doc. dr Mario Reljanović
docent Pravnog fakulteta
Univerziteta Union u Beogradu

UDK: 347.738(497.11)
347.78:004(497.11)

ZAŠTITA AUTORSKOG PRAVA I PRAVO NA PRIVATNOST ELEKTRONSKIH KOMUNIKACIJA U REPUBLICI SRBIJI

Rezime: *Razvoj elektronskih komunikacija pogoduje širenju neovlašćenog umnožavanja i stavljanja u promet primeraka autorskih dela na Internetu. Masovnost ove pojave poslednjih godina uzrokovala je različite reakcije nosilaca autorskog prava, od medijskih kampanja protiv piraterije, do većeg angažovanja na otkrivanju i procesuiranju osoba koje se bave nedozvoljenom distribucijom autorskih dela. U nastojanju da suzbiju ove negativne tendencije, nosioci autorskog prava u Republici Srbiji su pokrenuli praksu upućivanja pisama upozorenja protiv lica koja sa Interneta preuzimaju primerke autorskih dela koja su nezakonito učinjena dostupnim. Ova pisma upozorenja šalju se preko internet operatora. Na taj način se povređuje pravo na privatnost korisnika Interneta, budući da je sasvim izvesno da nosioci autorskog prava, odnosno njihovi zastupnici, nisu mogli na legalan način doći do podataka o sadržini elektronskih komunikacija pojedinaca. Ponašanje nosilaca autorskog prava otvara niz pitanja, među kojima su najvažnija: kako se korisnici mogu ponašati u slučaju da dobiju ovakvo pismo upozorenja, kakva je uloga internet operatora u ovakvom neobičnom odnosu, kao i na koji način se autorsko pravo na Internetu može efikasno zaštititi, bez ugrožavanja prava drugih lica? Rad se bavi iznalaženjem adekvatnih odgovora kroz analizu položaja sve tri strane u nastaloj situaciji (nosioci autorskog prava, internet operatori, korisnici) u pravnom sistemu Republike Srbije, kao i kroz analizu mogućih pravnih sredstava koja se mogu upotrebiti kako bi se nedozvoljena praksa prekinula. Takođe, ukazuje se na nove tendencije u rešavanju ovakvih problema nosilaca autorskog prava na alternativne načine, u postojećem pravnom okviru.*

Ključne reči: *Elektronske komunikacije. – Autorsko pravo. – Pravo na privatnost. – Visokotehnološki kriminal.*

1. UVODNA RAZMATRANJA

Pod elektronskim komunikacijama smatra se razmena elektronskih signala u najširem smislu. Zakon o elektronskim komunikacijama definiše pojam „komunikacije", kao „razmenu ili prenošenje informacija između određenog broja osoba putem javno dostupnih elektronskih komunikacionih usluga, izuzev informacija koje se prenose u sklopu usluga javnog emitovanja programa preko elektronskih komunikacionih mreža i koje se ne mogu po-

vezati sa određenim pretplatnikom ili korisnikom, odnosno primaocem"[1]. Zakon o privatnosti elektronskih komunikacija Sjedinjenih Američkih Država[2] pod elektronskim komunikacijama podrazumeva „svaki prenos znakova, signala, pisanog sadržaja, slike, zvuka, podataka ili drugih informacija, koje se u celini ili delimično prenose putem žičanih, radio, elektromagnetskih, fotoelektričnih ili fotooptičkih sistema." U skladu sa vremenom kada je nastala, ova definicija ne pominje računare – pod savremenim elektronskim komunikacijama se pre svega podrazumeva razmena informacija putem elektronskih transmisija između dva računara, ili slična elektronska uređaja (kao što su mobilni telefoni, kao i različite varijacije računara). Veći deo elektronske komunikacije, danas se odvija preko globalne mreže – Interneta, koji je Zakonom o elektronskim komunikacijama definisan kao „globalni elektronski komunikacioni sistem sačinjen od velikog broja međusobno povezanih računarskih mreža i uređaja, koji razmenjuju podatke koristeći zajednički skup komunikacionih protokola"[3].

Elektronske komunikacije u savremenom načinu života predstavljaju primarni način komuniciranja i informisanja. Slanje i primanje elektronske pošte, čitanje vesti na Internet sajtovima, razmena informacija na društvenim mrežama – deo je uobičajene svakodnevice gotovo svakog čoveka. Ovakav napredak svakako unapređuje kvalitet života i omogućava da se do informacija dođe praktično u trenutku kada one nastaju; moguće je upoređivati informacije o istom događaju koje dolaze iz više izvora, razvijati i deliti kritičko mišljenje o njima.

Osim nesumnjivo pozitivnih strana razvoja komunikacija, postoje međutim i negativni aspekti. Svakako je jedna od bitnijih opasnosti ugrožavanje privatnosti korisnika Interneta. Elektronske komunikacije podrazumevaju veliki broj informacija koje korisnik ostavlja u virtuelnom prostoru. Ove informacije može ostaviti dobrovoljno (na primer, veoma popularno „čekiranje" na različitim društvenim mrežama, koje se sastoji u davanju tačne lokacije korisnika u tom trenutku) pa do onih za koje nije ni svestan da ostavlja (kao što je adresa Internet protokola, o kojoj će više reči biti kasnije). Na osnovu podataka koji se na ove načine ostave na različitim računarima mogu se izvršiti različite zloupotrebe – od uznemiravanja i ugrožavanja privatnosti lica, do potpuno preuzimanja njegovog virtuelnog identiteta (takozvani *phishing*[4]). Zbog toga je privatnost korisnika elektronskih komunikacija veoma brzo po ekspanziji Interneta potpala pod zakonsku i sudsku zaštitu.

Sa druge strane, korisnici elektronskih komunikacija mogu počiniti različite akte koji se smatraju nemoralnim, neetičkim ili nedozvoljenim. I ovde,

1 Zakon o elektronskim komunikacijama, *Službeni glasnik RS*, br. 44/2010, 60/2013 - odluka US i 62/2014, čl, 4. tač. 23.

2 *Electronic Communications Privacy Act of 1986* (ECPA).

3 Član 4. tačka 15. Zakona o elektronskim komunikacijama.

4 Vid. detaljnije u: D. Prlja, Z. Ivanović, M. Reljanović, *Krivična dela visokotehnološkog kriminala*, Institut za uporedno pravo, Beograd 2011, 74-132.

kao i u prethodnom primeru, može doći do ponašanja koje neće imati neke teške posledice, čak ne mora biti ni inkriminisano kao nedozvoljeno (na primer, slanje neželjene pošte – popularno poznato kao *spamovanje*). Posledice mogu međutim biti i znatno teže, odnosno putem elektronskih komunikacija mogu se počiniti i teška krivična dela (kao što su prevara, širenje dečje pornografije, govor mržnje, i druga).

Jedno od pitanja koje se nameće razvojem elektronskih komunikacija, jeste: kako zaštititi autorsko pravo i srodna prava u svetu u kojem se – legalno ili nelegalno – u sekundi može načiniti i podeliti hiljade kopija jednog autorskog dela ili predmeta srodnopravne zaštite? Ovo pitanje dobija posebnu težinu kada je reč o korisnicima Interneta koji dolaze do nezakonito umnoženih primeraka autorskih dela. Da li je ovakvo ponašanje kažnjivo i u kojoj meri se mogu ograničiti komunikacije korisnika, da bi se ono sprečilo? Konkretni slučajevi koji će biti analizirani, odnose se na postupanja internet operatora i nosilaca autorskog prava, koji su pre nekoliko godina započeli praksu koja je i dalje aktuelna a koja se vezuje za sprečavanje kontinuirane i masovne povrede autorskog prava putem elektronskih komunikacija. Naime, nosioci autorskog prava obaveštavaju internet operatore o tome da pojedini korisnici vrše povredu autorskog prava na Internetu. Operatori potom prosleđuju korisnicima pisma upozorenja da je takva praksa nezakonita i da će snositi posledice ukoliko nastave sa pomenutim aktivnostima. Već na prvi pogled, opisana situacija je višestruko sporna. Sasvim je izvesno da u konkretnim slučajevima dolazi do sukoba između prava na privatnost korisnika Interneta, odnosno tajnost njihovih elektronskih komunikacija, i nosilaca autorskog prava u pokušaju da zaštite svoje interese.

Analiza koja sledi predstavlja osvrt na aktuelni zakonski okvir i praksu u Republici Srbiji, kada je reč o odgovorima na pitanja kako okvalifikovati praksu nosilaca autorskog prava i internet operatora, kako zaštiti tajnost elektronskih komunikacija i kako zaštiti autorsko pravo i srodna prava na Internetu.[5]

2. PRIVATNOST ELEKTRONSKIH KOMUNIKACIJA

Pravo na privatnost i pravo na zaštitu podataka o ličnosti spadaju u korpus osnovnih ljudskih prava. Ova prava regulisana su nizom međunarodnih instrumenata i detaljno zaštićena u pravnom sistemu Republike Srbije.

