Dragan Prlja
Mario Reljanović Zvonimir Ivanović

INTERNET PRAVO

Institut za uporedno pravo
Beograd, 2012.

KORICE

Dr Dragan Prlja

Dr Mario Reljanović

Dr Zvonimir Ivanović

INTERNET PRAVO

Izdavač

INSTITUT ZA UPOREDNO PRAVO BEOGRAD

Recenzenti

Dr Jovan Ćirić

Dr Miodrag Savović

Dr Katarina Damnjanović

Urednik

Dr Jovan Ćirić

Tiraž

300

ISBN 978-86-80059-83-9

www.comparativelaw.info

DR DRAGAN PRLJA

DR MARIO RELJANOVIĆ

DR ZVONIMIR IVANOVIĆ

INTERNET PRAVO

BEOGRAD

2012

SADRŽAJ

1. UVOD

Šta je to što se može nazvati „internet pravom“? Na ovo pitanje nema jednostavnog odgovora, ali je sigurno da pravne norme na međunarodnom i nacionalnom nivou moraju da obuhvate što veći broj novonastalih situacija i pruže jasna pravila po kojima će se ponašati učesnici u sajber prostoru kako bi imali što viši nivo pravne zaštite. Sajber prostor, kao virtualni prostor bez jasnih fizičkih granicasvakodnevno stavlja na muke veliki broj pravnika širom planete. Njihov je zadatak da osmisle međunarodne konvencije i nacionalne propise koji će u što većoj meri moći da pomognu u rešavanju mnogobrojnih konfliktnih situacija. Nedozvoljeni pristup računarima i računarskim sistemima, računarske prevare, računarske sabotaže, širenje računarskih virusa, krađa autorskih dela, preuzimanje virtuelnog indentiteta, preuzimanje kontrole nad tuđim računarima, izmena, brisanje ili unošenje netačnih podataka u bazama podataka, prisluškivanje, ometanje, i presretanje elektronskih komunikacija, virtuelni upadi u zaštićene mreže i bankarske sisteme, širenje pornogrfaskih sadržaja, širenje rasne, verske, nacionalne mržnje virtuelnim putem, prodaje nelegalnih supstanci i drugih predmeta preko računarskih mreža, upravljanje i kontrola nad sajber prostorom, bezbednost elektronskog potpisa i elektronskih ugovora, sukob nadležnosti kod sudskih postupaka, prikupljanje elektronskih dokaza u sudskim i drugim postupcima, i mnoga druga pitanja predstavljaju veliki izazov današnjice.

Knjiga koja se nalazi pred vama rezultat je nastojanja da se čitaocu ukaže na najveći broj pravnih problema koji mogu nastati korišćenjem sajber prostora za komunikaciju, za protok podataka i informacija, kao i za prodaju roba i usluga. Nastojali smo da predstavimo do sada postignute rezultate u pravnom regulisanju sajber prostora i posebno pitanja vezanih za autorska prava, za zaštitu podataka i privatnosti, elektronsko poslovanje, i visokotehnološki kriminal.

Istraživanje internet prava već danas predstavlja izuzetno važnu oblast, a sigurno je da će pravno regulisanje ove oblasti biti još i važnije u budućnosti, pa ova knjiga može da predstavlja početni korak u upoznavanju sa velikim brojem različitih problema koji nastaju u sajber prostoru, a kako se odražavaju na naš svakodnevni život oni moraju da budu adekvatno pravno regulisani.

Autori

2. AUTORSKA PRAVA I INTELEKTUALNA SVOJINA U SAJBER PROSTORU

Sajber prostor je trenutno najveći resurs informacija na svetu. On je široko otvoren za postavljanje i preuzimanje informacija. 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 krše autorska prava. Mnogi su čak sasvim pogrešno ubeđeni da autorska prava nisu zaštićena 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 je svako autorsko delo na internetu zapravo zaštićeno autorskim pravom na osnovu Bernske konvencije o autorskim pravima i na osnovu nacionalnih zakona o autorskim pravima bez obzira da li je to na samom delu naznačeno ili nije. Naravno postoji i veliki broj autorskih dela u sajber prostoru koja su u javnom domenu, odnosno čije slobodno korišćenje je svima dozvoljeno, ali to mora biti na samom autorskom delu izričito naznačeno. Autori se mogu odreći nekih svojih autorskih prava u korist korisnika u sajber prostoru, ali i to mora takođe biti izričito naznačeno. Postoje i autorska dela kojima su zbog protoka vremena istekla imovinska ovlašćenja autorskog prava. Ta autorska dela su takođe postala javno dobro, odnosno prešla u javni domen.

Da li korisnici interneta smeju da kopiraju autorska dela i šalju ih drugim korisnicima internet bez znanja autora? Šta je to "fer upotreba" autorskog dela? Kakvi sve oblici odgovornosti postoje i koji uslovi treba da budu ispunjeni da bi pojedinac, ili pravno lice odgovaralo za kršenje autorskih prava? Ova i mnoga druga pitanja predstavljaju danas, a predstavljaće i u budućnosti pitanja od izuzetnog značaja.

Razvoj informacionih tehnologija i interneta prouzrokovao je povećanje različitih oblika ugrožavanja intelektualne svojine u sajber prostoru. Gotovo neograničena dostupnost književnih dela, naučnih radova, muzičkih radova, video radova, i drugih autorskih dela u digitalnom obliku uzdrmala je iz temelja tradicionalni koncept autorskih prava. On je morao da doživi ograničenja i promene pod uticajem novih koncepata: licenci otvorenog sadržaja, *copyleft*-a, softvera otvorenog koda, znanja kao javnog dobra, licenci kreativne zajednice (*Creative Commons Licenses*), slobodne razmene informacija, itd.

2.1. O AUTORSKIM PRAVIMA I SAJBER PROSTORU

2.1.1. Intelektualna svojina i autorsko pravo

Razvojem informacionih tehnologija, interneta, digitalnog sveta, i sajber prostora doneo je mnogobrojne izazove klasičnim konceptima u mnogim oblastima prava, pa ni oblast intelektualne svojine i autorskih prava nije bila izuzetak.

Izraz „intelektualna svojina" definisan je u Konvenciji o osnivanju Svetske organizacije za intelektualnu svojinu donetoj 1967.g. i kasnije izmenjenoj 1979.g. U članu dva te Konvencije data je definicija intelektualne svojine kao *prava* koja se odnose na: - književna, umetnička i naučna dela, - interpretacije umetnika i izvođača, fonograme i radio i TV emisije, - pronalaske u svim oblastima ljudske aktivnosti, - naučna otkrića, - industrijski dizajn, - fabričke, trgovačke i uslužne žigove, kao i trgovačka imena i trgovačke nazive, - zaštitu od nelojalne utakmice i sva druga prava vezana za intelektualnu aktivnost u industrijskoj, naučnoj, književnoj i umetničkoj oblasti.".[1]

Pojam *intelektualna svojina* označava stvaralaštvo uma, odnosno ovaj pojam pre svega obuhvata pronalaske, književna i umetnička dela, simbole, imena i slike koje se koriste u trgovini. Intelektualna svojina nije konkretno, materijalno vlasništvo nad nekim predmetom, već *pravo* odnosno skup ovlašćenja koje pravni poredak zemlje priznaje nosiocu prava intelektualne svojine. Ova prava imaju autori, pronalazači i ostali nosioci prava intelektualne svojine.

Intelektualna svojina je unikatna i ona je plod lične kreativnosti i inovativnosti. To može biti bilo koja aktivnost iz bilo koje oblasti života: pronalazak iz bilo koje oblasti tehnike, ime pod kojim se prodaje proizvod ili nudi usluga, pesma, slika, film, i sl. Skoro u svakom pojedinačnom slučaju, intelektualna svojina stimuliše napredak, transformišući društvo i dodajući vrednost našem životu.[2]-

Intelektualna svojina je podeljena na dve kategorije: industrijsku svojinu i autorsko pravo.

Industrijska svojina obuhvata patente za pronalaske, žigove, industrijski dizajn i geografske oznake i oznake porekla, i topografiju integrisanih kola.

---

[1] *Convention Establishing the World Intellectual Property Organization*, Internet adresa: http://www.wipo.int/wipolex/en/wipo_treaties/text.jsp?doc_id=131054&file_id=190032#P50_1504, 22.11.2010.

[2] *Zaštita intelektualne svojine u Srbiji*, Internet adresa: http://www.scribd.com/doc/56780927/Zasitita-intelektualne-svojine, 20.02.2012.

Autorsko pravo kao koncept nastaje u 18 veku sa osnovnom idejom da se zaštite prava autora, jer su knjige preštampavane bez odobrenja autora i bez plaćanja naknade autorima. Autorsko pravo se prvo štitilo u štamparskoj industriji, a kasnije se proširilo i na sva ostala autorska dela.

U okviru intelektualne svojine neki autori posebno izdvajaju baze podataka kao novu *sui generis* oblast intelektulne svojine.[3]

Danas pojam autorsko pravo obuhvata zapravo *autorsko pravo* i *srodna prava*.

2.1.2. Autorsko pravo i srodna prava

Izraz autorsko pravo karakterističan je za evropsko pravo. U anglosaksonskom pravu se koristi izraz *kopirajt (copyright)*. Osnovna razlika između ova dva izraza je u tome što je autorsko pravo u suštini lično pravo autora bazirano na vezi između autora i njegovog dela, dok se kopirajt strikno odnosi na delo kao takvo.

Autorsko pravo uključuje, ali se ne ograničava, na književna dela (kao što su romani, poezija i drame), naučna dela (monografije, članci, predavanja), filmove, muzička dela, umetnička dela (kao što su crteži, slike, fotografije, koreografije, skulpture, itd.), referentna dela, novine, reklame, mape, tehničke crteže, kompjuterske programe, baze podataka i delo arhitekture.

Zakoni u nekim zemljama definišu autorsko pravo kao pravo autora književnih, naučnik, stručnih i umetničkih dela.[4] Pored autorskog prva postoje *i prava srodna autorskom pravu.* Autorskom pravu srodna prava odnose se na prava i obim pravne zaštite umetničkog izražaja, te zaštite organizacionih, poslovnih i finansijskih ulaganja u izvođenje, proizvodnju, distribuciju i radiodifuziju autorskih dela, a obuhvataju:

- prava umetnika izvođača na njihovim izvođenjem;
- prava proizvođača fonograma na njihovim fonogramima;
- prava filmskih producenata (proizvođača videograma) na njihovim videogramima;
- prava organizacija za radiodifuziju na njihovim emisijama;
- prava izdavača na njihovim izdanjima;

---

[3] Koumantas Georges, *Reflections on the Concept of Intellectual Property*, in: Inellectual Property and Information Law, Kluwer, 1998, pp. 41. Jehoram Tobias Cohen, *Copyright in Non-Orginal Wrutings Past - Present - Future ?*, in: Inellectual Property and Information Law, Kluwer, 1998, pp. 108.

[4] *Zakon o autorskim i srodnim pravima*, Službeni Glanik RS 104/2009, 99/2011.

- prava proizvođača baza podataka na njihovim bazama podataka.

Zakon o autorskim i srodnim pravima u Srbiji pod strodnim pravima obuhvata: „pravo interpretatora, pravo proizvođača fonograma, pravo filmskog producenta (proizvođača videograma), pravo proizvođača emisije, pravo proizvođača baze podataka, i pravo izdavača koje obuhvata dva osnovna prava: pravo prvog izdavača slobodnog dela (dela koje je u javnom domenu, a koje prethodno nije bilo izdato) i pravo izdavača štampanih izdanja na posebnu naknadu“.[5]

Autorsko pravo i srodna prava ključni su za ljudsko stvaralaštvo, jer pružaju autorima podsticaj u obliku priznanja i novčanih naknada, a s druge strane pružaju im određenu sigurnost da se njihova dela mogu distribuirati bez straha od neovlašćenog kopiranja ili piraterije, a ukoliko do toga dođe, osigurana im je određena zaštita autorskog prava.

2.1.3. Nosioci autorskih i srodnih prava

Nosiocima autorskog prava nazivaju se stvaraoci dela zaštićenih autorskim pravom i njihovi naslednici i pravni sledbenici.

Nosilac autorskog prava je fizička osoba - *autor* - koja je stvorila originalnu intelektualnu tvorevinu (autorsko delo), koja ima originalnost i određenu formu. Autoru pripada autorsko pravo na njegovom delu činom stvaranja dela bez ispunjavanja bilo kakvih formalnosti, kao što su registracija ili depozit dela.

Autorom se smatra ličnost čije je ime, pseudonim ili znak na uobičajen način označen na primercima dela dok se ne dokaže suprotno. Ako je više autora učestvovalo u izradi dela radi se o koautorskom delu. Ako je tako ostvareno delo nedeljiva celina, koautorima koji su učestvovali u stvaranju dela svojim stvaralačkim doprinosom, pripada zajedničko autorsko pravo na stvorenom delu. Ako dva ili više autora sastave svoja dela radi njihovog zajedničkog korišćenja, svaki od autora zadržava autorsko pravo na svom autorskom delu.

Nosilac srodnih prava može biti svaka fizička i pravna osoba, osim prava umetnika izvođača koje, po svojoj naravi, pripada fizičkoj osobi koja izvede delo iz književnog ili umetničkog područja ili izražaje folklora.

[5] *Ibidem.*

Korisnik srodnih prava može biti: interpretator (glumac ili muzičar) za izvođenje autorskog dela, proizvođač zvučnih zapisa (na kasetama, kompakt diskovima, itd) za njihove snimke, i organizacija za radiodifuziju za njihove radio ili TV programe, filmski producent, proizvođač baze podataka, itd.

2.1.4. Sadržina autorskog prava

Sadržaj atorskog prava obično određuje nacionalna zakonska regulativa u ovoj oblasti, a obično je to zakon o autorskim i srodnim pravima.[6] Na osnovu ovog zakona „nosioci autorskog prava" imaju isključivo pravo da koriste ili ovlaste druge da koriste delo pod dogovorenim uslovima. Nosilac (nosioci) prava na delo može da zabrani ili odobri: njegovo reprodukovanje u svim oblicima, uključujući štampanje i zvučne zapise; njegovo javno izvođenje i saopštavanje javnosti; njegovo emitovanje; njegovo prevođenje na druge jezike; i njegovu adaptaciju, kao što je roman koji se transponuje u scenario za film.

Mnogi tipovi dela, zaštićeni na osnovu zakona o autorskim i srodnim pravima, zahtevaju masovnu distribuciju, saopštavanje, i ozbiljno finansijsko investiranje za njihovo uspešno širenje i plasiranje (na primer, publikacije, zvučni zapisi i filmovi), stoga stvaraoci često ustupaju prava na svoja dela kompanijama koje će najbolje moći da razvijaju i plasiraju delo na tržištu, tražeći za uzvrat naknadu u obliku isplate i/ili autorskog honorara (naknada je zasnovana na procentu od prihoda koji donosi delo, ili paušalnoj naknadi).

Autorsko pravo se sastoji od:

- moralnih prava autora - štite lične i duhovne veze autora s njegovim delom,
- imovinskih prava autora - štite imovinske interese autora u pogledu korišćenja njegovih dela,
- drugih prava autora - štite ostale interese autora u pogledu njegovog dela.

Moralna prava autora obuhvataju:

- Pravo objavljivanja – autor ima pravo da odluči kada i kako će njegovo delo da postane pristupačno javnosti,
- Pravo na priznanje autorstva – autor ima pravo da bude priznat i označen kao autor dela (pravo paterniteta), i svaka ličnost koja javno koristi autorsko delo je dužna da na

[6] *Ibidem.*

odgovarajući način naznači autora dela (na primer na grafičkom izdanju dela, na programu koncertne izvedbe dela i sl.), osim ako autor u pisanom obliku izjavi da ne želi da bude naveden.

- Pravo na poštovanje autorskog dela i čast ili ugled autora – autor ima pravo da se usprotivi svakom deformisanju, sakaćenju ili drugoj izmeni svojeg dela (pravo integriteta) i svakom korišćenju dela koji ugrožava njegovu čast ili ugled (pravo na reputaciju),
- Pravo pokajanja – autor ima pravo da opozove pravo korišćenja dela i da spreči njegovo daljnje korišćenje uz nadoknadu štete korisniku toga prava, ako bi daljnje korišćenje škodilo njegovoj časti ili ugledu. Time se uvažava činjenica da je autorsko delo odraz autorove ličnosti, iz čega sledi da se autoru daje pravna mogućnost da na specifičan način utiče na buduće korišćenje svojeg već objavljenog ili izdatog dela. Pravo pokajanja traje za života autora i on ga se ne može odreći.[7]

Imovinska prava su isključiva prava autora, jer autor može da odobri ili zabrani korišćenje svog dela na bilo koji način. Time se potvrđuje apsolutnost (delovanje prema svima) autorskih imovinskih prava koja naročito obuhvataju pravo reprodukcije, pravo distribucije (stavljanja u saobraćaj), pravo saopštavanja javnosti te pravo prerade. Ona obuhvataju svaki oblik iskorištavanja autorskog dela kod kojeg dolazi do izražaja potreba za zaštitom imovinskih interesa autora. Imovinska prava autora prava manifestuju se naročito kao:

- pravo reprodukcije (pravo umnožavanja) – pravo izrade autorskog dela u jednom ili više primeraka, u celosti ili u delovima, neposredno ili posredno, privremeno ili trajno, bilo kojim sredstvima i u bilo kojem obliku.

