PRAVNI ZAPISI, God. IV, br. 1 (2013)
UDK 004.738.5:338.46]:347.78(497.11)

doi:10.5937/pravzap4-3861

IZVORNI NAUČNI ČLANAK

Doc. dr *Mario Reljanović*[*]

POSTUPANJA INTERNET OPERATORA POVODOM NAVODNOG KRŠENJA AUTORSKIH PRAVA – ZAKONODAVSTVO I PRAKSA U SRBIJI

Apstrakt: *Istraživanje obuhvata analizu aktuelnog sukoba interesa kada je reč o tri prava: pravu na privatnost komunikacije, pravu na zaštitu podataka o ličnosti i autorskom pravu. Ove tri grupe prava su predmet analize u svetlu važećih propisa Republike Srbije zbog konflikta koji postoji prilikom korišćenja elektronskih komunikacija radi kršenja autorskih prava. Ovaj konflikt je naročito došao do izražaja prilikom analize postupanja internet operatora u Srbiji koji su koristili tzv. „zadržane podatke" o korisnicima da bi reagovali na navodna kršenja autorskih prava. Rad se fokusira na postupanja operatora, korisnika i nosilaca autorskih prava, stavljajući akcenat na nedostatke postojećeg sistema zaštite koji se neizbežno manifestuju kroz kršenje prava na privatnost komunikacije i prava na zaštitu podataka o ličnosti.*

Ključne reči: pravo na privatnost elektronskih komunikacija, zaštita podataka o ličnosti, autorska prava, internet operatori, visokotehnološki kriminal.

Uvod

Direktan povod za ovu analizu jeste ponašanje više internet provajdera u Republici Srbiji, koji svojim korisnicima redovno šalju „pisma opomene" u kojima ih upozoravaju da je uočeno da krše autorska prava preuzimajući određene fajlove na internetu. U takvim pismima se navodi u koje vreme su i pod kojom *Internet Protocol* (u daljem tekstu: IP) adresom preuzimali fajl određenog imena, čiji sadržaj predstavlja autorsko delo. Navodi se da je u pitanju neautorizovano preuzimanje i kršenje zakona usled čega se obaveštavaju da će, ukoliko se tako nešto nastavi, biti primorani da isključe korisnika (privremeno ili trajno). Kao izvor informacija o nedozvoljenom preuzimanju sadržaja po pravilu se navode agencije ili

* Docent Pravnog fakulteta Univerziteta Union u Beogradu
e-mail: mario.reljanovic@pravnifakultet.rs

advokatske kancelarije koje predstavljaju nosioce kolektivnih autorskih prava, odnosno njihove pravne zastupnike. Korisnici se upozoravaju da odmah obrišu preuzeti fajl sa svog računara.[1]

Možda ovakvo postupanje laicima izgleda sasvim prihvatljivo – neko ko krši zakon mora se upozoriti da je njegovo ponašanje primećeno i da će biti adekvatno sankcionisano ukoliko se nastavi. Međutim, ko ovde zapravo krši zakone Republike Srbije: korisnici, operatori, nosioci autorskih prava ili svi zajedno? Inicirana ovim pitanjem, analiza obuhvata tri grupe prava koja su relevantna za davanje odgovora. Najpre će biti obrađeno pravo na privatnost (elektronskih) komunikacija, zatim pravo na zaštitu podataka o ličnosti u elektronskom obliku i konačno prava nosilaca autorskih prava i internet operatora u situacijama kada postoji sumnja da neko od korisnika krši autorska prava svojim aktivnostima na internetu. Na osnovu tih analiza doći će se do zaključka kako se pravno može okarakterisati postupanje nosilaca autorskih prava i internet operatora, ali i identifikovati kako bi njihova buduća praksa mogla (morala) da izgleda da bi se sprečilo lančano kršenje zakona koje počinje neautorizovanim preuzimanjem autorskih dela, ali se nastavlja kršenjem prava na privatnost građana i njihovog prava na zaštitu podataka o ličnosti.

1. PRAVO NA PRIVATNOST ELEKTRONSKE KOMUNIKACIJE I PODACI O LIČNOSTI NA INTERNETU

Pravo na privatnost i podaci o ličnosti u eri elektronskih komunikacija ozbiljno su ugroženi. Mogućnosti stvaranja, pohranjivanja i prenošenja podataka o ličnosti, koji predstavljaju deo njenog intimnog života i smatraju se privatnima, izuzetno su se razvile u poslednjoj deceniji. Nažalost, ovakav nesumnjivo pozitivan razvoj tehnologije uslovio je i umnožavanje načina kršenja prava na privatnost komunikacije, zloupotrebu podataka o ličnosti i generalno uveo značajan stepen nesigurnosti u elektronske komunikacije.

Pozitivno pravo Republike Srbije štiti privatnost komunikacije u više akata, usvojenih na međunarodnom i nacionalnom nivou. Valjalo bi naj-

1 Primeri ovakvih pisama, koja su pojedini internet operatori poslali svojim korisnicima u prethodnom periodu, mogu se videti u analizi *Kako internet provajderi u Srbiji uništavaju poverenje korisnika narušavajući privatnost,* (http://piratska.org/nekonasposmatra/, 20.04.2013). Na osnovu obraćanja korisnika interneta Piratskoj partiji RS, sprovedeno je šire pravno-tehničko istraživanje o postupanjima internet operatora i nosilaca autorskih prava. Rezultati su javno objavljeni u više tekstova, a na osnovu njih je Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti odlučio da izvrši vanrednu kontrolu postupanja operatora u Srbiji. Više o tome: *Uskoro nadzor nad operatorima,* (http://poverenik.rs/index.php/yu/aktuelnosti/ 1550-uskoro-nadzor-nad-operatorima.html, 20.04.2013).

pre pomenuti član 3. Konvencije o visokotehnološkom kriminalu[2] (u daljem tekstu: KVTK) pod nazivom *Nezakonito presretanje*: „Svaka Strana ugovornica treba da usvoji zakonodavne i druge mere, neophodne da bi se kao krivično delo u domaćem pravu propisalo protivpravno presretanje prenosa računarskih podataka koji nisu javne prirode, ka računarskom sistemu, od njega ili unutar samog sistema, uključujući i elektromagnetna emitovanja iz računarskog sistema kojim se prenose takvi podaci, kada je učinjeno sa namerom i uz pomoć tehničkih uređaja. Strana ugovornica može da uslovi da je delo učinjeno sa nečasnom namerom ili u vezi sa računarskim sistemom koji je povezan sa drugim računarskim sistemom." Dakle, kažnjivo je svako *protivpravno presretanje prenosa računarskih podataka* koji se ne mogu smatrati javnim.

Evropska konvencija za zaštitu osnovnih prava i ljudskih sloboda[3] (u daljem tekstu: EKLJP) u članu 8. takođe uspostavlja pravo na privatnost ličnosti, odnosno pravo na poštovanje privatnog i porodičnog života: „Svako ima pravo na poštovanje svog privatnog i porodičnog života, doma i prepiske. Javne vlasti neće se mešati u vršenje ovog 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 morala, ili radi zaštite prava i sloboda drugih." Zaštićena je, dakle, i prepiska kao oblik ostvarivanja privatne komunikacije; domašaj ove zaštite se odnosi i na elektronsku prepisku, odnosno elektronsku komunikaciju.[4]

Ustav Republike Srbije[5] dalje razrađuje načelo privatnosti prepiske u članu 41. pod nazivom *Tajnost pisama i drugih sredstava opštenja*: „Taj-

2 Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu, *Sl. glasnik RS*, br. 19/09.

