između država, s tim što se ovaj proces uglavnom odvija putem usvajanja zakona i drugih propisa te državnih strategija i politika²⁴.

Međutim, ono što se smatra možda i najvećom promjenom ili dostignućem ali i najvećom kontraverzom Uredbe je njeno teritorijalno važenje koje je definisano članom 3. Uredbe i reflektuje jasnu intenciju da ovaj akt ima pravnu snagu i izvan teritorije EU. Tako već stav 1. glasi: “Ova se Uredba odnosi na obradu osbnih podataka u okviru aktivnosti poslovnog nastana voditelja obrade ili izvršitelja obrade u Uniji, neovisno o tome obavlja li se obrada u Uniji ili ne”. Ova generalna formulacija koju nije neophodno posebno komentarisati se razrađuje u narednom stavu kome treba posvetiti posebnu pažnju. Prema ovom stavu, Uredba se, prije svega, primjenjuje na obradu ličnih podataka ispitanika u Uniji koju obavlja voditelj obrade ili izvršitelj obrade bez sjedišta u Uniji, “ako su aktivnosti obrade povezane s nuđenjem robe ili usluga takvim ispitanicima u Uniji, neovisno o tome treba li ispitanik izvršiti plaćanje”²⁵.

Ovakve formulacije ove odredbe i pored svoje uopštenosti djeluje prilično jasno i striktno u odnosu na kompanije koje dolaze iz trećih zemalja. Međutim, zvanično obrazloženje uz ovu odredbu nam ukazuje na znatno umjerenije tumačenje.

²³ G. Greenleaf, Global Convergence of Data Privacy Standards and Laws Speaking Notes for the European Commission Events on the Launch of the General Data Protection Regulation (GDPR) in Brussels & New Delhi, 25 May 2018.

²⁴ Kohler-Koch, B., & Rittberger, B. (2006). The ‘governance turn’ in EU studies. *JCMS: Journal of Common Market Studies*, 44, 27-49;

²⁵ Član 3. stav 2. tačka a) Uredbe.

Naime, da bi se ustanovilo da, u smislu ove odredbe, kompanija iz treće zemlje, nudi robe ili usluge subjektima u EU nije dovoljno da postoji web stranica, e-mail ili drugi kontakt podaci koji su jednostavno dostupni u EU. Potreban je niz drugih faktora, kao što je korištenje jezika koji se ne koristi u zemlji u kojoj je sjedište kompanije, nego jezika koji se koristi u jednoj ili više zemalja EU. Dalje, jedan od faktora koji ukazuje da li su subjekti u EU osnovna "meta" kompanije, može biti i spominjanje drugih kupaca ili partnera u EU.

Naročito je interesantan drugi kriterij za primjenjivost Uredbe, a to je situacija u kojoj se aktivnosti obrade sprovode praćenjem ponašanja ispitanika dokle god se njihovo ponašanje odvija unutar Unije²⁶. Očigledno je da ova odredba cilja na operatere društvenih mreža, administratore sistema i e-mail adresa koji imaju mogućnost da sistematski prate ponašanje ispitanika u EU. Prvo pitanje koje se nameće jeste koje su to aktivnosti koje se mogu definisati kao praćenje ponašanja. To bi morale biti aktivnosti koje pomoći kojih se određuju ili predviđaju lične preference, ponašanja ili stavovi. U suštini praćenje ponašanja se može dovesti u nazuš vezu sa "profiliranjem", koje je u članu 4 definisano kao „izrada profila” znači svaki oblik automatizirane obrade osobnih podataka koji se sastoji od upotrebe osobnih podataka za ocjenu određenih osobnih aspekata povezanih s pojedincem, posebno za analizu ili predviđanje u vezi s radnim učinkom, ekonomskim stanjem, zdravljem, ličnim sklonostima, interesima, pouzdanošću, ponašanjem, lokacijom ili kretanjem tog pojedinca.

Na kraju: "Uredba se primjenjuje na obradu osobnih podataka koju obavlja voditelj obrade koji nema poslovni nastan u Uniji, već na mjestu gdje se pravo države članice primjenjuje na temelju međunarodnog javnog prava"²⁷. Ova odredba ima vrlo ograničen domet i odnosi se, uglavnom, na diplomatska i konzularna predstavništva.