- pravo distribucije (pravo stavljanja u saobraćaj) i iznajmljivanje – pravo distribucije je isključivo pravo stavljanja u saobraćaj izvornika ili primeraka autorskog dela prodajom ili na koji drugi način. Iznajmljivanje označava davanje na korišćenje izvornika ili primeraka

[7] U Zakonu o autorskom i srodnim pravima ova prava su nabrojana kako sledi i pod ovim nazivima: pravo paterniteta, pravo na naznačenje imena, pravo objavljivanja, pravo na zaštitu integriteta dela (koje se sastoji od tri prava- zabrana izmena, suprotstavljanje javnom saopštavanju dela u izmenjenoj ili nepotpunoj formi, dozvola prerade dela), pravo na suprotstavljanje nedostojnom iskorišćavanju dela (to je ugrožavanje časti i ugleda autora), dok je pravo na pokajanje predviđeno ne u članovima koji regulišu moralna prava već u delu koji se odnosi na izdavački ugovor.

dela u ograničenom periodu, radi ostvarivanja neposredne ili posredne imovinske ili komercijalne koristi, kao i o pravu davanja primeraka dela u zakup.

- pravo saopštavanja autorskog dela javnosti obuhvata:
    - pravo javnog izvođenja (npr. izvođenje uživo na priredbi ili koncertu, recitovanjem ili sviranjem i pevanjem),
    - pravo javnog predstavljanje scenskih dela (npr. scenska izvedba dramskog dela u pozorištu)
    - pravo javnog prenošenja izvođenja ili predstavljanja (npr. kada se muzičko delo koje se javno izvodi uživo u koncertnoj dvorani, istovremeno saopštava javnosti izvan prostora te dvorane pomoću zvučnika ili na ekranu),
    - pravo javnog saopštavanja fiksiranog dela (npr. puštanje muzike s CD-a putem muzičkih linija i CD plejera),
    - pravo javnog prikazivanja,
    - pravo radiodifuzijskog emitovanja,
    - pravo radiodifuzijskog reemitovanja (slučaj kada se delo koje je primarno emitovala jedna organizacija za radiodifuziju istovremeno u celosti i u neizmijenjenom obliku reemituje putem kablovske mreže ili od strane druge organizacije za radiodifuziju),
    - pravo javnog saopštavanja radiodifuzijskog emitovanja (slučajevi javnog saopštavanja kao što su oni kada se u ugostiteljskom objektu javno pušta muzika s radija ili televizije bez naplate ulaznica),
    - pravo stavljanja na raspolaganje javnosti (pravo saopštavanja javnosti putem Interneta ili druge slične globalne digitalne mreže).
- pravo prerade - isključivo je pravo na prevođenje, prilagođavanje, muzičku obradu ili koju drugu prepravku autorskog dela.

Takozvana *prava autora prema vlasniku primerka autorskog dela* su prava koja nose obeležja i imovinskih i moralnih prava, a ne mogu da se svrstaju ni u jednu od navedenih kategorija. Ona obuhvataju pravo sleđenja (pravo autora na odgovarajući udeo od prodajne cene, ostvarene svakom preprodajom originala njegova likovnog dela koja usledi nakon prvog otuđenja dela od strane autora, pod određenim uslovima) i ostala druga prava autora (pravo pristupa delu,

pravo zabrane javnog izlaganja dela – primerka dela likovne umetnosti, kao i preče pravo autora na preradu primerka dela arhitekture).

Vlasnik autorskih prava ima ekskluzivno pravo da reprodukuje delo zaštićeno autorskim pravom, da ga prerađuje i na osnovu toga stvara novo autorsko delo, da distribuira kopije autorskog dela, da izvodi autorsko delo ili ga predstavlja u javnosti. Svaka osoba koja neko od ovih prava koristi bez dozvole autora krši autorska prava autora, osim u slučajevima kada se to može kvalifikovatiu kao fer upotreba autorskog dela ili u slučajevima kada je autorsko pravo isteklo i autorsko delo je postalo javni domen.[8]

2.1.5. Autorska dela

Autorsko delo je originalna intelektualna tvorevina iz književnog, naučnog i umetničkog područja koja ima individualni karakter, bez obzira na način i oblik izražavanja, vrstu, vrednost ili namenu. Prema tome, bitne karakteristike, da bi se neko delo smatralo autorskim, su:

- *originalnost* intelektualnog (kreativnog) ostvarenja, odnosno ostvarenja ljudskog duhovnog stvaralaštva - originalnost (izvornost) u smislu autorskog prava ne zahteva apsolutnu novost, već se traži tzv. subjektivna originalnost (izvornost), odnosno novost u subjektivnom smislu. Delo se smatra subjektivno originalnim ako autor ne oponaša drugo njemu poznato delo i nosi „lični pečat“ autora.
- *književno, naučno,stručno ili umetničko područje* dela - navedena sintagma ima u autorskom pravu značajno šire značenje, nego što u teoriji književnosti znače književna dela, a u istoriji umetnostiumetnička dela.

Zaštitu autorskog prava uživaju izražaji, što podrazumeva vidljivu formu određene ideje koja se postiže pomoću različitih sredstava izražavanja, kao što su npr. pisana ili izgovorena reč, pokret tela, zvuk, kao različiti dvodimenzionalni ili trodimenzionalni oblik.

Autorska dela jesu naročito:

- jezična dela (pisana dela, govorna dela, računarski programi) - npr. romani, pesme, priručnici, novinski članci;
- muzička dela, s rečima ili bez reči;
- dramska i dramsko-muzička dela;

[8] Overbeck Wayne, Belmas Genelle, *Major Principles of Media Law*, Stamford: Cengage Learning, 2011, p. 238.

- koreografska i pantomimska dela;
- dela likovne umetnosti (s područja slikarstva, vajarstva i grafike), bez obzira na materijal od kojega su načinjena, te ostala dela likovnih umetnosti;
- dela arhitekture;
- dela primenjenih umetnosti i industrijskog dizajna;
- fotografska dela i dela proizvedena postupkom sličnim fotografskom;
- audiovizuelna dela (kinematografska dela i dela stvorena na način sličan kinematografskom stvaranju) - u pravilu filmovi;
- kartografska dela;
- prikazi naučne ili tehničke prirode kao što su crteži, planovi, skice, tabele i dr.

Prevodi, prilagodbe, muzičke obrade i druge prerade autorskog dela, koje su originalne intelektualne tvorevine individualnog karaktera, zaštićeni su kao samostalna autorska dela. Prevodi službenih tekstova iz područja zakonodavstva, uprave i sudstva zaštićeni su osim ako su učinjeni radi službenog informisanja javnosti i kao takvi objavljeni.

Zbirke samostalnih autorskih dela, podataka ili druge građe kao što su enciklopedije, zbornici, antologije, elektronske baze podataka i sl., koje prema izboru ili rasporedu sastavnih elemenata čine sopstvene intelektualne tvorevine njihovih autora, zaštićene su kao takve.

Narodne književne i umetničke tvorevine u izvornom obliku nisu predmetom autorskog prava, ali se za njihovo saopštavanje javnosti plaća naknada kao za saopštavanje javnosti zaštićenih autorskih dela.

Šta je to autorsko delo definiše svako nacionalno zakonodavstvo posebno, pa je to u Srbiji prema Zakonu o autorskim i srodnim pravima "orginalna duhovna tvorevina autora, izražena u određenoj formi, bez obzira na njegovu umetničku, naučnu ili drugu vrednost, njegovu namenu, veličinu, sadržinu i način ispoljavanja"[9].

Ovaj Zakon posebno, kao autorska dela navodi:

- pisano delo (knjiga, brošura, članak, prevod, računarski program u bilo kom obliku njihovog izražavanja, uključujući i pripremni materijal za njihovu izradu i dr.);
- govorno delo (predavanja, govori, besede i dr.);

[9] *Zakon o autorskim i srodnim pravima*, *op.cit.*

- dramsko, dramsko-muzičko, koreografsko i pantomimsko delo, kao i dela koja potiču iz folklora;
- muzičko delo, sa rečima ili bez reči;
- filmsko delo (kinematografska i televizijska dela);
- delo likovne umetnosti (slike, crteži, skice, grafike, skulpture i dr.);
- delo arhitekture, primenjene umetnosti i industrijskog oblikovanja;
- kartografsko delo (geografske i topografske karte);
- plan, skica, maketa i fotografija; i
- pozorišna režija[10].

2.1.6. Ograničenja autorskih prava

Objavljenim autorskim delom može da se koristi bez autorovog odobrenja ili bez autorovog odobrenja i bez plaćanja naknade, samo u slučajevima kada to zakon izričito dopušta:

- privremene radnje reprodukcije autorskog dela;
- reprodukcija autorskog dela – fizičko lice može reprodukovati autorsko delo na bilo koju podlogu ako to čini za privatno korišćenje, kao i reprodukovati autorsko delo u obliku fotokopije i za drugo sopstveno korišćenje, koje nema direktno ili posredno komercijalnu svrhu i nije namenjeno ili pristupačno javnosti. Nije dopuštena reprodukcija cele knjige osim ako su primerci te knjige rasprodani najmanje dve godine, notnih zapisa, elektroničkih baza podataka, kartografskih dela kao ni izgradnja arhitektonskog objekta;
- efemerne snimke - organizacija za radiodifuziju koja ima odobrenje za emitovanje autorskog dela može da snimi to delo sopstvenim sredstvima na nosač zvuka, slike ili teksta za potrebe sopstvenog emitovanja;
- javne arhive, javne biblioteke, obrazovne i naučne ustanove, ustanove za predškolski odgoj i socijalne (karitativne) ustanove, a koje svoje usluge ne naplaćuju, mogu iz vlastitog primerka reprodukovati autorsko delo na bilo koju podlogu u najviše jednom primerku;

[10] *Ibidem*.

- korišćenje autorskog dela u nastavi ili naučnom istraživanju, sudskim i upravnim odlukama, u svrhu informisanja javnosti;
- citati – dopušteno je doslovno navođenje odlomaka autorskog dela koje je na zakonit način postalo pristupačno javnosti, radi naučnog istraživanja, nastave, kritike, polemike, recenzije, osvrta, u meri opravdanoj svrhom koja se želi da se postigne i u skladu s dobrim običajima, time da se mora naznačiti izvor i ime autora;
- dopušteno je reprodukovanje autorskih dela koja su trajno smeštena na ulicama, trgovima, parkovima ili drugim mestima pristupačnim javnosti te distribuisanje i priopštavanje javnosti takvih reprodukcija, uz određene izuzetke;
- dopuštena je prerada autorskog dela u parodiju u meri koja je potrebna za njen smisao, kao i karikaturu, a uz navođenje dela koje se prerađuje i njegovog autora, prerada dela za lične potrebe koja nije namenjena i nije dostupna javnosti i prerada u vezi sa dozvoljenim korišćenjem dela, koja je prouzrokovana samom prirodom ili načinom tog korišćenja;
- za potrebe osoba sa invaliditetom, dozvoljeno je bez dozvole autora i bez plaćanja autorske naknade, umnožavanje i stavljanje u promet autorskog dela, ako to delo ne postoji u traženom obliku, ako je njegova upotreba u direktnoj vezi sa invaliditetom tih osoba i u obimu koji zahteva određena vrsta invaliditeta i ako to umnožavanje i stavljanje u promet nije učinjeno radi ostvarivanja posredne ili neposredne imovinske koristi.

Autorsko pravo *traje za života autora i sedamdeset godina nakon njegove smrti*, bez obzira kada je autorsko delo objavljeno.

Autorsko pravo na anonimnom autorskom delu i delu objavljenom pod pseudonimom traje sedamdeset godina od objave tog dela.

Prestankom autorskog prava, autorsko delo postaje javno dobro, te može slobodno da se koristi uz obavezu priznanja autorstva, poštovanja autorskog dela te časti ili ugleda autora.

Autorsko pravo ne štiti ideje, naučna otkrića, postupke, metode rada i matematičke koncepte, službene tekstove iz područja zakonodavstva, uprave i sudstva (npr. pravne propise, upravne akte, sudske presude), kao ni njihove zbirke koje su objavljene radi službenog

informisanja javnosti (službena glasila, dnevne novosti i druge vesti koje imaju karakter obične medijske informacije.

2.1.7. Kršenje autorskih prava u sajber prostoru

Razmena fajlova

Razmena fajlova u sajber prostoru danas predstavlja najčešći oblik ugrožavanja autorskih prava. Poznat je slučaja „Napster" iz 2000.g. Napster je kao „*peer to peer*" servis za razmenu muzičkih fajlova omogućio milionima korisnika da razmenjuje uglavnom autorskim pravima zaštićene muzičke fajlove. Ovo je naravno izazvalo brojne sudske sporove, Napster je bankrotirao, ali se broj ovakvih servisa u sajber prostoru uvećao do neslućenih razmera. Ovi servise-i danas ne nude samo muzičke fajlove, već i sve druge fajlove, od fajlova muzičkih zapisa, video zapisa, filmova, pa sve do fajlova razne vrste softvera, odnosno kompjuterskih programa.

Kompanija Apple je 2003.g, uz dogovor sa kompanijama iz muzičke industrije i uz poštovanje autorskih prava, postavila svoj servis za razmenu muzičkih fajlova „iTune" namenjen korisnicima „iPoda" - muzičkih plejera, „iPhona" – mobilnog telefona, a danas i „iPada" - tablet kompjutera.

Kompanija *Google* je organizovala digitalnu biblioteku knjiga u okviru koje se nalazi ogroman broj digitalizovanih knjiga, ali komapnija nije imala odobrenje od velikog broja autora za digitalizaciju njihovih knjiga pa je u sporu koji su vodili izdavači protiv *Google*-a tokom 2011.g. sud odlučio da je *Google* dužan da nadoknadi troškove autorima.[11]

Upravljanje digitalnim pravima

Upravljanje digitalnim pravima (*Digital rights management, DRM)* je termin koji označava tehnologije kojima se kontroliše pristup informacijama u digitalnom svetu od strane izdavača, odnosno vlasnika autorskih prava kako bi se ogrničilo korišćenje digitalnih sadržaja. To je samo jedan oblik zaštite autorskih prava i predstavlja digitalno zaključavanje intelektualne svojine da ne bi bila ukradena. Tipičan praktičan primer digitalnog upravljanja pravima je iTunes američke kompanije Apple. Ovakav vid upravljanja digitalnim sadržajem podržan je nizom

[11] Overbeck Wayne, Belmas Genelle, *Major Principles of Media Law*, Stamford: Cengage Learning, 2011, p. 281.

međunarodnih pravnih akata. U tehnološkom smislu upravljanje digitalnim pravima obezbeđuje kontrolu nad korišćenjem digitalnih medija ograničavanjem pristupa, kopiranja ili konverzije u druge formate od strane krajnjeg korisnika.

Protivnici koncepta upravljanja digitalnim pravima iznose argument da se tim vidom digitalne kontrole onemogućavaju korisnici da čine nešto što je potpuno u skladu sa zakonom: npr. da prave kopije CD-a ili DVD-a za svoje potrebe, da pristupaju radovima u javnom domenu, da koriste materijale za istraživanja i u obrazovne svrhe, u skladu sa fer upotrebom. Ovim argumentima brani se teza da je upravljanje digitalnim pravima u suprotnosti sa važećim propisima o autorskim pravima.

Važno je istaći razliku između analognih i digitalnih snimaka. Analognim audio ili video snimcima na pločama, magnetnim trakama, audio ili video kasetama skladišti se signal kao neprekidni talas za razliku od digitalnog signala (bilo kao audio ili kao video signal) koji se danas koristi, a koji se zapravo sastoji od podataka, kao jedan vid kombinacija brojeva: jedinica i nula. U slučaju analognog snimanja radi se o fizičkom snimanju na medijum (ploču ili kasetu), a u slučaju digitalnog snimanja radi se o upisivanje podataka u neki vid kompjuterske memorije . Analogni mediji ne mogu se kopirati bez gubitka kvaliteta, a kvalitet se kod analognih medija gubi i samim normalnim korišćenjem, dok se digitalni snimci mogu kopirati bez gubitka kvaliteta, a oni ne gube na kvalitetu usled korišćenja. Analogne snimke moguće je konvertovati u digitalne snimke jednostavnim postupkom od strane svakakog korisnika kompjutera.

Tehnologije upravljanja digitalnim pravima koriste se pre svega u industriji zabave (muzika, video, e-knjige, kompjuterske igrice, TV i Radio emitovanje, itd.). Ova tehnologija se zasniva na ugovorima sa ograničenim licencama na koje korisnici moraju da pristanu da bi imali pristup određenom web sajtu ili da bi preuzeli odgovarajući softver. Ovom tehnologijom se kontroliše pristup i reprodukcija online informacija, pa čak i njihovo kopiranje za ličnu upotrebu.

2.1.8. Javni domen

Pitanje javnog domena, odnosno javnog vlasništva je jedno od najčešće raspravljanih pitanja u vezi sa intelektualnom svojinom.

Danas javni domen označava *javno vlasništvo* intelektualne svojine. To je pravni institut anglosaksonskog prava i označava znanje i inovacije u odnosu na koje nijedna osoba, ili drugi pravni subjekt ne može (ili ne želi) da uspostavi ili održava vlasničke interese, pa ovakva

autorska dela i inovacije čine *deo opšteg kulturnog i intelektualnog nasleđa čovečanstva* koje u principu svako može da koristi ili iskorišćava.[12]

U istorijskom smislu javni domen je predhodio zaštiti intelektialne svojine. Prvo su sva kulturna i naučna dela predstavljala javni domen, pa se tek razvojem štamparske industrije i tržišta donose pravni propisi o zaštiti autorskih prava. Pojam javnog domena uobličen je krajem 19 veka. Viktor Igo, francuski književnik, 1878.g. je odredio dva glavna obeležja javnog domena: prvo da delo nakon što ga autor objavi nije više jedino njegovo vlasništvo već pripada i ljudskom duh, postaje *društveno javno dobro*, i drugo da je sigurna sudbina dela da jednog dana postane javno dobro. Bernska konvencija iz 1886.g. poziva se na javni domen kome pripadaju dela koja nemaju više autorsko pravnu zaštitu.[13]

Javni domen kao argument koriste mnogi kritičari sadašnjeg sistema zaštite intelektualne svojine. Pitanjem javnog dobra bavi se Svetska organizacija za intelektualnu svojinu, kao i mnogi političari i vlade. Mnogi projekti digitalizacija kulturnog nasleđa baziraju se na javnom domenu.[14]

Nikakva dozvola nije potrebna da bi se koristitio ili kopirao, odnosno distribuirao materijal koji je deo javne svojine bez obzira na svrhu ili namenu kako privatnu tako i komercijalnu (industrijsku). To se možete činiti potpuno besplatno, bez plaćanja prava na korišćenje, trajni, ili privremeni zakup licence i slično.