3 Zakon o ratifikaciji evropske Konvencije za zaštitu ljudskih prava i osnovnih sloboda, izmenjene u skladu sa Protokolom broj 11, protokola uz Konvenciju za zaštitu ljudskih prava i osnovnih sloboda, Protokola broj 4 uz Konvenciju za zaštitu ljudskih prava i osnovnih sloboda kojim se obezbeđuju izvesna prava i slobode koji nisu uključeni u Konvenciju i Prvi protokol uz nju, Protokola broj 6 uz Konvenciju za zaštitu ljudskih prava i osnovnih sloboda o ukidanju smrtne kazne, Protokola broj 7 uz Konvenciju za zaštitu ljudskih prava i osnovnih sloboda, Protokola broj 12 uz Konvenciju za zaštitu ljudskih prava i osnovnih sloboda i Protokola broj 13 uz Konvenciju za zaštitu ljudskih prava i osnovnih sloboda o ukidanju smrtne kazne u svim okolnostima, *Sl. list SCG – Međunarodni ugovori*, br. 9/03.

4 Videti slučajeve pred Evropskim sudom za ljudska prava: *Copland protiv Ujedinjenog Kraljevstva* (predstavka 62617/00, presuda od 3. aprila 2007. godine); *Liberty i ostali protiv Ujedinjenog Kraljevstva* (predstavka 58243/00, presuda od 1. jula 2008. godine). Odlučujući o eventualnom kršenju člana 8. u navedenim slučajevima, Evropski sud za ljudska prava jasno je poistovetio elektronsku komunikaciju sa klasičnim oblicima komunikacije.

5 Ustav Republike Srbije, *Sl. glasnik RS*, br. 98/06.

nost pisama i drugih sredstava komuniciranja je nepovrediva. Odstupanja su dozvoljena samo na određeno vreme i na osnovu odluke suda, ako su neophodna radi vođenja krivičnog postupka ili zaštite bezbednosti Republike Srbije, na način predviđen zakonom." Vredi pomenuti i naredni, 42. član, koji se bavi zaštitom podataka o ličnosti: „Zajemčena je zaštita podataka o ličnosti. Prikupljanje, držanje, obrada i korišćenje podataka o ličnosti uređuju se zakonom. Zabranjena je i kažnjiva upotreba podataka o ličnosti izvan svrhe za koju su prikupljeni, u skladu sa zakonom, osim za potrebe vođenja krivičnog postupka ili zaštite bezbednosti Republike Srbije, na način predviđen zakonom. Svako ima pravo da bude obavešten o prikupljenim podacima o svojoj ličnosti, u skladu sa zakonom, i pravo na sudsku zaštitu zbog njihove zloupotrebe."

Sasvim je jasno da je privatnost komunikacije jedno od osnovnih ljudskih prava i da se ono proteže i na savremene vidove elektronske komunikacije bez obzira na tehnologiju i nosač podataka o komunikaciji. Sud je instanca na koju se poziva Ustav kada pojašnjava eventualne moguće izuzetke. Ovi izuzeci su dalje regulisani različitim zakonima; sva takva rešenja biće posebno analizirana.

Izvedeni zaključci značajni su za analizu pre svega zbog toga što bi valjalo objasniti posledice kršenja prava na privatnost komunikacije, kao i situacije u kojima je takvo kršenje dozvoljeno radi zaštite nekog pretežnijeg interesa, kako je definisano u članu 8. EKLJP.

Zakonik o krivičnom postupku[6] (u daljem tekstu: ZKP) presretanje komunikacije podvodi pod posebne dokazne radnje, koje se mogu primeniti samo za određena (najteža) krivična dela iz člana 162. ZKP-a, a među kojima sasvim logično nema krivičnih dela koja bi se mogla povezati sa kršenjem autorskih prava. Osim niza preduslova koji moraju biti ispunjeni, na osnovu čl. 166. do 170. ZKP-a, sasvim je izvesno da se tajni nadzor komunikacije može vršiti samo po odluci suda, na zahtev javnog tužilaštva, a da ga sprovode isključivo policija, Bezbednosno-informativna agencija ili Vojnobezbednosna agencija. Ovi podaci su tajni i može ih upotrebiti isključivo javno tužilaštvo u krivičnom postupku. Takođe, ZKP poznaje i pretraživanje računarskih podataka kao posebnu dokaznu radnju. Na osnovu čl. 178. do 180. ZKP-a, jedino je sud nadležan da odredi takvu meru, na osnovu obrazloženog predloga javnog tužioca (uz važenje svih pomenutih prethodnih ograničenja, uključujući i ono iz člana 162). ZKP, dakle, jasno postavlja granicu razlikovanja između zakonitog i nezakonitog presretanja podataka, koje definiše pomenuti član 3. KVTK-a.

6 Zakonik o krivičnom postupku, *Sl. glasnik RS*, br. 72/11, 101/11, 121/12.

Krivični zakonik[7] (u daljem tekstu: KZ) za potrebe analize dvostruko je značajan. Najpre, u članu 112. tačka 27. elektronska komunikacija poistovećuje se sa svakim drugim oblikom zaštićene privatne komunikacije građana: „Spis, pismo, pošiljka i dokument mogu biti i u elektronskom obliku." Imajući ovu odredbu u vidu, sasvim je ispravno tumačiti član 142. KZ-a (*Povreda tajnosti pisma i drugih pošiljki*) kao način zaštite privatne elektronske komunikacije: „(1) Ko neovlašćeno otvori tuđe pismo, telegram ili kakvo drugo zatvoreno pismeno ili pošiljku ili na drugi način povredi njihovu tajnost ili ko neovlašćeno zadrži, prikrije, uništi ili drugom preda tuđe pismo, telegram ili drugu pošiljku ili ko povredi tajnost elektronske pošte ili drugog sredstva za telekomunikaciju, kazniće se novčanom kaznom ili zatvorom do dve godine. (2) Kaznom iz stava 1. ovog člana kazniće se i ko saopšti drugom sadržinu koju je saznao povredom tajnosti tuđeg pisma, telegrama ili kakvog drugog zatvorenog pismena ili pošiljke ili se tom sadržinom posluži. (3) Ako delo iz st. 1. i 2. ovog člana učini službeno lice u vršenju službe, kazniće se zatvorom od šest meseci do tri godine." Komunikacija je, dakle, nepovrediva, osim u slučajevima predviđenim ZKP-om, kako je već izloženo. Sledeći, 143. član KZ-a inkriminiše i neovlašćeno prisluškivanje i snimanje: „(1) Ko posebnim uređajima neovlašćeno prisluškuje ili snima razgovor, izjavu ili kakvo saopštenje koji mu nisu namenjeni, kazniće se novčanom kaznom ili zatvorom od tri meseca do tri godine. (2) Kaznom iz stava 1. ovog člana kazniće se i ko omogući nepozvanom licu da se upozna sa razgovorom, izjavom ili saopštenjem koji su neovlašćeno prisluškivani, odnosno tonski snimani. (3) Ako je delo iz st. 1. i 2. ovog člana učinilo službeno lice u vršenju službe, kazniće se zatvorom od šest meseci do pet godina." Svako snimanje, presretanje, prisluškivanje ili bilo kakvo drugo otkrivanje elektronske komunikacije koje je neovlašćeno (protivno odredbama ZKP-a) predstavljaće krivično delo.

