

eudaimonia

Revija za pravnu, političku i
socijalnu teoriju i filozofiju

Vol. 8 No. 1 • 2024.

Izdavač

IVR **S**RBIJA

Srpsko udruženje za pravnu
i socijalnu filozofiju

EVROPSKA REGULACIJA ZAŠTITE PODATAKA NA INTERNETU

Marija Vojisavljević

Strane: 105–122

Marija Vojisavljević*

EVROPSKA REGULACIJA ZAŠTITE PODATAKA NA INTERNETU

Pravo na privatnost je posebno ugroženo pojavom novih informacionih tehnologija. U vremenu koje karakteriše obrada ogromne količine najrazličitijih podataka, tzv. eri velikih podataka, lični podaci se tretiraju kao najznačajniji resurs. Internet je omogućio pristupanje podacima koji se mogu zloupotrebiti. Prepoznajući opasnosti koje internet sobom nosi, članice Evropske unije su preduzele brojne značajne aktivnosti sa ciljem da se zaštite prava korisnika interneta i da im obezbede sigurnost na mrežama. U ovom radu su predstavljene odredbe i principi zaštite podataka o ličnosti i privatnosti na internetu sadržane u Evropskoj konvenciji za zaštitu ljudskih prava i osnovnih sloboda, Direktivi 95/46, Povelji Evropske unije o osnovnim pravima, Direktivi 2002/58, Direktivi 2016/680 i Uredbi 2016/679. Konvencije, uredbe i direktive se razmatraju da bi se utvrdilo u kojoj je meri Evropska unija uspjela u svojoj namjeri na pronadže adekvatnu pravnu regulativu zaštite podataka na internetu.

Ključne reči: internet, onlajn pretnje, podatak o ličnosti, pravni akti Evropske unije, privatnost

1. UVOD

Internet je revolucionarni pronalazak čije žile prodiru u gotovo sve sfere čovekovog postojanja i rada (Šarkić *et al.* 2007, 120). U svetu koji se menja neverovatnim tempom, tehnološke inovacije dešavaju nam se pred očima. Kako tehnologija napreduje, često se zapitamo kako smo uopšte živeli bez telefona, tableta, interneta. Kako smo ispunjavali dane, noći, vikende (Kol 2021, 15)?

* Autorka je studentkinja osnovnih akademskih studija na Pravnom fakultetu Univerziteta u Beogradu, marijavojisavljevic2003@gmail.com.

Život u 21. veku nezamisliv je bez tehnologije i interneta. Svojom pojavom internet je doneo brojne pogodnosti koje su olakšale odvijanje svakodnevnog života. Čovek ga koristi da uči, da se zabavlja, trguje, kupuje, traži ili nudi zaposlenje, pa čak i da obavlja svoje redovne poslove (Šarkić *et al.* 2007, 120). Sve informacije su nam na dohvat ruke, možemo komunicirati sa bilo kim na svetu, a virtuelni svet je postao sastavni deo našeg stvarnog života. Nema više gledanja sporog učitavanja podataka, lutanja po bibliotekama kako bismo pronašli neku informaciju, slanja pisama... Sada većinu problema rešavamo kod kuće, uz pomoć nekoliko klikova.

Istovremeno, ljudi uglavnom nisu svesni svih negativnih strana interneta i često sami sebe nepromišljeno čine lakom metom raznih zloupotreba. Danas pojedinac, šta god da uradi, bilo da se tiče njegovog poslovnog, porodičnog ili ljubavnog života, ne može a da to ne podeli sa svima putem društvenih mreža i sav sadržaj podeljen putem interneta postaje lako dostupan svima. Privatnost na internetu jedva da postoji i u najvećem broju slučajeva mi smo ti koji je narušavamo svojim neodgovornim ponašanjem (Milovanović 2019). Korisnici društvenih mreža najčešće ne razmatraju opasnost zloupotrebe ostavljenih podataka i olako smatraju da nisu ugroženi.

Na taj način mreže postaju jedinstvene socijalne platforme sa velikom bazom razmene ličnih podataka. Nesmotrenost na mrežama uzrokovala je mnoge incidente širokog spektra, što je uticalo da internet korisnici počnu da izražavaju zabrinutost zbog značajnog objavljivanja i korišćenja njihovih ličnih podataka (Acquisti, Gross 2006). Lični podaci se često distribuiraju bez znanja korisnika, dok fotografije mogu da se iskoriste ne samo za zlonamerna prikazivanja već i za prepoznavanje lica, što je posebno interesantno državnim organima (Baltezarević 2015, 243). Zbog korišćenja moderne tehnologije živimo u potpuno povezanom svetu, u kome skoro svaki potez ostavlja digitalni trag. Lako je navići se na nove funkcionalnosti, ali takođe moramo da razmotrimo i opasnosti koje idu podruku sa tehnološkim napretkom, a još važnije je da pronađemo način kako da se od njih zaštitimo (Kol 2021, 7).

Cilj ovog rada je da istražimo traganje Evrope za adekvatnom pravnom regulativom zaštite podataka na internetu. Osim toga, u radu će biti obrađene i teme koje se tiču toga na koje sve načine ostavljamo podatke na internetu, kao i pitanje njihove zloupotrebe.

2. PRIVATNOST NA INTERNETU – ONLAJN PRETNJE

Privatnost se načelno može definisati kao pravo nekog lica da određeni krug podataka i informacija koje se na njega odnose sakrije od oka javnosti. Još je Aristotel u delu *Politika* istakao razliku između javne i privatne sfere. Prva se odnosi na organizaciju države i života u njoj, pa je samim tim od opšteg značaja, a potonja se vezuje za lični i porodični život, pa se tiče pojedinca ili grupe pojedinaca, a ne društva u celini. Kako su se, u narednim vekovima, sve više razvijale političke, društvene i ekonomske prilike, razvijao se i koncept privatnosti. Važno je istaći da opštu evoluciju koncepta privatnosti karakterišu i uspostavljanje i izgradnja tzv. prava na privatnost. Prepoznavanje i priznavanje prava na privatnost nastalo je iz potrebe da se obezbede što efikasniji mehanizmi zaštite privatnosti jer su, sa društvenim i tehnološkim napretkom, mogućnosti njene povrede postale sve dostupnije.