Javni domen se može definisati i kao suprotnost raznim oblicima zaštite intelektualne svojine, javni domen stoji nasuprot zaštićenim robnim markama (kod nas je prihvaćen termin „žig“), patentima i slično. Za materijal pod „javnim vlasništvom“ nema zakona koji ga čuva od korišćenja od strane članova društva. Može se reći da materijal koji je predmet javne svojine služi kao *osnov za novi kreativan rad*.

Prilikom definisanja pojma *javnog vlasništva* odnosno *javne svojine* može se reći da da je to ono što pripada svim ljudima. Kod korišćenja dela koji je deo javnog domena nema ni obaveze pozivanja na originalnog autora, iako se to smatra učtivim i fer odnosom. Međutim, treba imati na umu da iako je dozvoljena kreativna upotreba dela u javnom vlasništvu, kao i njegovo, menjanje, unapređivanje i/ili inkorporacija u druga dela, to ne znači da i novo delo koje može

[12] *Javno vlasništvo*, Internet adresa: http://sr.wikipedia.org/, 6.11.2010.g.
[13] Dusollier Séverine, *Scoping Study on Copyright and Related Rights and the Public Domain*, WIPO, 2010, Internet adresa: http://www.wipo.int/ip-development/en/ agenda/pdf/scoping_study_cr. pdf, 6.11.2010.
[14] *Ibidem*.

nastati tom prilikom predstavlja javnu svojinu, ono može da sadrži i delove koji spadaju pod domen zaštite autorskih prava, to jeste može biti vlasništvo autora koji ga je stvorio, te ukoliko nije jasno naznačeno da i to novo delo autor stavlja u javno vlasništvo treba predpostaviti da postoje neka zadržana prava.

Autorska prava centralnu pažnju poklanjaju eksploataciji rada, ali nikada ne regulišu sam pristup i upotrebu dela dok je kod javnog domena u prvom planu mogućnost intelektualnog pristupa delima u javnom domenu.[15]

Autorska prava bi trebala da ostvare fer balans između prava autora da kontroliše širenje svoga dela i javnog interesa da se delo što više širi i budu dostupno što većem broju ljudi.[16]

Javno dobro je generalno definisano kao materijal koji ne podleže zaštiti autorskih prava ili je materijal kome su autorska prava istekla, prestala da važe. Javno vlasništvo upućuje na potpuno odsustvo autorske zaštite dela, odnosno na intelektualnu svojinu koja nije kontrolisana od strane nekog.

Materijal, rad deklarisan kao javni domen ili vlasništvo se može smatrati delom "*javnog kulturnog nasleđa*", svaki član društva *s*e podstiče da ga koristi za svaku svrhu, uključujući kopiranje, modifikovanje, unapređenje, čak ga možete i prodati odnosno koristiti u komercijalne svrhe.

Autorsko delo postaje deo javnog domena ili onda kada originalni autor dela stavi delo na raspolaganje društvu, kada se svesno, dobrovoljno i neopozivo odrekne prava koja mu kao autoru dela sleduju, ili još češće kada prava na kopiranje i korišćenje nekog dela isteknu, odnosno kada delo dostigne određenu starost, ili kada originalni autor, odnosno nosilac prava ne produži prava koja ima ili ih se odrekne.

Autorska dela i inovacije mogu se naći u javnom domenu na različite načine:

1. *Izostankom pravne zaštite* zato što su: kreativna dela koja su nastala pre donošenja zakonske regulative u ovoj oblasti (dela Vilijama Šekspira, Ludviga van Betovena, Arhimedovi pronalasci, itd.), dela; narodne umotvorine, tradicionalni folklor; dela za koje se ne može utvrditi ko je autor, nekreativna dela koja zbog nedostatka kreativnosti ne podpadaju pod zaštitu zakona o

[15] *Ibidem*.
[16] Dworkin Gerald, *Judical Control of Copyright on Public Policy Grounds,* in: Inellectual Property and Information Law, Kluwer, 1998, pp. 137.

autorskim pravima (matematičke formule, sudske odluke, legislativa, intuitivno organizovane zbirke podataka, azbučni spiskovi, rezultati pretraživanja, itd.).[17]

2. *Istekom pravne zaštite* zato što je prošao rok. Većina autorskih prava ima rok trajanja i kad prođe taj rok delo ili patent prelazi u javno vlasništvo. Kod patenata taj rok je uobičajeno 20 godina, a kod autorskih prava je potrebno da se ispuni više uslova. Ti uslovi su: da je delo objavljeno pre 1.1.1923.g. ili najmanje 95 godina pre 1. januara tekuće godine, da je vlasnik autorskih prava umro najmanje 70 godina pre 1. januara tekuće godine, da nijedna država potpisnica Bernske konvencije o autorskim pravima nije odredila trajna autorska prava na određenom delu, da SAD i EU nisu donele pravni akt o produženju trajanja autorskih prava.

3. *Odricanjem od pravne zaštite*. Zakonom o autorskim pravima SAD sva dela stvorena od strane Vlade SAD stavljaju se u javno vlasništvo. Pojedine institucije i autori mogu se odreći pravne zaštite i preneti svoja dela u javni domen uz pomoć recimo GNU licenci za slobodnu dokumentaciju, licence slobodnog softvera, "copyleft" licenci, "Creative Common 0" licence. U slučaju kada je autor dela svesno, dobrovoljno i neopozivo stavio svoje delo u javni domen, on se odrekao svih prava koje je imao nad tim delom i ne može ih kasnije (u slučaju da proceni drugačije) opozvati, odnosno povratiti prava nad dotičnim delom. To znači da je u momentu stavljanja dela bio svestan da će se njegovo delo moći koristiti bez ikakve naknade, od bilo koga i na bilo koji način. Na primer, autori dela koji su svoje radove stavljali u javno vlasništvo pre 20-30 godina verovatno nisu mogli ni da predpostave da će se njihova dela koristiti u medijumu kao što je internet i na načine i u svrhe u koje se koriste. Preporukom Uneska iz 2003. godine koja se odnosi na univerzalni pristup sajber prostoru u okviru definicije javnog domena uključuju se i javni podaci i zvanične informacije koje stvaraju vlade i međunarodne organizacije i dobrovoljno im omogućuju pristup.[18] Praktično može se reći da materijal koji je deklarisan licencom "javno dobro" zapravo materijal sa nultom licencom. Odricanje od sadašnjih i budućih autorskih prava moguće je na osnovu pravnih propisa američkog zakonodavstva, koje reguliše "javni domen". U našem pravu takva mogućnost prenosa svih autorskih prava ili odricanja od svih autorskih prava ne postoji.[19]

---

[17] *Javno vlasništvo*, Internet adresa: http://sr.wikipedia.org/, 6.11.2010.g.
[18] Dusollier Séverine, *Scoping Study on Copyright and Related Rights and the Public Domain*, WIPO, 2010, Internet adresa: http://www.wipo.int/ip-development/en/ agenda/pdf/scoping_study_cr. pdf, 6.11.2010.
[19] *CreativeCommons*, Internet adresa: http://creativecommons.org.rs/faq. 6.11.2010.

Značaj postojanja javnog domena je veliki iz više razloga: obrazovnog, demokratskog, ekonomskog i slobodne konkurencije. Ta uloga je jednakog značaja kao i uloga postojanja autorskih prava, jer omogućuje kulturnu raznolikost, slobodu stvaranja, inovacije, razvoj kulture i nauke. Snažan i jak javni domen u kulturi i nauci omogućava stvaranja kulturnog blaga čovečanstva i dostupnost tog blaga svima. To je osnovni pokretač društvenog i ekonomskog razvoja i štiti od privatizacije, prisvajanja i predstavlja balans u odnosu na postojanje isključivosti intelektualne svojine.[20]

Veliku pretnju javnom domenu predstavljaju pokušaji stvaranja digitalnih monopola uz pomoću tehnoloških metoda ograničavanja pristupa digitalnim sadržajima.

Upravljanje digitalnim pravima predstavlja termin koji pokriva nekoliko različitih sistema i mehanizama *globalne kontrole sadržaja*. Drugim rečima, DRM je bi trebalo da ozakoni sisteme kontrole koji omogućavaju potpuno kontrolisanje digitalnih sadržaja, bilo koja upotreba da je u pitanju. Rani primer DRM-a su kriptovani DVD sadržaji koji su kodirani određenom enkripcijom čiji je ključ u vlasništvu DVD foruma i drži se u tajnosti, pa proizvođači DVD playera moraju potpisati određene ugovore kako bi mogli da reprodukuju kriptovani DVD sadržaj. Ovo je samo jedan od primera kako DRM propisi onemogućavaju slobodnu razmenu sardžaja, pa se često može čuti da bi skraćenica DRM trebalo da označava Digital Restrictions Management.[21]

2.1.9. Izazovi konceptu autorskih prava

Dugo se nije dovodio u pitanju koncept autorskog prava, ali sa pojavom i razvojem novih informacionih tehnologija i interneta koncept autorskih prava počinje da se značajno menja, odnosno da dobija alternativu u vidu otvorenog pristupa informacijama.

Nova politika autorskih 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".[22]

U drugoj polovini devedesetih godina uporedo sa razvojem informacionih tehnologija razvijala se i ideje stvaranja softvera otvorenog koda, odnosno besplatnog softvera. Autori

---

[20]Dusollier Séverine, *Scoping Study on Copyright and Related Rights and the Public Domain*, WIPO, 2010, Internet adresa: http://www.wipo.int/ip-development/en/ agenda/pdf/scoping_study_cr. pdf, 6.11.2010.

[21] Jelić Ivan, *Zajednica u savremenom informatičkom društvu*, 2006, Internet adresa: http://www.bos.rs/ cepit/idrustvo2/tema14/zajednica.pdf, 4.11.2010.

[22] Dimitrijević Predrag, *Pravo informacione tehnologije*, SVEN, Niš, 2010, str. 286.

ovakvog softvera omogućavali su drugima da softver: besplatno koriste, pristupaju izvornom kodu, distribuiraju, i da ga unapređuju, odnosno menjaju.[23]

Komisija Evropske unije 2007.g. ustanovila je licencu za besplatan softver odnosno softver otvorenog koda pod nazivom "The European Union Public Licence" (EUPL). Zvanična verzija ove licence dostupna je na 22 zvanična jezika EU. Danas u svetu postoji preko 100 različitih licenci ta besplatan softver, odnosno softver otvorenog koda.[24]

Pojava kopileft (eng. Copyleft) licence i licence otvorenog sadržaja (Open Content License) ukazuju na potrebu radikalne promenom međunarodne postojeće regulative autorskih prava u cilju stvaranja fundamentalnih prava na fer i javnu upotrebu u digitalnom svetu. Kopileft i Licence otvorenog sadržaja stvaraju samo subkulturalna ostrva slobodne upotrebe i distribucije radova u okviru velikog moru ne-slobodne medijske kulture.[25]

Ideja o stvaranju softvera otvorenog koda vremenom se sasvim očekivano proširila i na ostala autorska dela. Ova ideja stvaranja slobodnog softvera, odnosno otvorenog sadržaja, koja se pojavljuje sa nastankom digitalnog sveta radikalno menja koncept autorskih prava. Nasuprot ideji o genijalnom autoru koji svoje delo štiti autorskim pravima i drugima omogućava samo da budu pasivni korisnici suprotstavlja se ideja o autoru koji želi da omogući krajnjem korisniku da postane koautor, odnosno da može softver ili drugo delo da kopira, menja, unapređuje. Tako da te nove digitalne slobode, nova digitalna kultura omogućava običnom korisniku, običnom čoveku da postane koautor, da stvori novu vrednost, novo umetničko, književno ili drugo delo. Ovakav model fundamentalno menja tradicionalno shvatanje autorskih prava.Osnova ove nove ideje je da stvaralaštvo počiva na kreativnoj upotrebi postojećih dela u javnom domenu. Deo ove nove ideje je i saradnja desetina ili stotina autora u stvaranju jednog novog dela. Neka dela kao što su recimo velike enciklopedije moguće je stvoriti samo saradnjom velikog broja autora širom sveta. Dobar primer kako se na osnovu postojećeg autorskog dela uz pomoć kreativnosti stvara novo autorsko delo je hip hop muzika. Mnoge novostvorene kulturne vrednosti zapravo su zasnovane na kopiranju već postojećih autorskih dela. Dizajniranje novih medija, recimo na internetu, zasnovano je u velikoj merio na kopiranju postojećih fontova, skriptova, alata, itd. Nasuprot

---

[23]Dusollier Séverine, *Scoping Study on Copyright and Related Rights and the Public Domain*, WIPO, 2010, Internet adresa: http://www.wipo.int/ip-development/en/ agenda/pdf/scoping_study_cr. pdf, 6.11.2010.

[24] Internet adresa: http://www.osor.eu/eupl, 14.11.2010.

[25]Lawrence Liang, *Guide to Open Content Licenses*, 2004, Internet adresa: http://media.opencultures. net/open_content_guide/ocl_v1.2.pdf, 4.11.2010.

klasične ideje o autorskom pravu koje onemogućava dalje korišćenje i izmenu autorskog dela stoji ideja saradnje u stvaranju na bazi *slobodne razmene informacija u digitalnom svetu*. Pasivni korisnici autorskih dela postaju kreativni saradnici koji neprekidno obogaćuju javni domen dostupan svima. Javni domen predstavlja zajednički resurs koji je dostupan svima i koji se može koristiti bez potrebe dobijanja bilo kakvih odobrenja i dozvola. Nešto slično ulicama, parkovima, igralištima, koji su u javnom domenu i svi ih mogu koristiti.[26]

Enormnim povećanjem brzine protoka informacija i dostupnosti autorskih dela u svim oblicima dovelo je u nesrazmeru klasičan koncept autorskih prava sa potrebom postojanja javnog domena i mogućnosti dostupnosti znanja, kao i mogućnosti stvaranja novog znanja kao javnog dobra proisteklog iz javnog interesa.

Puno je razloga za omogućavanje pristupa autorskom delu kao otvorenom sadržaju. neki od tih razloga su:

- Autori koji još uvek nisu postali poznati žele da se što veći broj ljudi upozna sa njihovim delom, odnosno žele da ga popularišu kako bi izgradili svoju reputaciju. Na taj način se mogu obezbediti novi nastupi, novi sponzori, itd.,
- Izbegavaju se posrednici, distributeri i omogućava se direktan kontakt sa autorima,
- Autori koji dela ne stvaraju da bi zaradili već iz drugih razloga da bi širili svoje ideje,
- Ideja otvorenog sadržaja omogućava da se i zaradi tako što se akademskoj zajednici i neprofitnim organizacijama može omogućiti slobodan pristup, a zadržavaju se prava na komercijalnu upotrebu dela,
- Nepoznati autori mogu svoja dela ponuditi kao potpuno slobodan sadržaj, a ponuditi onima koji to žele da daju donacije onoliko koliko žele,
- Autori koji dela objavljuju na klasičan način, recimo u štampanim medijima, ako istovremeno objave svoje delo i na internetu kao otvoreni sadržaj obično tako pospešuju prodaju svog štampanog dela, jer omogućavaju kupcima da se sa njim upoznaju pre kupovine,

[26] *Ibidem*.