Dakle ovaj pregled odredbi o teritorijalnom važenju, ukazuje na složenost ovog pitanja, a zbog broja različitog faktora koje treba uzeti u obzir. Ključan je balans između teritorijalnog principa, neophodne fleksibilnosti koje zahtijeva digitalno doba, a s druge strane potrebe da zakon bude provodiv, te da se izbjegne biranje nadležnosti ("forum shopping"), tako uobičajen u međunarodnom poslovnom pravu. Autori se uglavnom slažu da je generalni princip, ukoliko ne ciljate EU, ni EU neće ciljati vas²⁸.

Sve do sada navedeno se uglavnom odnosi privredno poslovanje, odnosno na odnose između privrednih subjekata bez obzira da li su u

²⁶ Član 3. stav 2. tačka b) Uredbe

²⁷ Član 3. stav 3. Uredbe

²⁸ P. de Hert/ M. Czerniawski, *Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context*, International Data Privacy Law, 6(3), 230-243, 2016.

privatnom ili državnom vlasništvu. Odnos između javnih organa zemalja članica, odnosno između uprave i pravosuđa, sa trećim zemljama je regulisan članom 48. Uredbe, kojim se suštinski dozvoljava prijenos ili otkrivanje ličnih podataka ukoliko se te radnje zasnivaju na međunarodnom sporazumu, kao što je ugovor o međunarodnoj pravnoj pomoći. Službeno obrazloženje ovog člana²⁹ ne nudi dodatna objašnjenja za ovaj važan aspekt, obzirom da sadržajem predstavlja praktično opširnije prepričavanje same odredbe. Međutim, prilična autonomija koja se daje državama članicama i organima EU u odnosima sa trećim zemljama kroz ovaj član održava intenciju Uredbe da se urede i ograniče raspolaganja ličnim podacima od strane korporacija i privatnih lica, a ojača uloga državnih organa. Ovakav ton Uredbe, a konkretno ovaj član je direktno motivisan posebnim odnosima između EU i SAD, i problemima koji su uslijedili nakon poznatog slučaja *Edward Snowden* (Edvard Snouden)³⁰. Međutim, ono što je važno u ovoj situaciji za Bosnu i Hercegovinu, jeste da je ovo još jedna oblast u kojoj državni organi, bez zakonskih izmjena, mogu primjenu Uredbe učiniti znatno «bezbolnjom», aktivnijim obavljanjem svojih funkcija, u ovom slučaju sklapanjem novih i revidiranjem postojećih relevantnih sporazuma.

4.1. Poštivanje Konvencije kao ključni element uslov za treće zemlje

46

Iz perspektive trećih zemalja, te tako i Bosne i Hercegovine, treba istaći važnost Konvencije prilikom utvrđivanja primjerenoosti stepena zaštite koje određena zemљa ispunjava da bi se lični podaci iz Evropske Unije mogli prenositi. Naime, direktnom primjenom Konvencije, indirektno se primjenjuje i Povelja koja se u relevantnom dijelugotovo u potpunosti referira na Konvenciju.

Dakle, član 45. stav 1. Uredbe, predviđa da se prijenos ličnih podataka trećoj zemlji ili međunarodnoj organizaciji može realizovati pod uslovom da Komisija odluči da treća zemlja osigurava primjerenu zaštitu. Ova primjerenoost se ocjenjuje kroz uopštena tri elementa.

Prvi element počinje sa najuopštenijim zahtjevom vladavine prava i temeljnih ljudskih sloboda. Pored ove direktne asocijacije na Konvenciju, i na određeniji se način upućuje na Konvenciju, tačnije na član 13. Konvencije, sa zahtjevom za “postojanje djelotvornih i provedivih prava ispitanika te učinkovite upravne i sudske zaštite ispitanika čiji se osobni

²⁹ Recital 115.

³⁰ Rossi, A. (2018). How the Snowden Revelations Saved the EU General Data Protection Regulation. *The International Spectator*, 53(4), 95-111.