Jedan od lako dostupnih instrumenata pomoću kojeg se može povrediti pravo na privatnost jeste i internet (Popović, Jovanović 2017, 123). Internet je omogućio praćenje komunikacija, analizu fotografija, pristupanje ličnim podacima korisnika i njihovo dalje distribuiranje, bez saglasnosti i znanja osobe čiji su podaci. Otkrivanjem ličnih podataka korisnici sami doprinose stvaranju digitalnih zapisa o njima. Tako ostavljene informacije i podaci sa korisničkog profila mogu biti zloupotrebjeni na različite načine. Podaci mogu da se iskoriste za pričinjavanje štete korisnicima i eventualnu ucenu, krađu identiteta, sajber nasilje i slične oblike zloupotrebe (Baltezarović 2017, 244). U vremenu koje karakteriše obrada ogromne količine najrazličitijih podataka, tzv. eri velikih podataka, lični podaci se tretiraju kao resurs. Svoje „besplatne” usluge kompanije naplaćuju korisnicima tako što za uzvrat traže sve više ličnih podataka. Podaci o korisnicima, njihovim aktivnostima i ponašanju na internetu koriste se za analizu i kreiranje ličnih socijalno-psiholoških profila, ciljano plasiranje komercijalnih proizvoda prilagođenih individualnim karakteristikama i potrebama korisnika, za prodaju kompanijama ili servisima. (Kuzmanović 2019, <https://digitalni-vodic.ucpd.rs/zastita-licnih-podataka-i-privatnosti-na-internetu/?lng=lat>). Dakle, koliko god da je okolnost da su od svega udaljeni „samo jedan klik” ljudima učinila život lakšim i udobnijim, toliko ih je i izložila riziku da njihovi lični podaci i privatne informacije lako završe kod onih kojima nisu namenjeni. Da bi se stekla slika

o dostupnosti podataka i ugroženosti privatnosti na internetu, dovoljno je setiti se samo nekoliko poznatih, relativno novijih slučajeva. U julu 2017. godine u Švedskoj je izbio skandal kada se saznalo da je dve godine ranije švedska transportna agencija na jedan klaud server postavila, a zatim greškom elektronskom poštom neovlašćenim licima poslala baze podataka sa imenima, fotografijama i kućnim adresama miliona švedskih državljana, uključujući i pripadnike tajnih jedinica policije i vojske, učesnika programa zaštite svedoka...¹ U maju 2014. godine čuvena plaforma za kupovinu putem interneta *eBay* objavila je da je bila žrtva hakerskog napada usmerenog na preuzimanje imena, adresa, datuma rođenja i kriptozaštićenih lozinki oko 145 miliona korisnika ove platforme.

Svemu tome treba dodati i rizike kojima se korisnici interneta ponekad sami izlažu nedovoljno pažljivim skladištenjem podataka na udaljenim serverima ili postavljanjem ličnih, odnosno privatnih informacija na raznim društvenim mrežama (Popović, Jovanović 2017, 123–124). Privatnost korisnika, na primer, na Fejsbuku, narušena je samom objavom bilo kojih informacija na toj društvenoj mreži. Te informacije automatski pripadaju toj kompaniji i ostaju sačuvane u njihovim serverima, čak i u slučaju gašenja naloga. Da bi se kreirao nalog na toj, kao i na ostalim društvenim mrežama, korisnik mora da navede svoje ime, e-adresu, datum rođenja i pol i one spadaju u javno dostupne informacije. Osim navedenih, u javno dostupne informacije spadaju i profilna slika, mreža, korisničko ime i korisnički ID i te informacije su dostupne svima na internetu. Te informacije mogu biti zloupotrebene i korisnik može biti izložen riziku od krađe identiteta. Krađa identiteta najčešće je zločin za finansijsku dobit.

Takođe, kada korisnik objavi fotografiju ili video-zapis, to omogućava i dobijanje dodatnih podataka poput vremena, datuma i mesta fotografisanja ili pravljenja video-zapisa. Podaci se prikupljaju i sa računara, mobilnog telefona ili nekog drugog uređaja posredstvom koga se pristupa internetu. U te podatke mogu da spadaju lokacija, vrsta pretraživača ili stranice koje korisnici posećuju. Zanimljivo je i to da se na većini sajtova društvenih mreža od korisnika zahteva da prihvate polisnu o uslovima korišćenja, pre nego što mu dopuste da koriste njihove usluge. Kontroverzno je to što polisa o uslovima korišćenja koju korisnik mora da prihvati često sadrži klauzule koje

¹ Više o tome: Khandelwal Swati, Sweden Accidentally Leaks Personal Details of Nearly All Citizens 2017. <https://thehackernews.com/2017/07/sweden-data-breach.html>.

dozvoljavaju operatorima društvenih mreža da skladište podatke o korisnicima, ili da ih čak dele trećim licima, najčešće marketinškim kompanijama. U većini slučajeva, polise su koncipirane tako da su za korisnika nerazumljive i preobimne, pa ih najčešće prihvata i ne čitajući ih (Popović 2016, 37–41).

Svi ti rizici, koji ne iscrpljuju sve opasnosti po lične podatke i privatnost sa kojima se korisnici interneta susreću prilikom gotovo svakog korišćenja svetske mreže, dovoljno upečatljivo ukazuju na potrebu uspostavljanja i razvoja instrumenata i mehanizama pravne zaštite podataka o ličnosti i privatnosti na internetu, što će biti tema u nastavku rada (Popović, Jovanović 2017, 124).

3. EVROPSKA REGULACIJA ZAŠTITE PODATAKA NA INTERNETU

Trenutno važeći pravni okvir zaštite podataka o ličnosti² u pravu Evropske unije (EU) rezultat je višedecenijske evolucije.