- Neki od autora su privučeni idejom intelektualne saradnje, odnosno idejom idealizma i njihov broj na internetu nije mali, i
- Mnogi autori finansirani su za svoj rad iz javnih sredstava pa je logično da njihova dela budu dostupna kao javno intelektualno dobro.[27]

2.1.10. Licence otvorenog sadržaja

Nove ideje o slobodnom softveru, slobodnom pristupu informacijama dobile su i svoje konkretne oblike u raznim licencama otvorenog sadržaja koje su trebale da predstavljaju sredstva ostvarivanje zajedničkog cilja proširenja dela dostupnih u javnom domenu. Ako je autor odlučio da omogući pristup svom delu kao otvorenom sadržaju sam autor donosi odluku o tipu licence koji želi da izabere, a kojom će preciznije definisati koja prava želi da zadrži. Naravno prva pretpostavka davanja licence otvorenog sadržaja je da autor ima važeće autorsko pravo kako bi mogao svoje ekskluzivna prava preneti na druge. Bez odobrenja autora u okviru određene licence nije moguće koristiti delo, odnosno ono se nalazi pod punom zaštitom autorskog prava. Sve licence otvorenog sadržaja u stvari određuju koje su slobode u odnosu na delo dozvoljene. Neka prava su zajednička za sve licence otvorenog sadržaja, kao što je to pravo na kopiranje, dok su druga vezana samo za određenu vrstu licenci, kao što je na primer prerada dela. Svako delo koje je stvoreno na osnovu postojećeg dela je prerađeno delo. Osnovna razlika između različitih vrsta licenci otvorenog sadržaja je baš u tome kako rešavaju pitanja vezana za novonastalo prerađeno delo. Kod GNU licenci zahteva se obavezno da delo koje je prerađeno na osnovu dela koje je pod GNU licencom mora biti licencirano pod GNU licencom. To zapravo znači da kada neko ima priliku da koristeći delo koje je pod licencom otvorenog sadržaja i na bazi njega stvori prerađeno delo nemože to delo sada učiniti nedostupnim, već ga mora licencirati kao otvoreni sadržaj. Na ovaj način se onemogućava da to novo prerađeno delo izađe iz javnog domena, kada je već nastalo na osnovu dela koje je u javnom domenu. Pitanje mogućnosti kontrole prerađenih radova na osnovu licence najvažnije je pitanje licenci otvorenog sadržaja. Još jedno jako važno pitanje licenci otvorenog sadržaja je pitanje korišćenja dela u komercijalne i nekomercijalne svrhe. Autor sam odlučuje da li će dozvoliti samo nekomercijalnu ili i komercijalnu upotrebu svog dela. Ako se odluči da omogući nekomercijalno korišćenje njegovog dela on i dalje može na osnovu svog

[27] *Ibidem*.

autorskog prava sklopiti ugovor sa izdavačem i objaviti svoje delo i ostvariti ekonomsku naknadu. Većina licenci otvorenog sadržaje zahtevaju poštovanje striktne procedure kako bi se moglo smatrati da je delo licencireno pod licencom otvorenog sadržaja. Licenciranje pod licencom otvorenog sadržaja nema nikakav uticaj na pravo fer korišćenja autorskih prava. To znači da i onaj ko ne želi da traži odobrenje autora, odnosno da prihvati licencu može koristiti svoje pravo na fer upotrebu dela u nekomercijalne i obrazovne svrhe. Karakteristika licenci otvorenog sadržaja da imaju standardnu klauzulu da ne daju nikakvu vrstu garancija, što je i očekivano jer se ne zahteva finansijska nadoknada za upotrebu dela.[28]

Licence otvorenog sadržaja mogu se podeliti na osnovu toga da li su opšteg tipa kao "Licence kreativne zajednice" li su namenjene za neki određen medij, kao što je na primer softver ili muzička dela. Prema prirodi licence otvorenog sadržaja mogu se podeliti na one koje promovišu "apsolutne " slobode sa malim ograničenjima, i one koje određuju jasna ograničenja sloboda korišćenja dela, kao što to čine "Licence kreativne zajednice".[29]

Slobodna umetnička licenca pojavila se 2000 godine i ona je omogućavala kopiranje, distribuciju i preradu dela pod uslovom da je jasno naznačena ova licenca, da je naveden autor orginala i da je naznačeno gde se orginal može pronaći. Prerađeni rad nastao na osnovu ove licence ostaje u javnom domenu i to pod Slobodnom umetničkom licencom.[30]

GNU pokret i zajednica koja se stvorila oko ideje slobodnog softvera predstavlja jednu od prvih praktičnih incijativa koja je urodila plodom omogućavajući ljudima da slobodno koriste prednosti informatičkih tehnologija. Ovaj pokret je osnovan 1984. godine sa ciljem stvaranja slobodnog operativnog sistema sličnog UNIX-u. GNU General Public Licence (GNU opšta javna licenca) - GNU GPL predstavlja svakako jednu od najpoznatijih licenci. Nastala je za potrebe stvaranja slobodnog softvera i njegovog pravnog regulisanja. Ova licenca omogućava četiri bazične slobode: sloboda korišćenja, kopiranja, modifikacije i distribucije modifikovanih verzija programa. Pored poštovanja sloboda korisnika, GNU GPL je ustanovio princip koji je nazvan "Copyleft", što u znači da se, u slučaju slobodnog softvera, on mora distribuirati pod istim uslovima pod kojima je dobijen. Na taj način je sloboda zaštićena u oba smera jer GPL daje slobodu i korisniku i softveru. Edukativni materijal i umetnička dela se takođe mogu objavljivati

[28] *Ibidem*.
[29] *Ibidem*.
[30] *Ibidem*.

pod uslovima koji korisnicima obezbeđuju zadovoljavanje u najmanju ruku elementarnih ljudskih prava korisnika i autora. Pored licence za softver, GNU projekat je iznedrio još jednu licencu koja je namenjena objaviljvanju dokumentacije pod nazivom GNU Free Documentation Licence (GNU licenca za slobodnu dokumentaciju) - GNU FDL. FDL je nastao za potrebe objavljivanja dokumentacije za slobodan softver i grubo rečeno omogućava dokumentaciji ono što GPL omogućava softveru. Ova licenca je jedna od najliberalnijih licenci za pisani materijal[31]

GNU Licenca za slobodnu dokumentaciju prevashodno je bila namenjena za dokumentaciju koja ide uz softver. Kasnije je ta licenca korišćena i za druge sadržaje, posebno kolektivna dela (na primer pod tom licencom je nastala Wikipedija). Ovom licencom se daje pravo kopiranja, distribucije, prerade i nekomercijalnog i komercijalnog korišćenja, ali prerađeni radovi moraju biti dati na korišćenje pod istom GNU licencom (copyleft).[32]

Licence kreativne zajednice (Creative Commons Licenses) danas predstavljaju najvažniji oblik licenci otvorenog sadržaja. Njima je predhodila Licenca otvorenog sadržaja (od 1998 do 2004) koja se inkorporirala u Licence kreativne zajednice. Ideja Kreativne zajednice je znatno šira od ponude samih licenci i ona se bazira na širenju znanja o autorskim pravima, javnom domenu, slobodi govora, itd. "Licence kreativne zajednice" omogućuju autoru da prvo izabere da li želi da zaštiti svoje delo ili ne, a potom ako se odluči za neku vrstu zaštite dela može da bira jednu od 6 vrsta licenci.[33]

2.1.11. Licence kreativne zajednice (Creative Commons Licenses)

Kreativno zajednicu, kao projekt i organizaciju, osnovao je Lawrence Lesing 2001.godine, ekspert za pitanja sajber prava, sa glavnom idejom da, slično kao i pokret za slobodan sofver, omogući korisnicima osnovne slobode kopiranja i distribuiranja radova zaštićenih autorskim pravima uz pomoć više različitih licenci koje se ne odnose na softver, već na sve druge oblike autorskih dela.[34]

---

[31] Jelić Ivan, *Zajednica u savremenom informatičkom društvu*, 2006, Internet adresa: http://www.bos.rs/ cepit/idrustvo2/tema14/zajednica.pdf, 4.11.2010.

[32]Lawrence Liang, *Guide to Open Content Licenses*, 2004, Internet adresa: http://media.opencultures.net/ open_content_guide/ocl_v1.2.pdf, 4.11.2010.

[33]*Ibidem*.

[34]Dusollier Séverine, *Scoping Study on Copyright and Related Rights and the Public Domain*, WIPO, 2010, Internet adresa: http://www.wipo.int/ip-development/en/ agenda/pdf/scoping_study_cr. pdf, 6.11.2010.

Osnovno pitanje kada se govori o delu koje se daje na korišćenje širokom krugu korisnika je način distribucije, odnosno zaštita autorskih prava autora dela. U svojim počecima, kopirajt je služio kao zaštita koju je autor primenjivao na svoje delo u cilju omogućavanja ili onemogućavanja kopiranja od strane izdavača. Krajnji korisnici nisu imali previše razloga protiv, jer se on odnosio samo na izdavače ne pogađajući konzumente dela koje mu je podlegalo. Razvoj računarskih tehnologija i mreža je omogućio masovnu razmenu informacija i znanja. Kopiranje i deljenje knjiga, muzičkih sadržaja ili bilo čega drugog je postalo lako i brzo. U tom momentu je *copyright* postao ograničenje i za korisnike, koji su sve navedene mogućnosti savremenih tehnologija imali u svojim rukama. Kreativna sloboda i mogućnost nesmetanog protoka informacija i znanja na žalost nisu postale civilizacijske tekovine. Izdavački i medijski lobiji su iskoristili kopirajt kao metod represije i kontrole pa umesto da zakoni štite korisnike i omogućavaju im slobodan pristup znanju, počeli su da služe kompanijama kao sredstvo kontrole. Moderna primena *copyright* u velikoj meri odstupa od njegove inicijalne primene. Umesto kontrole izdavača od strane autora, *copyright* služi kao sredstvo kontrole u rukama izdavača u oba smera: prema korisnicima i prema autorima. Sloboda je postala rezidualna kategorija dok autorska prava umesto autoru pripadaju izdavačkoj kompaniji za koja objavljuje njegov rad.[35]

Pojavljivanjem slobodnih licenci koje su omogućile stvaranje slobodnih sadržaja, pravila su dovedena u službu korisnika omogućavajući pravnu zaštitu slobode.[36]

Jedan od pokušaja zaustavljanja medijskih kompanija u ostvarivanju ekstraprofita predstavljaju fleksibilne licence koje autorima vraćaju pravo na svoja dela koja im producentske kuće u neku ruku uskraćuju. Licence kreativne zajednice predstavljaju set licenci koje autorima omogućavaju brzo i lako objavljivanje dela čime oni sami postavljaju uslove korišćenja svog dela umesto medisjkih kompanija koje to danas rade.[37]

Licence kreativne zajednice su svojim postojanjem omogućile određenu fleksibilnost u definiciji uslova pod kojima se delo objavljuje. Set licenci kreativne zajednice čini šest licenci koje se razlikuju po fleksibilnosti, od najslobodnije do najrestriktivnije. Njihova zajednička karakteristika je da korisnik ima pravo kopiranja sadržaja. Bitna karakteristika licenci kreativne zajednice je i to što autorima pomoću nekoliko klikova mišem i odgovora na vrlo trivijalna

---

[35] Jelić Ivan, *Zajednica u savremenom informatičkom društvu*, 2006, Internet adresa: http://www.bos.rs/cepit/idrustvo2/tema14/zajednica.pdf, 4.11.2010.
[36] *Ibidem.*
[37] *Ibidem*.

pitanja obezbeđuju pravnu regulativu za objavljivanje dela bez potrebe za saradnjom sa medijskim korporacijama.[38]

Šest licenci kreativne zajednice su:

1. *Autorstvo*

Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način odredjen od strane autora ili davaoca licence, čak i u komercijalne svrhe. Ovo je najslobodnija od svih licenci.

2. *Autorstvo - nekomercijalno*

Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način odredjen od strane autora ili davaoca licence. Ova licenca ne dozvoljava komercijalnu upotrebu dela.

3. *Autorstvo - nekomercijalno - bez prerade*

Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, bez promena, preoblikovanja ili upotrebe dela u svom delu, ako se navede ime autora na način odredjen od strane autora ili davaoca licence. Ova licenca ne dozvoljava komercijalnu upotrebu dela. U odnosu na sve ostale licence, ovom licencom se ograničava najveći obim prava korišćenja dela.

4. *Autorstvo - nekomercijalno - deliti pod istim uslovima*

Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način odredjen od strane autora ili davaoca licence i ako se prerada distribuira pod istom ili sličnom licencom. Ova licenca ne dozvoljava komercijalnu upotrebu dela i prerada.

5. *Autorstvo - bez prerade*

Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, bez promena, preoblikovanja ili upotrebe dela u svom delu, ako se navede ime autora na način odredjen od strane autora ili davaoca licence. Ova licenca dozvoljava komercijalnu upotrebu dela.

6. *Autorstvo - deliti pod istim uslovima*

Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način odredjen od strane autora ili davaoca licence i ako se prerada

[38] *Ibidem*.

distribuira pod istom ili sličnom licencom. Ova licenca dozvoljava komercijalnu upotrebu dela i prerada. Slična je softverskim licencama, odnosno licencama otvorenog koda

Ako se izabere neka od licenci kreativne zajednice to podrazumeva i da se u delo unese digitalni kod koji će u okviru metapodataka omogućiti pretraživačima da delo identifikuju kao delo objavljeno pod "Licencom kreativne zajednice".

Pored pojedinaca koji koriste "Licence kreativne zajednice" sve je veći broj i institucija, pa i vlada pojedinih zemalja koje se odlučuju za korišćenje ". Vlada Holandije je u martu 2010. godine otpočela sa korišćenjem "nulte Licence kreativne zajednice" (Creative Commons Zero - CC0) za sadržaje web site prezentacija 5 ministarstava (do kraja 2010.g. biće predstavljena i ostala ministarstva) pomoću kojih će se promovisati otvorena razmena informacija javnog sektora. Ovu odluku Holandska vlada je donela na osnovu istraživanja Amsterdamskog instituta za informaciono pravo (Amsterdam's Institute for Information Law) o upotrebi "Licenci kreativne zajednice" kao licenci za informacije u javnom sektoru.[39]

[39] *New Governmental Usage of Open Licences in the Netherlands and UK*, 7 April, 2010, Internet adresa: http://www.edri.org/edrigram/number8.7/open-content-government-uk-netherlands, 4.11.2010.

2.2. O MEĐUNARODNIM I NACIONALNIM PRAVILIMA ZAŠTITE AUTORSKIH PRAVA U SAJBER PROSTORU

Na međunarodnom planu ova materija regulisana je Bernskom Konvencijom (o zaštiti literarnih i umetničkih radova)[40] iz 1886.godine. Izmene su načinjene u Parizu 1896.godine, Berlinu 1908.godine. u prvom mahu dovršene u Bernu 1914., konvencija je revidirana u Rimu 1928.god. Briselu 1948.god. Štokholmu 1967. i Parizu 1971. da bi 1979.god. bila izmenjena amandmanima. A kao jedan od značajnih nedostataka ove konvencije bili su njeno neregulisanje Interneta i informaciono- komunikacionih tehnologija, što je rezultiralo usvajanjem sporazuma WIPO (The World Intellectual Property Organization Copyright Treaty) 1996.god. Svetska trgovinska organizacija kao jedan od uslova za članstvo zahteva od budućih članica da usvoje odredbe Bernske konvencije koje i jesu sastavni deo Sporazuma o trgovinskim aspektima prava intelektualne svojine.

Pored Bernske od značaja za materiju je i Rimska Konvencija o zaštiti prava izvođača, proizvođača fonograma i organizacija za radiodifuziju koja je otvorena za potpisivanje 26. oktobra 1961.god. kada su je usvojile članice BIRPI[41] prethodnice WIPO[42].

Takođe, od značaja u ovoj oblasti je i Ženevska Konvencija o zaštiti proizvođača fonograma od neovlašćenog umnožavanja iz 1971 o tretiranju zaštite autorskih prava u pogledu zvučnih zapisa. Ovom konvencijom je data mogućnost i ovlašćenja da se preduzmu mere protiv uvoza piraterije u obliku neovlašćeno stvorenih muzičkih snimaka kao i lica koja ih distribuiraju i preprodaju.

WIPO administrira 24 Konvencije, sporazuma i protokola od kojih je Srbija potpisnica svih[43].

---

[40] Od septembra 2008.god. ova Konvencija ima 164. zemlje potpisnice. Tekst Konvencije može se pronaći na internet adresi: http://www.wipo.int/treaties/en/ip/berne/index.html poslednji put pristupljeno 25.01.2012.

[41] United International Bureaux for the Protection of Intellectual Property, više o istoj na internet adresi: http://en.wikipedia.org/wiki/BIRPI poslednji put pristupljeno 24.01.2012.

[42] Konvencija o osnivanju Svetske organizacije za zaštitu prava intelektualne svojine (Convention Establishing the World Intellectual Property Organization) potpisana je u Štokholmu 14. jula 1967.god. i na snazi je uključujući amandmane od 28. septembra 1979. Tekst je dostupan na internet adresi: http://www.wipo.int/treaties/en/convention/trtdocs_wo029.html, 25.01.2012. 1974.god. UN su uvrstile ovu organizaciju kao specijalizovanu međunarodnu organizaciju u sastavu UN. Ova organizacija je potvrdila svoj značaj i proširila domašaj svoje važnosti potpisivanjem sporazuma 1996.god. sa Svetskom trgovinskom organizacijom (STO). Danas ova organizacija administrira 24 sporazuma.

2.2.1.ACTA - TRGOVINSKI SPORAZUM PROTIV FALSIFIKOVANJA

Razvoj informacionih tehnologija i interneta prouzrokovao je povećanje različitih oblika ugrožavanja intelektualne svojine u sajber prostoru. Gotovo neograničena dostupnost književnih dela, naučnih radova, muzičkih radova, video radova, i drugih autorskih dela u digitalnom obliku omogućila je ogroman broj zloupotreba i raznih oblika kršenja prava intelektualne svojine pa je bilo neophodno međunarodnim sporazumima osmisliti efikasne sisteme zaštite intelektualne svojine, koji su u skladu sa vremenom u kome dominiraju digitalne tehnologije.

Velike međunarodne organizacije, kao što su Ujedinjene nacije, Evropska unija, Svetska trgovinska organizacija, kao i pojedine države (pre svega SAD), nastojale su u poslednjih dvadeset godina da usvoje međunarodna pravna akta koja će ograničiti i sankcionisati zloupotrebu intelektualne svojine.

U okviru Svetske trgovinske organizacije (STO) usvojen jeTRIPS **(***Agreement on Trade Related Aspects of Intellectual Property Rights – Sporazum o trgovinskim aspektima prava intelektualne svojine***).** Ovaj sporazum je rezultat pregovora i uobličenja teksta iz 1994. godine. TRIPS je obavezan za sve članice Svetske trgovinske organizacije.

U okviru Svetske organizacije za intelektualnu svojinu (SOIS), zaključen je niz međunarodnih sporazuma, od kojih je najznačajniji Sporazum o autorskom pravu (Copyright Treaty) iz 1996.g.

U okviru EU, 2004. godine, usvojena je Direktiva o zaštiti prava intelektualne svojine 2004/48 (usvojili su je Evropski parlament i Evropski savet).

U SAD doneto je više zakonskih propisa u vezi sa zaštitom intelektualne svojine, ali posebnu pažnju su izazvali predlozi Zakona o sprečavanju online piraterije SOPA i Zakon o sprečavanju onlajn pretnji ekonomskoj kreativnosti i krađa intelektualne svojine - PIPA pripremljeni u drugoj polovini 2011.g. Ti akti su imali za cilj otežavanje prodaje i distribucije piratskog materijala zaštićenog autorskim pravima (filmovi, muzika, ali i fizička dobra).