podaci prenose”³¹. Dalje se razrađuje opšte i sektorsko zakonodavstvo, mjere sigurnosti uključujući i pravila o dalnjem prenosu podataka trećoj zemlji, itd. Drugi, ipak nešto konkretniji uslov, jeste pitanje postojanja nezavisnog nadzornog tijela koje, između ostalog, treba da ima odgovornost osiguravati poštivanje pravila o prijenosu i raspolaganju ličnim podacima. Jasno je da bi u Bosni i Hercegovini ovo tijelo trebala biti Agencija za zaštitu ličnih podataka, koja i jeste definisana kao zasebna upravna organizacija i čije su nadležnosti očigledno definisane u skladu sa Konvencijom o zaštiti fizičkih lica u pogledu automatske obrade ličnih podataka (Vijeće Evrope, 1981)³², odnosno dodatnim protokolom uz Konvenciju koji se odnosi na nadzorni organ i prekogranični protok podataka³³, te Direktivom 95/46/EZ (Opća uredba o zaštiti podataka). Na kraju, treći element, a koji je opet u direktnoj vezi sa poštivanjem Konvencije, se odnosi na međunarodne obveze koje je dotična treća zemlja ili međunarodna organizacija preuzela, ili druge obveze koje proizlaze iz pravno obvezujućih konvencija ili instrumenata. Dakle, čak dva od tri elementa koja su odlučujuća za nastavak prijenosa ličnih podataka iz Evropske unije prema trećim zemljama direktno ili indirektno se vežu za poštivanje Konvencije.

5. Kratki osvrt na domaću praksu

Sud Bosne i Hercegovine je ovlašten da postupa u upravnim sporovima protiv akata Agencije za zaštitu ličnih podataka. Ova praksa je prilično bogata, i to ne toliko po broju predmeta već po raznovrsnosti pitanja koja su raspravlјana. Naime, odlučivano je, između ostalog, i u predmetima koji se odnose na: prikupljanje uvjerenja o nekažnjavanju u proceduri po Javnom pozivu za imenovanje vještaka na području Federacije BiH, traženje na uvid lične karte prilikom ovjere zdravstvene legitimacije, vraćanje prijavne dokumentacije neizabranim kandidatima nakon konkursne procedure i utvrđivanje mjera sigurnosti ličnih podataka, itd.. U nekoliko predmeta koji će niže biti predstavljeni, Sud BiH sa direktno pozvao na Konvenciju. Međutim, pored relativno rijetkog pozivanja na Konvenciju, može se reći i nedovoljnog, ne može se tvrditi da principi Konvencije nisu našli svoje mjesto u značajnom broju odluka Suda Bosne i Hercegovine, i to, indirektno, kroz institute Zakona o slobodi pristupa informacijama, “Službeni glasnik BiH”, br. 28/00, 48/06 i 102/09. Naime, pitanje preklapanja nadležnosti, pa i

47

³¹ Član 45. stav 2. tačka a) Uredbe

³² Vijeće Evrope, Konvencija o zaštiti lica u pogledu automatske obrade ličnih podataka, Evropski sporazumi ETS No. 108, Strasbourg, 28. 1. 1981.

sukoba između Zakona o slobodi pristupa informacijama i Zakona o zaštiti ličnih podataka se neumitno nameće u velikom broju sporova, a poznato je da je institut "javnog interesa", dominantan u upravnom ili sudskom odlučivanju koji postupcima koji se vode na osnovu ovog zakona, kao što je to slučaj i sa predmetima u "konvencijskim predmetima". Odnos Zakona o pristupu informacijama i Zakona o zaštiti ličnih podataka je široka tema i nije predmet ovog rada. Međutim, u širem kontekstu odnosa ljudskih prava, odnosno Konvencije, na šta nas upućuju i uvodne odredbe Zakona o pristupu informacijama i Uredbe ne može se izbjegći i kratki osvrt na pravo na slobodu izražavanja koje uključuje i slobodu primanja i saopštavanja informacija i ideja bez miješanja javne vlasti i bez obzira na granice (član 10. Konvencije). Ovo naročito obzirom na interesantne promjene u stavovima ESLJP u relativno skorijem periodu. Naime, ESLJP u članu 10. Konvencije dugo nije prepoznavao pozitivnu obligaciju države da omogući pristup informacijama. Ovakav stav je zauzet u predmetu *Leander v Sweden* (1987) 9 EHRR 43 i često citiran u drugim presudama: "...da pravo na slobodu primanja informacija u osnovi zabranjuje Vladi da ograničava osobu da primi informacije koje joj drugi žele ili su spremni dati. Članak 10. ne dodjeljuje pojedincu, u okolnostima poput onih u ovom predmetu, pravo pristupa registru koji sadrže informacije o njegovu osobnom položaju, niti utjelovljuje obvezu Vlade da mu takvu informaciju daju." Međutim, u nizu relativno novijih presuda ESLJP je stao na stanovište da član 10. ne jamči samo pravo na saopštavanje informacija, već i pravo javnosti da ih primi, te se moraju pružiti osobito jaki razlozi za svaku mjeru koja ograničava pristup informacijama koje javnost ima pravo primiti. ESLJP je pokazao senzibilitet za situacije u kojima su tražiocи informacija mediji, odnosno nevladine organizacije, smatrajući da je uloga društvenog, odnosno javnog čuvara zaista od javnog interesa.