Prvi implus za izgradnju tog pravnog okvira došao je spolja. Organizacija za ekonomsku saradnju i razvoj je 1980. godine usvojila *Preporuke o smernicama za zaštitu privatnosti i prekogranični protok ličnih podataka*. Smernice nisu imale pravno obavezujući karakter, tako da nisu u značajnijoj meri doprinele harmonizaciji pravnog okvira za zaštitu ličnih podataka u državama članicama Organizacije. Nešto značajniji korak učinjen je godinu dana kasnije – 1981. godine, kada je pod okriljem Saveta Evrope sačinjena Konvencija o zaštiti lica u odnosu na automatsku obradu podataka. Predlagač Konvencije je imao nameru da zemlje potpisnice usklade svoja nacionalna zakonodavstva sa osnovnim načelima i preporukama sadržanim u ovom dokumentu. Poštujući vladavinu prava, ljudska prava i osnovne slobode, cilj Konvencije je bio da poveže svoje članice, da proširi zaštitu osnovnih prava i sloboda pojedinca, naročito njegovog prava na privatnost prilikom automatske obrade njegovih ličnih podataka (Bosnić 1998, 27). Konvenciji, koja je stupila na snagu 1985. godine, brzo su pristupile i neke države članice (tadašnje) Evropske ekonomske zajednice (EEZ), pa se

² Podatak o ličnosti je svaki podatak o čoveku. To može biti, na primer, podatak o imenu lica, adresi, sedištu, broju telefona, podatak o obrazovanju, podatak o zaradi, podatak o imovini, podatak o nacionalnoj pripadnosti, podatak o bolesti od koje se leči.

očekivalo da će u kratkom roku sve države članice iskazati saglasnost na obavezanost Konvencijom. Kako se to za prvih pet godina važenja konvencije nije desilo, Evropska komisija je pristupila izradi direktive kojom bi se osnovna pitanja zaštite podataka na jednoobrazan način uredila u EEZ. Poduhvat Evropske komisije je okončan 1995. godine usvajanjem Direktive 95/46. Nešto više od jedne decenije kasnije, Savet EU je doneo Okvirnu odluku 2008/977/JHA o zaštiti podataka o ličnosti obrađenih u okviru policijske i pravosudne saradnje u krivičnim stvarima, kojom se nastojala postići minimalna harmonizacija propisa u oblasti zaštite podataka koji su se ticali tadašnjeg tzv. trećeg stuba EU.³ Evolucija pravnog okvira za zaštitu podataka nastavljena je i nakon stupanja na snagu Lisabonskog sporazuma nedavnim usvajanjem Uredbe 2016/679, koja će zameniti Direktivu 95/46, i Direktive 2016/680, koja će zameniti Okvirnu odluku 2008/977/JHA (Popović, Jovanović 2017, 130–131).

U nastavku rada predstavice ćemo odredbe i principe zaštite podataka o ličnosti i privatnosti na internetu sadržane u Evropskoj konvenciji za zaštitu ljudskih prava i osnovnih sloboda, Direktivi 95/46, Povelji EU o osnovnim pravima, Direktivi 2002/58, Direktivi 2016/680 i Uredbi 2016/679.

3.1. Evropska konvencija za zaštitu ljudskih prava i osnovnih sloboda

Evropska konvencija za zaštitu ljudskih prava i osnovnih sloboda (EKLJP) jeste međunarodni ugovor donet pod okriljem Saveta Evrope 4. novembra 1950. godine i kasnije sukcesivno menjan i dopunjavan protokolima, koji čine sastavni deo Konvencije. EKLJP je doneta po ugledu na Univerzalnu deklaraciju o pravima čoveka iz 1948. godine, koju je usvojila Generalna skupština Ujedinjenih nacija. EKLJP je stupila na snagu 1953. godine i obavezuje sve članice Saveta Evrope. Nadzor i kontrola nad sprovođenjem EKLJP i njenih protokola u nadležnosti su Evropskog suda za ljudska prava.⁴ Nacrt konvencije Saveta

³ Evropsku uniju čine tzv. tri stuba. Prvi stub čine tri međunarodne organizacije (Evropska zajednica za uglj i čelik, Evropska ekonomska zajednica i Evropska zajednica za atomsku energiju). Drugi stub predstavlja zajednička spoljna i bezbednosna politika EU, dok treći stub čine policijska i pravosudna saradnja u krivičnim stvarima.

⁴ Evropski sud za ljudska prava je međunarodni sud sa sedištem u Strazburu. Broj sudija je jednak broju zemalja članica Saveta Evrope koje su ratifikovale Konvenciju o zaštiti ljudskih prava i osnovnih sloboda. Sudije Evropskog suda za ljudska prava

Evrope težio je tome da se postigne da obrada ličnih podataka zadovolji određeni minimalni standard ispravnosti i zakonitosti obrade, da građani dobiju mogućnost da se obaveste o obrađivanim podacima i da mogu da traže njihovu ispravku i neke druge intervencije. Formulirana su načela zaštite podataka, među kojima su i sledeća: da se lični podaci smeju obrađivati samo u svrhe za koje su prikupljeni, da se smeju obrađivati samo dok za tim postoji potreba, da podaci moraju da budu ažurirani, da svako ima pravo da bude obavешten o podacima koji se obrađuju (Šarkić *et al.* 2007, 153).

Pravni osnov za jemstvo zaštite podataka i privatnosti na internetu sadržan je u članu 8 EKLJP. Ta odredba nosi naziv „Pravo na poštovanje privatnog i porodičnog života” i ona garantuje da svako ima pravo na poštovanje svog privatnog i porodičnog života, doma i prepiske (st. 1) i da se javne vlasti neće mešati u vršenje tog prava, sem ako to nije u skladu sa zakonom i neophodno u demokratskom društvu u interesu nacionalne bezbednosti, javne bezbednosti ili ekonomske dobrobiti zemlje, radi sprečavanja nereda ili kriminala, zaštite zdravlja ili koralala ili radi zaštite prava i sloboda drugih (st. 2).