---

[43] U pitanju su Bernska Konvencija, Briselska Konvencija, Budimpeštanski ugovor, Haški sporazum, Lisabinski sporazum, Sporazum iz Lokarna, Madridski sporazum (Indikatori izvora), Madridski sporazum (oznake), Madridski Protokol, Ugovor iz Nairobija, Pariska Konvencija, Ugovor o saradnji u pogledu patenata, Ugovor o patentnom pravu, Ženevska Konvencija o fonogramima, Rimska Konvencija, Singapurski Ugovor, Strazburški sporazum, Ugovor o pravu trgovinskih marki, Bečki ugovor, i Vašingtonski sporazum. O ovome više na internet adresi: http://www.wipo.int/treaties/en/ShowResults.jsp?search_what=C&country_id=189C, 25.01.2012.

Posledica je bila gašanje niza sajtova mežu kojima i Megaupload.com i hapšenje vlasnika sajta pod optužbom za nanošenje ogromne materijalne štete nosiocima autorskih prava. Nakon toga mnogi sajtovi su se sami ugasili kako bi izbegli pravne posledice (kao btjunkie.org). Odgovor internet zajednice je bio napad hakerske grupacije Anonimusi na sajtove FBI-a, Ministarstva pravde SAD, sajtove muzičke i filmske industrije kao i političkih moćnika. Širom Evrope i sveta 11 februara 2012.g. desetine hiljada ljudi u više stotina protesta iskazalo je svoje protivljenje sporazumima o zaštiti intelektualne svojine. Posledica reakcije internet zajednice i javnosti bila je prolongiranje glasanja o SOPI i PIPA u Kongresu SAD i pokretanje postupka pred Evropskoim sudom pravde o usklađenosti ACTA sa pravom Evropske unije.

Trgovinski sporazum protiv falsifikovanja (*Anti - Counterfeiting Trade Agreement),* poznatiji u javnosti kao ACTA, je jedan u nizu multilateralnih međunarodnih sporazuma čiji je cilj da se zaštiti intelektualna svojina. Svakako se ne radi o jedinom međunarodnom sporazumu ovakve vrste, jer ih je bilo i ranije, ali je ovaj multilateralni sporazum izazvao izuzetno oštru reakciju javnosti u mnogim zemljama, uključujući i našu, pa je to još jedan razlog više da se upoznamo sa detaljima sadržine ovog akta i da analiziramo posledice koje iz njega mogu proisteći.

Trgovinski sporazum protiv falsifikovanja (ACTA) je potpisan 1. oktobra 2011.g. u Tokiju od strane SAD-a, Japana, Kanade, Maroka, Novog Zelanda, Singapura i Južne Koreje, a ovom sporazumu se pridružila i Evropska unija početkom 2012.g. Od zemalja članica Evropske unije 22 zemlje su potpisale ACT-u dok su od potpisivanja, za sada, odustale Nemačka, Holandija, Češka, Poljska, Slovačka i Slovenija. U nekim slučajevima, ova uzdržanost je bila posledica masovnih protesta, u drugim, posledica mišljenja eksperata za pravo intelektualne svojine o odredbama ACTA koje su u suprotnosti sa pravom EU i evropskim standardima uživanja i zaštite ljudskih prava.[44]

Pregovore o Trgovinskom sporazumu protiv falsifikovanja (ACTA) otpočele su SAD 2006.g. sa Japanom, Švajcarskom i Evropskom unijom, a 2008.g. pregovorima su se pridružile Australija, Južna Koreja, Maroko, Novi Zeland, Meksiko, i Singapur. Pregovori su vođeni u tajnosti, jer su uglavnom svi pregovarači pregovore proglasili državnom tajnom, sve dok o pregovorima javnost nije obaveštena 2008.g. uz pomoć Wikileaks-a.

[44] Rakić Vodinelić Vesna, *Opasne pravne posledice ACTA*, Internet adresa: http://pescanik.net/2012/02/ opasne-pravne-posledice-acta/, 15. 03.2012..

Veliku podršku pregovorima o Trgovinskom sporazumu protiv falsifikovanja - ACTA pružile su velike medijske korporacije koje proizvode filmove, serije, muziku, itd, kao i korporacij ekoje se bave proizvodnjom lekova.

Osnovani prigovori na proces donošenja ovog sporazuma su da nije bilo *transparentnosti*, da nije bilo *demokratskog procesa* i da nije bilo *uticaja javnosti* na tekst sporazuma. Sva tri prigovora su u potpunosti opravdani. Pošto su pregovori vođeni u tajnosti naravno da nije bilo trasparentnosti. Demokratski proces je izostao jer su iz pregovora bili isključeni Svetska trgovinska organizacija i Svetska organizacija za intelektualnu svojinu, a onemogućavanje javnosti, odnosno nizu nevladinih organizacija i eksperata da daju svoje mišljenje o sporazumu sigurno nije doprinelo kvalitetu konačnog teksta sporazuma. Poznata izreka sjajnog pravnika Valtazara Bogišića "Što se grbo rodi vrijeme ne ispravi" u potpunosti se može odnositi na Trgovinski sporazum protiv falsifikovanja.

Trgovinski sporazum protiv falsifikovanja - ACTA se sastoji iz šest glava: (1) uvodne odredbe i opšti pojmovi; (2) pravni okvir za zaštitu prava intelektualne svojine; (3) prakse pravne zaštite; (4) međunarodna saradnja; (5) institucionalna pravila i (6) završne odredbe. U formalnom smislu, radi se o odredbama koje su uobičajene u multilateralnim međunarodnim sporazumima: one nameću državama koje potpišu i ratifikuju ACTA, obavezu prilagođavanja njihovog unutrašnjeg prava odredbama tog sporazuma. Bez obzira što su namere redaktora izražene u preambuli legitimne (zaštita autorskih prava i drugih prava intelektualne svojine, suzbijanje falsifikovanja intelektualnih dobara i sprečavanje piraterije) pravni metodi koje sadrže ACTA su agresivni i protivni brojnim međunarodnim i regionalnim dokumentima o ljudskim pravima. Ljudska prava koja se u Trgovinskom sporazumu protiv falsifikovanja najviše ugrožavaju jesu: *pravo na privatnost, sloboda izražavanja, pravo na lečenje* (pristup medikamentima) i *pravo na pravično odlučivanje* (suđenje).[45]

Cilj Trgovinskog sporazuma protiv falsifikovanjaj,e kako proističe iz samog sporazuma, da primora internet kompanije i internet provajdere da nadziru svoje korisnike i da cenzurišu sadržaje. Jedan od ciljeva ovog međunarodnog sporazuma je i da zaštiti interese velikih farmaceutskih kompanija, odnosno da omogući tretiranje generičkih lekova (lekovi koji su proizvedeni u zemljama u kojima ne važi patent ili je on istekao) kao falsifikat. Takođe se štite i

[45] *Ibidem.*

interesi kompanija koje se bave biotehnologijom pa bi kompanije koje zaštite neki od patenata u oblasti biotehnologije – genetike u više zemalja bile pod zaštitom Trgovinskog sporazuma protiv falsifikovanjai lakše mogle da ostvara svoja prava.

Iako Trgovinski sporazum protiv falsifikovanja - ACTA kreće od legitimnih ciljeva, po oceni naše stručne javnosti on ipak pati od niza nedostataka. Na javnoj debati o sporazumu ACTA u Beogradu održanoj 9 marta 2012.g. Saša Gajin je konstatovao da ovaj sporazum može ugroziti slobodan pristup informacijama, privatnost, i da ne sadrži dovoljnu meru procesnih garancija za pravično suđenje.[46]

Vesna Rakić Vodinelić ističe pet krupnih nedostataka Trgovinskog sporazuma protiv falsifikovanja – ACTA:[47]

1. ACTA ne pravi razliku između korisnika za koje postoji osnovana sumnja da povređuju pravo intelektualne svojine i drugih korisnika. Dovoljno je da nosilac prava tvdi da je određeni korisnik njegovo pravo povredio. U ovom pogledu, naglašava se, ACTA ide znatno dalje od TRIPS-a, koji ovakvu obavezu provajdera propisuje samo za one korisnike za koje je dokazano da vređaju pravo intelektualne svojine. Na ovaj način se uspostavlja pretpostavka da je svaki korisnik istovremeno i prekršilac.

2. ACTA, pored građanskopravne zaštite, nameće državama potpisnicama obavezu krivičnopravne zaštite, tj. kriminalizaciju povreda prava intelektualne svojine, što odstupa od EU standarda, jer Direktiva EU 2004/48 uopšte ne predviđa kriminalizaciju. Pored toga ACTA ne obezbeđuje pravično suđenje i zaštitu procesnih prava okrivljenih. Iako se državama potpisnicama nameće obaveza kriminalizacije, u ACTA se ne pravi razlika između kopiranja koje je korisnik izvršio za sopstvenu upotrebu i onog za nezakonito sticanje profita, budući da se pojam komercijalne upotrebe intelektualnog dobra neodređeno i široko definiše.

3. U čl. 12 ACTA nisu sadržane uobičajene procesne garantije za tuženog (navodnog prekršioca prava intelektualne svojine), zato što se privremene mere oduzimanja i zaplene njegovih dobara, za koje se tvrdi da su rezultat povrede prava intelektualne svojine, mogu izreći, a da se tuženom i ne pruži prilika da se izjasni (*inaudita altera parte).*

---

[46] *ACTA u Srbiji: Protest i debata*, Internet adresa: http://www.b92.net/tehnopolis/ aktuelno.php?yyyy=2012&mm=03&nav_id=589563, 9. 3. 2012.

[47] Rakić Vodinelić Vesna, *Opasne pravne posledice ACTA*, Internet adresa: http://pescanik.net/ 2012/02/opasne-pravne-posledice-acta/, 15. 03.2012.

4. Državni organi koji kontrolišu granicu, na osnovu ACTA mogu uživati ovlašćenja koja inače, sme da ima samo sud: prema nekim tumačenjima granični službenici carine mogu da narede pregled lap topa ili IPad-a i njihovo oduzimanje na osnovu obične sumnje da sadrže falsifikovana intelektualna dobra (snimke muzike, filma i sl.) koji bi navodno bili namenjeni komercijalnoj, a ne, kao što uobičajeno jesu, ličnoj upotrebi.

5. U Evropskom parlamentu je naglašavano da se ACTA odnosi i na generične medikamente (lekove sa generičnim imenom), iako se ne radi o falsifikovanim lekovima, nego i o onim za koje je isteklo vreme zaštite ili se iz razloga unutrašnjeg prava, stavljaju u promet pod generičnim imenom. Zaplena i uništavanje takvih lekova kao falsifikovanih sprečiće pristup lečenju naročito u nerazvijenim zemljama.

Jedna od najproblematičnijih odredbi Trgovinskog sporazuma protiv falsifikovanja - ACTA je ona koja se odnosi na *internet provajdere*, odnosno član tog sporazuma koji predviđa mogućnost da zemlje potpisnice mogu da ovlaste nadležne organe da traže od internet provajdera podatke o korisnicima za koje se sumnja da krše autorska prava sa svojih internet adresa.

Trgovinskim sporazumom protiv falsifikovanja - ACTA predviđa se i uspostavljanje globalne agencije za suzbijanje falsifikovanja i besplatnog preuzimanja filmskog, muzičkog i drugih sadržaja sa interneta uz pretnju zatvorskim i novčanim kaznama.

Evropski sud pravde je 16. februara 2012.g. odbacio zahtev da društvene mreže i internet provajderi uvedu "filtere" kojima će korisnicima onemogućiti da razmenjuju sadržaje zaštićene autorskim pravima. Evropski sud pravde je odbacio tužbu Agancija za zaštitu autorskih prava iz Belgije uz obrazloženje da bi se time kršili principi slobodne trgovine i slobode izražavanja, kao i da se time ugrožava privatnost korisnika interneta. Ova odluka Evropskog suda pravde imaće sigurno značajne posledice na buduće slične slučajeve.

Trgovinski sporazum protiv falsifikovanja – ACTA bio je otvoren za potpisivanje do 31. marta 2012.g. za zemlje koje su učestvovale u pregovorima i za članice Svetske trgovinske organizacije. Od zemalja Evropske unije njih 20 od ukupno 27 je potpisalo ACTA sporazum. Da bi ovaj sporazum stupio na snagu bilo je potrebno da ga ratifikuje Evropski parlament, ali je on, nakon negativne reakcije javnog mnjenja i mišljenje Odbora za međunarodnu trgovinuEvropskog parlamenta, odbio 4, jula 2012.g. da ga ratifikuje sa 478 glasova p33rotiv 39 za i 165 uzdržanih uz obrazloženje da ovaj sporazum predstavlja pretnju za lične slobode i privatnost građana Evropske unije.

Bez obzira što Trgovinski sporazuma protiv falsifikovanja – ACTA nije ratifikovan od strane Evropskog parlamenta i neće se primenjivati u Evropi, sigurno je da nas u narednom periodu očekuje još međunarodnih sporazuma iz oblasti zaštite intelektualne svojine koji će, posle reakcije javnosti na Trgovinski sporazuma protiv falsifikovanja – ACTA morati biti mnogo bolje pripremljeni uz posebno vošenje računa da se ne ugrožavaju lične slobode i privatnost građana.

2.2.2.GRUPA KRIVIČNIH DELA PROTIV INTELEKTUALNE SVOJINE U ZAKONODAVSTVU SRBIJE

Propisivanjem ovih krivičnih dela upotpunjena je zaštita u našem pravnom sistemu u pogledu prava intelektualne svojine. Na ovom mestu govorićemo o krivičnim delima kojima se inkriminišu radnje koje predstavljaju po zakonodavcu najteža dela koja lica mogu izvršiti u našem pravnom sistemu.

Povreda moralnih prava autora i interpretatora

Član 198

Prvi oblik čini lice koje pod svojim imenom ili imenom drugog u celini ili delimično objavi, stavi u promet primerke tuđeg autorskog dela ili interpretacije, ili na drugi način javno saopšti tuđe autorsko delo ili interpretaciju (novčana kazna ili zatvor do tri godine).

Drugi oblik vrši onaj ko bez dozvole autora izmeni ili preradi tuđe autorsko delo ili izmeni tuđu snimljenu interpretaciju (novčana kazna ili zatvor do jedne godine). Oba prikazana oblika se gone po predlogu. Ovlašćeno lice za stavljanje predloga je autor odnosno lica ovlašćena da postupaju u ime i za račun autora[48].

Treći oblik čini ono lice koje stavlja u promet primerke tuđeg autorskog dela ili interpretacije na način kojim se vređa čast ili ugled autora ili izvođača (novčana kazna ili zatvor do šest meseci), ovaj oblik se goni po privatnoj tužbi. Predmeti korišćeni u svim opisanim oblicima će se oduzeti.

Neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava

Član 199[49]

---

[48] Prema čl.3.tač 2. Zakona o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine (Službeniglasnik RS, 46/06) u daljem tekstu ZOPOIS: nosilac prava je izvorni sticalac prava intelektualne svojine ili njegov pravni sledbenik.

[49] *Neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava* iz čl. 199. st. 3. u vezi sa st.1 i 2. Krivičnog zakonika u vezi sa čl.33. KZ: Po optužnici Posebnog tužilaštva KTVTK.br.42/08, presudom Okružnog suda u Beogradu K1.vtk.br.19/08 od 10.10.2008.god., zbog internet piraterije, oglašeni su krivim Ž.J. (36) i S.M.

Ovo krivično delo je veoma široko definisano. Prvim stavom propisan je prvi oblik koji čini lice koje neovlašćeno[50] objavi, snimi, umnoži ili na drugi način javno saopšti u celini ili delimično autorsko delo, interpretaciju, fonogram, videogram, emisiju, računarski program ili bazu podataka (kazna zatvora do tri godine) pri čemu za postojanje krivičnog dela nije od

(35) Presudom br.*K1 VTK broj 19/08* kojom su okrivljeni osuđeni na uslovnu kaznu zatvora u trajanju od šest meseci sa rokom proveravanja od dve godine iz Kraljeva. Oni su, u periodu od 21.06.2005.godine, pa sve do dana 03.06.2008. godine, kada su lišeni slobode, na teritoriji opštine Kraljevo, po prethodnom dogovoru, u nameri da sebi pribave imovinsku korist, putem bežične Internet mreže (*wireless*), za novčanu nadoknadu neovlašćeno stavljali u promet preko 500 (pet stotina) primeraka raznovrsnih autorskih dela, različitih nosilaca autorskih prava na taj način što su tokom 2005. godine pa nadalje, na osnovu zajedničkih finasijskih ulaganja, izgradili i pustili u eksploataciju bežičnu internet mrežu koja je funkcionisala neregistrovano pod neformalnim nazivom „eXcalibur Wireless“ (EkskaliburVajrles), što su činili u okviru poslovnog prostora – privrednog društva „EXCALIBUR COM D.O.O.“ tokom kog perioda su u navedenom prostoru primali novčane uplate korisnika interneta i FTP servisa kojima je nakon izvršenih uplata bilo omogućeno da na svoje kućne računare preuzimaju neovlašćeno umnožene primerke raznovrsnih autorskih dela. Krivično delo *Neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava* iz čl. 199. st. 3. u vezi sa st. 2. Krivičnog zakonika: Po optužnici Posebnog tužilaštva KTVTK br.70/08, presudom Okružnog suda u Beogradu K1.vtk.br.44/08 od 28.11.2008.god, zbog internet piraterije, oglašen je krivim M.S. (30) iz Beograda što je, u periodu od 01.01.2005. godine do 03.09.2008. godine, u Beogradu, na adresi svog prebivališta, u nameri pribavljanja imovinske koristi, neovlašćeno umnožavao i stavljao u promet različita videogramska i fonogramska autorska dela većeg broja oštećenih nosilaca autorskih prava, u vidu optičkih diskova u „DVD“ i „DivX“ formatu na taj način što je neovlašćeno nabavljene kopije autorskih dela prethodno nasnimavao na optičke, kao i tvrde diskove svojih računara nakon čega je njihovu prodaju, sa katalogom odo ko 15.000 (*petnaesthiljada*) pojedinačnih naslova i cenovnikom, oglašavao putem svoje elektronske adrese poštanskog servisa yahoo.com, što je činio sve do intervencije ovlašćenih službenih lica Odeljenja za borbu protiv visokotehnološkog kriminala, SBPOK-a, UKP, MUP-a Republike Srbije koja su nakon obavljenog pretresa stana i drugih prostorija, od osumnjičenog uz potvrdu privremeno oduzeli dva računara, 10.327 (*desethiljadatristotinedvadestisedam*) komada neovlašćeno umnoženih optičkih diskova sa neovlašćeno umnoženim autorskim delima u vidu filmova, televizijskih serija, muzike, stripova i drugih multimedijalnih sadržaja.