5 Rad je zasnovan na rezultatima istraživanja objavljenih u izvornom naučnom članku istog autora „Postupanja internet operatora povodom navodnog kršenja autorskih prava – zakonodavstvo i praksa u Srbiji", *Pravni zapisi* 1/2013, 126-144. Novije istraživanje koje je uključeno u ovaj rad je međutim prošireno i obuhvata i izmene i dopune relevantnih zakonskih i podzakonskih akata koje su u međuvremenu nastupile, kao i detaljniju analizu pojedinih instituta i pojmova kojima nije bilo posvećeno dovoljno pažnje, a sve u cilju stvaranja kompletnije slike o kompleksnom pravnom odnosu koji se istražuje.

Evropska konvencija za zaštitu osnovnih prava i ljudskih sloboda[6] (u daljem tekstu: EKLJP) 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*."[7] Prepiska je dakle jedan od zaštićenih aspekata privatnosti svakog lica. U svojoj praksi, Evropski sud za ljudska prava (u daljem tekstu: ESLJP, Sud) je jasno utvrdio da elektronska komunikacija spada pod zaštitu člana 8. U presudi slučaja *Liberty protiv Ujedinjenog Kraljevstva*, Sud je naglasio da postoji ustanovljena praksa posmatranja elektronskih komunikacija kao zaštićenih u smislu pojmova „privatnog života" i „komunikacija" iz člana 8.[8]

U skladu sa određenjem elektronskim komunikacija kao tajnih, odnosno privatnih, svako presretanje elektronske komunikacije je kažnjivo. Konvencija o visokotehnološkom kriminalu[9] sadrži odredbu o inkriminisanju nezakonitog presretanja onih podataka koji se ne mogu smatrati javnim: „*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.*"[10]

---

6 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; Zakon o ratifikaciji Protokola br. 14 uz Evropsku konvenciju za zaštitu ljudskih prava i osnovnih sloboda, kojim se menja kontrolni sistem Konvencije ("Sl. list SCG - Međunarodni ugovori", br. 5/2005 i 7/2005 – ispr.)

7 Čl. 8. EKLJP.

8 *Liberty i ostali protiv Ujedinjenog Kraljevstva* (predstavka 58243/00, presuda od 1. jula 2008. godine), §56. Videti takođe: *Copland protiv Ujedinjenog Kraljevstva* (predstavka 62617/00, presuda od 3. aprila 2007. godine), §41.

9 Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu, *Službeni glasnik RS*, br. 19/09.

10 Čl. 3. Konvencije o visokotehnološkom kriminalu.

Ustav Republike Srbije[11] sadrži različita prava koja se mogu smatrati razradom ljudskog prava na privatan život. Jedno od njih je tajnost pisama i drugih sredstava opštenja: „*Tajnost 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.*" Ustav takođe štiti i podatke 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.*"[12]

Konačno, Krivični zakonik Republike Srbije[13] (u daljem tekstu: KZ) predviđa kao posebna krivična dela različite radnje povrede privatnosti nekog lica. Ovim zakonom elektronska komunikacija poistovećena je sa klasičnom komunikacijom[14], tako da zaštita elektronske komunikacije spada u isti režim privatnosti.

U tom smislu, krivičnim delom „Povreda tajnosti pisma i drugih pošiljki"[15] obuhvaćena je i elektronska komunikacija. Svako neovlašćeno presretanje komunikacije spada u neko od inkriminisanih postupanja:

- neovlašćeno otvaranje tuđeg pisma, telegrama ili kakvog drugog zatvorenog pismena ili pošiljke;
- povreda tajnosti tuđeg pisma, telegrama ili kakvog drugog zatvorenog pismena ili pošiljke na drugi način;
- neovlašćeno zadržavanje, prikrivanje, uništavanje ili predaja tuđeg pisma, telegrama ili druge pošiljke drugom licu;
- povreda tajnosti elektronske pošte ili drugog sredstva za telekomunikaciju;
- saopštavanje drugom licu sadržine koju je izvršilac saznao povredom tajnosti tuđeg pisma, telegrama ili kakvog drugog zatvorenog pismena ili pošiljke;
- korišćenje sadržine tuđeg pisma, telegrama ili kakvog drugog zatvorenog pismena ili pošiljke na drugi način.

Krivičnim delom „Neovlašćeno prisluškivanje i snimanje"[16] označeno je kao kažnjivo svako neovlašćeno prisluškivanje ili snimanje tuđeg razgovora, upotrebom posebnih uređaja.

---

11 Ustav Republike Srbije, *Službeni glasnik RS*, br. 98/06.

12 Čl. 41. i 42. Ustava.

13 Krivični zakonik, *Službeni glasnik RS*, br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013 i 108/2014.

14 Čl. 112. tač. 27 KZ.

15 Čl. 142. KZ.

16 Čl. 143. KZ.

Opisanim krivičnim delima u potpunosti je zaštićen svaki vid elektronske komunikacije, čime je garantovano pravo na privatnost korisnika Interneta.

3. PODACI KOJI NASTAJU TOKOM ELEKTRONSKE KOMUNIKACIJE

Trebalo bi ukazati na podatke koji čine sadržinu elektronske komunikacije, njihovu prirodu i pravni režim pod koji potpadaju.

U toku elektronske komunikacije putem računara, razmenjuju se dve vrste podataka, koje nastaju kao posledica izvršavanja unapred određenih i definisanih komunikacionih protokola na Internetu. Jedna vrsta podataka (primarni podaci) odnosi se na sadržinu komunikacije; druga se međutim odnosi na tehničke podatke koji nastaju u komunikaciji dva, ili više računara (sekundarni podaci). Veoma lako se može napraviti paralela između ovih podataka i podataka u „klasičnoj" poštanskoj komunikaciji. Svrha slanja poštanske pošiljke jeste u prenošenju određenih podataka ili predmeta – oni predstavljaju sadržinu komunikacije, odnosno primarne podatke. Da bi pošiljka stigla kome je upućena mora ipak sadržati i različite sekundarne podatke – adresu pošiljaoca i primaoca, način slanja pošiljke, njenu težinu, i slično. Ovo su sekundarni podaci u komunikaciji. Primarni podaci poznati su samo pošiljaocu i primaocu – niko ne može otvarati tuđa pisma ili pakete. Sekundarni podaci su međutim takve prirode da moraju biti poznati i drugim licima, onima čiji je zadatak da komunikaciju izvrše. Zbog toga se govori o *tajnosti sadržine komunikacije*, koja spada u pravo na tajnost prepiske kao dela prava na privatan život lica i *privatnosti (zaštićenosti) sekundarnih podataka*, koje ona lica koja ih saznaju u vršenju svojih poslova (usluga kojima se komunikacija omogućava) ne mogu preneti drugim licima.

Sekundarni podaci koji nastaju tokom elektronske komunikacije smatraju se podacima o ličnosti, budući da svako ko ima pristup ovim podacima može ustanoviti identitet osoba koje elektronski razmenjuju podatke. Prema članu 3. stav 1. tačka 1. Zakona o zaštiti podataka o ličnosti[17] (u daljem tekstu: ZZPL) „*(...) 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*".

„*Lice na koje se podaci odnose ima pravo da odredi na koji način će se izvršiti obrada tih podataka. Obrada nije dozvoljena ako: 1) fizičko lice nije dalo*

17 Zakon o zaštiti podataka o ličnosti, *Službeni glasnik RS*, br. 97/2008, 104/2009 - dr. zakon, 68/2012 - odluka US i 107/2012.

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."[18] Izuzeci koje ZZPL predviđa, kada se neki podatak neće smatrati podatkom o ličnosti, postavljeni su relativno usko i nikako se ne može reći da sekundarni podaci pripadaju nabrojanim izuzecima.[19] Ovo je značajno za elektronske komunikacije jer ugovor između internet operatora i korisnika Interneta predstavlja osnov za prikupljanje sekundarnih podataka i pristanak korisnika za njihovo pohranjivanje u određenom vremenskom periodu, u skladu sa zakonom. Ugovor između operatora i korisnika međutim nije i ne može biti osnov za davanje ovih podataka bilo kojem trećem licu, osim u zakonom predviđenim izuzecima u krivičnom postupku.

Kao što će dakle biti objašnjeno u nastavku teksta, postoje izuzeci koji su regulisani posebnim sistemskim zakonima koji se odnose na specifične situacije kada nadležni državni organi mogu sprovesti mere kojima se vrši (privremena) invazija u privatnost komunikacije lica, kako u odnosu na primarne tako i u odnosu na sekundarne podatke iz obavljene elektronske komunikacije.

---

18 Čl. 8. ZZPL.

19 Čl. 5. ZZPL: "*Osim ako očigledno pretežu suprotni interesi lica, pojedine odredbe ovog zakona o uslovima za obradu, kao i o pravima i obavezama u vezi sa obradom ne primenjuju se na obradu:*

1) podataka koji su dostupni svakome i objavljeni u javnim glasilima i publikacijama ili pristupačni u arhivama, muzejima i drugim sličnim organizacijama;

2) podataka koji se obrađuju za porodične i druge lične potrebe i nisu dostupni trećim licima;

3) podataka koji se o članovima političkih stranaka, udruženja, sindikata, kao i drugih oblika udruživanja obrađuju od strane tih organizacija, pod uslovom da član dâ pismenu izjavu da određene odredbe ovog zakona ne važe za obradu podataka o njemu za određeno vreme, ali ne duže od vremena trajanja njegovog članstva;

4) podataka koje je lice, sposobno da se samo stara o svojim interesima, objavilo o sebi.