Možemo primetiti da se u samoj odredba člana 8 EKLJP ne pominje eksplicitno zaštita privatnosti na internetu. Norma je formulirana na opšti način, pa je upravo takva opšta formulacija omogućila EKLJP da, u skladu sa tehnološkim napretkom evropskog društva, pod domašaj te odredbe podvede i povrede prava na privatnost koje se dešavaju na internetu.

3.2. Direktiva 95/46

Direktiva⁵ o zaštiti lica u odnosu na obradu ličnih podataka i slobodnom prometu tih podataka (Direktiva 95/46) usvojena je 1995.

deluju samostalno i ne predstavljaju nijednu zemlju, mada svaka država ima po jednog člana koji je izabran od Parlamentarne skupštine Saveta Evrope. U radu sa predstavkama sud sarađuje sa Sekretarijatom, koji uglavnom čine pravnici iz zemalja članica. Oni su takođe potpuno nezavisni od naloga svojih država i ne smeju da predstavljaju podnosiocima predstavki. Sud primenjuje EKLJP. Njegov zadatak je da obezbedi da države članice poštuju pravila koja su navedena u konvenciji. On to sprovodi tako što razmatra predstavke podnete od pojedinaca ili ponekad država. Presude su obavezujuće: država na koju se presuda odnosi je u obavezi da deluje u skladu sa njom i o tome se stara Komitet ministara koji, ako je potrebno, vrši politički pritisak na državu da izvrši odluku suda. Osim presuda, sud iznosi i savetodavna mišljenja.

⁵ Direktiva, kao sekundarni izvor prava EU, po pravilu ne stvara neposredno prava i obaveze za fizička i pravna lica, već su njihovi adresati države članice. Dakle,

godine. Njoj je prethodila Konvencija o zaštiti lica u odnosu na automatsku obradu podataka iz 1985. godine. Predlagač konvencije je imao nameru da zemlje potpisnice usklade svoja nacionalna zakonodavstva sa osnovnim načelima i preporukama sadržanim u tom dokumentu. Budući da je do početka 1990. godine svega šest od 12 država članica (tadašnje) EEZ iskazalo saglasnost na obaveznost konvencijom, Evropska komisija je pristupila izradi Direktive 95/46 sa namerom da ujednači nivo zaštite prava na privatnost u EEZ (Poglavlje 3).

Direktiva 95/46 izražava težnju da se ostvare dva osnovna cilja: 1) zaštita osnovnih ljudskih prava i sloboda, i to naročito zaštita prava na privatnost u kontekstu obrade ličnih podataka, i 2) slobodan promet podataka o ličnosti između država članica EU (čl. 1).

Direktiva 95/46 se primenjuje na svaku obradu ličnih podataka, a ne samo na automatizovanu (čl. 3).

Ključne kategorije lica čija su prava i obaveze uređene Direktivom 95/46 jesu lica čiji se podaci obrađuju⁶ i nadzornici.⁷ Osnovna prava lica čiji se podaci obrađuju su pravo na obaveštenost, pravo na pristup prikupljenim podacima i pravo na protest.

U vezi sa pravom na obaveštenost lica čiji se podaci obrađuju izdvajamo članove 10 i 11 Direktive 95/46. U Direktivi 95/46 razlikuju se dve situacije: kada se podaci prikupljeni neposredno od lica čiji se podaci obrađuju (član 10) i kada su ti podaci prikupljeni posrednim putem (čl. 11). Direktivom 95/46 se proširuju obaveze obrađivača podataka, obavezujući ga da subjektu od koga bi da prikupi podatke već prilikom prikupljanja informacija pruži bitne informacije o

direktiva obavezuje države članice da donesu propise kojima će ostvariti ciljeve sadržane u datoj direktivi. Postupak donošenja direktive naziva se njenom transpozicijom. Kako je rok za transpoziciju Direktive 95/46 istekao krajem oktobra 1998. godine, sve države članice EU su usvojile odgovarajuće propise kojima ostvaruju ciljeve utvrđene u toj direktivi.

⁶ Prema Directive 95/46/EC on the protection of persons in connection with the processing of personal data OJ L 281 of 23/11/1995, Art 2 (a), *lice čiji se podaci obrađuju* jeste svako lice čiji je identitet određen ili se može odrediti. Smatraće se da se identitet lica može odrediti kad kod je to na osnovu nekog podatka neposredno ili posredno moguće, a naročito kada se navode matični ili neki drugi identifikacioni broj nekog lica, odnosno jedan ili više elemenata karakterističnih za fizički, fiziološki, mentalni, ekonomski, društveni ili kulturni identitet tog lica.

⁷ Prema Directive 95/46/EC on the protection of persons in connection with the processing of personal data OJ L 281 of 23/11/1995, Art 2 (d), *nadzornik* je fizičko ili pravno lice, organ javne vlasti, agencija ili drugo telo koje samostalno ili zajedno sa drugima utvrđuje svrhu i način obrade podataka o ličnosti.

cilju, obaveznosti ili dobrovoljnosti davanja podataka, o posledicama koje će ga pogoditi za slučaj da ne dâ podatke, kao i da ga obavesti o važnim pitanjima za njega i u slučaju da je podatke o njemu prikupio od trećeg lica.