Kao što će biti jasnije u nastavku teksta, od značaja je i pitanje pravnog statusa sekundarnih podataka, koji ne predstavljaju sadržinu komunikacije već se vezuju za nju – npr. nepovredivost sadržine pisma se odnosi na tekst pisma, ali šta se dešava sa adresom pošiljaoca i primaoca, da li je i ona zaštićena na neki način? Kada se govori o elektronskim komunikacijama, ustaljeno je mišljenje da su u pitanju privatni podaci koji mogu (moraju) biti poznati samo onim osobama kojima ih je sam nosilac podataka otkrio, i to za određenu svrhu (u našem primeru, to bi bila poštanska služba koja je dužna da, po nalogu pošiljaoca i nakon plaćene naknade za izvršenje usluge, pismo dostavi primaocu). Kada je reč o elek-

7 Krivični zakonik, *Sl. glasnik RS*, br. 85/05, 88/05 – ispr., 107/05 – ispr., 72/09, 111/09, 121/12.

tronskim komunikacijama, podaci koji nastaju povodom tih komunikacija smatraju se podacima o ličnosti. Na osnovu njih se npr. mogu otkriti detalji iz ličnog života korisnika interneta (npr. na osnovu IP adrese se može otkriti identitet i fizička – zemaljska – adresa pretplatnika). Podaci o ličnosti se nalaze u posebnom pravnom režimu koji je utvrđen Zakonom o zaštiti podataka o ličnosti[8] (u daljem tekstu: ZZPL). Prema članu 3. stav 1. tačka 1. ZZPL-a, „podatak o ličnosti je svaka informacija koja se odnosi na fizičko lice, bez obzira na oblik u kome je izražena i na nosač informacije (papir, traka, film, elektronski medij i sl.), po čijem nalogu, u čije ime, odnosno za čiji račun je informacija pohranjena, datum nastanka informacije, mesto pohranjivanja informacije, način saznavanja informacije (neposredno, putem slušanja, gledanja i sl., odnosno posredno, putem uvida u dokument u kojem je informacija sadržana i sl.), ili bez obzira na drugo svojstvo informacije". Od izuzetne je važnosti činjenica da je fizičko lice na koje se podatak odnosi jedino ovlašćeno da odredi na koji način će se podatak prikupiti, čuvati, *upotrebiti*, zakonskom terminologijom „obraditi": Obrada nije dozvoljena ako: 1) fizičko lice nije dalo pristanak za obradu, odnosno ako se obrada vrši bez zakonskog ovlašćenja; 2) se vrši u svrhu različitu od one za koju je određena, bez obzira da li se vrši na osnovu pristanka lica ili zakonskog ovlašćenja za obradu bez pristanka; 3) svrha obrade nije jasno određena, ako je izmenjena, nedozvoljena ili već ostvarena; 4) je lice na koje se podaci odnose određeno ili odredivo i nakon što se ostvari svrha obrade; 5) je način obrade nedozvoljen; 6) je podatak koji se obrađuje nepotreban ili nepodesan za ostvarenje svrhe obrade; 7) su broj ili vrsta podataka koji se obrađuju nesrazmerni svrsi obrade; 8) je podatak neistinit i nepotpun, odnosno kada nije zasnovan na verodostojnom izvoru ili je zastareo." (član 8. ZZPL). Sve ovo se može primeniti i na podatke koji nastanu korišćenjem interneta od strane bilo kojeg pojedinca u Srbiji. Samo prikupljanje podataka je regulisano članom 14. ZZPL-a i ugovor između internet operatora i korisnika se može smatrati validnim osnovom. Korisnik, međutim, ovim ugovorom pristaje da se podaci o njegovom internet saobraćaju i elektronskoj komunikaciji preko interneta uopšte mogu prikupljati, obrađivati i upotrebiti samo u određene svrhe, ostvarivanja komunikacije i svih prava koje korisnik prema tom ugovornom odnosu ima. Pri tome, valja imati na umu i to da podaci koji nastanu elektronskom komunikacijom korisnika interneta sasvim sigurno ne potpadaju pod izuzetke iz čl. 5. i 12. ZZPL-a. Ostaje, dakle, konstatacija da je jedini validni organ koji može naložiti uvid u podatke, kao i bilo kakav oblik presretanja elektronskih komunikacija – nadležni sud Republike Srbije.

8 Zakon o zaštiti podataka o ličnosti, *Sl. glasnik RS*, br. 97/08, 104/09 – dr. zakon.

2. ZAKON O ELEKTRONSKIM KOMUNIKACIJAMA I ZAKON O AUTORSKOM I SRODNIM PRAVIMA

Ako su standardi zaštite prava na privatnost komunikacije građana Srbije kao i zaštite njihovih ličnih podataka postavljeni kako je prethodno opisano, u tom kontekstu bi valjalo analizirati odredbe o tome kakav je položaj internet operatora u sistemu elektronskih komunikacija, kao i nosilaca autorskih prava koji smatraju da su njihovi interesi ugroženi, odnosno povređeni.

Prema Zakonu o elektronskim komunikacijama[9] (u daljem tekstu: ZEK), opšti uslovi za obavljanje delatnosti elektronskih komunikacija pretpostavljaju, između ostalog, da operatori imaju zadatak da primene mere za sprečavanje i suzbijanje zloupotreba i prevara u vezi sa korišćenjem elektronskih komunikacionih mreža i usluga, ali i da imaju dužnost zaštite podataka o ličnosti i privatnosti u oblasti elektronskih komunikacija, u skladu sa odredbama tog zakona i zakona kojim se uređuje zaštita podataka o ličnosti.[10] Upravo ovlašćenje da se primene mere za sprečavanje i suzbijanje zloupotreba i prevara jeste ključna tačka na koju se operatori pozivaju prilikom izvršavanja „naloga" koje su dobili od nosilaca autorskih prava. Ova ovlašćenja ipak nisu bliže definisana ZEK-om, kao ni drugim aktima koji su na osnovu ovog zakona doneti. Pravilnik o opštim uslovima za obavljanje delatnosti elektronskih komunikacija po režimu opšteg ovlašćenja, koji je donela Republička agencija za elektronske komunikacije 27. maja 2011. godine (u daljem tekstu: Pravilnik), dalje razrađuje sve opšte uslove koji su navedeni pomenutim članom 37. ZEK-a. Međutim, kada je reč o ovlašćenjima koja se odnose na sprečavanje i suzbijanje zloupotreba i prevara, u Pravilniku jednostavno stoji ponovljena formulacija iz ZEK-a: „Operator je dužan da, u skladu sa propisima, primeni odgovarajuće tehničke i druge mere, u cilju sprečavanja zloupotreba i prevara u vezi sa korišćenjem elektronskih komunikacionih mreža i usluga." (član 32). Koje su to mere, ostaje nepoznato. Čini se da su ključne reči u ovoj odredbi „u skladu sa propisima", tj. onako kako je regulisano drugim zakonskim aktima (uključujući i pomenute čl. 178. do 180. ZKP-a). U nedostatku razrade ove odredbe, izuzetno je korisno osvrnuti se na član 31. Pravilnika, koji se odnosi na zaštitu podataka o ličnosti korisnika, kao i na presretanje elektronskih komunikacija: „Presretanje elektronskih komunikacija kojima se otkriva sadržaj komunikacije nije dopušteno bez pristanka korisnika, osim na određeno vreme i na osnovu odluke suda, ako je to neophodno radi vođenja krivičnog postupka ili zaštite bezbednosti

9 Zakon o elektronskim komunikacijama, *Sl. glasnik RS*, br. 44/10.

10 Član 37. stav 2. tač. 14. i 15. Zakona o elektronskim komunikacijama.