[50] Prema čl.20 Zakona o autorskim i srodnim pravima: 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. U st 2. navodi se: Delo se umnožava naročito, grafičkim postupcima, fotokopiranjem i drugim fotografskim postupcima kojima se postiže isti rezultat, zvučnim ili vizuelnim snimanjem, izgradnjom dela arhitekture, smeštanjem dela u elektronskom oblikuu memoriju računara.Prema čl.22. Autor ima isključivo pravo da drugome zabrani ili dozvoli davanje originala ili umnoženih primeraka svog dela u zakup. Davanje u zakup, u smislu ovog zakona, je davanje originala ili umnoženih primeraka dela drugome na korišćenje na ograničeno vreme u svrhu ostvarivanja neposredne ili posredne imovinske koristi. Pravo iz stava 1. ovog člana se ne iscrpljuje prodajom ili drugim radnjama stavljanja u promet originala ili umnoženih primeraka dela. Prema članu 54a dozvoljena je slobodna prerada objavljenog autorskog dela ako se radi o:

1) parodiji ili karikaturi, ako to ne stvara zabunu ili ne može dovesti do stvaranja zabune u pogledu izvora dela;

2) preradi dela za lične potrebe koja nije namenjena i nije dostupna javnosti;

3) preradi u vezi sa dozvoljenim korišćenjem dela, koja je prouzrokovana samom prirodom ili načinom tog korišćenja.

Prema članu 54b ovlašćeni korisnik objavljene baze podataka ili njenog umnoženog primerka može slobodno da umnožava ili preradi tu bazu podataka ako je to potrebno radi pristupa njenom sadržaju i redovnog korišćenja tog sadržaja.

značaja broj kopija[51]. Drugi oblik postoji kada lice stavi u promet, ili u nameri stavljanja u promet, neovlašćeno drži umnožene ili neovlašćeno stavljene u promet primerke autorskog dela, interpretacije, fonograma, videograma, emisije, računarskog programa ili baze podataka (za koje je predviđena ista kazna kao za prethodni oblik). Stavljanje u promet podrazumeva činjenje dostupnim javnosti primeraka tuđeg autorskog dela, a pod tim treba podrazumevati prodaju, razmenu, rasturanje, poklanjanje i sve druge delatnosti kojima se ostvaruje suština neovlašćenog činjenja dostupnim[52].

Trećim stavom je propisan teži oblik koji postoji ukoliko je lice učinilo prethodna dva oblika u nameri pribavljanja imovinske koristi za sebe ili drugog (propisana kazna zatvora od tri meseca do pet godina). Četvrti stav predviđa poseban oblik ovog dela, po kojem će se lice koje 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 koje takve uređaje koristi u cilju povrede autorskog ili srodnog prava, kazniti novčanom kaznom ili kaznom zatvora do tri godine[53]. Ovim poslednjim stavom inkriminisane su pripremne radnje za izvršenje svih ostalih oblika ovog krivičnog dela ali i drugih krivičnih dela iz ove grupe.

Ovo krivično delo najzastupljenije je u poslednje vreme, globalno gledano, a, naročito, u Srbiji. Mnogi su pokušaji objašnjenja u pogledu zastupljenosti i rasprostranjenosti ovog

[51]Ali navedeno jeste značajno sa aspekta nadležnosti za postupanje u ovom krivičnom delu u smislu člana 3. Zakona o organizaciji i nadležnosti državnih organa u borbi protiv visokotehnološkog kriminala. U nadležnost SBPOK – a i posebnog tužioca za VTK, spadaju samo oni slučajevi sa preko 2000 primeraka umnoženih autorskihdela ili kada je nastala šteta od preko 1.000.000 dinara. Ovo i predstavlja svojevrsnu materijalno-pravnu i formalnu među za ovlašćenja organa koji sprečavaju i suzbijaju kriminalitet. Naime, ovo jeste osnov za razgraničenje nadležnosti organa koji postupaju po osnovu zloupotrebe prava intelektualne svojine. Na osnovu izloženog moguće je diferencirati nadležnost osnovnog suda (i tužilaštva), kao i ostalih jedinica policije za postupanje u odtalim slučajevima, kao i drugih organa kada su u pitanju prekršaji i privredni prestupi.

[52]Gerke, Midr., *Priručnik za istragu krivičnih dela u oblasti VTK, Savet Evrope, 2008.*, str.133.

[53]Tokom 2008. godine Tužilaštvu za borbu protiv visokotehnološkog kriminala je podneto 319 krivičnih prijava protiv 332 lica zbog izvršenja ukupno 379 krivičnih dela koja se odnose na povredu intelektualne svojine, a ukupno su oduzeta 131.232 optička diska i 50 tehničkih uređaja. Imajući u vidu opisano stanje kriminala, na osnovu dogovora sa istražnimo deljenjem Okružnog suda u Beogradu, da se u cilju što efikasnijeg rešavanja ovih predmeta primenjuje postupak za kažnjavanje i izricanje presude od strane istražnog sudije, saglasno članu 455. Zakonika o krivičnom postupku. Ova vrsta postupka primenjuje se onda kada je to opravdano, a u obzir se naročito uzima ranija osuđivanost osumnjičenih lica i motivi za izvršenje krivičnog dela. Navedeno prema Komlen Nikolić, L. *et alia, op.cit*.

krivičnog dela, od kojih su neki dostupnost različitih softvera kojima se veoma lako i veoma brzo prenose digitalni sadržaji putem Interneta od torent klijenata do P2P prenosa. Činjenici zastupljenosti pogoduju mnogi faktori od onih na strani siromašnih zemalja u tranziciji i nemogućnosti da njihovo stanovništvo odgovori skupim zahtevima imalaca prava, do strateške neujednačenosti na globalnom nivou u pogledu različitih oblika zaštite medija putem kojih se prenose digitalni sadržaji.

Neretko „izvršioci" na svojim Internet stranicama nude i više desetina hiljada naslova a da se, u stvari, njih pronađe svega par stotina kopija. Ovakav postupak diktira tržište ali omogućavaju različiti servisi na Internetu, kao npr. Rapidshare, MediaFire, YouSendIt, File savr, File dropper, a posebno, do skora, jedan od najpopularnijih Megaupload[54]. U pretkrivičnom postupku je potrebno sačiniti potvrdu o predmetima koji su oduzeti od okrivljenog. U njoj moraju biti navedeni naslovi svih filmova, programa ili muzičkih dela, koja su stavljena u promet, format i medijum na kom se nalaze, kao i određeni nosioci prava koji su ovom prilikom oštećeni. Popisivanje je neophodno kako bi bila izvršena identifikacija ovlašćenih nosilaca prava koji su oštećeni izvršenjem krivičnog dela[55]. Ovo stvara teškoće i oduzima mnogo vremena policijskim službenicima, naročito kada se broj naslova meri desetinama hiljada i predstavlja glavni razlog zbog koga se broj uličnih prodavaca piratskih diskova ne smanjuje. Identifikacija nosilaca prava opterećuje i tužioce, pa je radi ubrzavanja pretkrivičnog postupka, Tužilaštvo za borbu protiv visokotehnološkog kriminala napravilo bazu podataka sa naslovima filmova, muzičkih dela i softvera, kao i ovlašćenim distributerima istog sadržaja[56]. No bez obzira na ovo moguće je zamisliti veličinu problema ukoliko bi se ovaj problem preneo na nivo Rapidšera ili nekog sličnog hosting domena.

Što se dokazivanja tiče veoma je značajno uspostaviti vezu između lica koje je izvršilac i predmeta koji su corpora delicti ovog krivičnog dela. Veza se može ustanoviti npr. upoređivanjem digitalnih karakteristika vremena nastanka, vremena prenosa na određene nosioce – medije, konkretnog autorskog dela ili video zapisom sa javnog saopštavanja ili interpretacije

[54] Potonji je poslednji put bio u upotrebi do 19.01.2012. kada su vlasnici hašđeni po osnovu kršenja zakona o autorskim pravima u SAD. više o tome na: http://venturebeat.com/2012/01/19/megaupload-shut-down-swiss-beatz-ceo-fbi-piracy/ poslednji put pristupljeno 23.01.2012.

[55] Isto je rezultat stava Vrhovnog suda Republike Srbije, iznet u presudi Kzz.br.10/06 od 16.03.2006.godine, prema kojem, radnja izvršenja krivičnog dela Neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava iz čl.199. KZ-a opisana u presudi, mora biti bliže određena objektom delao dnosno, nazivom autorskog dela i subjektom autorskog prava.

[56] Navedeno prema Komlen Nikolić, L. *et alia, op.cit*.

tuđeg autorskog dela, ili tragova nastalih prilikom aploadovanja datoteka na Interentu – serverima hosting domena. Bitna karakteristika je da izvršilac ima svest o tome da je u pitanju tuđe autorsko delo ili interpretacija, kao i da svesno objavljuje pod tuđim ili svojim imenom. U suštini neophodno je da postoje elementi obmane ili lažnog prikazivanja da je interpretacija ili autorsko delo delo lica koje objavljuje ili nekog trećeg a ne oštećenog, ili da je izvršilac lice, lažno ovlašćeno da, u njegovo ime i za njegov račun, postupa. Dakle, izvršilac može biti svako lice.

U praktičnom postupanju značajno je uočiti razlike između legalnog i „piratskog“ izdanja muzičkog diska, neke od njih bi bile:

1.) Različita slika i grafička obrada spoljnog omota kutije i samog diska

2.) “Piratski” disk nema: šifru stampera, oznake kodova (ima reljefno oštećenje na mestu SID koda - Source Identification Code, identifikacioni kod za autentičnost diska, takođe, može imati ali i ne mora RID kod - Recorder Identification Code) listu pesama na disku[57]

3.) Oznaka zaštitnog znaka - žiga - loga nije ista kao na originalu LBR kod mastera: označava pogon u kojem je izrađen.

Dokazi za krivično delo se mogu pribaviti prikupljanjem i utvrđivanjem određenih činjenica, na primer:

1) Nepostojanje ugovora ili drugog pravnog osnova za korišćenje autorskih prava
2) Privremeno oduzeti muzički ili video optički diskovi u proizvodnji, magacinima gotovih proizvoda i više prodajnih objekata
3) Stamperi
4) Popisne liste i katalozi naslova
5) Interne evidencije šefa proizvodnje
6) Ugovori između SOKOJ-a i vlasnika autorskih prava predstavljaju tzv. komparativne dokaze
7) Rešenje Zavoda za intelektualnu svojinu o izdavanju dozvole SOKOJ-u za obavljanje delatnosti kolektivnog ostvarivanja autorskih imovinskih prava
8) Fotodokumentacija i video zapis
9) Veštačenje muzičkih i video optičkih diskova (upoređenje sa referentnim optičkim diskom nesporno proizvedenim na mašini otkrivenoj u proizvodnom pogonu)
10) Podaci sadržani na hard diskovima personalnih računara, u vlasništvu ili državini učinilaca
11) Podaci sadržani na optičkim diskovima

[57]Za boje i zaštite koje diskovi različitih kapaciteta i tehnologija nose videti na internet adresi: http://en.wikipedia.org/wiki/Rainbow_Books, 28.06.2010. i internet adresi: http://en.wikipedia.org/wiki/IFPI, 28.06.2010.

12) Muzički kompakt diskovi na kojima se neovlašćeno nalaze oznake tuđeg zaštitnog znaka, žiga - loga
13) Papirni omoti na kojima se nalaze iste oznake
14) Rešenja Zavoda za intelektualnu svojinu o zaštiti zaštitnog znaka, žiga - loga
15) Slike i grafičke pripreme za štampu zaštitnih znakova, žigova - loga
16) Fotodokumentacija i video zapis
17) Kod kalupa : označava pogon u kojem je proizveden

Identifikaciona obeležja orginalnog proizvoda su:

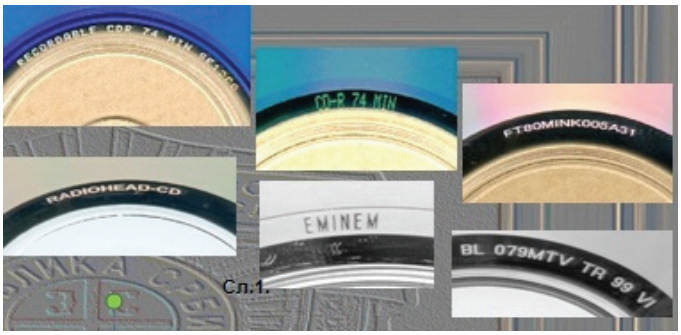
- ime diskografske ili izdavačke kuće,
- ime izvođača ili sastava tj. grupe, naziv producenta i nosilaca prava distribucije
- jasno otisnuti logotipi i zaštićeni znakovi, praćeni i hologramskim zaštitama
- kataloški broj
- kopija logotipa autorskog udruženja
- upozorenje o zaštićenim autorskim pravima
- oznake © i ® sa datumom i imenom diskografske kuće
- zemlja proizvodnje (roba proizvedena u EU navodi EU kao mesto proizvodnje)
- u slučaju SD-a i DVD-a obično je naveden SID kod, kojeg danas koriste 80% proizvođača optičkih diskova
- ponekad je istaknut potpun popis naziva pesama ili snimaka
- omoti moraju biti jasno otisnuti na kvalitetnom papiru

Takođe i: svi tonski zapisi moraju biti označeni datumom zaštite autorskih prava i objavljivanja, gore navedeno se obično nalazi i na nosaču zvuka i na omotu diska,

© Copyright – označava vlasnika autorskih prava na snimku na navedeni datum, a oznaka ® Publication– označava datum objavljivanja zvučnog snimka.

Krivotvorenje (falsifikovanje) diskova:

Krivotvorine (falsifikati) se kopiraju i pakuju tako da nalikuju originalu, u praktičnom postupanju je veoma bitno, na omotu proviriti sledeće: oštrinu izgleda naslovne fotografije, kontrast boja, kvalitet papira, kvalitet dubine štampe, postojanje hologramskih zaštitnih oznaka, fotokopije na papiru u boji, štampanje na samo jednoj strani papira, uklonjen logotip, nepostojanje kataloškog broja, kvalitet reza ili oblika omota, postojanje paradoksalnih situacija: poznati izvođač, nepoznata diskografska kuća, veoma često, visok kvalitet reprodukcije zvuka.



Сл.1.

Ilustracija

Matrični brojevi: neke informacije s ruba unutrašnjeg pojasa (blizu središta diska) često sadrže slova CD-R i dužinu trajanja diska, kao što je prikazano u gornjem redu na slici (to nije uobičajeno na DVD-R_ovima).

U donjem redu na ilustraciji prikazani su CD_ovi koji pružaju i informacije o sadržaju na disku, što nije slučaj sa CD-R_ovima. Matrični pojas CD-R_a obično ne nosi nikakva obeležja, ili sadrži samo neki alfanumerički kod. Na matričnom pojasu se ne mogu pojaviti obeležja kao što su logotip diskografske kuće ili kataloški broj. CD-R_ovi nisu obeleženi LBR kodovima, jer nisu podvrgnuti procesu masteringa kao industrijski CD – ovi. CD-R – ovi obično nisu obeleženi kodovima kalupa. Međutim, u nekim zemljama su proizvođači zakonski obavezni na svakom kalupu navesti i kod kalupa, tako da se i kalupi za CD-R – ove kodiraju, tako da takvi diskovi nose kod koji je dodeljen proizvođaču u zemlji u kojoj se proizvodi CD-R. Obično je očitavana strana CD-R – a obojena (najčešće zelenom ili plavom bojom), a primetan je „efekat duge“, za razliku uobičajenog srebrnastog završnog sloja koji se nalazi na CD – u, što je prikazano na gornjoj slici u crvenom okviru. Veliki deo izloženog se može koristiti i u slučaju krivičnog dela Neovlašćeno uklanjanje ili menjanje elektronske informacije o autorskom i srodnim pravima iz člana 200. KZ. Prema čl.4. ZOPOIS veoma je značajno određuje se da su proizvodnja, držanje i promet robe, odnosno pružanje usluga, kojima se povređuju prava intelektualne svojine utvrđena zakonom ili međunarodnim ugovorom, zabranjeni.