Osim prava na obaveštenost, lica čiji se podaci obrađuju imaju i pravo na pristup tim podacima, što možemo primetiti u članu 12 Direktive 95/46. Države članice jemče svakom licu koje je predmet podataka pravo da, bez ograničenja u razumnim intervalima i bez prekomernog odgađanja ili troškova, od nadzornika dobije pre svega potvrdu o tome da li se podaci koji se na njega odnose obrađuju i obaveštenje barem o nameni obrade, kategoriji podataka o kojima je reč, o primaocima ili kategorijama primalaca kojima se ti podaci obelodanjuju, zatim da se to lice u razumljivom obliku obavesti o podacima koji se obrađuju, da mu se dostave sve raspoložive informacije o njihovom izvoru i da razume logiku na kojoj počiva svaka automatska obrada podataka koji se na njega odnose.⁸

Osim toga, pravo na pristup podacima podrazumeva i pravo lica čiji se podaci obrađuju da zatraži ispravke, brisanje ili blokiranje podataka čija obrada nije obavljena u skladu sa odredbama Direktive 95/46, posebno zbog nepotpune ili netačne prirode podatka, kao i da treće strane kojima su podaci bili obelodanjeni budu obavestene o svakoj ispravci, brisanju ili blokiranju, sem ukoliko se pokaže da to nije moguće ili podrazumeva nesrazmeran napor.⁹

U vezi sa pravom lica čiji se podaci obrađuju da se suprotstavi obradi izdvajamo član 14 Direktive 95/46. Lice čiji se podaci obrađuju može da se, iz posebnih ličnih razloga, suprotstavi onoj obradi podataka o njemu koja je inače dopuštena i nadzornik tada podatke mora da obriše, osim ako obradom izvršava zakonsku obavezu. Da bi prava lica čiji se podaci obrađuju na odgovarajući način bila zaštićena, u Direktivi 95/46 je utvrđen čitav niz principa koji moraju biti primenjeni u postupcima prikupljanja i obrade podataka o ličnosti, koji su sadržani u članu šest Direktive 95/46 (Popović, Jovanović 2017, 134). Osnovni princip u vezi sa prikupljanjem podataka jeste da se podaci o ličnosti smeju prikupljati u tačno određene, jasne i legitimne svrhe.

⁸ Vid. Directive 95/46/EC on the protection of persons in connection with the processing of personal data OJ L 281 of 23/11/1995, Art 12 (a).

⁹ Vid. Directive 95/46/EC on the protection of persons in connection with the processing of personal data OJ L 281 of 23/11/1995, Art 12 (b) i (c).

Direktiva 95/46 je značajna i zbog toga što uvodi presumpciju krivice obrađivača podataka u pogledu štete koja je prouzrokovana obradom (čl. 24), obavezuje države članice da uvedu nezavisan kontrolni organ koji se stara o primeni prava zaštite podataka o ličnosti (čl. 28–30), potpuno uređuje prekogranični prenos, to jest prenos podataka u zemlje koje nisu članice EU (čl. 25 i 26), čime se sada bavi i Dodatni protokol uz Konvenciju Saveta Evrope 108 (čl. 2).

3.3. Povelja EU o osnovnim pravima

Povelju EU o osnovnim pravima su 7. decembra 2000. godine svečano proglasili čelnici Evropskog parlamenta, Saveta EU i Evropske komisije. Povelja EU o osnovnim pravima je definitivno i u celini stekla pravnu obaveznost stupanjem na snagu Lisabonskog sporazuma 1. decembra 2009. godine (Popović, Jovanović 2017, 129).

Poveljom EU o osnovnim pravima garantuje se da svako ima pravo na zaštitu ličnih podataka u svim aspektima života: kod kuće, na poslu, prilikom kupovine, na lečenju, u policijskoj stanici ili na internetu (Baltezarević 2017, 246). Za pitanje zaštite ličnih podataka i privatnosti na internetu značajna je i odredba člana 8. Povelje EU o osnovnim pravima. Ta odredba nosi naziv „Zaštita podataka o ličnosti” i prema njoj svako ima pravo na zaštitu podataka o svojoj ličnosti (st. 1). Takođe, takvi podaci moraju biti obrađeni pošteno za unapred određenu svrhu i na osnovu informisanog pristanka osobe ili na nekom drugom legitimnom osnovu uređenom zakonom i svako ima pravo da pristupi prikupljenim podacima o svojoj ličnosti i pravo da zatraži njihovu ispravku (st. 2), a postupanje po tim pravilima je pod kontrolom nezavisnog organa (st. 3)

Tom odredbom se na opšti način uređuje pitanje zaštite ličnih podataka nezavisno od oblika u kome su sadržani i medijuma na kome su pohranjeni.

Osim u Povelji EU o osnovnim pravima, opšte odredbe o zaštiti podataka i privatnosti nalaze se i u Ugovoru o funkcionisanju Evropske unije (UFEU). Odredbom člana 16 Ugovora takođe je zajemčeno opšte pravo na zaštitu ličnih podataka. Prema toj odredbi, Evropski parlament i Veće utvrđuju pravila o zaštiti pojedinaca s obzirom na obradu ličnih podataka u institucijama, telima, uređima i agencijama EU, kao i u državama članicama kada obavljaju svoje aktivnosti u

području primene prava EU, a poštovanje tih pravila podleže nadzoru nezavisnih tela (st. 2).

Dakle, osnovna razlika između člana 16 UFEU i člana 8 Povelje EU o osnovnim pravima je ta što UFEU obavezuje Evropski parlament i Veće da, u skladu sa redovnim zakonodavnim postupkom, usvoje pravila kojima će se uređivati postupanje sa podacima o ličnosti i njihova obrada, a koja će obavezivati institucije, tela, službe i agencije EU, ali i države članice kada sprovode delatnosti i radnje u stvarima koje su uređene pravom EU.

3.4. Direktiva 2002/58

S obzirom na to da su nove napredne digitalne tehnologije zavladaile mrežama javne komunikacije u društvu, pojavile su se posebne potrebe zaštite ličnih podataka i privatnosti korisnika. EU je 2002. godine usvojila novu regulativu – Direktivu o privatnosti i elektronskim komunikacijama (Direktiva 2002/58), (Milić 2019, <https://www.milic.rs/internet-pravo/direktiva-o-privatnosti-i-elektronskim-komunikacijama-epd-i-uredba-o-e-privatnosti-epr/>).

Pre Direktive 2002/58, neka pitanja zaštite podataka o ličnosti u sektoru telekomunikacija bila su uređena Direktivom o obradi podataka o ličnosti i zaštiti privatnosti u sektoru telekomunikacija. Međutim, ubrzan razvoj tehnologije je već u prvim godinama 21. veka učinio jasnim da tu direktivu treba osavremeniti, a privatnosti u sektoru elektronskih komunikacija pružiti sveobuhvatniji sistem zaštite, pa je tako stupanjem na snagu Direktive 2002/58 Direktiva o obradi podataka o ličnosti i zaštiti privatnosti u sektoru telekomunikacija prestala da važi.