Republike Srbije, na način predviđen zakonom." Ova odredba praktično ponavlja ono što je već regulisano ZKP-om, ali je važna zbog toga što se direktno odnosi na elektronske komunikacije i postupanja operatora. Stav 3. istog člana dalje ograničava moguće delovanje operatora: „Korišćenje elektronskih komunikacionih mreža i usluga radi čuvanja ili pristupanja podacima pohranjenim u terminalnoj opremi pretplatnika ili korisnika, dozvoljeno je pod uslovom da je pretplatniku ili korisniku dato jasno i potpuno obaveštenje o svrsi prikupljanja i obrade podataka, u skladu sa zakonom kojim se uređuje zaštita podataka o ličnosti, kao i da mu je pružena prilika da takvu obradu odbije."

Konačno, Zakon o autorskom i srodnim pravima[11] (u daljem tekstu: ZASP) predviđa jasnu proceduru kojom nosioci autorskih prava mogu zatražiti zaštitu ukoliko smatraju da se njihova prava krše delovanjem korisnika interneta. Članovima 210. do 212. ZASP-a opisana je procedura koja ima za posledicu efikasnu zaštitu autorskih prava: „Na zahtev nosioca prava koji učini verovatnim da je njegovo autorsko ili srodno pravo povređeno, ili da će biti povređeno, sud može da odredi privremenu meru oduzimanja ili isključenja iz prometa predmeta kojima se vrši povreda, odnosno meru zabrane nastavljanja započetih radnji kojima bi se mogla izvršiti povreda. Na zahtev nosioca prava koji učini verovatnim da je njegovo autorsko ili srodno pravo povređeno, odnosno da može doći do povrede tog prava ili da postoji opasnost od nastanka neotklonjive štete, kao i da postoji opravdana bojazan da će dokazi o tome biti uništeni ili da će ih kasnije biti nemoguće pribaviti, sud može odrediti meru obezbeđenja dokaza bez prethodnog obaveštenja ili saslušanja lica od koga se dokazi prikupljaju. Obezbeđenjem dokaza, u smislu stava 1. ovog člana, smatra se pregled prostorija, knjiga, dokumenata, baza podataka i dr., kao i zaplena dokumenata i predmeta kojima je povreda izvršena, ispitivanje svedoka i veštaka. Licu od koga se dokazi prikupljaju, sudsko rešenje o određivanju mere obezbeđenja dokaza biće uručeno u trenutku prikupljanja dokaza, a odsutnom licu čim to postane moguće. Privremene mere, odnosno obezbeđenje dokaza iz čl. 210. i 211. ovog zakona mogu se tražiti i pre podnošenja tužbe, pod uslovom da se tužba podnese u roku od 30 dana od dana donošenja rešenja o određivanju privremene mere, odnosno rešenja o određivanju obezbeđenja dokaza. U slučaju da se tužba ne podnese u roku od 30 dana od dana donošenja rešenja o određivanju privremene mere, odnosno rešenja o određivanju obezbeđenja dokaza, primenjuju se odredbe zakona kojim se uređuje izvršni postupak. Žalba protiv rešenja kojim je sud odredio privremenu meru iz člana 210. ovog zakona ne odlaže izvršenje rešenja." Suština ovog rešenja jeste da se nosilac autorskih prava

11 Zakon o autorskom i srodnim pravima, *Sl. glasnik RS*, br. 104/09, 99/11, 119/12.

koji se smatra ugroženim *može obratiti sudu za izricanje privremene mere*. Nosilac mora učiniti verovatnim (dakle, ne mora dokazati) da je njegovo pravo povređeno, ali mora i svoju ozbiljnost pokazati podnošenjem tužbe protiv prekršioca autorskih prava, u određenom roku. Sud će izreći meru obezbeđenja i prikupljanja dokaza, koja uključuje i podatke o saobraćaju koji se nalaze kod internet operatora.

3. „NALOZI" NOSILACA AUTORSKIH PRAVA I NEDOZVOLJENA PRAKSA INTERNET OPERATORA

Nakon što je uspostavljen pravni okvir u kojem tri strane (operatori, nosioci autorskih prava i korisnici) deluju u Republici Srbiji, valjalo bi analizirati njihova postupanja.

Internet operatori prihvataju zahteve nosilaca autorskih prava za identifikacijom korisnika, utvrđuju njegov identitet i šalju „upozorenje" da je sa njihovih naloga primećena neka „nelegalna" aktivnost. Da li je neka aktivnost nelegalna ili nije, može da proceni samo sud. Međutim, ovo nije osnovni problem u ovakvoj situaciji. Postavlja se pitanje zašto operatori pristaju da izvrše „naloge" nosilaca autorskih prava kada je sasvim očigledno reč o privatnim licima koja takve zahteve pred njih ne mogu postaviti? Postoje dve situacije koje se mogu smatrati relevantnim u situaciji kada operator dobije obaveštenje nosioca autorskog prava da korisnik krši njegova autorska prava i izvršava „nalog" da se korisnik opomene da su njegova postupanja nezakonita i da će trpeti sankcije ukoliko nastavi sa takvom praksom. Ove situacije se razlikuju u pravnoj kvalifikaciji, u zavisnosti od činjenice kako su nosioci autorskih prava došli do podataka o kršenju autorskih prava, ali su obe apsolutno nezakonite:

- Kada se na osnovu „naloga" proverava identitet korisnika interneta koji navodno krši autorska prava, i ti podaci se dostavljaju nosiocu autorskih prava kako bi ovaj dalje odlučio da li će pokrenuti odgovarajući sudski postupak ili na drugi način pokušati da zaštiti svoja prava. Ovo je očigledno nezakonito delovanje operatora. Podaci o korisniku su zaštićeni i njih može tražiti samo sud, odnosno nadležan državni organ na osnovu sudskog naloga. Nosilac autorskih prava ih može tražiti takođe samo putem sudskog naloga, i to ukoliko prethodno pokrene parnični postupak protiv počinioca kako bi tražio naknadu štete. Ovo je regulisano već citiranim članovima Zakona o autorskom i srodnim pravima.
- Na osnovu „naloga" nosioca autorskih prava, operator saznaje identitet korisnika i upućuje mu „opomenu". Glavni argument

onih koji tvrde da je ovakvo ponašanje operatora sasvim legalno, jeste da se pri tome ne otkriva identitet korisnika nosiocu autorskih prava. Postoji ipak samo „privid legalnosti", moguć ako se posmatra isključivo privatnost korisnika u smislu sadržine komunikacije koju vrši. Kršenje zakona je, međutim, evidentno kada je reč o zaštiti podataka o ličnosti. Ova situacija biće detaljnije analizirana u daljem tekstu.

Problemi koji se mogu uočiti u ovakvoj situaciji dovode do nekoliko zaključaka.

Najpre, nosilac autorskih prava *nema zakonski osnov* da naloži bilo kakvu radnju operatorima. Jedina mogućnost koja mu stoji na raspolaganju jeste obraćanje sudu, i to na osnovu već pomenutih članova Zakona o autorskom i srodnim pravima. Potom, operatori ne mogu, kada dobiju obaveštenje nosilaca autorskih prava o kršenju autorskih prava, znati da podaci u njemu odgovaraju realnosti. Štaviše, ne mogu znati ni da li su prikupljeni izvršenjem nekog krivičnog dela, direktnim presretanjem komunikacije korisnika. Ne mogu znati ni da li je korisnik o kome je reč uopšte izvršio bilo šta što mu se stavlja na teret, čak i ako se ustanovi da je zaista sa određene IP adrese u određeno vreme obavljao aktivnost koja je navedena.[12] Sadržina te komunikacije korisnika nikada ne može biti predmet samostalne „istrage" operatora.