Čl. 12. ZZPL: Obrada bez pristanka je dozvoljena:

1) da bi se ostvarili ili zaštitili životno važni interesi lica ili drugog lica, a posebno život, zdravlje i fizički integritet;

2) u svrhu izvršenja obaveza određenih zakonom, aktom donetim u skladu sa zakonom ili ugovorom zaključenim između lica i rukovaoca, kao i radi pripreme zaključenja ugovora;

2a) u svrhu prikupljanja sredstava za humanitarne potrebe;

3) u drugim slučajevima određenim ovim zakonom, radi ostvarenja pretežnog opravdanog interesa lica, rukovaoca ili korisnika."

U prilog uskog tumačenja ovih odredbi ide i Odluka Ustavnog suda US IUz broj 41/2010 od 30. maja 2012. godine, *Službeni glasnik RS*, br. 68/2012, kojom su ukinute mogućnosti da se drugim propisom odredi još neki izuzetak od pravila postavljenih u ZZPL.

4. KADA ZAKON DOZVOLJAVA PRESRETANJE ELEKTRONSKE KOMUNIKACIJE KORISNIKA INTERNETA?

Nesumnjivo je dakle da je pravo na tajnost elektronskih komunikacija deo prava na privatan život svakog građanina Republike Srbije, i kao takvo zaštićeno Ustavom i potvrđenim međunarodnim instrumentima. Sledeće pitanje na koje se mora dati odgovor jeste: kada se mogu učiniti izuzeci od ovog prava, odnosno kada je dozvoljeno presretati elektronsku komunikaciju nekog lica? Evidentno je da se mogu razlikovati zakonito i nezakonito presretanje komunikacije uopšte, pa i elektronskih komunikacija. Zakonito presretanje (odnosno prisluškivanje) ograničeno je na načine određene specifičnim zakonima; ono je postavljeno veoma restriktivno, budući da predstavlja izuzetak od opšteg pravila i način sužavanja osnovnih ljudskih prava građana. Zbog toga su izuzeci regulisani sistemskim krivičnim zakonima.

Zakonik o krivičnom postupku[20] (u daljem tekstu: ZKP) uređuje institut „posebnih dokaznih radnji". U pitanju su specifične metode istraživanja krivičnih dela koje se sprovode onda kada se na drugi način ne mogu prikupiti dokazi za krivično gonjenje, ili bi njihovo prikupljanje bilo znatno otežano, odnosno kada se na drugi način krivično delo ne bi moglo otkriti, sprečiti ili dokazati ili bi to izazvalo nesrazmerne teškoće ili veliku opasnost. Ove radnje se mogu preduzeti kada postoje osnovi sumnje da je lice počinilo, ili priprema izvršenje krivičnog dela. Ne mogu se, međutim, upotrebiti za istragu ili sprečavanje bilo kojeg krivičnog dela, već samo onih najtežih koja su taksativno nabrojanja u ZKP.[21] Čak i tada, kada su ispunjeni svi navedeni preduslovi, prilikom odlučivanja o određivanju i trajanju posebnih dokaznih radnji organ postupka će posebno ceniti da li bi se isti rezultat mogao postići na način kojim se manje ograničavaju prava građana.[22] Među nabrojanim krivičnim delima, u članu 162. stav 3. ZKP navodi se krivično delo „neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava", iz člana 199. Krivičnog zakonika. Prilikom izvršenja ovog krivičnog dela, moguće je sprovesti posebnu dokaznu radnju iz člana 166. ZKP, a to je nadzor i snimanje komunikacije, uključujući i elektronsku komunikaciju.

Krivično delo „Neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava"[23] inkriminiše sledeća postupanja:

– neovlašćeno objavljivanje, snimanje, umnožavanje, ili na drugi način javno saopštavanje u celini ili delimično autorskog dela, interpretacije, fonograma, videograma, emisije, računarski programa ili baze podataka;

20 Zakonik o krivičnom postupku, *Službeni glasnik RS*, br. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 i 55/2014.

21 Čl. 162. ZKP.

22 Čl. 161. ZKP.

23 Čl. 199. Krivičnog zakonika

– stavljanje u promet ili u nameri stavljanja u promet držanje neovlašćeno umnoženih ili neovlašćeno stavljenih u promet primeraka autorskog dela, interpretacije, fonograma, videograma, emisije, računarskog programa ili baze podataka;
– 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 autorskog i srodnih prava, ili ko takve uređaje ili sredstva koristi u cilju povrede autorskog ili srodnog prava.

Teži oblik krivičnog dela predviđen je za slučajeve kada je ovo krivično delo učinjeno u nameri pribavljanja imovinske koristi za sebe ili drugog.

Šta se može zaključiti iz ove parcijalne analize? Pre svega, da se posebne dokazne radnje mogu primeniti na slučajeve takozvane „piraterije". Članovi 166. do 170. ZKP detaljno uređuju ko može i pod kojim uslovima, odnosno na koji način, primeniti ovu meru prema licu za koje postoje osnovi sumnje da je počinilo, odnosno da može počiniti navedeno krivično delo[24].

Naredbu o tajnom nadzoru komunikacije određuje sudija za prethodni postupak. Ona mora biti obrazložena i sadrži „ *(...) raspoložive podatke o licu prema kojem se tajni nadzor komunikacije određuje, zakonski naziv krivičnog dela, označenje poznatog telefonskog broja ili adrese osumnjičenog, odnosno telefonskog broja ili adrese za koju postoje osnovi sumnje da je osumnjičeni koristi, razloge na kojima se zasniva sumnja, način sprovođenja, obim i trajanje posebne dokazne radnje.*"[25] Iako se u odredbi ne pominje, sasvim je izvesno da će naredba sadržati i druge tehničke podatke koji su od značaja za nadzor elektronskih komunikacija. Nadzor komunikacija je privremenog karaktera, i može trajati najduže tri meseca a zbog neophodnosti daljeg prikupljanja dokaza se može produžiti najviše za tri meseca. Ako je reč o krivičnim delima za koje postupa tužilaštvo posebne nadležnosti, tajni nadzor može se izuzetno produžiti još najviše dva puta u trajanju od po tri meseca. Sprovođenje nadzora se prekida čim prestanu razlozi za njegovu primenu.[26]

---

24 Iako zakonska formulacija dozvoljava primenu ovih mera i kada postoje osnovi sumnje da se priprema izvršenje krivičnog dela, analizirajući biće krivičnog dela „Neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava" izvesno je da će ovde postojati specifična situacija da je delo već izvršeno, ili da se počinilac bavi kontinuiranim izvršenjem ovog krivičnog dela u odnosu na različita autorska dela. Teško je zamisliti situaciju u kojoj se dozvoljava prisluškivanje elektronske komunikacije lica (i uopšte postojanje osnova sumnje da će delo biti izvršeno) u fazi pripreme za izvršenje.

25 Čl. 167. st. 1. i 2. ZKP.

26 Čl. 167. st. 3. ZKP. Interesantno je videti kako će se u praksi tumačiti izraz „tužilaštvo posebne nadležnosti", budući da je neizvesno da li se pod time može podrazumevati i posebno odeljenje Višeg javnog tužilaštva za visokotehnološki kriminal (član 4. Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, *Službeni glasnik RS*, br. 61/2005 i 104/2009). U svakom slučaju bi tumačenje moralo biti restriktivno, budući da se povreda autorskog prava ne može smatrati naročito teškim krivičnim delom zbog kojeg bi bilo dozvoljeno čak godinu dana vršiti tajni nadzor komunikacija.

Naredbu sudije za prethodni postupak izvršavaju policija, Bezbednosno-informativna agencija ili Vojnobezbednosna agencija. O sprovođenju tajnog nadzora komunikacije sačinjavaju se dnevni izveštaji koji se zajedno sa prikupljenim snimcima komunikacije, pismima i drugim pošiljkama koje su upućene osumnjičenom ili koje on šalje dostavljaju sudiji za prethodni postupak i javnom tužiocu na njihov zahtev. Poštanska, telegrafska i druga preduzeća, društva i lica registrovana za prenošenje informacija dužna su da državnom organu koji izvršava naredbu omoguće sprovođenje nadzora i snimanja komunikacije i da, uz potvrdu prijema, predaju pisma i druge pošiljke[27] – opet, iako ova odredba nije izvedena do kraja u odnosu na elektronske komunikacije, sasvim je izvesno da se nadležnom državnom organu mora omogućiti i nadzor nad elektronskim komunikacijama od strane internet operatora. Isto se odnosi i na član 169. ZKP kojime se reguliše eventualno proširenje praćenja komunikacije – terminološki zastarelo, ali sasvim sigurno sa namerom da se obuhvate sva sredstva komunikacije, bez izuzetka.

