P. Dimitrijević, *Pravna regulacija elektronske komunikacije i pravo na privatnost*, Zbornik radova, Pravni fakultet Univerziteta u Istočnom Sarajevu, 2011, str. 199–211.

UDK 342.738:004.7(094.5)

Prof. dr Predrag Dimitrijević

Pravni fakultet Univerziteta u Nišu
Pravni fakultet Univerziteta u Istočnom Sarajevu

PRAVNA REGULATIVA ELEKTRONSKE KOMUNIKACIJE I PRAVO NA PRIVATNOST

Elektronska komunikacija je novo izazovno područje koje zahteva pravno regulisanje. Svaka država zakonima i podzakonskim aktima reguliše ponašanje na Internetu u svojim nacionalnim granicama. Međutim, država se ne može ograničiti samo na državne granice jer su elektronski odnosi ili elektronska komunikacija globalnog karaktera.

Privatnost je jedno od osnovnih ljudskih prava što znači da se odnosi na ona prava koja su vezana za ličnost čoveka i predmete koji su neposredno vezani za nju. Razvoj novih informacionih tehnologija doveo je do stvaranja sistema koji omogućuju masovno praćenje, nadzor i prisluškivanje komunikacija, njihovu obradu na digitalnim medijima i povezivanje s drugim podacima. Problematika privatnosti postala je goruća praktična tema u uslovima elektronske komunikacije i upotrebe informaciono-komunikacione tehnologije.

Pravna regulativa ove materije ima dve osnovne sfere. Jedna se tiče tehničkih pitanja, a druga pravnih pitanja, koja sa svoje strane imaju građanskopravnu, pravno-ekonomsku i javnopravnu dimenziju. Ova poslednja je predmet naše pažnje. Pravno regulisanje elektronske komunikacije obuhvata brojne odnose koji su stvoreni u novim tehnološkim uslovima, kao što su odnosi povodom: nezatraženih poruka, podataka o ličnosti u javnom telefonskom imeniku, podataka o saobraćaju i lokaciji, pitanja bezbednosti i integriteta javnih komunikacionih mreža i usluga, tajnosti elektronskih komunikacija, pitanja (zakonitog) presretanja elektronskih komunikacija i problemi zadržavanja podataka (obaveze zadržavanja, vrste i zaštitu zadržanih podataka).

Središnje pravno pitanje je da li je pravno zaštićeno pravo privatnosti u navedenim i drugim elektronskim komunikacijama. Odgovor je negativan jer jedan zakon (npr. zakon o elektronskoj komunikaciji) otvara

vrata za povredu privatnosti od strane drugog (npr. zakona o tajnosti podataka), ili trećeg, a oni svi daju odrešene ruke podzakonskoj regulatornoj funkciji državnih i nedržavnih organa (raznih agencija i regulatornih tela).

S druge strane, ovakvo stanje neusklađene i disperzivne pravne regulative gotovo je standardizovano na regionalnom i evropskom planu, pa se zaključuje da zloupotreba prava privatnosti čini da se ono mora pojačano kontrolisati. Problem je što se moraju ponuditi adekvatne i efikasne pravne procedure zaštite ovog prava.

Ključne reči: Elektronska komunikacija; Pravo na privatnost.

1. UVOD

Svaka država zakonima i podzakonskim aktima reguliše ponašanje na Internetu u svojim nacionalnim granicama. Međutim, država se ne može ograničiti samo na državne granice jer su elektronski odnosi ili elektronska komunikacija globalnog, dakle internacionalnog karaktera. Nacionalne vlade ne mogu da obuzdaju ogromne mogućnosti sajber prostora baš zbog prirode globalne tehnologija koja ne može ograničiti broj subjekata koji su u globalnoj mreži. Kibernetskim prostorom putuju različite informacije, a pri tome autori tih različitih sadržaja nemaju mogućnost kontrole nad upotrebom i obradom svojih informacija na Internetu. Postoji neverovatna lakoća kojom se digitalni materijal može kopirati, slati i na razne načine obrađivati. Dok, s jedne strane, postoji mišljenje o zabrani upotrebe ili striktnoj kontroli elektronskih informacija, s druge strane, postoji i mišljenje da globalna javnost treba da slobodno raspolaže ovakvim sadržajima, na isti način na koji je tradicionalno raspolagala kopijama knjiga, muzike i ostalih autorskih dela.