Operatori su se u odgovorima na inicijalno obraćanje povodom slanja „opomena" korisnicima uglavnom pozivali na član 37. stav 2. tačka 15. Zakona o elektronskim komunikacijama, koji određuje kao jednu od delatnosti operatora i primenu mera za sprečavanje i suzbijanje zloupotreba i prevara u vezi sa korišćenjem elektronskih komunikacionih mreža i usluga; pri tome se očigledno zanemaruje već citirana tačka 14. istog stava, koja uvodi obavezu zaštite podataka o ličnosti i privatnosti u oblasti elektronskih komunikacija, u skladu sa odredbama tog zakona i zakona kojim se uređuje zaštita podataka o ličnosti. Već je rečeno da je Pravilnik koji bi morao da razradi ove obaveze operatora izuzetno škrt kada je reč o primeni mera za sprečavanje i suzbijanje zloupotreba i prevara, ali da se iz

12 Otuda se IP adresa korisnika ne može smatrati isključivim dokazom na sudu. Ona samo služi identifikaciji fizičke lokacije računara sa kojeg je izvršeno krivično delo, odnosno sa kojeg su prekršena autorska prava. Na osnovu te informacije se saznaju adresa i identitet korisnika, odnosno pretplatnika i dobija nalog suda da se izvrši uvid u prostorije i računar koji se na toj adresi nalaze. Tek ukoliko se uvidom u sadržinu računara otkrije nedozvoljeni sadržaj, to može predstavljati dokaz da su prava prekršena. Ni to, međutim, ne znači da je pretplatnik/korisnik izvršilac tog dela; u pitanju može biti računar koji koristi više lica, računar u internet kafeu, računar koji se nalazi u poslovnim prostorijama i nije posebno zaštićen ili je zaštićen a pristup tom računaru ima više zaposlenih itd.

samog teksta i konteksta te odredbe jasno vidi da se ne može preduzimati nijedna invazivna mera u privatnost korisnika, bez odluke suda. Iz ovih odredaba nikako ne proističe pravo operatora da „uparuju" podatke koje dobiju od nosilaca autorskih prava sa tehničkim (zadržanim) podacima i na taj način dođu do fizičke adrese i identiteta korisnika. Još manje iz navedenih odredaba proističe da imaju ovlašćenje da u ime nosilaca autorskih prava šalju pisma „opomene". Citirane odredbe definitivno upućuju na zaključak da se prema podacima koje operatori poseduju o korisnicima mora postupati kao prema podacima o ličnosti. Prema ZZPL, podatkom o ličnosti se *smatra svaka informacija koja se odnosi na fizičko lice, bez obzira na oblik u kome je izražena i na nosač informacije* (papir, traka, film, elektronski medij i sl.), po čijem nalogu, u čije ime, odnosno za čiji račun je informacija pohranjena, datum nastanka informacije, mesto pohranjivanja informacije, način saznavanja informacije (neposredno, putem slušanja, gledanja i sl., odnosno posredno, putem uvida u dokument u kojem je informacija sadržana i sl.) ili bez obzira na drugo svojstvo informacije. Dakle, podaci koji se pohranjuju o aktivnostima korisnika na internetu pripadaju kategoriji podataka o ličnosti. „Ukrštanje" podataka o IP adresi i ličnih podataka korisnika mora se posmatrati kao njegova identifikacija i korišćenje podataka koje je ostavio protivno svrsi u koju su prikupljeni, samim tim se takvo ponašanje mora okarakterisati kao protivzakonito.

U skladu sa prethodnom analizom, jasno je da se *svako postupanje* operatora u ovakvim slučajevima može odrediti kao protivno pravu i kršenje prava na privatnost i zaštitu podataka o ličnosti korisnika. Sa pravno-tehničke strane, međutim, može biti zanimljivo razmotriti i situacije u kojima nosioci autorskih prava dolaze do podataka da je neko njihovo autorsko pravo prekršeno kroz elektronsku komunikaciju korisnika interneta,[13] a u direktnoj vezi sa tim analizirati i kako operatori mogu izvršiti uvid u tzv. zadržane podatke o korisnicima i identifikovati ih na osnovu podataka koje su dobili od nosilaca autorskih prava.[14] Ovo razmatranje je relevantno da bi se uočilo kako sve nosioci autorskih prava mogu postupati i koje od tih opcija predstavljaju legalno ponašanje u cilju zaštite zakonskih prava koja poseduju.

13 U daljem tekstu su navedeni slučajevi prema analizi koja je objavljena na internet adresi: http://piratska.org/kako-do-podataka-korisnika-torenta-5-slucajeva/, pristupljeno 20.04.2013. Analiza je sprovedena u okviru već pomenutog šireg pravno-tehničkog istraživanja ovakvog postupanja (videti *supra*, fusnota 1), u kojem je učestvovao i autor (http://piratska.org/privatnost-postupanja-internet-provajdera/, 29.04.2013); njeni tehnički zaključci su preuzeti u ovom radu.

14 Prema članu 84. ZKP-a, svaki dokaz koji je pribavljen suprotno zakonu ne može se koristiti u krivičnom postupku. Kada je reč o korišćenju ovih dokaza u parničnom postupku koji nosioci autorskih prava mogu pokrenuti prema ZASP-u, izričita zakonska zabrana ne postoji a stručna mišljenja i sudska praksa su podeljeni.

Jedini legalan način da se dođe do podataka o korisnicima jeste na osnovu odluke suda. Sud, na osnovu svojih ovlašćenja i diskrecione procene, nalaže prikupljanje dokaza u krivičnom ali i parničnom postupku. Međutim, da bi se dobila odluka suda na zahtev nosioca autorskog prava, ovaj prethodno (ili najkasnije u roku od 30 dana od izdavanja naloga) mora pokrenuti parnicu, odnosno tužiti korisnika zbog kršenja autorskih prava.[15]

Do podataka o kršenju autorskih prava nosioci autorskih prava mogu doći i na druge specifične načine. Jedan od njih je međunarodna saradnja sa određenim državnim ili drugim ovlašćenim institucijama, odnosno organizacijama. Naime, ukoliko neki ovlašćeni organ strane zemlje dolazi na legalan način (prema pravu te zemlje) do određenih informacija koje upućuju na kršenje autorskih prava i prosleđuje ih nosiocima autorskih prava, isti su legalno došli do podataka na osnovu kojih mogu učiniti verovatnim da se autorska prava krše putem elektronske komunikacije. Identična situacija će biti i kada takve informacije dobiju od domaćih službi koje su ovlašćene za njihovo prikupljanje na zakonit način (npr. od policije koja vrši istragu i presreće komunikaciju po nalogu suda). Oni, međutim, iz razloga koji su već pojašnjeni, sa tim podacima ne mogu „naložiti" operatorima da identifikuju korisnika, već se jedino mogu obratiti sudu, prema već citiranim članovima ZASP-a ili ih proslediti javnom tužilaštvu kako bi se izvršila istraga o eventualnim izvršenim krivičnim delima. Ukoliko strani državni organ prosledi podatke kroz kanale međudržavne saradnje u krivičnim stvarima srpskom tužilaštvu za VTK (to se u praksi dešava relativno često), tužilaštvo procenjuje da li ima elemenata krivičnog dela i traži sudski nalog – time se analiza svodi na prvi opisani slučaj.