Sud Bosne i Hercegovine je odlučivao i o aktuelnom pitanju video nadzora na radnom mjestu, u kojem se javlja i kompleksno pitanje privatnosti na radnom mjestu³⁴.

Naime, Federalnom ministarstvu finansija je Agencija za zaštitu ličnih podataka naložila da doneše odluku o obradi ličnih podataka do kojih se došlo putem video nadzora koji je postavljen unutar prostorija Ministarstva i da kamere podesi tako da ne pokrivaju ulaze u kancelarije. U tužbi kojom je protiv ove odluke Agencije Ministarstvo pokrenulo upravni spor, navedeno je da je ovakva odluka donesena radi zaštite opreme, sigurnosti zaposlenih i važnih podataka koji se odnose na finansijsko poslovanje. Tužba je odbijena i Sud BiH se prilikom donošenja ove odluke, osim pozivanja na Zakon o zaštiti ličnih podataka, istina uopšteno, pozvao i na Konvenciju

³⁴ Sud Bosne i Hercegovine, Presuda broj: S1 3 U 14576 14 U od 06. 10. 2015. godine.

odnosno na član 8. Konvencije. Međutim, interesantno je da je Sud BiH, u ovom predmetu koji je sličnog činjeničnog opisa kao i goreopisani predmet protiv Crne Gore, donio istu odluku kao ESLJP i to dvije godine ranije.

Upravni spor koji je „LRC Inženjering“ d.o.o. Sarajevo pokrenuo pred Sudom BiH³⁵ protiv rješenja Agencije za zaštitu ličnih podataka u BiH, je interesantan i zbog značajnog javnog interesa. Naime, pomenuta kompanija bavi se vođenjem baze podataka fizičkih i pravnih lica o kreditnim i nekreditnim zaduženjima i koja je podatke obrađivala bez saglasnosti nosilaca ličnih podataka. Upravo je jedan od argumenata koje je pokretač spora istakao bio i značajan javni interes da se ovi podaci obrađuju i da banke i druga pa i fizička lica imaju ove podatke kako bi se izbjegle zloupotrebe.

Sud je dao prilično uopštenu ocjenu da je pravo građana i pravnih subjekata za zaštitom njihovih ličnih podataka zagarantirano odredbama Konvencije i Ustavom BiH, te da ova prava: „predstavljaju osnovna ljudska prava i slobode koje su upravo uspostavljena u cilju osiguranja ostvarivanja općeg, dakle, javnog interesa, bitno su ugrožena bilo kojim djelovanjem suprotno odredbama Zakona o tajnosti ličnih podataka“. Osim uopštenosti, mora se primjetiti i da je Sud BiH pojednostavio odnos između prava na privatnost i zaštite ličnih podataka, izjednačujući ih.

U narednom predmetu Sud BiH je već bio konkretniji i pozvao se i na praksi ESLJP. Naime, radi se o upravnom sporu³⁶, pokrenutom protiv odluke Agencije za zaštitu ličnih podataka u BIH, a kojom je odbijen kao neosnovan prigovor tužiteljice podnosen protiv njenog poslodavca da je neovlašteno tražio i dobio lične podatke od JZU Zavoda za medicinu rada i sporta RS Banja Luka i JZU Dom zdravlja Banja Luka u vezi sa bolovanjem tužiteljice.

49

Sud je odbio tužbu, između ostalog pozivajući se i na praksi ESLJP u vezi otkrivanja medicinskih podataka i to, konkretno, na gore pomenuti predmet *Z. Protiv Finske*. U navedenom predmetu radilo se o uzimanju medicinskih podataka i njihovom priključenju dokumentima iz krivične istrage, bez prethodne saglasnosti pacijenta u postupku koji je vođen protiv njega, i u kojem je ESLJP zaključio da nije bilo povrede člana 8. Konvencije (pravo na privatnost) u vezi sa nalogom medicinskom osoblju za davanje medicinskih dokaza, niti u vezi sa oduzimanjem medicinskih podataka i njihovim priključivanjem spisima iz istrage tokom krivičnog postupka.