Korisnici Interneta, zbog njegovog multinacionalnog karaktera, teže popustljivim propisima, odnosno izbegavanju propisa, pa im se često i omogućava izbegavanje propisa koji im ne odgovaraju.[1] Tačnije, veb-sajt lako može biti smešten van jurisdikcije granica države i tako ne biti limitiran njenim zakonima. Ovo *off-shore* pravosuđe sa minimumom pravnih propisa može pretvoriti Internet u raj za kockanje i ostale radnje koje su zabranjene na drugim mestima. Ovde se pojedinačnim, ili kolektivnim postupcima vrši potiskivanje nacionalne i internacio-

[1] *Korisnik Interneta* je fizičko ili pravno lice koje koristi Internet usluge i/ili ostale usluge prenosa podataka po osnovu zaključenog ugovora ili na drugi predviđeni način.

nalne regulative jer nedostaju efikasna nacionalna i internacionalna tela koja će voditi računa o tome.[2]

2. PRAVO NA PRIVATNOST

Privatnost je jedno od *osnovnih ljudskih prava*, što znači da se odnosi na ona prava koja su vezana za ličnost čoveka i predmete koji su neposredno vezani za nju. Iako na prvi pogled izgieda da je nepotrebno isticati vezanost prava privatnosti za fizičko lice, njegovu ličnost i život, ono je ipak neophodno jer predstavlja osnov ovog prava. Kao lično pravo, pravo privatnosti je neotuđivo pravo svakog pojedinca i ne može se preneti na drugog pojedinca ili instituciju.[3]

Od mnogih pitanja nastalih pojavom kompjuterske informatičke tehnologije, pravna pitanja koja proizlaze iz tzv. napada na privatnost (*assault on privacy*), i pitanja zaštite i bezbednosti podataka u kompjuterizovanim informacionim sistemima, na čelu su tog pravnog izazova.[4]

Tome ide na ruku i opšti pravni princip u ovoj materiji da podaci koji su javno dostupni, odnosno koje javnost ima pravo da zna u skladu sa zakonom o slobodnom pristupu informacijama od javnog značaja, ne smatraju se tajnim podacima, odnosno poslovnim tajnama.

Razvoj novih informacionih tehnologija doveo je do stvaranja sistema koji omogućuju masovno praćenje, nadzor i prisluškivanje komunikacija, njihovu obradu na digitalnim medijima i povezivanje s drugim podacima. Tehnologija elektronskog praćenja i nadzora izuzetno se brzo razvija. To postavlja pitanje privatnosti i pravne zaštite ličnih podataka građana prilikom vođenja različitih evidencija državnih i nedržavnih organa i organizacija. Sredstva za elektronsko praćenje i nadzor omogućuju čak i ispitivanje psihičkih reakcija analizom glasa, analizom moždanih talasa, itd. Moguće je čak ustanoviti i emocionalno stanje pojedinca, itd.

---

[2] P. Dimitrijević, *Pravo informacione tehnologije*, Sven, Niš 2010.

[3] M. Drakulić, *Osnovi kompjuterskog prava*, DOPIS, Beograd 1996.

[4] „Pojedini stručnjaci iz oblasti informatike predlažu uvođenje ličnog broja za svakog pojedinca radi identifikacije u vezi s pitanjem poreza, bankarskih poslova, obrazovanja, socijalne zaštite, vojne obaveze, kao i zbog drugih razloga. (...) Nije teško zamisliti opasnosti koje proizlaze iz ove tehnologije za buduće generacije. Neprijatna istina je ta da mnogi aspekti primene informatičke tehnologije predstavljaju potencijalno ili stvarno ugrožavanje privatnosti.“ – A. R. Miller, *The Assault on Privacy - Computers Data Banks and Dosiers*, The University of Michigan Press, Ann Arbour, MI 1971, 4.

Razvojem komunikacionih mreža, naročito Interneta kao globalne svetske mreže ili „mreže svih mreža“, javlja se pojam „umreženog društva“, virtuelnog sveta u kojem svako komunicira sa svakim.[5] Internet je globalni elektronski komunikacioni sistem sačinjen od velikog broja međusobno povezanih računarskih mreža i uređaja koji razmenjuju podatke koristeći zajednički skup komunikacionih protokola.[6] Globalni elektronski sistem komunikacija postaje izvor najraznovrsnijih podataka o ljudima. U virtuelnom svetu, čovek je daleko manje oprezan nego u realnom. Prividna nevidljivost i udaljenost stvara u njemu osećaj anonimnosti i sigurnosti, pa ponekad daje i lične podatke ili preduzima i one radnje koje u fizičkom svetu sigurno nikada ne bi.