Pojašnjeni su, dakle, legalni načini da nosioci autorskih prava dođu do odgovarajućih podataka. Sve ostale aktivnosti se mogu smatrati suprotnim zakonu. Najčešći slučajevi su da *nosioci autorskih prava skidaju sadržaj postojećih nelegalnih torenata i otkrivaju IP adrese onih koji to isto čine* ili da *provajderi za račun nosilaca autorskih prava vrše kontinuirano presretanje podataka korisnika*. U prvoj situaciji nosioci autorskih prava postupaju nelegalno, kao i internet operatori ako postupe po njihovim zahtevima. Kao što je već objašnjeno, IP adresa koju korisnik koristi predstavlja zaštićeni podatak o ličnosti. Prilikom stupanja u ugovorni odnos sa internet operatorom, svaki od korisnika je pristao na određene usluge, samim tim i na neminovnu produkciju podataka o ličnosti koji će nastati pri realizaciji tog ugovora, odnosno usluga na koje se pretplatio – time ograničava internet operatora na koji način takve novonastale podatke o

15 Već citirani čl. 211. i 212. ZASP-a. Više o građanskopravnoj zaštiti autorskog prava u: Damnjanović, K., Marić, V., 2012, *Intelektualna svojina*, Beograd, str. 103–107.

ličnosti može koristiti. Po istoj analogiji, kada stupa u daunloud nekog torenta, koji je po prirodi javni fajl, korisnik ne daje saglasnost da se njegova IP adresa javno vidi, da mogu da se prikupljaju podaci vezani za njegovu aktivnost, i da ti podaci mogu biti dostupni svakome. To što tehnička priroda razmene elektronskih fajlova putem torenata omogućava da svako ko se bavi tom radnjom istovremeno vidi IP adrese nekih od korisnika koji rade to isto u istom trenutku, ne znači da postoji pristanak tih korisnika da se takvi podaci koriste za bilo koju svrhu osim one na koju su izričito pristali, dakle razmene fajlova.[16] Dakle, korisnicima je i na ovaj način moguće povrediti pravo na zaštitu podataka o ličnosti.

U drugoj navedenoj situaciji, reč je o nelegalnom prisluškivanju koje konstituiše krivična dela iz čl. 142. i 143. KZ-a (videti *supra*, pod 1). Ono što bi valjalo napomenuti, jeste da su u ovom slučaju i nosioci autorskih prava i internet operatori saučesnici u izvršenju ovih krivičnih dela, kao i da korisnici imaju pravo na zaštitu, odnosno obraćanje policiji i/ili nadležnom javnom tužilaštvu.

Konačno, primećeni su i neki drugi načini na koje se može doći do podataka o nelegalnom daunloudu i pohranjivanju autorskih dela. Kompanije koje su nosioci autorskih prava ponekad pribegavaju „navođenju" korisnika interneta na nedozvoljene radnje, i to najčešće tako što postavljaju svoje torent servere i prate ko skida sadržaj. Ovaj, u praksi primenjiv i popularan, scenario prikupljanja podataka ima veliku manu – prema ZASP-u autor, odnosno nosilac autorskog prava ima pravo objavljivanja dela – pravo da odredi način na koji će se njegovo delo objaviti (član 16). Član 20. stav 1. ZASP-a je takođe eksplicitan kada govori o pravu na umnožavanje: *Autor ima isključivo pravo da drugome dozvoli ili zabrani beleženje i umnožavanje svog dela u celosti ili delimično, bilo kojim sredstvima, u bilo kom obliku, na bilo koji trajni ili privremeni, posredni ili neposredni način*. Ako autor reši da želi da podeli svoje delo sa internet zajednicom besplatno (stavljanje torenta sa tim delom se svodi na način njegovog objavljivanja ili umnožavanja), korisnici interneta koji daunlouduju to delo *ne krše nijedan propis*. Zbog toga je izlišno govoriti da će svaka naredna akcija nosioca autorskih prava u pogledu sprečavanja takvih aktivnosti ili otkrivanja identiteta korisnika koji koriste „velikodušnost" autora biti nelegalna.

Trebalo bi u ovom delu analize napomenuti i tendenciju da standardi zaštite podataka o ličnosti koji nastaju kao proizvod elektronske komu-

16 Pri tome bi valjalo napomenuti da razmena fajlova putem torenata nikako ne mora da znači da je u pitanju nelegalna aktivnost ili bilo kakvo kršenje autorskih prava; putem torenata se može deliti svaki materijal, uključujući i onaj na kome ne postoje autorska prava ili na kome postoje posebne licence koje omogućavaju deljenje sadržaja autorskog dela.

nikacije evoluiraju, budući da su u potencijalnom „odmeravanju snaga" sa kršenjem autorskih prava očigledno označeni kao pretežniji interes.[17] Prihvatanje ovakvog koncepta omogućilo bi operatorima oslobođenje od obaveze o prikupljanju zadržanih podataka, kao i daleko efikasniji mehanizam zaštite podataka o ličnosti – jednostavno, oni se ne bi nigde pohranjivali i bili bi privremenog karaktera, tj. samo dok pretplatnik koristi dinamičku IP adresu koja mu je u tom trenutku dodeljena. Ovo naravno otvara pitanje dokazivanja kršenja autorskih prava u sudskom postupku, koje bi na ovaj način bilo dodatno otežano budući da podaci o aktivnostima korisnika na internetu jednostavno ne bi postojali (uvek bi postojala mogućnost presretanja komunikacije u realnom vremenu, odnosno prisluškivanja, ali je ona sasvim ispravno predviđena kao mogućnost samo za daleko teža krivična dela od kršenja autorskih prava i u svakom slučaju bi pomenuti test pretežnosti interesa imao isti rezultat u korist privatnosti korisnika).

4. KAKO ZAŠTITITI AUTORSKA PRAVA NA INTERNETU?

Čini se da nosioci autorskih prava koji se obraćaju za (nelegalnu) asistenciju internet operatorima, po pravilu velike kompanije koje angažuju određene agencije ili advokatske kancelarije u Republici Srbiji kako bi zastupale njihove interese, imaju sasvim pogrešnu percepciju pravnog sistema u kojem deluju. Na osnovu opisanih metoda postupanja, koji se očigledno kose sa važećim propisima, utisak je da svrha njihovog delovanja nije u konačnom kažnjavanju onih koji krše autorska prava već u njihovom *zastrašivanju*. Ovo je naročito evidentno kroz analizu potencijalnog pokretanja krivičnog postupka protiv prekršilaca autorskih prava – nijedan od prikupljenih podataka ne bi mogao biti iskorišćen kao dokaz na sudu. Ni u parničnom postupku ne bi postojala značajnija šansa za uspeh; već je rečeno da dokazi koji se na ovaj način prikupe nisu zakoniti, nisu podobni da se izvede konačan zaključak o postojanju kršenja a još manje o počiniocu, a na njima se nikako ne može zasnivati odluka suda, ukoliko nisu potkrepljeni drugim, na zakonit način pribavljenim dokazima.