Po završetku tajnog nadzora komunikacije organ koji sprovodi naredbu dostavlja sudiji za prethodni postupak snimke komunikacije i poseban izveštaj koji sadrži: vreme početka i završetka nadzora, podatke o službenom licu koje je nadzor sprovelo, opis tehničkih sredstava koja su primenjena, broj i raspoložive podatke o licima obuhvaćenim nadzorom i ocenu o svrsishodnosti i rezultatima primene nadzora. Sav materijal dobijenim sprovođenjem tajnog nadzora komunikacije, dostaviće se javnom tužiocu. Svi materijali koji su nastali, odnosno dokazi koji su dobijeni suprotno opisanoj proceduri, izdvojiće se kao nezakoniti i neće se moći koristiti u eventualnom krivičnom postupku protiv nadziranog lica.[28]

Zaključak koji se može izvesti iz kratkog pregleda odredbi o tajnom nadzoru komunikacije jeste da je u pitanju detaljno uređen postupak koji se može izvesti samo kada se za to steknu zakonski uslovi, kao i u okvirima u kojima je to dozvolio sud svojom naredbom. Nadležni javni tužilac, kao i policijski organi koji sprovode mere tajnog nadzora, moraju u svakom slučaju poštovani zakonom određene granice nadzora i o svojim postupanjima podneti izveštaje, odnosno ostaviti dokumente u kojima se precizno navode sve preduzete radnje. Otuda ovaj postupak ne predstavlja ništa drugo nego izuzetak koji potvrđuje pravilo nepovredivosti privatnosti, odnosno tajnosti, komunikacija građana – elektronskih, kao i svih drugih.

Zakon o elektronskim komunikacijama[29] (u daljem tekstu: ZEK) određuje da se delatnost elektronskih komunikacija zasniva na opštim uslovima, u koje između ostalih spadaju i zaštita podataka o ličnosti i privatnosti u oblasti elektronskih komunikacija, u skladu sa odredbama tog zakona i Zakona o zaštiti podataka o ličnosti, kao i primene mera za sprečavanje i suzbijanje zlo-

27 Čl. 168. ZKP.

28 Čl. 170. ZKP.

29 Zakon o elektronskim komunikacijama, *Službeni glasnik RS*, br. 44/2010, 60/2013 - odluka US i 62/2014.

upotreba i prevara u vezi sa korišćenjem elektronskih komunikacionih mreža i usluga.[30] Oba principa su dakle sadržana u osnovnim postulatima na kojima internet operatori moraju da zasnivaju svoj rad. I to je sasvim razumljivo, budući da bi kršenje i jednog i drugog principa nosilo društvenu opasnost i u svakom slučaju predstavljalo društveno nepoželjno ponašanje. Navedena načela nisu međutim detaljnije regulisana ZEK, kao ni drugim propisima koji se odnose na elektronske komunikacije. Pravilnik o opštim uslovima za obavljanje delatnosti elektronskih komunikacija po režimu opšteg ovlašćenja[31], koji je donela Republička agencija za elektronske komunikacije (u daljem tekstu: Pravilnik), dalje razrađuje sve opšte uslove koji su navedeni pomenutim članom 37. ZEK. „Međutim, kada je reč o ovlašćenjima koja se odnose na sprečavanje i suzbijanje zloupotreba i prevara, u Pravilniku jednostavno stoji ponovljena formulacija iz ZEK: „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."[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). 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 Republike Srbije, na način predviđen zakonom.*" Ova odredba praktično ponavlja ono što je već regulisano ZKP, 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.*"[33]

Nema dakle nikakvih nedoumica kako se može doći do primarnih i sekundarnih podataka elektronskih komunikacija. Primarni podaci mogu biti obezbeđeni od strane suda, u parničnom postupku koji pokrene nosilac autorskog prava (koji će biti detaljnije analiziran u daljem tekstu), ili u krivičnom postupku. Sekundarni podaci mogu se otkriti samo na osnovu odluke suda koju će izvršiti zakonom određeni nadležnih organi, isključivo u pretkrivičnom postupku. Svako drugo otkrivanje sadržine elektronskih

30 Čl. 37. st. 2. t. 14 i 15 ZEK.

31 Pravilnik o opštim uslovima za obavljanje delatnosti elektronskih komunikacija po režimu opšteg ovlašćenja, *Službeni glasnik RS*, br. 38/2011, 44/2011 - ispr. i 13/2014.

32 Čl. 32. Pravilnika.

33 M. Reljanović, 132-133.

komunikacija, kao i pratećih podataka uz elektronske komunikacije, predstavlja povredu privatnosti korisnika Interneta, kao i izvršenje krivičnog dela.

5. AUTORSKO PRAVO I SRODNA PRAVA U ELEKTRONSKOM OKRUŽENJU

Koncept autorskog prava i srodnih prava mora pratiti digitalizaciju sadržine autorskih dela, kao i savremene koncepte elektronske komunikacije. Veliki broj autorskih dela danas se može naći na Internetu, beplatno ili uz određenu naknadu. Uz ovakve brze i korenite izmene kada je reč o dostupnosti autorskih dela putem računara i drugih elektronskih uređaja, nužno se javljaju problemi i mnoga otvorena pitanja kada je reč o opstanku tradicionalnog koncepta autorskog prava. „Mnogi korisnici Interneta usled nedovoljnog poznavanja prava smatraju da sve što je na Internetu mogu koristiti na svaki način koji požele tako da često prelaze crvenu liniju i vrše povredu autorskog prava. Mnogi su čak sasvim pogrešno ubeđeni da autorsko pravo nije zaštićeno u sajber prostoru. Veliki broj korisnika Interneta misli da ukoliko na samom delu u digitalnoj formi ne postoji zabeleška o „kopirajtu", odnosno zaštićenom autorskom pravu to delo se može koristiti slobodno, odnosno da ono nije zaštićeno autorskim pravom. Ovo su zablude koje korisnike Interneta mogu skupo koštati, jer jer su drzave dužne da priznaju zaštitu delima na osnovu međunarodnih sporazuma, a pre svega Bernske konvencije[34], kao i direktno domaćim pravom, po načelu neformalnosti (bez potrebe da se na primerku dela naznačuje da uživa autorskopravnu zaštitu). Naravno postoji i veliki broj autorskih dela u sajber prostoru koja su u javnom domenu, odnosno čije slobodno korišćenje je svima dozvoljeno. Autori se mogu odreći svog autorskog prava u korist korisnika u sajber prostoru, ali i to mora takođe biti izričito naznačeno."[35] Osim nevlašćenog umnožavanja kompletnog autorskog dela, postoje i drugi problemi vezani za široku dostupnost autorskih dela u elektronskom obliku, kao što su plagiranje autorskih dela, ili preuzimanje i dorada tuđih autorskih dela da bi se dalje distribuirala kao posebna autorska dela (stvaranje dela prerade, a da se pri tome na radi o dozvoljenim intervencijama vezanim za stvaranje parodije, karikature, i slično).

Kao što je već napomenuto, zaštita autorskog prava prati nove tendencije u elektronskim komunikacijama, koje omogućavaju masovne povrede propisa o autorskom pravu i srodnim pravima. Zakon o autorskom i srodnim pravima[36] (u daljem tekstu: ZASP) predviđa da nosilac autorskog prava, interpretator, proizvođač fonograma, proizvođač videograma, proizvođač

34 Zakon o ratifikaciji Bernske konvencije za zaštitu književnih i umetničkih dela, *Službeni list SFRJ*, br. 14/75 i *Službeni list SFRJ - Međunarodni ugovori*, br. 4/86 – uredba.