³⁵ Sud Bosne i Hercegovine, Presuda broj: S 13 U 0001889 10 U od 06. 10. 2010. godine.

³⁶ Sud Bosne i Hercegovine, Presuda broj: S 13 U 010156 12 U od 26. 02. 2014. godine.

ZAKLJUČAK

Dakle, pravo na zaštitu ličnih podataka nije zaštićeno izričito Konvencijom te je, isto tako, jasno da ne postoji znak jednakosti između prava na privatnost i zaštite ličnih podataka. Naime, nije svako uživanje, kao ni povreda prava na privatnost, u vezi sa zaštitom ličnih podataka, kao što ni zaštita ličnih podataka ne uključuje uvijek pitanje prava na privatnost kao ljudskog prava. Za razliku od Konvencije, Povelja eksplisitno garantuje pravo zaštite ličnih podataka. Dalje, zaštita ličnih podataka, se i normativno i praktično, najčešće razmatra sa praktičnog, pa može se reći i tehničkog aspekta. Međutim, potrebno je istaći da je trenutni režim zaštite ličnih podataka rezultat razvoja različitih društvenih sfera: politike, ekonomije i prava, a iznad svega razvoja ljudskih prava, i to ne samo prava na privatnost, već i slobode mišljenja i izražavanja. Stoga se osnovni principi zaštite privatnih podataka u svakom društvu, bilo u EU ili izvan nje najbolje štite dosljednom primjenom Konvencije, te je i strateški i praktični odnos između EU i trećih zemalja značajno uvjetovan principima Konvencije. Iz toga slijedi da se, u određenoj mjeri, horizontalno i vertikalno usklađivanje sa Uredbom postiže i primjenom Konvencije, a čime se indirektno, u ključnim dijelovima primjenjuje i Povelja. Razumljivo, sve ovdje navedeno se odnosi i na Bosu i Hercegovinu, a jasno je i da je zakonodavna aktivnost u pravcu usklađivanja sa Uredbom neophodna. Međutim, i prije i poslije zakonskih izmjena, veliki je prostor i brojna su pitanja koja zahtijevaju prilagođavanje u radu i javnih i privatnih subjekata koji na bilo koji značajniji način sarađuju, odnosno posluju sa Evropskom unijom. Prvenstveno će čuvanje i zaštita podataka morati biti unaprijeđena i u tehničkom i u normativnom smislu i to će zahtijevati zajednički rad, kako IT stručnjaka, tako i pravnika. Akademска zajednica, u svakom slučaju, može i mora dati svoj doprinos u ovom izuzetno kompleksnom poslu i u tom smislu treba usmjeriti budući rad i istraživanja koja će često zahtijevati multidisciplinarni pristup.

GENERAL DATA PROTECTION REGULATION: RELATION OF THE RIGHT TO PRIVACY AND PROTECTION OF PERSONAL DATA REGARDING TO BOSNIA AND HERZEGOVINA

ABSTRACT

First of all, this paper tries to explain the principles of the General Data Protection Regulation (EU) 2016/67 of April 27 2016, which entered into the force on May 25 2018. Special attention was given to the territorial scope, and the influence on third countries, considering that the changes introduced by the Regulation are among the most important and at the same time the most controversial. Of course, this aspect of the Regulation is particularly important for Bosnia and Herzegovina, having in mind the obligations arising from the Stabilization and Association Agreement and the general economic, political and security orientation towards the European Union. Furthermore, in this paper, relation between protection of personal data and the right to privacy is considered, in accordance with the provisions of the Regulation and the Convention on Human Rights as well as Charter of Fundamental Rights of the European Union and in a very concise form relevant practice of the European Court of Human Rights in Strasbourg. Finally, this article suggests that, even though the Regulation is considered to be one of the most important and complex parts of the European Union legislation, which touches different spheres of life and society, and therefore the rights, respect for fundamental human rights and consistent application of the Convention in significant part results in respect for fundamental principle and essence of the Regulation.

51

Keywords: *Protection of personal data, Right to privacy, European Union law, General Data Protection Regulation, Territorial scope, Horizontal and vertical harmonization, Application in Bosnia and Herzegovina, European Convention on Human Rights, Charter of Fundamental Rights of the European Union*