Razvojem elektronske komunikacije otvoren je čitav niz pitanja, a pre svega pitanje zaštite prava građanina na privatnost, odnosno prava na nepovredivost integriteta njegove ličnosti, time što se štite određeni podaci koji se tiču njegove ličnosti.[7] To je imalo za posledicu da se uoči „pravo na privatnost“, kao jedno od osnovnih ljudskih prava i da se pravnici počnu baviti pravnom zaštitom podataka o ličnosti. Pitanje zaštite podataka o ličnosti (ličnih podataka) je složeno pitanje, između ostalog i zbog teškoća u vezi sa uobličavanjem („konstruisanjem“) jedne precizne pravne definicije privatnosti.

Pitanje privatnosti (*privacy*) i prava na privatnost godinama je predmet burnih teorijskih rasprava. Klasična koncepcija privatnosti izneta je u radu „Pravo na privatnost“ (*The Right to Privacy*) američkih sudija *Samuel Warren*-a i *Louis Brandais*-a, krajem XIX veka, gde se „pravo privatnosti“ definiše kao „pravo da se bude ostavljen na miru“ (*right to be left alone*).[8]

[5] P. Dimitrijević, „Umrežena javna uprava“, *Pravni život* 11/2009.

[6] Zakon o elektronskim komunikacijama, *Službeni glasnik RS*, br. 45/10, čl. 4.

[7] S. Lilić, *Pravna informatika*, Zavod za udžbenike i nastavna sredstva, Beograd 2006, 140.

[8] S. Warren, L. Brandais, *The Right to Privacy*, Harvard Law Review, 1890. Problem „*privacy*“ javlja se krajem prošlog veka u SAD, a prvi članak o pravu privatnosti (*The Right to Privacy*) publikovali su u *Harvard Law Review* 1890. godine *S. Voren* i *L. Brandis*. Ovu frazu skovao je Tomas M. Kuli i tek nakon toga su S. Voren i L. Brandis predložili termin „*right of privacy*“, u pomenutom članku.

Nedavno, u jednom intervjuu koji je dao *Bil Gejts*, opisuju se blagodeti komunikacionog društva, ali se pri tome ističe da u tom raju postoji jedan problem koji se naziva odbrana privatnosti. U informatičkom društvu može se reći da mi postajemo svoja sopstvena informacija, koja nas obeležava, definiše i klasifikuje. Steći mogućnost da se ovlada cirkulacijom informacije, moć da se kontroliše onaj koji je koristi, znači konačno steći vlast nad samim sobom. Cilj je da se garantuje jedno funda-

Pravo na privatnost jedno je od osnovnih, neotuđivih i apsolutnih ljudskih prava svakog pojedinca kojim se obezbeđuje integritet i dignitet ljudske ličnosti, a radi očuvanja tajnosti i slobode njegovog privatnog života.[9] Karakteristike i sadržaj prava na privatnost su: privatnost je jedno od osnovnih ljudskih prava, pravo na privatnost obezbeđuje integritet i dignitet ličnosti, ono čuva tajnost i slobodu privatnog života i to je apsolutno pravo.

Pravo privatnosti štiti tri vrste interesa: a) čovekove interese autonomije odlučivanja u intimnim i ličnim stvarima; b) interes pojedinca da se zaštiti od otkrivanja ličnih okolnosti; c) interes pojedinca da se obezbedi od neosnovane prismotre od strane vlasti.

Međutim, problematika privatnosti postala je goruća praktična tema u uslovima upotrebe informaciono-komunikacione tehnologije i elektronske komunikacije. Ona je stvorila neograničene mogućnosti za koncentraciju podataka, njihovo grupisanje i pretraživanje po raznim obeležjima, kao i mogućnost korišćenja od strane širokog kruga korisnika. To je imalo za posledicu masovnu pojavu podataka o ličnosti po raznim evidencijama, registrima i drugim zbirkama podataka. Opasnosti za privatnost koje donose informacione tehnologije sastoje se u stvaranju digitalnih informacionih dosijea o građanima koji se mogu zloupotrebiti (npr. „krađa identiteta“) i stvaranju ogromnog tržišta ličnih podataka.[10] Informaciona tehnologija može se iskoristiti za stvaranje kompleksnih dosijea o građanima, ne samo od strane državnih institucija, radoznalih hakera ili zlonamernih kriminalaca, već i za potrebe privatnog sektora koji se njima sve češće koristi u komercijalne svrhe. Doduše, problemi koji zadiru u privatnost građana mogu proizaći iz grešaka u programima, sigurnosnih slabosti komunikacionih protokola ili skrivenih mogućnosti postojećih programa. Zabrinjavajuće je što se informaciona tehnologija može koristiti za praćenje aktivnosti disidenata, aktivista za ljudska prava, novinara, studentskih vođa, manjina, sindikalnih vođa, političkih oponenata itd.