Ovakva praksa je, naravno, nedozvoljena. Postoji nekoliko stvari koje se mogu preporučiti akterima ovih odnosa. Naime, u opisanom problemu postoje tri strane: nosioci autorskih prava, internet operatori i korisnici/

17 U prilog ovoj tezi jeste i presuda Nemačkog višeg regionalnog suda u postupku koji su pokrenuli nosioci autorskih prava protiv Vodafona, mobilnog i internet operatora koji ne skladišti zadržane podatke o svojim korisnicima koji imaju tzv. dinamičke IP adrese: *ISPs Cannot Be Forced To Store Data on File-Sharers, Court Rules,* (http://torrentfreak.com/isps-cannot-be-forced-to-store-data-on-file-sharers-court-rules-130326/?utm_ source=dlvr.it&utm_medium=twitter, 20.04.2013).

pretplatnici interneta. Analiza uglavnom sagledava pravnu situaciju iz ugla onih faktički najslabijih – korisnika interneta. Internet operatorima je najlakše da, pod pritiskom advokatskih kancelarija i različitih agencija, krenu linijom manjeg otpora i krše pravo na privatnost svojih korisnika, od kojih oni opstaju na tržištu. Zato cilj ove analize mora biti da se skrene pažnja na problem, ali i da se skrene pažnja operatorima da je njihova praksa nezakonita i da ih država može zaštititi ako odbiju nelegalne aktivnosti sa kojima su suočeni.

Kako, međutim, zadovoljiti potrebu za pravnom zaštitom autora i nosilaca autorskih prava, koja realno postoji? Oni su zaštićeni u pravnom sistemu na već opisane načine, ali nikako ne smeju biti zaboravljeni. Pre svega, čini se da je njihova zaštita nedovoljna. To je najverovatnije i uzrok zašto posežu za merama koje se nalaze na ivici prihvatljivih ili spadaju u potpuno nezakonite, kao što je zastrašivanje korisnika – pojedinaca, čak i kada nije realno da će takve mere imati nekog efekta na korisnike. Parnični postupak protiv pojedinaca koji su skinuli sa interneta samo jedno ili nekoliko autorskih dela nije celishodan, kako zbog dugog i neizvesnog postupka dokazivanja, tako i zbog realno neznatne štete koja je na ovaj način uzrokovana nosiocu autorskog prava.[18]

Zbog svega navedenog, predlozi mera Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti, kojima se između ostalog zahteva i efikasnija sudska zaštita nosilaca autorskih prava i potpunija zaštita prava na privatnost korisnika interneta, deluju kao dobar početak za iznalaženje kvalitetnog normativnog odgovora na sve postojeće zahteve i interese triju strana.[19] U nizu preporuka, koji je nazvan „Paket 14 mera", naročito bi trebalo obratiti pažnju na one koje se odnose na: primenu efikasnijih organizacionih mera i IT rešenja koja ubrzavaju prethodnu sudsku kontrolu i odlučivanje o zahtevima za pristup komunikacijama i podacima o komunikacijama; ujedinjavanje postojećih paralelnih tehničkih mogućnosti različitih agencija i policije u jednu nacionalnu agenciju koja, kao provajder, pruža tehničke usluge neophodne za presretanje komunikacija i drugih signala svim autorizovanim korisnicima; ujedinjenju procedura prema pružaocima elektronskih komunikacija, kao i njihovih obaveza.

18 Ovo je u principu i najveći problem nosilaca autorskih prava, jer njihova šteta u pojedinačnim slučajevima može da se smatra neznatnom, ali omasovljeno kršenje autorskih prava dovodi do daleko veće ukupne štete. Ovo je, međutim, samo još jedan od razloga zašto se nosioci autorskih prava moraju okrenuti sprečavanju organizovanog kršenja autorskih prava radi sticanja materijalne koristi – deljenja autorskih dela između pojedinačnih korisnika realno ne mogu da ugroze njihove interese.

19 http://www.poverenik.rs/index.php/sr/aktuelnosti/1386-konferencija-za-medije.html, 20.04.2013.

Umesto zaključnih razmatranja, može se izneti niz preporuka i ideja koje se odnose na poboljšanje kvaliteta zaštite prava na privatnost i podataka o ličnosti, ali i bolje zaštite autorskih prava:

Internet operatori moraju prestati da izvršavaju nezakonite zahteve individualnih ili kolektivnih nosilaca autorskih prava. Ukoliko dođu u posed inkriminišućih dokaza o nosiocima autorskih prava koji krše pravo na tajnost komunikacije građana Srbije, moraju se obratiti nadležnom javnom tužilaštvu, kako bi ono istražilo kako su nosioci autorskih prava došli u posed takvih informacija; tek ukoliko se utvrdi da je sve izvršeno po osnovu sudskog naloga, mogu dati tražene informacije. Ovakvo ponašanje je njihova zakonska obaveza.

Korisnici/pretplatnici interneta mogu po prijemu „upozoravajućih pisama" tražiti zaštitu od javnog tužilaštva, koje bi moralo da istraži da li je došlo do prisluškivanja elektronskih komunikacija, odnosno kako su nosioci autorskih prava došli do informacija o elektronskim komunikacijama korisnika. Kada je reč o krivičnom postupku, korisnici ne mogu biti krivično gonjeni zbog bespravnog posedovanja autorskih dela, osim ukoliko su ona namenjena daljoj prodaji, odnosno ukoliko ih učine dostupnim drugim korisnicima interneta ili drugim licima na bilo koji način (šerovanje, narezivanje diskova, postavljanje sajtova i fajlova za nazakonitu razmenu itd.) i to jasno reguliše član 199. KZ-a.[20] Kada je, međutim, reč o

20 Član 199. KZ-a inkriminiše delo *neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava*:

„(1) Ko neovlašćeno objavi, snimi, umnoži, ili na drugi način javno saopšti u celini ili delimično autorsko delo, interpretaciju, fonogram, videogram, emisiju, računarski program ili bazu podataka, kazniće se zatvorom do tri godine. (2) Kaznom iz stava 1. ovog člana kazniće se i ko stavi u promet ili u nameri stavljanja u promet drži neovlašćeno umnožene ili neovlašćeno stavljene u promet primerke autorskog dela, interpretacije, fonograma, videograma, emisije, računarskog programa ili baze podataka. (3) Ako je delo iz st. 1. i 2. ovog člana učinjeno u nameri pribavljanja imovinske koristi za sebe ili drugog, učinilac će se kazniti zatvorom od šest meseci do pet godina. (4) Ko proizvede, uveze, stavi u promet, proda, da u zakup, reklamira u cilju prodaje ili davanja u zakup ili drži u komercijalne svrhe uređaje ili sredstva čija je osnovna ili pretežna namena uklanjanje, zaobilaženje ili osujećivanje tehnoloških mera namenjenih sprečavanju povreda autorskih i srodnih prava, ili ko takve uređaje ili sredstva koristi u cilju povrede autorskog ili srodnog prava, kazniće se novčanom kaznom ili kaznom zatvora do tri godine. (5) Predmeti iz st. 1. do 4. ovog člana oduzeće se i uništiti." Dakle, stavom 1. je kao kažnjivo određeno „javno saopštavanje" autorskog dela, u celini ili delimično, dok je stav 2. inkriminisao isključivo stavljanje u promet ili držanje u nameri stavljanja u promet primeraka autorskog dela do kojih se došlo nezakonitim putem. *Samo držanje radi lične upotrebe, kao što je skidanje i pohranjivanje filma ili muzičke numere na računaru, ne predstavlja krivično delo.* Više o ovom krivičnom delu i sudskoj praksi u Republici Srbiji: Prlja, D., Ivanović, Z., Reljanović, M., 2011, *Krivična dela visokotehnološkog kriminala*, Beograd, str. 29–39.

građanskoj odgovornosti, oni mogu biti predmet parničnog postupka, u kojem bi nosioci autorskih prava mogli da zahtevaju naknadu štete.