35 D. Prlja, M. Reljanović, Z. Ivanović, *Internet pravo*, Institut za uporedno pravo, Beograd 2012, 12-15.

36 Zakon o autorskom i srodnim pravima, *Službeni glasnik RS*, br. 104/2009, 99/2011 i 119/2012.

emisije, proizvođač baze podataka i sticalac isključivih ovlašćenja na autorska i srodna prava može tužbom da zahteva naročito: utvrđenje povrede prava; prestanak povrede prava; uništenje ili preinačenje predmeta kojima je izvršena povreda prava, uključujući i primerke predmeta zaštite, njihove ambalaže, matrice, negative i slično; uništenje ili preinačenje alata i opreme uz pomoć kojih su proizvedeni predmeti kojima je izvršena povreda prava, ako je to neophodno za zaštitu prava; naknadu imovinske štete; objavljivanje presude o trošku tuženog. Autor, odnosno interpretator ima pravo na tužbu za naknadu neimovinske štete zbog povrede svojih moralnih prava.[37] Predviđena je dakle građanskopravna zaštita od povrede autorskog prava, pred nadležnim sudom. ZASP čak predviđa i neku formu kaznene odštete u članu 206: „*Ako je povreda imovinskog prava učinjena namerno ili krajnjom nepažnjom, tužilac može, umesto naknade imovinske štete, zahtevati naknadu do trostrukog iznosa uobičajene naknade koju bi primio za konkretni oblik korišćenja predmeta zaštite, da je to korišćenje bilo zakonito.*" Postupak po tužbi zbog povrede autorskog i srodnih prava je hitan.[38] Postoji dakle dobra osnova da se interesi nosilaca autorskog prava zaštite. ZASP je pokrio praktično sve oblike mogućeg elektronskog narušavanja autorskog prava, pa će se tako povredom smatrati i: iskorišćavanje bilo kog predmeta zaštite uz upotrebu neovlašćeno umnoženih primeraka tog predmeta zaštite, odnosno na osnovu neovlašćene emisije; držanje u komercijalne svrhe primeraka autorskog dela ili predmeta srodnog prava, ako držalac zna ili ima osnova da zna da je reč o neovlašćeno proizvedenom primerku; proizvodnja, uvoz, stavljanje u promet, prodaja, davanje u zakup, reklamiranje u cilju prodaje ili davanja u zakup ili držanje u komercijalne svrhe uređaja, proizvoda, sastavnih delova, računarskih programa, koji su prevashodno konstruisani, proizvedeni ili prilagođeni da omoguće ili olakšaju zaobilaženje bilo koje efikasne tehnološke mere, i koji nemaju drugu značajniju svrhu osim navedene; zaobilaženje bilo koje efikasne tehnološke mere ili pružanje ili reklamiranje usluge kojom se to omogućava ili olakšava; uklanjanje ili izmena elektronske informacije o pravima, ili stavljanje u promet, uvoz, emitovanje ili na drugi način javno saopštavanje autorskog dela ili predmeta srodnopravne zaštite sa kojeg je elektronska informacija o pravima neovlašćeno uklonjena ili izmenjena, a da pri tom počinilac zna ili ima osnova da zna da time podstiče, omogućuje, olakšava ili prikriva povredu autorskog prava ili srodnog prava.[39]

U slučaju da smatra da u povredi autorskog prava postoje i elementi krivičnog dela, nosilac autorskog prava može podneti i krivičnu prijavu nadležnom javnom tužiocu ili policiji. Prema Zakonu o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, posebno odeljenje za borbu protiv visokotehnološkog kriminala Višeg javnog tužilaštva u Beogradu biće nadležno za krivična dela protiv intelek-

37 Čl. 205. st. 1. i 2. ZASP.

38 Čl. 207. st. 2. ZASP.

39 Čl. 208. st. 1 ZASP.

tualne svojine ako broj primeraka autorskih dela prelazi 2000 ili nastala materijalna šteta prelazi iznos od 1.000.000 dinara, i to za teritoriju cele Republike Srbije.[40]

6. POSTUPANJA NOSILACA AUTORSKOG PRAVA I INTERNET OPERATORA U SLUČAJEVIMA NAVODNIH POVREDA AUTORSKOG PRAVA

Nakon što je izvršena detaljna analiza pravnog okvira zaštite autorskog prava na Internetu, mogu se bliže analizirati i postupanja nosilaca autroskih prava i internet operatora u opisanim slučajevima dostavljanja „upozorenja" korisnicima.

Nosioci autorskog prava, odnosno lica koja oni ovlaste, dolaze do podataka o neovlašćenom deljenju primeraka autorskih dela putem elektronskih komunikacija. Podatak koji se odnosi na korisnika koji (navodno) povređuje autorsko pravo jeste njegova IP adresa. Način na koji oni do takvih podataka dolaze je nepoznat. Kako će međutim biti pojašnjeno u daljoj analizi, tehnički gledano postoji nekoliko mogućnosti da se do takvih podataka dođe – i nijedan od tih mehanizama nije zakonit. Nakon što se dođe do podataka koji od korisnika povređuje autorsko pravo, njegova IP adresa i podatak o tome o kojem autorskom delu se radi i u kojem vremenskom periodu je korisnik vređao autorsko pravo, prosleđuje se internet operatoru kojem ta IP

40 Čl. 3. tač. 2 Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala. Ova formulacija je očigledno zastarela i prevaziđena, budući da se veoma teško može utvrditi broj autorskih dela koji je neovlašćeno distribuiran. Odredba je uvedena, i imala smisla, u vreme kada je bila aktuelna takozvana „ulična piraterija", neautorizovana prodaja autorskih dela pohranjenih na CD ili DVD nosačima koje su prodavali ulični prodavci. Na osnovu tada postavljene prakse, da bi se uspostavila nadležnost posebnog odeljenja javnog tužilaštva bilo je dovoljno da postoji 2000 kopija nekog autorskog dela. Nije bilo potrebno da se radi o 2000 različitih autorskih dela, što je logično tumačenje norme. Ovaj uslov za zasnivanje nadležnosti posebnog odeljenja u najvećem broju slučajeva nije se dovodio u pitanje, budući da je na primer bilo dovoljno pronaći nekoliko .mp3 kompilacija muzičkih autorskih dela da bi broj narastao na 2000. U elektronskom okruženju se stvari međutim moraju posmatrati drugačije – na primer, neautorizovano deljenje jednog jedinog autorskog dela putem torent fajla moglo bi se smatrati dovoljnim uslovom za zasnivanje nadležnosti, ukoliko bar 2000 korisnika Interneta koristi elektronske komunikacije putem torenta da bi to autorsko delo preuzeli na svoje računare. Kada je reč o materijalnoj šteti koja je time načinjena, takođe je diskutabilno kako će se ona određivati. Prilikom zaplena nosača autorskih dela, šteta je procenjivana na osnovu vrednosti diskova zatečenih kod prodavca. U svetu elektronske razmene ovakav kriterijum je teže primeniti. Sa jedne strane veoma teško se može utvrditi broj preuzetih primeraka (naročito kada se komunikacija odvija preko P2P sistema, čiji će način funkcionisanja biti objašnjen u daljem tekstu) dok sa druge strane ovakva razmena nema lukrativni karakter – autorsko delo se ne prodaje, već se deli sa ostalim korisnicima bez ostvarivanja dobiti. Realno je očekivati da će glavni parametar biti procenjena šteta u odnosu na vrednost pojedinačne kopije autorskog dela u autorizovanoj prodaji (time se međutim ne rešava tehnički problem utvrđivanja broja kopija autorskog dela koje su „podeljene").

adresa pripada.[41] Internet operatori primaju ovakve „naloge"[42] i izvršavaju ih šaljući korisnicima pisma upozorenja u kojima se navodi da su povredili autorsko pravo (najčešće samo navodeći autorsko delo u pitanju bez drugih detalja, mada se tu praksa razlikuje pa se ponekad navode i IP adresa koju su koristili i naziv fajla, kao i vremenski okvir u kojem su navodno neovlašćeno preuzimali autorsko delo u pitanju) uz upozorenje da će snositi pravne posledice ukoliko sa takvim ponašanjem nastave. Posledice se najčešće svode na privremeno smanjenje protoka Internet saobraćaja, ili potpuno isključenje sa Interneta na određeni period.

Ovakva praksa nije nepoznata u svetu. U zavisnosti od zakonskog okvira, neke od navedenih aktivnosti mogu biti dozvoljene; čini se ipak da nije realno očekivati da će se u bilo kojem scenariju ovakvo ponašanje tretirati kao zakonito, kao ni da će nosioci autorskog prava na ovaj način moći da se zaštite. U tom smislu je zanimljivo analizirati kako je funkcionisao anti-piratski program nazvan „Sistem za upozorenje povodom povrede autorskog prava" (eng. *The Copyright Alert System*), koji su privatne kompanije pustile u rad 2013. godine u SAD.[43] Program je korišćen za ispitivanje takozvane *peer-to-peer* (P2P) elektronske komunikacije, koja se sastoji u prenošenju elektronskih podataka (fajlova) u direktnoj komunikaciji dva ili više računara, koje povezuje zajednički program za deljenje fajlova. Najčešći savremeni način ovakve komunikacije se odvija putem torent programa (eng. *torrent*). Uvezivanjem zainteresovanih korisnika Interneta u mrežu računara koji automatski dele neki elektronski fajl, svaki od njih istovremeno pohranjuje delove fajla sa računara drugih korisnika i omogućava isto tim korisnicima u odnosu na delove fajla koje on poseduje u tom trenutku. Na ovaj način se komunikacija ubrzava (brzina zavisi od broja računara koji su uključeni u deljenje)

---

41 IP adresa (eng. *Internet protocol adress*) je jedinstveni set brojeva na osnovu kojeg je moguće ustanoviti sa kojeg računara u mreži dolazi elektronska komunikacija. Svaki računar komunikaciju na Internetu vrši putem odgovarajućih unapred ustanovljenih pravila – komunikacionih protokola. Prilikom povezivanja računara korisnika sa bilo kojim drugim računarom na Internetu (dakle, i prilikom pregledanja bilo kojeg Internet sajta, aktiviranja računarskog programa koji koristi Internet komunikaciju, i slično), računar korisnika šalje podatak o IP adresi koju dobija u trenutku povezivanja na Internet. Ova adresa je jedinstvena za svaki računar u datom trenutku (moguće je da više računara koristi jednu IP adresu, ali nikada u isto vreme). IP adresa dakle predstavlja „poštansku adresu" računara na Internetu, na osnovu koje korisnik može fizički da se locira. Budući da IP adresa predstavlja niz brojeva, a da svaki internet operator ima unapred određeni sistem i dodeljeni numerički okvir za formiranje IP adresa, na osnovu IP adrese može se odrediti kojem internet operatoru pripada korisnik sa određene IP adrese.