---

mentalno pravo u budućem društvu koji mnogi nazivaju društvom bez papira („*paperless society*“).

[9] Protiv ovakve „negativne definicije“ prava privatnosti danas su izražene brojne i ozbiljne kritike. Pokušaj da se privatnost izjednači sa neuznemiravanjem, tj. s idejom da se bude ostavljen na miru, filozofi nazivaju negativnom slobodom.

[10] Tržište ličnih informacija, skriveno od pogleda javnosti, već je 1999. po nekim procenama premašilo vrednost 1,5 milijardi dolara. Osim za marketinške potrebe, takvi podaci mogu dovesti i do tzv. „krađe identiteta“, pri čemu su najčešće zloupotrebe za činjenje raznih krivičnih dela kao što su računarske prevare.

Opasnost od tehnologije postaje veća, jer s gledišta sigurnosti Internet ima velike slabosti. Glavni razlog za to je, prije svega, što je on zamišljen da obezbijedi najveći mogući stepen elastičnosti, pa zbog toga ne zadovoljava u pogledu neovlašćenog korišćenja podataka. Postojanje svih ovih opasnosti i rizika ukazali su na neophodnost formiranja jednog sistema načela i mera za zaštitu prava pojedinca na privatnost i tajnost podataka koji se odnose na privatnost.

Privatnost je sastavni deo lične ali i socijalne sigurnosti u informacionom društvu i masovne elektronske komunikacije. Zbog toga, savremeni „aktivni" koncept privatnosti polazi od toga da u informacionom društvu niko ne može biti ostavljen na miru jer su podaci o pojedincima i pravnim licima deo složenih informacionih sistema (e-države). Da bi se pravo na privatnost moglo zaista pravno zaštititi, moramo imati jednu realnu koncepciju, koja će samu privatnost shvatiti u kontekstu globalnog komunikacionog okruženja, koje ima tendenciju entropije. „Privatnost je pravo da zaštitimo sebe od uticaja spoljneg sveta. To je mera kojom se koristimo radi uspostavljanja ograničenja na zahteve organizacije i ljudi. To je pravo koje tražimo radi zaštite naše lične slobode, naše autonomije i našeg identiteta."[11]

Pojam prava privatnosti proširio se na mnoge sfere i situacije koje mogu predstavljati izvor diskriminacije na radnom mestu kao i na sve društvene odnose. Napuštajući shvatanje proste zaštite čovekove intime, pravo na privatnost shvaćeno je kao zaštita prava na slobodan izbor, bez uslovljavanja ili diskriminacije koje određuje slika koju su drugi o nama stvorili.

Savremeni koncept privatnosti stavlja naglasak na tzv. kontrolu informacija, jer se ne može isključiti realno „komunikaciono" okruženje u kojem se čovek danas stvarno nalazi. Savremena pravna teorija posmatra pravo privatnosti sa tzv. aktivnog stanovišta. Interes pojedinca je da sazna da se podaci o njemu prikupljaju i čuvaju, zašto su neophodni, kako će se koristiti i od strane koga, u koje svrhe i sl. Interes samoodređivanja sopstvene elektronske komunikacije sa drugima, odražava želju pojedinca i grupa da saopštavaju informacije o sebi. Privatnost je pravo pojedinca, grupa ili institucija da sami za sebe odrede kada, kako i u kojoj meri će se informacije o njima saopštavati drugim licima. Prema tome, informaciona privatnost je privatnost kao pravo

[11] S. Davies, *How to Beat Goliath: The Strong Privacy Protection Is the Best Defense Against Information Warfare.*

pojedinca da kontroliše koji podaci, za koga i kako mogu postati dostupni drugima.