Nosioci autorskih prava moraju prestati sa nezakonitom praksom. Ukoliko je njihova aktivnost zakonita, moraju pribaviti sudsku odluku i postupati u skladu sa odredbama ZASP-a. *Akcije nosilaca autorskih prava moraju pre svega biti usmerene ka oštrijim i efikasnijim zakonima i procedurama prema onima koji masovno krše autorska prava i od toga ostvaruju (po pravilu, nemalu) protivpravnu imovinsku korist od toga.* Zadiranje u privatnost korisnika interneta kao pojedinca, sigurno neće rešiti problem kršenja autorskih prava, a proizvešće nove probleme svim stranama uključenim u ovaj odnos.

Nadležni državni organi koji su zakonom određeni da štite privatnost komunikacije moraju reagovati kako bi se utvrdilo ko, kako i zašto vrši pristup privatnim komunikacijama građana Srbije?[21] Takođe, jedna od važnih funkcija države jeste da dodatno zaštiti nosioce autorskih prava i omogući efikasnu proceduru zaštite autorskih prava na internetu, odnosno u elektronskim komunikacijama uopšte. Član 37. ZEK-a i član 32. Pravilnika moraju se daleko detaljnije razraditi kako ne bi postojala nedoumica koja su ovlašćenja internet operatora. Posebna preporuka se može odnositi na jasno podvajanje situacija u kojima se autorska prava krše na sistematski, organizovan način, koji po pravilu predstavlja krivično delo i vrši se radi ostvarivanja materijalne koristi počinilaca, od situacija kada je reč o individualnim korisnicima koji dele podatke, odnosno autorska dela za svoju ličnu upotrebu i bez namere da se nosiocima autorskih prava nanese šteta. Ovo je sasvim na tragu sve jačih zahteva „dekriminalizacije" pojedinih ponašanja korisnika elektronskih komunikacija i snaženja novog koncepta autorskih prava koji bi se približio realnosti neprofitnog deljenja i veće dostupnosti elektronskim putem, odnosno liberalnijih licenci za autorska dela koja se dalje mogu deliti elektronskim putem.[22]

---

21 Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti je već odreagovao na nezakonitu praksu, pokrenuvši, kao organ nadležan za nadzor nad sprovođenjem ZZPL-a, vanrednu kontrolu rada internet operatora. Više na internet adresi: http://www.poverenik.rs/index.php/sr/aktuelnosti/1550-uskoro-nadzor-nad-operatorima.html, 20.04.2013. Ovo nije prvi put da Poverenik upozorava na nedostatak zakonitosti u različitim situacijama kada se pristupa tzv. „zadržanim podacima" (http://www.poverenik.rs/index.php/sr/iz-medija/1488-intervju-rodoljub-sabic-nisu-krive-samo-sluzbe-i-policija.html, 20.04.2013).

22 Nova politika prava u sajber prostoru „trebalo bi da reafirmiše prava autora u svetu globalnih digitalnih komunikacija, ali ne bi trebalo da stvara podršku za beskonačne monopole i tehnološku diskriminaciju". Dimitrijević, P., 2010, *Pravo informacione tehnologije*, Niš, str. 286; citirano prema: Prlja, D., Ivanović, Z., Reljanović, M., 2012, *Internet pravo*, Beograd, str. 24. U tom smislu je indikativno postojanje i širenje *Creative Commons* licenci (http://creativecommons.org/, 20.04.2013), kao jednog od naj-

Literatura

1. Damnjanović K., Marić V., 2012, *Intelektualna svojina*, Beograd.
2. Dimitrijević, P., 2010, *Pravo informacione tehnologije*, Niš.
3. *ISPs Cannot Be Forced To Store Data on File-Sharers, Court Rules,* (http://torrentfreak.com/isps-cannot-be-forced-to-store-data-on-file-sharers-court-rules-130326/?utm_ source=dlvr.it&utm_medium=twitter).
4. *Kako internet provajderi u Srbiji uništavaju poverenje korisnika narušavajući privatnost,* (http://piratska.org/nekonasposmatra/).
5. Krivični zakonik, *Sl. glasnik RS,* br. 85/05, 88/05 – ispr., 107/05 – ispr., 72/09, 111/09, 121/12.
6. Lessig, L., 2004, *Free Culture*, New York.
7. Prlja, D., Ivanović, Z., Reljanović, M., 2012, *Internet pravo*, Beograd.
8. Prlja, D., Ivanović, Z., Reljanović, M., 2011, *Krivična dela visokotehnološkog kriminala*, Beograd.
9. Reljanović, M., *Privatnost: postupanja-internet-provajdera,* (http://piratska.org/privatnost-postupanja-internet-provajdera/).
10. Zakon o autorskom i srodnim pravima, *Sl. glasnik RS*, br. 104/09, 99/11 i 119/12.
11. Zakon o elektronskim komunikacijama, *Sl. glasnik RS*, br. 44/10.
12. Zakonik o krivičnom postupku, *Sl. glasnik RS*, br. 72/11, 101/11 i 121/12.
13. Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu, *Sl. glasnik RS*, br. 19/09.
14. Zakon o ratifikaciji evropske Konvencije za zaštitu ljudskih prava i osnovnih sloboda, izmenjene u skladu sa Protokolom broj 11, protokola uz Konvenciju za zaštitu ljudskih prava i osnovnih sloboda, Protokola broj 4 uz Konvenciju za zaštitu ljudskih prava i osnovnih sloboda kojim se obezbeđuju izvesna prava i slobode koji nisu uključeni u Konvenciju i Prvi protokol uz nju, Protokola broj 6 uz Konvenciju za zaštitu ljudskih prava i osnovnih sloboda o ukidanju smrtne kazne, Protokola broj 7 uz Konvenciju za zaštitu ljudskih prava i osnovnih sloboda, Protokola broj 12 uz Konvenciju za zaštitu ljudskih prava i osnovnih sloboda i Protokola broj 13 uz Konvenciju za zaštitu ljudskih prava i osnovnih sloboda o ukidanju smrtne kazne u svim okolnostima, *Sl. list SCG – Međunarodni ugovori*, br. 9/03.
15. Zakon o zaštiti podataka o ličnosti, *Sl. glasnik RS*, br. 97/08 i 104/09 – dr. zakon.
16. *Uskoro nadzor nad operatorima,* (http://poverenik.rs/index.php/yu/aktuelnosti/ 1550-uskoro-nadzor-nad-operatorima.html).
17. Ustav Republike Srbije, *Sl. glasnik RS*, br. 98/06.

značajnijih oblika novog vida regulisanja autorskih prava. O mogućnostima razvoja koncepta autorskih prava u sajber okruženju videti takođe: Lessig, L., 2004, *Free Culture*, New York.

CONDUCT OF INTERNET OPERATORS REGARDING ALLEGED COPYRIGHT INFRIGEMENT – LAW AND PRACTICE IN SERBIA

Mario Reljanović

SUMMARY

Research covers the analysis of ongoing clash of interests on three different types of legal rights: right to privacy of communication, right to protection of personal data and copyright. These three groups of rights are subjected to analysis of current legal framework in Republic of Serbia, through the prism of conflict of rights when electronic communications are being used for copyrights infringements. This is especially visible within analysis of misconduct of internet operators in Serbia who use so-called "retained data" on their subscribers in order to react to alleged copyrights infringements. Paper is based on their actions, as well as actions and rights of subscribers and copyright owners, all with the aim to point out deficiencies of the current system of legal protection which cause violations of right to privacy of communication and right to protection of personal data.

Key words: Right to privacy of electronic communication, protection of personal data, copyright, internet providers, cybercrime.

Dostavljeno Redakciji: 7. maja 2013. god.
Prihvaćeno za objavljivanje: 25. juna 2013. god.