42 Navedeni izraz nije tačan, budući da ne postoji pravni osnov da nosilac autorskog prava izda bilo kakav obavezujući dokument operatoru, niti je ovaj dužan da postupi po njemu; ipak, u praksi se redovno dešava da operatori izvršavaju ono što dobiju od advokatskih kancelarija koje zastupaju nosioce autorskog prava, pa će stoga u tekstu njihova obraćanja operatorima biti označena ovim izrazom.

43 Izvor: T. Klosowski, The Copyright Alert System: How the New "Six Strikes" Anti-Piracy Program Works, *http://lifehacker.com/5986961/the-copyright-alert-system-how-the-new-six-strikes-anti-piracy-program-works* (1.4.2015).

a svaki od korisnika istovremeno preuzima i deli zajednički fajl. Suština delovanja programa sastojala se u presretanju komunikacije između korisnika, kako bi se otkrio nedozvoljeni sadržaj. Nakon toga, sistem bi uputio podatke o povredi autorskog prava internet operatoru korisnika za kojeg je utvrđeno da nedozvoljeno deli materijal zaštićen autorskim pravom. Internet operator bi slao upozorenje korisniku o nedozvoljenosti onoga što radi, sa podacima o kojem autorskom delu je reč. U zavisnosti od toga koliko puta je izrečena ovakva vrsta opomene korisniku, on je snosio određene sankcije (upozorenje, slanje edukativnog materijala o autorskom pravu, smanjenje Internet protoka, isključenje iz mreže, „primoravanje" korisnika da pogleda edukativni video ili obavi edukativni razgovor pre korišćenja Interneta, i slično[44]).

Lansiranje ovog programa u sajber prostor nije napravilo značajnu razliku kada je reč o obimu piraterije u SAD, tačnije nije moglo da se očekuje da će biti shvaćen ozbiljno budući da je pretpostavljao nedozvoljeno presretanje elektronske komunikacije korisnika – dakle, shema delovanja nosilaca autorskog prava bila je slična onoj koju primenjuju nosioci autorskog prava u Srbiji osim što nije poznato koji se softer koristi u slučaju Srbije (tačnije, uopšte nije poznato kako se dolazi do podataka o elektronskim komunikacijama korisnika). U tom smislu je cela akcija bila relativno ograničenog dometa, budući da se velika većina podataka koje je program sakupio nije mogla koristiti kao dokazni materijal u eventualnim sudskim postupcima, čega su korisnici dosta brzo postali svesni.

Još dva praktična pitanja koja su se postavila u slučaju ovog programa. Prvo se odnosi na preuzimanje materijala na kojem korisnici nemaju autorsko pravo. Da li je dovoljno preuzeti bilo koji deo materijala, da bi se smatralo da je povređeno autorsko pravo? Da bi neko na primer odgledao film koji preuzima na ovaj način, mora preuzeti ceo fajl – jedan ili više delova fajla neće biti dovoljni za tako nešto. Kako se onda može govoriti o nekoj koristi tog korisnika, i da li je uopšte potrebno da lice pribavi sebi neku korist ili je dovoljno da se načini šteta nosiocu autorskog prava? Ovaj problem je naročito zanimljiv i sa stanovišta određivanja broja neautorizovanih „kopija" autorskog dela, koje je korisnik poslao drugim korisnicima – po našem mišljenju, sporno je da li se može smatrati umnoženim primerkom autorskog dela njegov neupotrebljivi fragment. Druga grupa pitanja se odnosi na otvorene bežične mreže, koje su postale pravilo u mnogim kafićima, hotelima, bibliotekama, na aerodromima, pa čak i na otvorenom (parkovi, igrališta, gradski prevoz, i slično). U ovim sistemima nije moguće identifikovati korisnika putem IP adrese[45]. Moglo bi se govoriti o potencijalnoj identifikaciji na

44 Izvor: A. Fitzpatrick, ISPs Finally Explain How 'Six Strikes' Anti-Piracy Program Will Work, *http://mashable.com/2013/02/27/isps-six-strikes/* (1.4.2015).

45 Identifikacija bi eventualno bila moguća ukoliko je potrebno da se korisnik prijavi (uloguje) u mrežu i ostavi neki svoj lični podatak, iako je mreža otvorena i besplatna za korišćenje. Čak i u ovom slučaju, podaci koje korisnik ostavi na ovakav način, nikako ne mogu biti podeljeni ni sa kim drugim osim sa nadležnim državnim organima na osnovu odluke suda.

manje prometnim mestima putem razgovora sa svedocima (na primer, zaposleni u kafiću) ili putem pregledanja video nadzora mesta na kojima se koristi besplatna bežična mreža. U tim slučajevima bi se eventualno moglo doći do potencijalnih izvršilaca. Ova sredstva istraživanja su međutim rezervisana samo i isključivo za zakonito sproveden istražni postupak kao deo pretkrivičnog postupka, od strane policije i tužilaštva. Ne postoji nikakva mogućnost da nosilac autorskog prava dođe do ovakvih podataka i ukrsti ih, na zakonit način. To zapravo znači da su mogućnosti navedenog programa, kao i akcije nosilaca autorskog prava uopšte, prilično ograničene u svakom slučaju a da je to naročito vidljivo kod pristupa korisnika otvorenim bežičnim mrežama.

Koji se sve zakonski propisi povređuju opisanom praksom nosilaca autorskog prava i internet operatora u Republici Srbiji? U praksi se mogu identifikovati dva načina postupanja.

Moguće je da operator dobije zahtev da nosiocu autorskog prava ili licu koje ga zastupa dostavi podatke o korisniku koji je navodno prekršio autorsko pravo korišćenjem elektronske komunikacije. Operator dostavlja ove podatke, na osnovu čega nosilac autorskog prava saznaje njegov identitet i adresu stanovanja i upućuje mu „pismo upozorenja". Druga situacija postoji kada nosilac autorskog prava dostavi uz „nalog" operatoru i podatke koje poseduje o navodnoj povredi autorskog prava. Operator dalje postupa samostalno, odnosno na osnovu pribavljenih podataka identifikuje korisnika i upućuje mu pismo upozorenja.

U obe situacije pisma upozorenja imaju sličnu sadržinu, kao što je već napomenuto. Ona na manje ili više detaljan nači opisuju navodnu povredu autorskog prava, način na koji je izvršeno i period vremena kada se događalo. Korisnik se upozorava da je u pitanju nezakonito ponašanje i da će snositi zakonske posledice ukoliko sa time nastavi. Dok nosioci autorskog prava (po pravilu ova pisma šalju advokatske kancelarije kao njihovi pravni zastupnici) predočavaju uglavnom krivičnopravne posledice, operatori se zadržavaju na posledicama koje se tiču ograničavanja ili uskraćivanja daljeg korišćenja njihovih usluga.

Ovakva postupanja predstavljaju višestruko kršenje zakona. „Najpre, nosilac autorskog prava nema zakonski osnov da naloži bilo kakvu radnju operatorima. Jedina mogućnost koja mu stoji na raspolaganju jeste obraćanje sudu, i to na osnovu Zakona o autorskom i srodnim pravima. Potom, operatori ne mogu, kada dobiju obaveštenje nosilaca autorskog prava o navodnoj povredi autorskog 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. Sadržina te komunikacije korisnika nikada ne može biti predmet samostalne „istrage" operatora."[46] Povreda prava na privatnost

46 M. Reljanović, 135.

komunikacija je krivično delo. Formalnopravno gledano, operatori koji dobiju podatke da je neko lice saznalo da se vrši povreda autorskog prava tako što je presrelo tuđu elektronsku komunikaciju, moralo bi nadležnom tužilaštvu da prijavi izvršenje krivičnog dela vezanog za povredu tajnosti pisma i drugih pošiljki ili neovlašćeno prisluškivanje, a ne da postupa prema nalozima koje dobije od tog lica. „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 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 autorskog 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 autorskog 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."[47]

Nosioci autorskog prava mogu od suda zatražiti zaštitu. Od suda mogu, kako u krivičnom tako i u parničnom postupku, zatražiti i prikupljanje podataka o korisnicima za koje smatraju da se bave piraterijom[48]. Zašto se onda nosioci autorskog prava ne obrate sudu? Zato što je veoma teško učiniti verovatnim da se neko lice *bavi* piraterijom, a još teže naravno da postoji neki izolovani incident u kojem je došlo do nezakonitog deljenja jednog ili više au-

47 *Ibid.*

48 Mogućnosti zaštite nosilaca autorskog prava prema važećem zakonodavstvu Republike Srbije biće izloženo u poslednjem delu rada.

torskih dela između dva korisnika Interneta. Iako sud u parničnom postupku nije obavezan da zanemari, odnosno isključi nezakonito pribavljene dokaze, teško je verovati da će fokus bilo kojeg sudije ostati na prijavi nezakonitog deljenja autorskog dela, ukoliko se kao dokaz za to prilože dokazi o počinjenom krivičnom delu od strane nosilaca autorskog prava. Drugim rečima, nosioci autorskog prava bi morali sebe da inkriminišu kao počinioce krivičnog dela, da bi ostvarili svoj interes u parnici. Otuda se oni mogu efikasno zaštititi samo od onih lica koja se piraterijom bave na očigledan način – na primer održavaju sajtove na kojima se mogu u celini preuzeti autorska dela, ili sajtove sa strimingom autorskih dela, ili katalogom autorskih dela koja korisnici mogu poručiti. U takvim situacijama obično je reč o *lukrativnom bavljenju* nedozvoljenom praksom i očiglednom masovnom kršenju autorskog prava, i neće biti nikakvih prepreka da se interesi nosilaca autorskog prava zaštite pred sudom. U svakom drugom slučaju to neće biti nimalo lako – otuda se verovatno sudska zaštita prava preskače, odnosno zanemaruje, i dolazi do pokušaja zastrašivanja korisnika Interneta preko njihovih operatora.