Ono što pravo tu stvarno može je da pojedincima pravno garantuje kontrolu nad informacijama o sebi. Pojedinci imaju pravo da znaju i kontrolišu ko koristi informacije o njima, kada i u koje svrhe, da li ima ovlašćenja za to, da li je došlo do promena tih informacija, zašto i u koje svrhe. Suština je u samoodređivanju sopstvene komunikacije sa drugim. Međutim, informaciona tehnologija u sprezi sa javnim interesom ozbiljno dovodi u pitanje pravo na privatnost. Imajući u vidu povećanu mogućnost zloupotrebe koja se može javiti zbog primene informacionih sistema, mnoge zemlje su pristupile donošenju odgovarajućih zakona i podzakonskih akata, s ciljem posebne i neposredne zaštite podataka odnosno „privatnosti".[12]

3. ELEKTRONSKA KOMUNIKACIJA

Elektronska komunikacija jeste masovni i umreženi sistem elektronskih komunikacionih odnosa u kome se prenose i obrađuju razne elektronske informacije između, po pravilu, neograničenog broja subjekata. Elektronska komunikacija funkcioniše kao umreženi sistem protoka informacija.

Elektronska komunikacija je sistemski pravno regulisana specijalnim *Zakonom o elektronskim komunikacijama* (ZoEK, 2010).[13] Jedan od važnih ciljeva i načela regulisanja odnosa u oblasti elektronskih komunikacija je i načelo obezbeđivanja visokog nivoa zaštite podataka o ličnosti i privatnosti korisnika, a u skladu sa Zakonom o zaštiti podataka o ličnosti i drugim zakonima i načelo osiguravanja bezbednosti i integriteta javnih komunikacionih mreža i usluga (član 3).

Zakon u delu kojim reguliše dostavljanje podataka i zaštitu tajnosti podataka izričito propisuje da je operater dužan da, na zahtev ***Agencije za elektronske komunikacije***, *dostavi sve podatke* neophodne za obavljanje poslova Agencije, a naročito one koji su potrebni za zaštitu podataka o ličnosti i privatnosti korisnika, podatke za procenu bezbednosti i integriteta e-komunikacione mreže. U tom smislu, Agencija je dužna da sarađuje sa organima i organizacijama nadležnim za zaštitu podataka o ličnosti (Poverenik).

[12] I. J. Lloyd, „The Data Protection Act – Little Brother fights back?", *The Modern Law Review*, Vol 48, Stevens&Sons Limited 1985, 190.

[13] Pre važećeg Zakona o elektronskim komunikacija ovu materiju pravno je regulisao Zakon o telekomunikacijama, *Službeni glasnik RS*, br. 44/03 i 36/06.

Zakon ime više mesta koja neposredno pravno uređuju pitanje privatnosti, odnosno pitanje ličnih podataka u e-komunikaciji.

1. ***Nezatražene poruke***. ZoEK (2010) određuje pojam *elektronske poruke* definišući je kao svaki tekstualni, glasovni, zvučni ili slikovni zapis, poslat preko javne komunikacione mreže, koji se može pohraniti u mreži ili u terminalnoj opremi primaoca sve dok je primalac ne preuzme ili joj pristupi (član 3). Ovde je reč o porukama koje korisnik (pretplatnik) elektronskog sistema prima, a nije ih tražio (tzv. *nezatražena* poruka).

Zakon polazi od principa da je korišćenje sistema e-komunikacije (npr. sistema za automatsko pozivanje i komunikaciju bez ljudske intervencije, faksa, elektronske pošte ili drugih elektronskih poruka), radi neposrednog oglašavanja, dopušteno samo uz prethodni pristanak korisnika, odnosno pretplatnika (primalac).

Zabranjeno je *neposredno* (lično) oglašavanje kojim se netačno (neistinito) prikazuje ili prikriva identitet pošiljaoca elektronskih poruka (npr. elektronske pošte), kao i (*neposredno*) oglašavanje bez naznake elektronske adrese (broja telefona). U tom slučaju, primalac poruka može bez naknade da zahteva sprečavanje daljeg slanja oglasnih poruka.

Zakon o elektronskim komunikacijama sadrži niz obaveza za operatera kao što su obaveze operatera da pretplatniku (korisniku sistema) omogući filtriranje nezatraženih i škodljivih elektronskih poruka, kao i jednostavan način za podešavanje ili isključivanje filtera.

Operater je dužan da javno objavi elektronsku adresu za prijavljivanje *nezatraženih* i *škodljivih* elektronskih poruka. Ovde je još jedan zakonski uslov, a to je da poruke budu kvalifikovane kao štetne.

Operater je dužan da, po prijemu dokaza o nezatraženim i škodljivim porukama koje su poslate od strane njegovih pretplatnika, utvrdi činjenično stanje i u zavisnosti od stepena zloupotrebe, opomene pretplatnika ili mu privremeno onemogući korišćenje usluge i o tome ga obavesti.