Pirati za svoje delovanje zloupotrebljavaju kompanije koje nude usluge čuvanja (engl. host) datoteka na svojim serverima, poput Rapidshare, Megaupload i dr. Pre postavljanja (engl. upload) originalni fajl se podeli na više manjih delova korišćenjem nekih od programa za deljenje poput „Winzip“, „ARJ“„Filesplitter“ ili „HjSplit“, koji se potom zaštićuju šifrom. Mali fajlovi dobijeni na ovaj način obično nemaju originalan naziv filma ili programa, zbog čega je nelegalan sadržaj teško otkriti. Linkovi koji vode ka ovim fajlovima se nalaze na veb sajtovima i

forumima specijalizovanim za razmenu piratskih sadržaja. Navedene kompanije ostavljaju mogućnost svojim korisnicima da u svakom trenutku prijave zloupotrebu, što pirate ne odvraća da i dalje postavljaju nelegalne sadržaje, zbog čega se serveri ovih kompanija danas smatraju glavnim izvorima piraterije na Internetu.

Još jedan veoma popularan način razmene fajlova koji se zloupotrebljava za pirateriju predstavljaju torenti, programi koji se baziraju na „P2P“ (engl. peer to peer) tehnologiji, kojom se ostvaruje direktna veza između dva računara radi razmene podataka između korisnika. Uspostavlja se veza između korisnika koji imaju određenu datoteku na svom računaru tzv. „sejači“ (engl. seeders) i klijenata koji traže istu tzv. „pijavice“ (leechers), a na ovaj način se najčešće razmenjuju različiti sadržaji: velike video datoteke, muzička dela i softver. Kako bi inicirao preuzimanje fajla (engl. download) „ličer“ pokreće torent, program koji ostvaruje vezu sa centralnim serverom – „trekerom“ (engl. tracker) na kome se nalaze podaci o „siderima“. Nakon toga klijent uspostavlja više simultanih „P2P“ konekcija sa „siderima“ i počinje da preuzima traženi fajl sa više lokacija odjednom. Karakteristika ovog procesa je da korisnik koji preuzima fajlove, u isto vreme postaje „sider“, odnosno deli te iste fajlove sa drugim korisnicima[58]. Sudovi izvršiocima krivičnih dela protiv intelektualne svojine najčešće izriču uslovne kazne zatvora[59]. Kao jedan od mogućih razloga za novu koncepciju i strateški okvir predstavljanja zašite autorskih i srodnih prava (prava intelektualne svojine) javlja se dostupnost ovakvih datoteka i obim i tendencija koju ova pojava ima. Šta više, postoje struje koje su usmerene na revolucionarne izmene u koncepcijama zaštite intelektualne svojine.

Iz uporednopravne prakse možemo izdvojiti primer kada je sud u Švedskoj osudio četvoricu vlasnika čuvene stranice pajratbej „The Pirate Bay“ na kazne zatvora od po godinu dana, s tim što im je naloženo da plate odštetu od tri i po miliona dolara kompanijama kao što su Warner Brothers, Sony i EMI.[60] U skorije vreme slična je situacija u perspektivi i kod pomenutog slučaja Megaupload – a. Na navedenoj stranici se nezakonito razmenjuju muzika,

---

[58] *BitTorrent (protocol)*, Wikipedia, Internet adresa: http://en.wikipedia.org/wiki/BitTorrent_(protocol), 10.05.2009.

[59] Mada je u 2008. godini Posebno odeljenje Okružnog suda u Beogradu osudilo dvojicu izvršilaca na zatvorske kazne, i to okrivljenog Ž.D. presudom K1 16/08 na kaznu zatvora u trajanju od šest meseci, a okrivljenog M.J. presudom K1 17/08 na kaznu zatvora u trajanju od jedanaest meseci. Ova lica su bila višestruki povratnici, a ranije su osuđivani isključivo zbog izvršenih krivičnih dela protiv intelktualne svojine.

[60] *Osuđeni osnivači Pirate Bay-a*, BBC Serbian, Internet adresa: http://www.bbc.co.uk/serbian/news/2009/04/090417_swedennetpiracy.shtml, 24.07.2010.

filmovi i računarske igrice, a ima oko 22 miliona korisnika.[61] Što se građansko pravne zaštite tiče najinteresantniji primer je civilna tužba holandskog udruženja za borbu protiv piraterije BREIN[62] protiv administratora i vlasnika najvećeg sajta za razmenu torent datoteka Mininova. Smisao tužbe je bio da vlasnici plate kazne veće od 5 miliona EUR –a ali su tuženi u ovom slučaju primenili jednu meru kojom su odgovorili zahtevima tužilaca. Naime, odbijen je pristup svim neautorizovanim sadržajima na serveru i tako onemogućila piratska razmena. Poseban slučaj je FTC u SAD koji je izrekao sankcije Comcast – u za pojačavanje i preusmeravanje saobraćaja preko BitTorrent[63]. Ovakvo sankcionisanje je ipak oglašeno nezakonitim Odlukom Federalnog apelacionog suda. Naime, dosledno sprovodeći stav VSS o kome je već razmatrano, svi državni organi gonjenja i suđenja, dužni su da u svojim pismenim aktima navedu sve naslove autorskih dela pri čemu, tužilaštvo i sud i podatke koji se odnose na oštećene subjekte autorskih prava, u vidu nabrajanja njihovih imena ili naziva nosilaca prava. U pojedinim (sve češćim) slučajevima „piraterije", koji podrazumevaju količine zaplenjenih optičkih diskova od 2.000 do 15.000 komada, dispozitivi optužnih akata i presuda znaju da broje po 50 i više strana, a vreme neophodno za utvrđivanje ovih informacija mere se danima. Mišljenja smo da je u takvoj situaciji nužno iznaći neko razumno rešenje, s obzirom na neprimereno trošenje vremena i materijalnih resursa.

Određeni autori[64], rešenje nude u inkorporiranju u procesni zakon odredbi čl. 22. „novog" ZKP-a[65] kojim definiše značenje izraza „spis, pismeno, pošiljka i drugi dokumenti"[66], na koji način bi prepisi optužnih akata tužilaštva i odluka suda, osim eventualno izvornika, mogli biti u celosti, ili samo delom - i u elektronskoj formi. U tom smislu ova odredba morala bi pretrpeti određene izmene, utoliko što bi se u samom tekstu na kraju rečenice, iza reči „sadržane u spisima", unele reči: „kao i na prepise optužnih akata i odluka suda, ili njihovih delove, osim izvornika koji moraju biti i u pismenoj formi". Ovakvo rešenje uvelo bi, prema ovim autorima,

---

[61]Knežević Ćosić, V. *Švedski pirati na naftnoj platformi prave piratsku državu*, *Borba*, 23.04.2009. Internet adresa: http://www.borba.rs/content/view/5127/36/, 10.05.2009.

[62]Internet adresa: www.torrentfreak.com/mininova-deletes-all-infringing-torrents-and-goes-legal-091126/, 09.05.2010.

[63] Internet adresa: http://www.nytimes.com/2010/05/06/technology/06broadband.html?ref=technology, 10.05. 2010.

[64]Komlen Nikolić, L. *et alia, op cit*, str.144

[65]Koji neće ni otpočeti sa primenom.

[66]Spis, pismeno, pošiljka i drugi dokumenti mogu biti i u elektronskom obliku i biti sadržani u odgovarajućim nosiocima podataka, kao što su CD, drugi diskovi, magnetne trake i bilo koji drugi nosioci podataka, što se odnosi i na dokaze i isprave sadržane u spisima.

„na velika vrata“ primenu elektronskog potpisa i elektronskog sertifikata, što podrazumeva ozbiljnu pripremu za njihovu primenu. Jedini problem jeste što ovaj Zakonik neće zaživeti, ali bi Zakonodavni organ ovo morao uzeti u obzir prilikom izrade novog ZKP ili kod izmena i dopuna postojećeg. U novom ZKP (Službeni glasnik RS br. 72/11) iz 2011.god. prema čl.177. pod naslovom Dostavljanje izveštaja i materijala, pominju se elektronski i drugi zapisi kao mogući materijali koji se dostavljaju nadležnim organima što jeste značajan korak unapred.

Neovlašćeno uklanjanje ili menjanje elektronske informacije o autorskom i srodnim pravima

Član 200

Prvi oblik vrši onaj ko neovlašćeno ukloni ili izmeni elektronsku informaciju o autorskom ili srodnom pravu, ili stavi u promet, uveze, izveze, emituje ili na drugi način javno saopšti autorsko delo ili predmet srodnopravne zaštite sa kojeg je elektronska informacija o pravima neovlašćeno uklonjena ili izmenjena (novčana kazna i zatvor do tri godine). Predmeti o kojima je reč oduzeće se i uništiti. Objekat krivičnog dela jeste elektronska informacija o pravima intelektualne svojine. Već kod razmatranja objekta jasno je da je neizbežna implikacija VTK. Ova elektronska informacija je oblik zaštite prava intelektualne svojine kojom se pokušava sprečiti krađa prava intelektualne svojine sa određenih medija i nosilaca datih podataka, predmeta pravne zaštite[67]. Izvršilac ovog krivičnog dela može biti svako lice koje ima sredstva ili znanja kojima se ova zaštita umišljajno može ukloniti, odnosno svako ko može javno saopštiti predmet prava intelektualne svojine sa kojeg je elektronska informacija o pravima neovlašćeno uklonjena ili izmenjena. U pogledu dokazivanja neophodno je utvrditi vreme i mesto radnje izvršenja, kao i način na koji je delo izvršeno. Ovde treba obratiti posebnu pažnju na sredstva kojima je delo izvršeno jer se, putem komparacije karakteristika datih uređaja i njihovih otisaka i utisaka, mogu neposredno dokazati prisustva istih. Veza ovih uređaja sa licima koja se smatraju izvršiocima ukazuje na njihovo učešće u krivičnom delu. Kod ovog krivičnog dela za prvi oblik veoma je značajno utvrditi postojanje određene zaštite autorskog i srodnog prava, u obliku

[67]Čl. 3. ZOPOIS navodi u tač. 8) sredstvo za izbegavanje zaštite jeste svako sredstvo, proizvod, komponenta, odnosno deo proizvoda koji je prevashodno napravljen ili prilagođen sa ciljem da omogući zaobilaženje efikasne tehnološke mere; i tač. 9) efikasna tehnološka mera jeste tehnološki postupak, sredstvo, proizvod, komponenta, odnosno deo kojim se kontroliše pristup zaštićenom autorskom delu ili predmetu srodnog prava ili kojim se sprečava njihovo neovlašćeno korišćenje, odnosno kojim se omogućava otkrivanje krivotvotvorenog žiga ili piratskog primerka autorskog dela, odnosno predmeta srodnog prava.

elektronske informacije, kao i vezu određenog lica sa uklanjanjem ove informacije, i njegovo svojstvo kao i da se uklanjanje vrši neovlašćeno. Veoma je bitno i utvrditi nosioca prava zaštite kako bi se mogla odrediti ustanova koja je oštećena. Način utvrđivanja postojanja povrede zavisi od njenog obima, kao i metoda i tehničkih sredstava koja su tom prilikom korišćena. Kod drugog oblika značajno je utvrditi vezu između radnji i lica koje ih vrši kako bi ustanovili vezu sa proturanjem nezakonitih dela. U svakom slučaju veoma je značajno evidentirati lokacije sredstva i prostore koji su korišćeni u vršenju dela. Kao što je napomenuto u dokaznom i tehničko forenzičkom smislu mogu se koristiti okolnosti i činjenice navedene ranije u tekstu kod krivičnog dela neovlašćenog iskorišćavanja autorskog dela ili predmeta srodnog prava iz člana 199.

Povreda pronalazačkog prava

Član 201

Prvi oblik čini lice koje neovlašćeno proizvodi, uvozi, izvozi, nudi radi stavljanja u promet, stavlja u promet, skladišti ili koristi u privrednom prometu proizvod ili postupak zaštićen patentom (novčana kazna ili zatvor do tri godine). Teži oblik postoji ukoliko je osnovnim oblikom pribavljena imovinska korist ili prouzrokovana šteta u iznosu koji prelazi milion dinara (zatvor od jedne do osam godina).

Prvi privilegovani oblik čini lice koje neovlašćeno objavi ili na drugi način učini dostupnim suštinu tuđeg prijavljenog pronalaska pre nego što je ovaj pronalazak objavljen na način utvrđen zakonom (novčana kazna ili zatvor do dve godine). Drugi teži oblik čini onaj ko neovlašćeno podnese prijavu patenta ili u prijavi ne navede ili lažno navede pronalazača (zatvor od šest meseci do pet godina). I u ovim slučajevima kao i u prethodnom delu predmeti se oduzimaju i uništavaju.

Neovlašćeno korišćenje tuđeg dizajna

Član 202.

Osnovni oblik vrši ono lice koje na svom proizvodu u prometu neovlašćeno upotrebi, u celosti ili delimično, tuđi prijavljeni, odnosno zaštićeni dizajn proizvoda (novčana kaznom ili zatvor do tri godine). Blaži oblik postoji onda kada neko neovlašćeno objavi ili na drugi način učini dostupnim javnosti predmet prijave tuđeg dizajna, pre nego što je objavljen na način

utvrđen zakonom (novčana kazna ili zatvor do jedne godine). Upravo kod prevara o kojima će biti reči kasnije može se videti da se izvršioci u cilju iskorišćavanja lakovernosti ili neopreznost građana kada im se neki zvanični organ obrati, koriste veoma lako okolnosti da se ne sumnja u zvanične dizajne i logoe npr. FBI.

Dalja zaštita u srpskom pravnom sistemu

Zakon o autorskom i srodnim pravima ("Sl. glasnik RS", br. 104/2009, 99/2011) reguliše i određenu materiju koja se odnosi na prekršaje i privredne prestupe lica u vezi sa autorskim pravima ali naravno i građansko – pravne odnose u oblasti prava intelektualne svojine. Pri ovome mora se imati u vidu da: - Do donošenja podzakonskih propisa predviđenih zakonom autorskim i srodnim pravima se primenjuju odredbe propisa donetih na osnovu Zakona o autorskom i srodnim pravima ("Službeni list SCG", broj 61/04), izuzev odredaba koje su u suprotnosti sa ovim zakonom. Takođe, i danom stupanja na snagu ovog zakona prestaju da važe: Zakon o autorskom i srodnim pravima ("Službeni list SCG", broj 61/04) i odredbe čl. 34, 35, 42, 43. i člana 44. stav 1. tač. 1. i 3. Zakona o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine ("Službeni glasnik RS", broj 46/06). Zakonodavac ukazuje i da se primena člana 29. stav 2. ovog zakona[68], odlaže do osnivanja u Republici Srbiji odgovarajuće organizacije za kolektivno ostvarivanje prava, a najkasnije do dana pristupanja Republike Srbije Evropskoj uniji. Privredni prestupi regulisani su članom 215. ovog zakona, prema istom kazniće se za privredni prestup novčanom kaznom u iznosu od 100.000 do 3.000.000 dinara privredno društvo ili drugo pravno lice koje:

1) neovlašćeno objavi, zabeleži, umnoži ili javno saopšti na bilo koji način, u celini ili delimično, autorsko delo, interpretaciju, fonogram, videogram, emisiju ili bazu podataka, ili stavi u promet ili da u zakup ili u komercijalne svrhe drži neovlašćeno umnožene ili neovlašćeno stavljene u promet primerke autorskog dela, interpretacije, fonograma, videograma, emisije ili baze podataka (čl. 16, 20, 21, 22, 25, 26, 27, 28, 29, 116, 126, 131, 136. i 140);

[68]Koji glasi: „U slučaju kablovskog reemitovanja autorskih dela, pravo autora ostvaruje se samo preko organizacije za kolektivno ostvarivanje autorskog i srodnih prava.“

2) u cilju pribavljanja imovinske koristi za sebe ili drugog protivpravno stavi u promet ili da u zakup primerke iz stava 1. ovog člana, za koje zna da su neovlašćeno objavljeni, zabeleženi ili umnoženi (čl. 16, 20, 21, 22, 25, 26, 27, 28, 29, 30, 116, 126, 131, 136. i 140);

3) u svojstvu profesionalnog trgovca umetničkim delima (prodajni saloni, umetničke galerije, aukcijske kuće i sl.) u roku od 30 dana od dana prodaje originala dela likovne umetnosti, ne obavesti autora dela o nazivu, odnosno imenu i adresi prodavca, posrednika i kupca njegovog dela, i o ceni po kojoj je delo prodato i ne plati autoru iznos naknade od prodajne cene dela (član 35. st. 1, 4, 5, 6, 7. i 9)

4) zaobilazi bilo koju efikasnu tehnološku meru ili pruža ili reklamira usluge kojima se to omogućava ili olakšava (član 208. stav 1. tačka 4);

5) ukloni ili izmeni elektronsku informaciju o pravima, ili stavi u promet, uveze, emituje ili na drugi način javno saopšti autorsko delo ili predmet srodnopravne zaštite sa kojeg je elektronska informacija o pravima neovlašćeno uklonjena ili izmenjena, i pri tom zna ili ima osnova da zna da time podstiče, omogućuje, olakšava ili prikriva povredu autorskog prava ili srodnog prava (član 208. stav 1. tačka 5);

6) u svojstvu vlasnika građevine izvrši određene izmene na građevini koja predstavlja materijalizovani primerak dela arhitekture, a preradu dela nije prvo ponudilo autoru dela (član 38);

7) organizaciji ne dostavi ili ne dostavi u propisanom roku, podatke o nazivu predmeta zaštite, učestalosti i obimu iskorišćavanja, kao i o drugim okolnostima koje su relevantne za obračun i raspodelu naknade koja se prema tarifi plaća (član 39. stav 7. i član 187. st. 2, 3, 4. i 5);

8) obavlja poslove kolektivnog ostvarivanja autorskog, odnosno srodnih prava bez dozvole nadležnog organa (član 160. stav 4).

Za radnje iz stava 1. ovog člana kazniće se za privredni prestup novčanom kaznom u iznosu od 50.000 do 200.000 dinara i odgovorno lice u privrednom društvu ili drugom pravnom licu.