„Do podataka o kršenju autorskog prava nosioci autorskog 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 povredu autorskog prava i prosleđuje ih nosiocima autorskog 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, 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."[49]

Nosioci autorskog prava će u praksi ipak u izvesnom broju slučajeva koristiti druge načine pribavljanja podataka. Ovi načini su suprotni zakonu i to je nešto što im je zajedničko. Mogu se uočiti različite aktivnosti ovog tipa.

Najjednostavniji pristup problemu jeste – pridružiti se onima koji preuzimaju neautorizovani sadržaj putem elektronskih komunikacija. Nosioci autorskog prava nalaze fajlove koji se neautorizovano dele, pristupaju istoj takvoj aktivnosti i na taj način njihovi računari dolaze u direktnu komunikaciju sa ostalim korisnicima, što je dovoljno da saznaju njihove IP adrese, a na osnovu sadržaja koji sami preuzmu u takvoj komunikaciji mogu se uveriti

49 M. Reljanović, 137.

u sadržinu komunikacije. Nakon toga IP adrese prosleđuju operatorima i dešavaju se već opisane situacije – ili operatori nezakonito proslede podatke o licima koje su dobili na osnovu podataka koje su dobili od nosilaca autorskog prava, ili podatke o licima nezakonito koriste kako bi im direktno prosledili pisma opomene. „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 ličnosti može koristiti. Po istoj analogiji, kada stupa u preuzimanje (engl. *download*) 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."[50]

Drugi način jeste prisluškivanje, odnosno nezakonito presretanje podataka elektronske komunikacije. Ovo se ne odnosi samo na sekundarne podatke koji nastaju prilikom komunikacije, već i na sadržinu komunikacije. Ovde je reč o nelegalnom prisluškivanju koje predstavlja krivično delo iz člana 143. Krivičnog zakonika. Ukoliko se pokaže da su operatori (samostalno, ili na podstrekivanje nosilaca autorskog prava) izvršili ova dela, ili da su nosioci autorskog prava sami upotrebili odgovarajuću tehniku da bi prisluškivali komunikacije, protiv jednih i/ili drugih svaki korisnik Interneta može podneti krivične prijave ili se obratiti policiji, odnosno nadležnom tužilaštvu.

Osim ovih, postoji i specifičan način dolaženja do podataka kojem se ponekad pribegava. Taj sistem bi se mogao opisati kao „navođenje na povredu autorskog prava". Naime, nosioci autorskog prava mogu sami postaviti svoja autorska dela namenjenih za preuzimanje sa njihovih servera, besplatno i otvoreno. Najčešće se za takve aktivnosti postavljaju posebni Internet sajtovi koji na prvi pogled nemaju nikakve veze sa nosiocima autorskog prava (drugim rečima, podsećaju na piratske sajtove). Na njima se postavljaju primerci autorskih dela i nakon toga se beleže podaci ko sa postavljenih servera učestvuje u elektronskoj komunikaciji, odnosno preuzima autorska dela. Na ovaj način, koji za sada nije zabeležen u Srbiji, nosioci autorskog prava dolaze do podataka o licima koja preuzimaju neautorizovani sadržaj i šalju im pisma opomene. Ovakvo ponašanje jeste naravno nemoralno, može se čak i raspravljati o apsurdu da se borbom protiv piraterije ista podstiče od strane najvećih protivnika, a sve to zbog zastrašivanja lica čija individualna preuzimanja zasigurno ne predstavljaju najznačajniju opasnost po nosioce autorskog prava.

Očigledno je da je pretežniji interes svake države zaštita podataka o ličnosti i prava na privatnost i tajnost komunikacije, što u značajnoj meri ote-

50 *Ibid.*

žava dokazivanje (ili čak činjenje verovatnim) da postoji povreda autorskog prava putem elektronske komunikacije. Zbog toga bi valjalo sagledati kako pristupe koji su na raspolaganju nosiocima autorskog prava prema važećem zakonodavstvu, tako i ukazati na moguće alternativne pristupe problemu piraterije na Internetu uopšte.

7. ZAŠTITA AUTORSKOG PRAVA NA INTERNETU – MOGUĆA REŠENJA BEZ UGROŽAVANJA PRIVATNOSTI KORISNIKA

Reakcije nosilaca autorskog prava, koje su opisane u prethodnom tekstu, pre se mogu okarakterisati kao pokušaj zastrašivanja građana nego zaštite ugroženog i povređenog autorskog prava. Ovakav pristup nažalost nije ispravan i ne samo što neće dati željene rezultate u smislu prevencije daljih masovnih povreda, već dovodi do opasne logike da je dozvoljeno kršiti zakon da bi se povredom jednog prava zaštitilo neko drugo pravo.

Ukoliko se međutim uporedi kvalitet zaštite, kao uostalom i kvalitet prava, u sukobu prava na privatnost lica i prava na poštovanje autorskog prava nosilaca autorskog prava, sasvim je jasno da će prednost imati zaštita prava na privatnost. Ovo je jedno od osnovnih ljudskih prava, bez kojih se savremeni pravni sistem i savremeno društvo ne mogu zamisliti. Davanje bilo kakvih diskrecionih ovlašćenja privatnim licima da mogu suspendovati to pravo bez odluke suda, nezamislivo je kako u Republici Srbiji, tako i u bilo kojoj demokratski uređenoj državi. Granice upliva u tuđu privatnost strogo su postavljene i izuzetaka ne može biti, osim onih koji se odnose na zaštitu zaista većeg društvenog dobra i interesa – a ta zaštita je po pravilu vezana za krivični postupak, odluku suda i njeno sprovođenje na zakonom određeni način od strane za to ovlašćenih državnih organa. Sve ostalo predstavlja nezakonito delovanje nosilaca autorskog prava, odnosno drugih lica koja su uključena u opisane mehanizme zastrašivanja.

Imajući sve ovo u vidu, a opet niti jednog trenutka ne dovodeći u pitanje nužnost zaštite autorskog prava, postavlja se pitanje kako se to može postići? Čini se da postoji nekoliko aspekata odgovora na ovo pitanje.

Novi koncept autorskog prava podrazumeva daleko veću fleksibilnost nosilaca autorskog prava kada je reč o elektronskom okruženju. Sasvim je izvesno da se piraterija ne može zaustaviti represivnim merama. Sa jedne strane, korisnici primenjuju jednostavnu tržišnu logiku – proizvod nabavljaju pod uslovima koji su za njih najpovoljniji u svakoj situaciji, pa i kada se radi o autorskim delima. Autorsko pravo masovno se povređuje i u mnogim drugim proizvodnim granama – kao što postoje piratizovani filmovi, tako postoje na primer i krivotvoreni odeća i parfemi. Daleko je međutim lakše masovno distribuirati onaj proizvod koji se može pojaviti u elektronskom obliku, pa je percepcija piratizovanih autorskih dela daleko jednostavnija, što ceo koncept čini prihvatljivijim za većinu ljudi.

Istovremeno, pojam „piraterija" se predstavlja od strane nosilaca autorskog prava kao nešto kriminogeno i nezakonito, kao pojava koja postoji u svakom pojedinačnom slučaju bez obzira na namere korisnika Interneta u konkretnom slučaju, svest o tome da li je to što rade zabranjeno, broj autorskih dela koji na ovaj način pribave, kao i odsustvo namere da na taj način pribave bilo kakvu materijalnu korist.[51] Ovakav pristup bio je kontraproduktivan – širok pojam piraterije nije doprineo njenom smanjenju, već naprotiv daljoj popularizaciji. Međutim, postoje i drugačiji pristupi savremenom tržištu. Počev od različitih servisa, koji su poslednjih godina sve masovniji, a koji omogućavaju korisnicima veliki broj autorskih dela po simboličnim pojedinačnim cenama ili pretplatama[52], preko tzv. „stripizacije" koncepta autorskih dela[53], pa do revolucionarnih koraka koje preduzimaju pojedine produkcijske kompanije i televizijske stanice[54], čini se da korisnici nikada nisu imali više mogućnosti da po (simboličnim) cenama dođu do originalnih, kvalitetnih kopija autorskih dela, potpuno bezbednih za korišćenje. Ovi koncepti, koji očigledno predstavljaju budućnost i realnu alternativu izazovima elektronskog doba[55], trebalo bi da preovladaju kada je reč o autorskim

51 Pre nekoliko godina bile su aktuelne marketinške poruke u kojima su se „pirati" izjednačavali sa kradljivcima u samoposlugama.