Cilj Direktive 2002/58 je, kako stoji u njenom članu 1, da dopuni Direktivu 95/46 i doprinese uspostavljanju jednakog nivoa zaštite osnovnih prava i sloboda, a pre svega prava na privatnost u obradi podataka o ličnosti u sektoru elektronskih komunikacija, i da obezbedi slobodu kretanja tih podataka i opreme za elektronsku komunikaciju u okviru EU. Direktiva 2002/58 je 2009. godine pretrpela značajne izmene i dopune (Popović, Jovanović 2017, 140).

Direktivom 2002/58 uređena su brojna važna pitanja zaštite podataka o ličnosti u kontekstu elektronskih komunikacija, kao što su bezbednost i poverljivost komunikacija, tretman podataka o saobraća-

ju poruka, spam (masovno slanje neželjenih poruka bez ikakvog kriterijuma) i tzv. kolačići.¹⁰

Sušтина obaveze pružanja bezbednosti je u tome da se obezbedi da podacima koji su predmet zaštite Direktive 2002/58 mogu da pristupe samo ovlašćena lica i da se spreči slučajno uništenje tih podataka. Pretnje po bezbednost podataka i komunikacije su tzv. špijunski programi, mrežne greške, skriveni identifikatori i druga slična sredstva koja mogu ući u korisnikov računar bez njegovog znanja, sa ciljem dobijanja pristupa informacijama, ubacivanja skrivenih informacija ili ulaženja u trag aktivnostima korisnika, čime mogu ozbiljno narušiti njegovu privatnost. Takva sredstva treba da budu dozvoljena isključivo u legitimne svrhe ili uz izričitu saglasnost korisnika. Jedno od tih sredstava su i tzv. kolačići (eng. *cookies*). Rani nacrti Direktive 2002/58 su predviđali potpunu zabranu korišćenja „kolačića” bez saglasnosti korisnika. Međutim, kako bi takav pristup imao negativne posledice na tehnološkom planu, postalo je jasno da se uređenju tretmana „kolačića” mora pristupiti na drugačiji način. U svojoj verziji iz 2002. godine Direktivom 2002/58 je bio predviđen tzv. *opt-out* pristup: države članice EU su bile dužne da obezbede da upotreba mreža za elektronsku komunikaciju u svrhu skladištenja informacija ili pristupa informacijama skladištenim u opremi pretplatnika ili korisnika bude dozvoljena samo pod uslovom da je pretplatnik ili korisnik na jasan i razumljiv način obavešten o svrsi obrade „kolačića” i da mu je bilo omogućeno da odbije tu ponudu. Prilikom izmena i dopuna Direktive 2009. godine ta odredba je promenjena i Direktiva sada prihvata tzv. *opt-in* pristup: obrada „kolačića” je dozvoljena ako je pretplatnik ili korisnik, pošto je na jasan i razumljiv način obavešten o svrsi obrade, dao svoju saglasnost za tu obradu.

U pogledu poverljivosti komunikacija,¹¹ Direktiva 2002/58 nalaže državama članicama da pravno onemoguće slušanje, prisluški-

¹⁰ „Kolačići” su obično kratki kodirani zapisi koje generiše posećeni veb-sajt i koji ostaju zapamćeni u veb-pretraživaču korisničkog računara. Oni imaju nekoliko važnih uloga. Prva je da olakšaju upravljanje sesijom pretraživanja i korišćenja interneta. Primera radi, pomoću „kolačića” veb-sajtovi kao što je *YouTube* generišu predloge video-zapisa sličnih onim koje je korisnik ranije pregledao. Sa ovim je povezana i uloga „kolačića” u personalizaciji korišćenja interneta. Karakterističan primer je aktiviranje zapamćenih lozinki za pristup određenim sajtovima ili elektronskim bazama podataka pomoću „kolačića”. Konačno, „kolačići” služe i za praćenje kretanja korisnika po svetskoj mreži, iz čega se mogu izvesti zaključci o njegovim interesovanjima, ukusu, navikama...

¹¹ Vid. Directive 2002/58/EC on privacy and electronic communications, OJ L 201 of 31/7/2002, Art 5.

vanje, skladištenje informacija o komunikacijama i bilo koji drugi vid presretanja ili nadzora elektronskih komunikacija bez saglasnosti korisnika na koje se ti podaci odnose. Zabrana nadzora i presretanja elektronskih komunikacija neće se primenjivati onda kada je to zakonom dozvoljeno, i to na način predviđen članom 15(1).

Tretman podataka o saobraćaju uređen je članom 6 Direktive 2002/58. Osnovna obaveza u tom pogledu jeste brisanje ili anonimizovanje podataka o saobraćaju koji se tiču pretplatnika ili korisnika čim dalje zadržavanje tih podataka postane nepotrebno za prenos komunikacije. Obaveza brisanja ili anonimizovanja podataka može biti izmenjena, odnosno ukinuta, pod uslovima predviđenim članom 15 (1) Direktive.

3.5. Direktiva 2016/680

Direktiva 2016/680 o zaštiti fizičkih lica u odnosu na obradu podataka od nadležnih organa u svrhe sprečavanja, istrage, otkrivanja ili vođenja postupaka za krivična dela, odnosno izvršenja krivičnih sankcija, i o slobodnom prometu takvih podataka usvojena je istovremeno sa Uredbom 2016/679. Počela je da se primenjuje 5. maja 2016. godine.