U slučaju ponovljene zloupotrebe, operater ima pravo da pretplatniku trajno onemogući korišćenje usluga (npr. raskine ugovor o korišćenju usluga).

2. ***Podaci o ličnosti u javnom telefonskom imeniku***. Pružalac usluga javnog telefonskog imenika dužan je da bez naknade obavesti pretplatnika o nameri da njegove lične podatke uključi u javno dos-

tupan telefonski imenik (u štampanoj ili elektronskoj formi), o svrsi imenika, dostupnosti ličnih podataka preko usluga obaveštenja, kao i mogućnostima za pretragu ličnih podataka od strane trećih lica preko funkcija pretrage u elektronskoj formi imenika.

Pretplatnik ima pravo da, po prijemu ovog obaveštenja, odbije saglasnost za uključivanje ličnih podataka u javno dostupan telefonski imenik.

Pretplatnik, čiji se lični podaci nalaze u javnom telefonskom imeniku, ima pravo na proveru ili ispravku podataka, kao i mogućnost povlačenja date saglasnosti, odnosno brisanja ličnih podataka iz imenika, na jednostavan način i bez naknade.

Međutim, treba pribaviti dodatni pristanak pretplatnika pre upotrebe podataka iz javnog imenika u druge svrhe, odnosno svrhe različite od kontaktiranja pretplatnika preko imena, prezimena, odnosno naziva pretplatnika ili njegovih drugih identitetskih oznaka.

3. ***Obrada podataka o mrežnom saobraćaju korisnika***. Operater javnih komunikacionih mreža, koji obrađuje i čuva podatke o saobraćaju korisnika, dužan je da te podatke obriše (obaveza brisanja) ili učini neprepoznatljivim korisnika, kada ovi podaci (o mrežnom saobraćaju) više nisu neophodni.[14]

Obaveza brisanja (nezadržavanja) ne postoji ako su (1) podaci potrebni za izradu računa za usluge, ali u okviru zakonskog roka za naplatu potraživanja ili (2) podatke operater koristi radi oglašavanja i prodaje usluga, ali uz pristanak korisnika[15] ili (3) podatke po zakonu treba čuvati – zadržavati.

Obradu podataka o saobraćaju sme da vrši samo ovlašćeno lice, odnosno lica koja za potrebe operatera obavljaju poslove izdavanja računa, upravljanja mrežom, davanja odgovora na pitanja korisnika, otkrivanja prevara, oglašavanja i prodaje usluga elektronskih komunikacija i sl. i to samo u meri koja je neophodna za obavljanje navedenih aktivnosti.

[14] Prethodno važeći Zakon o telekomunikacijama (član 54) predviđao je širu formulaciju po kojoj je operater dužan da nadležnim državnim organima omogući pristup i analizu podataka o saobraćaju korisnika koji se obrađuju radi uspostavljanja veza. Ove podatke inače operater može obrađivati samo u obimu koji je neophodan za ispostavljanje računa korisniku i može ih dostaviti samo pošiljaocu i primaocu poruka.

[15] Svoj pristanak korisnik može opozvati u bilo kom trenutku.

Ovo ne važi ako Agencija i drugi državni organi ostvaruju uvid u ovu vrstu podataka, a koji su od značaja za odlučivanje u sporovima (npr. povodom računa za usluge).

4. ***Obrada podataka o lokaciji korisnika***. Operater može obrađivati podatke o lokaciji korisnika samo pod uslovom da se korisnik učini neprepoznatljivim ili ako on na obradu prethodno pristane, ali samo u onoj meri i za ono vreme koje je potrebno za te svrhe.[16] Međutim, ovo ne važi za lokacijske podatke koji se zadržavaju po sili zakona – ZoEK, čl. 129 st. 1.[17] Međutim, ZoEK izričito zabranjuje zadržavanje podataka koji otkrivaju sadržaj komunikacije (čl. 129 st. 3).

Operater je dužan da pre pribavljanja pristanka obavesti korisnika o vrstama lokacijskih podataka koji će biti predmet obrade, cilju i trajanju obrade i da li će podaci biti dostavljani trećim.

Operater je dužan da korisniku koji je dao pristanak pruži mogućnost da odbije obradu podataka o lokaciji, pri svakom povezivanju na mrežu ili prenosu komunikacije, na način koji je jednostavan i besplatan.

Obradu ovih podataka mogu da vrše samo ovlašćena lica operatera, odnosno ovlašćena lica treće strane, u meri neophodnoj za pružanje usluge.