52 U pitanju je koncept sa kojim je svoje poslovanje započeo servis iTunes, a koncept su preuzeli mnogi drugi distributeri muzičkih i igranih autorskih dela.

53 Fenomen „stripizacije" autorskih dela novije je prirode i nastao je kao posledica suočavanja strip autora sa pomenutim problemima masovne neautorizovane distribucije autorskih dela putem elektronskih komunikacija. Pojedini strip autori su zbog toga rešili da svoja kompletna dela učine potpuno besplatnim na Internetu (ličnim sajtovima, putem društvenih mreža, inkorporirane u sadržinu drugih sajtova, i slično), uz neograničenu mogućnost distribicije (uz navođenje autora). Na ovaj način, njihovi stripovi su veoma brzo stekli globalnu popularnost, a „kompenzaciju" za ovakav ustupak autori vide upravo u popularizaciji njihovih strip junaka i prodaji sekundarnih, marketinških proizvoda vezanih za stripove koje crtaju (na primer, garderobe sa likova strip junaka, potpisanih knjiga ili postera sa stripovima, i slično). Izdavači i distributeri stripova u SAD takođe imaju „dan besplatnog stripa", kojim pokušavaju da privuku nove čitaoce (vid. na primer analizu: C.Pinchefsky, Free Comic Book Day: When Free Comic Books Mean Big Business, *http://www.forbes.com/sites/carolpinchefsky/2012/05/03/p1563/* (1.4.2015). Jedan od poznatijih strip autora je, u intervjuu datom časopisu Wired povodom novog pristupa problemu strip piraterije od strane jedne od najvećih izdavačkih kuća, izjavio da je „piraterija loša samo za nekvalitetnu zabavu" (izvor: A. Lawson, Why DRM-free comic books are a big deal, even if you don't read comics, *http://arstechnica.com/staff/2013/07/why-drm-free-comic-books-are-a-big-deal-even-if-you-dont-read-comics/* (1.4.2015).

54 Kompanija HBO je najavila da će premijera jedne njene popularne televizijske serije biti održana praktično istovremeno u velikom broju zemalja, kao i preko pojedinih onlajn servisa. Ovo je izuzetan iskorak i veoma mudra borba protiv piraterije, budući da se po prvi put dešava da gledaoci širom sveta mogu da odgledaju neko autorsko delo istovremeno, na legalan način. Ovim putem se u najvećem delu obesmišljava piraterija – izvesno je da će oni gledaoci koji su u mogućnosti radije izabrati legalan i komforniji način gledanja. Izvor: B.Kuchera, HBO is fighting Game of Thrones piracy in the best possible ways, *http://www.polygon.com/2015/3/10/8184071/hbo-game-of-thrones-piracy-apple* (1.4.2015).

55 Ne treba zaboraviti ni autore koji se odriču materijalne komponente autorskog prava i svoje autorska dela objavljuju pod specifičnim licencama koje omogućavaju dalju dis-

delima koja se mogu izraziti, preneti i umnožiti u elektronskom obliku, a koja su danas predmet nedozvoljenog prometa. Na taj način se, bez ugrožavanja njihovih prava, korisnicima stvara realna i legalna alternativa; sa druge strane, na taj način će se onemogućiti delovanje komercijalnih piratskih sadržaja, odnosno isti će se učiniti neisplativim.

Nezavisno od ovih novih koncepata, ni delovanje u okviru postojećeg pravnog okvira u Republici Srbiji takođe ne predstavlja „nemoguću misiju" za nosioce autorskog prava. Sa jedne strane, trebalo bi staviti akcenat na one prekršioce koji se bave masovnim povredama autorskog prava, odnosno na nelegalan način omogućavaju preuzimanje autorskih dela da bi sebi pribavili imovinsku korist. Potrebno je skrenuti pažnju na značajnu razliku između primera gde se neko autorsko delo pribavlja „za ličnu upotrebu" i bez namere jedne i druge strane (onoga ko pribavlja i onoga ko to omogućava) da ostvare imovinsku korist daljim stavljanjem u promet primerka tog dela i slučajeva u kojima se sistemski i u velikom broju, radi ostvarivanja imovinske koristi, autorska dela nude korisnicima (na primer, različiti sajtovi koji dopuštaju „striming" ili preuzimanje filmova i drugih igranih i dokumentarnih programa). I u takvim slučajevima, kada se radi o krivičnom delu, akcije nosilaca autorskog prava moraju biti isključivo zakonite i usmerene na saradnju sa nadležnim tužilaštvom, odnosno odeljenjem za visokotehnološki kriminal. Svako preuzimanje ovlašćenja koja poseduju isključivo policija i tužilaštvo, odnosno sud, predstavlja krivično delo. Sa druge strane, blagovremena reakcija državnih organa može proizvesti veoma dobar učinak kada je reč o ovakvim pojavama.[56]

Kao što je već napomenuto u prethodnom tekstu, ZASP predviđa zaštitu od povrede autorskog prava u parničnom postupku. U težim slučajevima povrede, nosilac autorskog prava može podneti krivičnu prijavu za počinjeno krivično delo „Neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava" iz člana 199. Krivičnog zakonika. Postupak u parnici je hitan, a članovima 210. do 212. ZASP predviđeno je i izricanje privremenih mera, kao i obezbeđenje dokaza: „*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*

tribuciju, reprodukciju i druge načine korišćenja autorskog dela. Vid.: D. Prlja, M. Reljanović, Z. Ivanović (2012) 27-32.

56 Vid. na primer: Zaustavljen sajt Baneprevoz, *http://www.novosti.rs/vesti/kultura.71.html:380424-Zaustavljen-sajt-Baneprevoz* (1.4.2015). U konkretnom slučaju, Udruženje izdavača i knjižara Srbije predalo je tužilaštvu krivičnu prijavu protiv lica koje je držalo sajt sa hiljada primeraka skeniranih knjiga. Akcijom tužilaštva, odnosno policije, sajt je ugašen a došlo se i do vlasnika domena koji je procesuiran, dok su skenirani materijali zaplenjeni.

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." Nosilac autorskog prava stavljen je ovim odredbama u dosta zavidan položaj. On mora učiniti verovatnim da je njegovo pravo povređeno, da bi pokrenuo čitav niz akcija koje služe njegovoj zaštiti. Sasvim je izvesno da pod meru obezbeđenja i prikupljanja dokaza potpadaju i podaci o Internet saobraćaju koji se nalaze kod internet operatora, i to je jedini legalni put za njihovo pribavljanje. Pri tome, valja napomenuti da se ovde radi samo o sekundarnim podacima elektronske komunikacije – prikupljanje primarnih podataka, odnosno sadržine komunikacije, ostaje rezervisano za krivični postupak.

Zadiranje u privatnost korisnika Interneta kao pojedinca ne može imati preventivni učinak, između ostalog zato što je nezakonito i jedino može da proizvede niz novih sporova između dve strane. Nosioci autorskog prava u takvoj pravnoj borbi nemaju puno šansi za uspeh, zbog toga se njihova politika mora drastično menjati. Pravna akcija stoga mora biti usmerena na one koji se organizovano bave vršenjem povreda autorskog prava, uz komplementarnu vanpravnu akciju – približavanje većeg broja autorskih dela korisnicima elektronskim putem, po pristupačnim cenama.

Mario Reljanović, Ph.D
Assistant Professor, University Union, Belgrade

COPYRIGHT AND THE RIGHT TO PRIVACY OF ELECTRONIC COMMUNICATIONS IN THE REPUBLIC OF SERBIA

Abstract: *The development of electronic communication favors the development of unauthorized copying and distribution of copyrighted works through the Internet. Massive scale of this phenomenon in recent years, has caused different reactions of copyright owners, from media campaigns against piracy to greater engagement in the detection and prosecution of persons engaged in the illegal distribution of copyrighted works. In an effort to combat these negative phenomena, copyright holders in the Republic of Serbia initiated the practice of sending „warning letters" against persons downloading copyrighted works that were illegally placed in the distribution. This „warning letters" were sent via Internet service providers, thus violating the right to privacy of Internet users since it was quite certain that the copyright holders or their legal representatives, could not find a legal way to get information about the contents of electronic communications of individuals on the Internet. The behavior of the copyright holders raised series of questions, among which the most important were: how Internet users had to behave in a case they got a warning letter? What was the role of Internet providers in this strange relationship? How could copyright holders be effectively protected without compromising the rights of others? Research aimed to find the appropriate responses by analyzing the position of all three parties in this situation (copyright holders, Internet service providers, Internet users) in the legal system of the Republic of Serbia, as well as through the analysis of possible remedies that could be used to stop unauthorized distribution of copyrighted works. It also pointed out to new tendencies in solving such problems in alternative ways, within the existing legal framework.*

Key words: *Electronic communication. – Copyright. – Right to privacy of communication. – Cybercrime.*