U Direktivi 2016/680 je izraženo nastojanje da se „preslikaju” osnovni principi utemeljeni Direktivom 95/46 i Uredbom 2016/679. Zato ne iznenađuje to što su opšta arhitektura Direktive 2016/680, a naročito prava lica čiji se podaci obrađuju i dužnosti nadzornika, u velikoj meri podudarni onima koji su predviđeni Direktivom 95/46, odnosno Uredbom 2016/679.¹²

Direktivom 2016/680 se štite pojedinci kada vlasti obrađuju njihove lične podatke u svrhu prevencije, istrage, otkrivanja ili gonjenja krivičnih dela ili za izvršavanje krivičnih kazni. Prema toj direktivi, svačiji lični podaci moraju da se obrađuju zakonito, pošteno i samo za određenu svrhu, koja je uvek povezana sa borbom protiv kriminala. Direktivom 2016/680 se osigurava da obrada ličnih podataka širom EU bude u skladu sa principima zakonitosti, proporcionalnosti i neophodnosti, uz odgovarajuće mere zaštite pojedinca. Takođe, njome se nacionalnim organima za zaštitu podataka obezbeđuje potpuno nezavisan nadzor.

¹² Baš kao i Uredba 2016/679, i Direktiva 95/46 u krivičnim stvarima predviđa postojanje oficira za zaštitu podataka, uvođenje nadzornog tela.

Iako je Direktiva 2016/680 izraz nastojanja da se prava država članica EU harmonizuju u širokom krugu pitanja zaštite podataka o ličnosti prikupljenih ili obrađenih u okviru policijske i pravosudne saradnje, u određenim aspektima se državama članicama ostavlja sloboda da pojedina pitanja urede na način koji je najprikladniji za pravnu tradiciju svake države pojedinačno (npr. čl. 56 i 57).

3.6. Uredba 2016/679

U EU je u maju 2018. godine na snagu stupila Opšta uredba o zaštiti podataka (Uredba 2016/679), kao finale dugogodišnjeg procesa. Usaglašavanje konačne verzije teksta trajalo je četiri godine (2012–2016), na sam tekst je podneto rekordnih 4000 amandmana, dok su u javnoj raspravi učestvovali gotovo svi relevantni akteri iz javnog, privatnog i civilnog sektora.

Iako se Uredba 2016/679 predstavlja kao svojevrsna revolucija koja iz korena menja pravila zaštite podataka, nova regulativa je ipak prirodni naslednik Direktive 95/46 i suštinski se nadovezuje na iste principe i norme. Regulatori su iskoristili priliku da dodatno urede brojna sporna pitanja nastala tokom razvoja interneta i novih tehnologija (Krivokapić *et al.* 2019, 13). Tako se, na primer, Uredbom 2016/679 uvode pojmovi povrede podataka o ličnosti, pseudonimizacije, biometrijskih podataka i, između ostalog, definiše pojam glavnog mesta poslovnog nastanjenja, što je veoma važno za primenu pravila o kontroli i ograničenjima slobode prikupljanja i obrade podataka.

Uredbom 2016/679 se uvodi i jedna nova kategorija subjekata. To je oficir za zaštitu podataka – lice zaduženo da obaveštava i savetuje nadzornika ili obrađivača, odnosno zaposlene na obradi podataka, o obavezama koje proizilaze iz Uredbe 2016/679 ili nacionalnih propisa država članica o zaštiti podataka i da saraduje sa nadzornim telima. U članu 37 Uredbe 2016/679 navodi se da je imenovanje oficira za zaštitu podataka obavezno kada podatke o ličnosti obrađuje javno telo (izuzev sudova, ali samo u sklopu obavljanja pravosudne funkcije), kada se suština aktivnosti nadzornika ili obrađivača sastoji od radnji obrade podataka koje zahtevaju stalan i sistematski nadzor velikog broja lica čiji se podaci obrađuju i kada se u velikom broju obrađuju posebno osetljive kategorije podataka i podaci koji se odnose na krivičnu osuđivanost (Popović, Jovanović 2017, 137).

Uredbom 2016/679, u odnosu na Direktivu 95/46, znatno se proširuju prava lica čiji se podaci obrađuju. Uredba 2016/679 sadrži pravo da se ograniči obrada podataka (čl. 18), pravo na prenosivost podataka (čl. 20) ili pravo protesta čak i u slučaju obrade podataka u naučne, istorijske ili statističke svrhe (čl. 21 st. 6 i čl. 83 st. 1). Iako se Uredba 2016/679 direktno primenjuje u svih 28 članica, EU i dalje ostavlja prostor državama članicama da mnoge detalje samostalno regulišu u skladu sa svojim nacionalnim propisima. Takođe, Uredba 2016/679 štiti prava građana EU, što znači da se njene odredbe odnose na svaku organizaciju u svetu koja obrađuje podatke stanovnika zemalja članica EU, bilo da im nudi robu i usluge ili prati njihovo ponašanje na internetu (Krivokapić *et al.* 2019, 15).

4. ZAKLJUČAK

Globalizacija, kao metod širenja i rasprostiranja svega što društvo prihvata i usvaja kao adekvatno za dalji rast i sve ono što ima potencijal da pomogne i unapredi trenutno stanje u kojem se nalazimo, najzaslužnija je i za neverovatan razvoj i primenu tehnologije na svim poljima koje čovek može da zamisli (Milovanović 2019). Nova informaciona tehnologija našla je široku primenu u mnogim oblastima života i rada. Izvorno nastale da bi se komunikacija među ljudima na internetu učinila jednostavnijom i bržom, te tehnologije su postale i predmet raznih zloupotreba, te ih vešti pojedinci danas koriste suprotno njihovoj osnovnoj nameni, da bi za sebe ili drugoga izvukli nekakvu korist (Šarkić *et al.* 2007,121).

Razvojem interneta otvoren je čitav niz pitanja, a pre svega pitanje zaštite prava građana na privatnost, odnosno prava na nepovredivost integriteta njegove ličnosti (Lilić 2006, 140). To je imalo za posledicu da „pravo na privatnost” počne da se posmatra kao jedno od osnovnih ljudskih prava.