5. ***Bezbednost i integritet javnih komunikacionih mreža i usluga***. Operater je dužan da s ciljem bezbednosti i integriteta e-mreža, tajnosti komunikacija i zaštite podataka o ličnosti, primeni adekvatne tehničke i organizacione mere primerene rizicima. Te mere posebno se odnose na prevenciju i minimizaciju uticaja bezbednosnih incidenata po korisnike i mreže, kao i na obezbeđivanje kontinuiteta rada mreža.

Kada postoji poseban rizik povrede bezbednosti i integriteta komunikacionih mreža (neovlašćeni pristup, značajan gubitak podataka, ugrožavanje tajnosti komunikacija, bezbednosti ličnih podataka i drugo), operater treba o tom riziku da obavesti pretplatnike. Ako je takav

[16] Svoj pristanak korisnik može opozvati u bilo kom trenutku.

[17] Naime, operater je dužan da zadrži taksativno određene podatke o elektronskim komunikacijama iz člana 129 stav 1 ZoEK-a za potrebe sprovođenja istrage, otkrivanja krivičnih dela i vođenja krivičnog postupka, kao i za potrebe zaštite nacionalne i javne bezbednosti. To su podaci potrebni za utvrđivanje: izvora, odredišta, početka, trajanja i završetka komunikacije, vrste komunikacije, identifikaciju opreme korisnika i za utvrđivanje lokacije mobilne opreme korisnika. Međutim, ZoEK izričito zabranjuje zadržavanje podataka koji otkrivaju sadržaj komunikacije (čl. 129 st. 3).

rizik van opsega obaveznih mera operatera, on je dužan da obavesti pretplatnike o mogućim merama zaštite i troškovima u vezi sa primenom tih mera.

Operater je dužan da obavesti Agenciju o svakoj povredi bezbednosti i integriteta mreža, a naročito o povredama koje su imale za posledicu narušavanje zaštite privatnosti korisnika. Agencija je ovlašćena da obavesti javnost o povredi bezbednosti i integriteta mreža ili traži od operatera da to sam uradi, kada proceni da je objavljivanje takve informacije u javnom interesu.

6. ***Tajnost e-komunikacija***. Presretanje e-komunikacija kojim se otkriva sadržaj komunikacije nije dopušteno bez pristanka korisnika. Pristanak korisnika nije potreban ako se presretanje čini na određeno vreme i na osnovu sudske odluke, ako je to neophodno radi vođenja krivičnog postupka ili zaštite državne bezbednosti.[18]

Međutim, dopušteno je snimanje komunikacija, radi dokazivanja komercijalnih transakcija ili drugih poslovnih odnosa, pod uslovom da su obe strane svesne ili su morale biti svesne ili su izričito upozorene na to da komunikacija može da bude snimljena.

Korišćenje e-komunikacije radi čuvanja ili pristupanja podacima u terminalnoj opremi korisnika dozvoljeno je pod uslovom da je korisniku dato jasno i potpuno obaveštenje o svrsi obrade podataka, u skladu sa zakonom kojim se uređuje zaštita podataka o ličnosti, kao i da mu je pružena prilika da takvu obradu odbije.

7. ***Presretanje (zakonito) e-komunikacija***. Operater je dužan da omogući zakonito presretanje e-komunikacija. Međutim, nadležni državni organ koji vrši zakonito presretanja dužan je da vodi evidenciju o tome, koja se smatra tajnom, u skladu sa zakonom o tajnosti podataka.[19]

8***. Zadržavanje podataka.*** Zakon jasno ističe da je zabranjeno zadržavanje podataka koji otkrivaju sadržaj komunikacije (čl. 129 st. 3).

Međutim, po zakonu operater ima obavezu da zadrži sve podatke o e-komunikacijama za potrebe sprovođenja istrage, otkrivanja krivič-

[18] Prethodno važeći Zakon o telekomunikacijama (ZoT) u članu 55 izričito zabranjuje sve aktivnosti kojima se *ugrožava* ili *narušava privatnost i poverljivost poruka* koje se prenose telekomunikacionim mrežama, osim kada postoji *saglasnost korisnika* ili ako se ove aktivnosti vrše u *skladu sa zakonom* ili *sudskim nalogom*.