Problematika privatnosti je postala jedna od najvažnijih tema u uslovima upotrebe informaciono-komunikacionih tehnologija. Opasnost od tehnologije postaje veća jer, sa gledišta sigurnosti, internet ima velike slabosti. Istovremeno, u virtuelnom svetu čovek je daleko manje oprezan nego u realnom. Prividna nevidljivost i udaljenost stvaraju osećaj anonimnosti i sigurnosti, pa korisnik često ostavlja lične

podatke ili preduzima radnje kojima nesvesno ugrožava svoju bezbednost (Dimitrijević 2011, 244).

Postojanje opasnosti i rizika ukazalo je na neophodnost formiranja jednog sistema načela i mera za zaštitu prava na privatnost i tajnost podataka koji se na nju odnose. Takav jedan sistem su pokušale da uspostave države članice EU (Bosnić 1998, 26).

U donetim pravnim regulativama države članice EU su utvrdile osnovne ciljeve, principe i načela zaštite podataka o ličnosti, kriterijume kvaliteta i legitimnosti obrade podataka o ličnosti, posebne kategorije podataka, prava lica o kojima se podaci vode na pristup podacima, izuzeća i ograničenja tih prava kao i mere za zaštitu lica na koja se podaci odnose (Bosnić 1998, 28).

Međutim, teško je sa sigurnošću tvrditi koliko će akti EU o zaštiti podataka o ličnosti pozitivno uticati na poslovne aktivnosti i pravne odnose. Već se pojavljuju mišljenja stručne javnosti da su pojedini akti EU nepotpuni i da njima nisu obuhvaćene pojedine oblasti novih tehnologija. Nažalost, praksa EU i svih ostalih država pokazuje da pravo sporo reaguje kada je razvoj tehnologije u pitanju i da je na sceni društveni paradoks: nove tehnologije se stalno menjaju i unapređuju, a pravo te promene sporo prepoznaje (Baltezarević 2017, 249).

LITERATURA

1. Acquist, Alessandro, Ralph Gross. 6/2006. Imagined communities: awareness, information sharing, and privacy on the Facebook. *Privacy Enhancing Technologies*. Cambridge, UK Volume: LNCS, 4258: 36–58
2. Baltezarević, Vesna, Radoslav Baltezarević. 1/2017. Zaštita privatnosti na internetu – evropski model. *Megatrend revija* 14: 241–252.
3. Baltezarević, Vesna, Radoslav Baltezarević. 7/2015. Sloboda na internetu i njene posledice. *Godišnjak Fakulteta za kulturu i medije*: 257–272.
4. Bosnić, Jadranka. 1–2/1998. Zaštita podataka o ličnosti. *Jugoslovenski časopis za pravnu informatiku* 6: 26–35.
5. Dimitrijević, Predrag. 2011. *Pravo informacione tehnologije*. Niš: Centar za publikacije Pravnog fakulteta u Nišu.
6. Kol, Erik. 2021. *Onlajn opasnost*. Beograd: Vulkan izdavaštvo.
7. Krivokapić, Danilo, Jelena Adamović, Dunja Tasić, Andrej Petrovski, Petar Kalezić, Đorđe Krivokapić. 3/2019. Novo doba zaštite podataka o ličnosti. *Prelom* 61: 13–15.

8. Lilić, Stevan. 2006. *Pravna informatika*. Beograd: Zavod za udžbenike i nastavna sredstva.
9. Milovanović, Sandra. 2019. *Nasilje na internetu – kriminološki aspekt*. Neobjavljeni rukopis. Niš: Pravni fakultet Univerziteta u Nišu.
10. Popović, Miloš. 2016. *Internet i mladi*. Neobjavljeni rukopis. Niš: Pravni fakultet Univerziteta u Nišu.
11. Popović, Dušan, Marko Jovanović. 2017. *Pravo interneta*. Beograd: Centar za izdavaštvo i informisanje.
12. Šarkić, Nebojša, Dragan Prlja, Katarina Damnjanović, Vesna Živković, Vladimir Marić, Vladimir V. Vodinelić, Nataša Mrvić Petrović. 2007. *Pravo informacionih tehnologija*. Beograd: Pravni fakultet Univerziteta Union u Beogradu – Javno preduzeće „Službeni glasnik”.
13. Kuzmanović, Dobrinka. 2019. Zaštita ličnih podataka i privatnost na internetu. <https://digitalni-vodic.ucpd.rs/zastita-licnih-podataka-i-privatnosti-na-internetu/?lng=lat>, poslednji pristup 20. jula 2023.
14. Khandelwai, Swati. 2017. Sweden Accidentally Leaks Personal Details of Nearly All Citizens. <https://thehackernews.com/2017/07/sweden-data-breach.html>, poslednji pristup 23. jula 2023.
15. Milić, Dragan. 2019. Direktiva o privatnosti i elektronskim komunikacijama (ePD) i Uredba o e-privatnosti (ePD). <https://www.milic.rs/internet-pravo/direktiva-o-privatnosti-i-elektronskim-komunikacijama-epd-i-uredba-o-e-privatnosti-epr/>, poslednji pristup 10. avgusta 2023.

Marija Vojisavljević*

EUROPEAN REGULATION OF DATA PROTECTION ON THE INTERNET

Summary: The right to privacy is particularly threatened by the emergence of new information technologies. In a time characterized by the processing of huge amounts of various data, the so-called “era of big data”, personal data is treated as the most important resource. The Internet has made it possible to access data that can be misused. Recognizing the dangers that the Internet brings with it, the members of the European Union have undertaken a number of important activities with the aim of protecting the rights of Internet users and providing them with security on the networks. This paper presents the provisions and principles of protection of personal data and privacy on the Internet contained in the European Convention for the Protection of Human Rights and Fundamental Freedoms, Directive 95/46, the Charter of the European Union on Fundamental Rights, Directive 2002/58, Directive 2016/680 and General regulation on data protection. Conventions, regulations and directives are reviewed to determine to what extent the European Union has succeeded in its intention to find adequate legal regulation of data protection on the Internet.

Key words: *Internet, Legal Acts of the European Union, Online threats, Personal data, Privacy*

* Author is an undergraduate student at the University of Belgrade – Faculty of Law, *marijavojisavljevic2003@gmail.com*.