[19] Evidencija presretnutih e-komunikacija sadrži: određenje pravnog akta (osnova) za presretanje, datum i vreme presretanja i identifikaciju ovlašćenog lica koje je vršilo presretanje pod uslovom da državni organ nije u mogućnosti da izvrši presretanje bez pristupa prostorijama, e-mreži, sredstvima ili opremi operatora.

nih dela i vođenja krivičnog postupka, u skladu sa ZoKP, kao i za potrebe zaštite nacionalne i javne bezbednosti.[20]

Zadržavanja podataka traje 12 meseci od dana obavljene komunikacije i treba biti takvo da se podacima bez odlaganja može pristupiti, odnosno dostaviti na zahtev nadležnog državnog organa.

Državni organ koji ostvaruje pristup zadržanim podacima dužan je da vodi evidenciju o pristupu ovim zadržanim podacima.[21]

Obaveza zadržavanja podataka operatera odnosi se na tačno određene ***vrste zadržanih podataka*** koje zakon takstivno nabraja (čl. 129 st. 1). To su podaci potrebni za utvrđivanje: izvora i odredišta komunikacije, utvrđivanje početka, trajanja i završetka komunikacije, utvrđivanje vrste komunikacije i identifikaciju lokacije i opreme korisnika.

Obaveza zadržavanja podataka obuhvata i podatke o pozivima koji su uspostavljeni ali se na njih nije odgovorilo, ali ne i o pozivima čije uspostavljanje nije uspelo.

Zakon uspostavlja i dužnost operatora da *štiti zadržane podatke.* **S ciljem zaštite zadržanih podataka, operater treba da obezbedi:**

1. Da zadržani podaci budu istog kvaliteta i podvrgnuti istim merama bezbednosti kao i podaci u e-mreži operatera;
2. Da zadržani podaci budu zaštićeni od uništenja (slučajnog ili nedopuštenog), slučajnog gubitka ili izmene, zaštićeni od čuvanja (neovlašćenog ili nezakonitog), obrade, pristupa ili otkrivanja, u skladu sa zakonom o zaštiti podataka o ličnosti, odnosno zakonom o zaštiti tajnih podataka;
3. Da se pristup zadržanim podacima ograniči na ovlašćena lica;
4. Da se zadržani podaci unište po isteku zakonskog roka.

Nadzor nad izvršenjem obaveza operatera vrši Poverenik za zaštitu podataka o ličnosti i organ nadležan za nadzor nad sprovođenjem zakona koji reguliše zaštitu tajnosti podataka.

[20] Međutim, operater nije dužan da zadrži podatke koje on nije proizveo niti obradio.

[21] Evidencija sadrži pravni osnov za pristup, datum i vreme pristupanja, identifikaciju ovlašćenog lica koje je pristupilo zadržanim podacima, kao i da ovu evidenciju čuva kao tajnu, u skladu sa zakonom kojim se uređuje tajnost podataka.

4. ZAKLJUČAK

Zakonom o elektronskim komunikacijama učinjen je korak napred u pravnom regulisanju e-komunikacija. Pravna regulativa je razuđena jer zahvata razna pravna pitanja, kao što su pitanje nezatraženih poruka, privatnosti u javnim telefonskim imenicima, obrade podataka o e-komunikaciji i lokaciji korisnika, bezbednosti i tajnosti e-komunikacije, presretanje i zadržavanje e-podataka. Navedeno pravno regulisanje detaljnije je u odnosu na prethodno važeći ZoT (Zakon o telekomunikacijama) sa očuvanim zajedničkim principima.

Zakon utvrđuje brojne obaveze za operatere koje imaju cilj zaštite privatnosti korisnika, ali i zaštitu nacionalne i javne bezbednosti i potreba vođenja krivičnog postupka. Iako zakonodavac, doduše neupadljivo, štiti sadržinu komunikacije, utisak je da državni interesi natkriljuju interese pojedinca u globalnom elektronskom prostoru, ostavljajući ga bez adekvatne pravne zaštite.

Professor Dr. Predrag Dimitrijević

Faculty of Law University of East Sarajevo
Faculty of Law University of Niš

LEGAL REGULATION OF ELECTRONIC COMMUNICATION AND THE RIGHT ON PRIVACY

Summary

Electronic communication is a new and provocative area which demands legal regulation. Each state regulates behavior on Internet by legal acts in its competence. However, electronic communication has global character which is why its regulation can't be restricted to competence of particular states.

Privacy is one of basic human rights which mean that it is about rights on personality. Development of new technologies brought to new systems which enable mass overlook, surveillance and monitoring of communications, their processing on digital media and amalgamation with other data. The issue of privacy became important in era of electronic communications and usage of information technology.

Key words: *Electronic communication; Right on privacy*.