Predmeti izvršenja privrednih prestupa i predmeti koji su bili upotrebljeni za izvršenje privrednog prestupa iz stava 1. ovog člana biće oduzeti, a predmeti izvršenja privrednih prestupa biće i uništeni.

Presuda kojom je učiniocu izrečena kazna za privredni prestup iz stava 1. ovog člana javno se objavljuje.

Članom 216. propisuje se odgovornost za preduzetnike. Za radnje iz člana 215. stav 1. tač. 1, 2, 3, 4, 5. i 7. ovog zakona kazniće se za prekršaj preduzetnik novčanom kaznom u iznosu od 50.000 do 500.000 dinara.

Za radnju iz člana 215. stav 1. tačka 6. ovog zakona kazniće se za prekršaj fizičko lice novčanom kaznom u iznosu od 10.000 do 50.000 dinara.

Predmeti izvršenja prekršaja i predmeti koji su bili upotrebljeni za izvršenje prekršaja iz st. 1. i 2. ovog člana biće oduzeti, a predmeti izvršenja prekršaja biće i uništeni.

Članom 217. reguliše se odgovornost za prekršaje. Prema ovom članu kazniće se za prekršaj novčanom kaznom u iznosu od 100.000 do 1.000.000 dinara privredno društvo ili drugo pravno lice koje:

1) bez navođenja imena autora ili interpretatora ili pod drugim imenom u celini ili delimično objavi, izvede, predstavi, prenese izvođenje ili predstavljanje ili emituje tuđe autorsko delo ili iskoristi tuđu interpretaciju (član 15. i član 114. stav 1. tačka 2);

2) bez dozvole autora izmeni ili preradi tuđe autorsko delo ili tuđu snimljenu interpretaciju (čl. 17. i 31. i član 114. stav 1. tačka 3);

3) u svojstvu profesionalnog trgovca umetničkim delima (prodajni saloni, umetničke galerije, aukcijske kuće i sl.) u roku od 30 dana od dana prodaje originala dela likovne umetnosti, ne obavesti autora dela o nazivu, odnosno imenu i adresi prodavca, posrednika i kupca njegovog dela, i o ceni po kojoj je delo prodato i ne plati autoru iznos naknade od prodajne cene dela (član 35. st. 1, 4, 5, 6, 7. i 9)

4) prilikom unošenja u evidenciju i deponovanja kod nadležnog organa, autorskog dela ili predmeta zaštite srodnog prava da neistiniti ili prikrije pravi podatak o svom autorskom delu ili predmetu zaštite srodnog prava (član 202. stav 4);

5) u svojstvu izdavača proda neprodate primerke dela kao staru hartiju, a da ih nije prethodno ponudio autoru, odnosno njegovom nasledniku da ih otkupi (član 81);

6) licima koja na osnovu odredbi ovog zakona o ograničenjima autorskog prava imaju zakoniti pristup primerku autorskog dela ili predmeta srodnog prava, ne omogući da ostvare sadržajna ograničenja prava, izmenom ili otklanjanjem tehnoloških mera ili na drugi način (član 208a stav 1);

7) na primerku autorskog dela ili predmeta srodnog prava izrađenom ili uvezenom u komercijalne svrhe, ne označi jasno i vidljivo upotrebu tehnoloških mera (član 208a stav 3)

Za radnje iz stava 1. ovog člana, kazniće se za prekršaj novčanom kaznom u iznosu od 10.000 do 50.000 dinara i odgovorno lice u privrednom društvu ili drugom pravnom licu.

Za radnje iz stava 1. ovog člana, kazniće se preduzetnik novčanom kaznom u iznosu od 10.000 do 200.000 dinara.

Za radnje iz stava 1. tač. 4. i 5. ovog člana, kazniće se i fizičko lice novčanom kaznom u iznosu od 10.000 do 50.000 dinara.

Novčanom kaznom u iznosu od 10.000 do 50.000 dinara kazniće se za prekršaj fizičko lice koje u roku od 30 dana od dana prodaje originala dela likovne umetnosti, ne obavesti autora dela o nazivu, odnosno imenu i adresi prodavca, posrednika i kupca njegovog dela i o ceni po kojoj je delo prodato i ne plati autoru iznos naknade od prodajne cene dela (član 35. st. 1, 4, 5, 6, 7. i 9).

Zakon o posebnim ovlašćenjima radi efikasne 3aštite prava intelektualne svojine („Službeni glasnik RS“, broj 46/06) takođe ima kaznene odredbe. Privredni prestupi određeni su članom 36. pa tako: novčanom kaznom od 100.000 do 3.000.000 dinara kazniće se za privredni prestup pravno lice koje postupi suprotno odredbi člana 70. stav 1. a u vezi člana 58. stav 1. i člana 33. Zakona o žigovima ("Službeni list SCG", br. 61/04 i 7/05), i to: neovlašćeno stavi na robu ili njeno pakovanje znak zaštićen žigom, ili znak za koji je podneta prijava za priznanje žiga;

neovlašćeno nudi, stavlja u promet, skladišti robu u te svrhe ili obavlja usluge pod znakom zaštićenim žigom ili znakom za koji je podneta prijava za priznanje žiga;

neovlašćeno uvozi ili izvozi robu zaštićenu žigom, ili znakom za koji je podneta prijava za priznanje žiga;

neovlašćeno, u poslovnoj dokumentaciji ili u reklami, koristi znak zaštićen žigom ili znak za koji je podneta prijava za priznanje žiga.

Takođe, novčanom kaznom iz stava 1. ovog člana kazniće se za privredni prestup i pravno lice koje postupi suprotno odredbi člana 70. stav 1. a u vezi sa članom 58. st. 2. i 3. Zakona o žigovima ("Službeni list SCG", br. 61/04 i 7/05), i to koje u prometu koristi:

1) znak nastao podražavanjem znaka zaštićenog žigom, ili znaka za koji je podneta prijava za priznanje žiga;

2) znak zaštićen žigom ili znak nastao podražavanjem znaka zaštićenog žigom uz koji su dodate reči "tip", "način", "po postupku" i sl.

(3) za radnje iz st. 1. i 2. ovog člana kazniće se i odgovorno lice u pravnom licu novčanom kaznom od 10.000 do 200.000 dinara.

(4) predmeti izvršenja privrednog prestupa i predmeti koji su bili upotrebljeni za izvršenje privrednog prestupa iz st. 1. i 2. ovog člana biće oduzeti, a predmeti izvršenja privrednog prestupa biće i uništeni.

Članom 37. propisuju se privredni prestupi. Prema istom novčanom kaznom od 100.000 do 3.000.000 dinara kazniće se za privredni prestup pravno lice, koje postupi suprotno odredbi člana 69. stav 1. a u vezi sa čl. 38. i 57. Zakona o pravnoj zaštiti dizajna ("Službeni list SCG", broj 61/04), i to koje neovlašćeno:

1) na osnovu primene zaštićenog dizajna, odnosno dizajna za koji je podneta prijava izrađuje, na industrijski ili zanatski način, proizvode za tržište;

2) upotrebi u privrednoj delatnosti proizvod zaštićen dizajnom, odnosno proizvode izrađene na osnovu dizajna za koji je podneta prijava;

3) nudi, stavlja u promet i skladišti u te svrhe proizvode zaštićene dizajnom, odnosno proizvode izrađene na osnovu dizajna za koji je podneta prijava;

4) uvozi ili izvozi proizvode koji sadrže zaštićeni dizajn, odnosno proizvode izrađene na osnovu dizajna za koji je podneta prijava.

Stavom 2 predviđa se da će se novčanom kaznom iz stava 1. ovog člana kazniti za privredni prestup pravno lice koje postupi suprotno odredbi člana 69. stav 1. a u vezi sa članom 57. stav 2. Zakona o pravnoj zaštiti dizajna ("Službeni list SCG", broj 61/04), i to koje učini radnju iz stava 1. tač.1. do 4. sa proizvodima nastalim podražavanjem zaštićenog dizajna, odnosno dizajna za koji je podneta prijava.

Stavom 3. predviđa se i odgovornost za odgovorna lica u pravnim licima prema kojoj će se za radnje iz st. 1. i 2. ovog člana kazniti i odgovorno lice u pravnom licu novčanom kaznom od 10.000 do 200.000 dinara.

Predmeti izvršenja privrednog prestupa i predmeti koji su bili upotrebljeni ili namenjeni za izvršenje privrednog prestupa iz stava 1. ovog člana biće oduzeti, a predmeti izvršenja privrednog prestupa biće i uništeni.

Privredni prestupi se tretiraju i članom 38. Novčanom kaznom od 100.000 do 3.000.000 dinara kazniće se za privredni prestup pravno lice koje postupi suprotno odredbi člana 69. stav 1,

a u vezi sa čl. 38. i 57. Zakona o pravnoj zaštiti dizajna ("Službeni list SCG", broj 61/04), i to koje neovlašćeno obavi prijavu tuđeg dizajna.

(2) Za radnje iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu novčanom kaznom od 10.000 do 200.000 dinara.

Slično je i sa članom 39. Novčanom kaznom od 100.000 do 3.000.000 dinara kazniće se za privredni prestup pravno lice ako neovlašćeno proizvodi, uvozi, izvozi, nudi radi stavljanja u promet, stavlja u promet, skladišti ili koristi u komercijalne svrhe proizvod ili postupak zaštićen patentom, odnosno malim patentom.

Za radnje iz stava 1. ovog člana kazniće se odgovorno lice u pravnom licu novčanom kaznom u iznosu od 10.000 do 200.000 dinara.

Predmeti izvršenja privrednog prestupa i predmeti koji su bili upotrebljeni za izvršenje privrednog prestupa iz stava 1. ovog člana biće oduzeti, a predmeti izvršenja privrednog prestupa biće i uništeni.

Prekršaji su obrađeni članom 41. Po njemu novčanom kaznom od 50.000 do 1.000.000 dinara kazniće se za prekršaj pravno lice koje postupi suprotno odredbi člana 72. stav 1. Zakona o žigovima ("Službeni list SCG", br. 61/04 i 7/05) i članom 71. stav 1. Zakona o pravnoj zaštiti dizajna ("Službeni list SCG", broj 61/04), i to koje se neovlašćeno bavi zastupanjem pred organom nadležnim za zaštitu prava intelektualne svojine.

Za radnje iz stava 1. ovog člana kazniće se odgovorno lice u pravnom licu novčanom kaznom u iznosu od 5.000 do 100.000 dinara.

Članom 44. propisuje se odgovornost fizičkih lica. Novčanom kaznom od 5.000 do 50.000 dinara, kazniće se za prekršaj fizičko lice: tač. 2) za radnje iz člana 41. stav 1. ovog zakona koje postupi suprotno odredbi člana 72. stav 3. Zakona o žigovima ("Službeni list SCG", br. 61/04 i 7/05) i članom 71. stav 3. Zakona o pravnoj zaštiti dizajna ("Službeni list SCG", broj 61/04);

2.3. AUTORSKA DELA U SAJBER PROSTORU

2.3.1. PISANA AUTORSKA DELAU SAJBER PROSTORU

2.3.1.1. KNJIŽEVNA I SRODNA DELA

„Pisana dela ... su autorska dela izražena jezikom u pisanom obliku.“[69] Ova jednostavna i očekivana definicija dobija na značaju i dodatno se komplikuje kada je reč o pisanim delima u elektronskom obliku, tj. onima koja su podesna da se objave i/ili interpretiraju u celini ili delimično u digitalnom okruženju. Digitalno objavljivanje autorskog dela (eng. *electronic publishing*) je neprecizan i nedovoljno jasan, ali može uključivati čitav niz raznorodnih aktivnosti koje vode istom cilju – predstavljanju nekog autorskog dela širem broju korisnika, u digitalizovanoj formi. Neke od tih aktivnosti su i proizvodnja, prodaja, iznajmljivanje ili činjenje dostupnim na drugi način fizičkog objekta na kojem se nalazi autorsko delo u digitalizovanom obliku; prenošenje autorskog dela u digitalizovanom obliku putem elektronske komunikacije (npr. preuzimanje sa interneta, *e-mail* komunikacija, i sl.); emitovanje autorskog dela putem sredstava elektronske komunikacije.[70] Naravno, svaka od ovih aktivnosti se može raditi uz znanje i odobrenje autora, ili bez njega (dakle, protivpravno). Pisana dela nisu izuzetak od takve prakse – dok se legalne opisane aktivnosti nazivaju elektronskim izdavaštvom, druga ilegalna varijanta spada u jednu od vrsta „piraterije“.

Prema članu 2. Bernske konvencije, izraz „književna i umetnička dela“ obuhvata sve tvorevine iz književne, naučne i umetničke oblasti, bez obzira na način njihovog izražavanja. Književna dela su na taj način svrstana u jednu od osnovnih kategorija stvaralaštva i onih dela koja su zaštićena režimom autorskih prava. Među oblicima književnih – preciznije bi bilo reći pisanih – dela, izričito se pominju knjige, brošure i ostali spisi,druga dela iste prirode. Sam pojam „književna i naučna dela“ nije dovoljno precizan. I književna dela mogu biti naučna. Takođe, mnogi oblici pisanog izražavanja ne moraju biti književni – govori i razgovori iz navedenog primera. Naposletku, postoje oblici književnog i naučnog izražavanja koji sasvim sigurno uživaju

[69]Vidoje Ž. Spasić, *Autorska dela u digitalnom okruženju*, Niš, 2011, str. 83.
[70]David Bainbridge, *Introduction to Computer Law*, Pearson Education Limited, London, 2000, str. 74.

autorskopravnu zaštitu a koji nisu navedeni – ovde se najpre misli na računarske programe, o kojima će posebno biti reči, ali i na različite druge forme naučnoistraživačkog rada i rezultata.

Sa druge strane, novododati član 2bis. Bernske konvencije ostavlja mogućnost državama da određene oblike pisanog izražavanja izričito liše autorskopravne zaštite – politički govori, kao i govori odnosno podnesci izraženi tokom sudskih postupaka. Oni mogu biti deo pisanih dela ukoliko se objave, odnosno učine javnim u pisanoj formi, ali mogu biti i besede, usmeno iskazana dela. S time u vezi je i član 10bis. Konvencije, koji ne oduzima mogućnost autorskopravne zaštite delima koja se bave aktuelnim ekonomskim, političkim ili verskim pitanjima, ali dopušta mogućnost da se takva dela prenesu, tj. citiraju preko drugih glasila (uključujući i elektronska) bez izričitog odobrenja autora, odnosno tako nešto neće biti moguće samo ukoliko je autor izričito zabranio. I ovo je logična posledica svrhe nastanka ovakvih pisanih dela – sva ona dela koja se bave aktuelnim društveno-političkim temama nastala su da bi se analize i zaključci koji su u njima izraženi što efikasnije i masovnije prenosili.

Bernska kovencija takođe dopušta dva izuzetka koja su karakteristična za pisana dela. Naime, moguće je citirati pisano delo i bez izričitog odobrenja autora ako je takva praksa uobičajena i ako je to u skladu sa ciljem koji se želi postići; takođe, moguće je bez posebnog odobrenja autora koristiti njegova pisana dela u procesu nastave. Naravno, u oba slučaja se mora izričito navesti koje je delo u pitanju, kao i ko je autor citiranog dela – dakle, pravila citiranja se moraju dosledno poštovati.[71] Iako su ovi izuzeci logični i poželjni, postavlja se pitanje da li se pod uobičajenom praksom podrazumeva i navođenje autorskih dela (uz pravilno citiranje) i u radovima koji se objavljuju elektronski, odnosno na internetu? Čini se da bi odgovor morao biti potvrdan, a i praksa to jasno pokazuje. Svrha izuzetaka jeste naučno usavršavanje, naučno istraživanje, kao i obrazovanje – sredstva kojima se dolazi do željenog cilja (elektronska ili tradicionalna) nisu i ne mogu biti predmet posebnog režima ako je već ovakvo korišćenje pisanih dela dozvoljeno. Osim ovih i prethodno pojašnjenih izuzetaka, članovi 11bis – 12. Konvencije je sasvim izričit: autori pisanih dela jedini imaju pravo da odobre (ili ne) bilo kakvo reprodukovanje njihovih dela, uključujući tu i elektronske verzije i reprodukcije, izvedene u celini ili delimično, kao i bilo kakve izmene, adaptacije i prerade tih dela (ovo je inače opšti režim koji se primenjuje na sva autorska dela osim ukoliko nije primenjen neki od izuzetaka). Ono što je takođe posebno

[71] Član 10. Bernske konvencije.

važno u odnosu na analizu kinematografskih dela, jeste da autori pisanih dela imaju isključivo pravo da dozvole adaptaciju njihovih dela u kinematografske svrhe.[72]

Zakon o autorskom i srodnim pravima u članu 2, stav 2, tačka 1. navodi kao jedan od oblika autorskog dela i pisana dela, i među njima naročito izdvaja (ali se na njih ne ograničava) knjige, brošure, članke, prevode, računarske programe u bilo kojem obliku njihovog izražavanja, uključujući i pripremni materijal za izradu ovih pisanih dela. Dakle, tekst Zakona je savremeniji od teksta Bernske konvencije i prepoznaje računarske programe kao jedan od oblika pisanih autorskih dela.

U članu 6. Zakona se razrađuje opisano rešenje iz člana 2bis. Bernske konvencije, tako što se izričito lišavaju statusa autorskog dela: zakoni, podzakonski akti i drugi propisi; službeni materijali državnih organa i organa koji obavljaju javnu funkciju; službeni prevodi propisa i službenih materijala državnih organa i organa koji obavljaju javnu funkciju; podnesci i drugi akti u upravnom ili sudskom postupku. Zanimljiv je i prvi stav ovog člana, prema kojem autorskopravnom zaštitom nisu obuhvaćene opšte ideje, postupci, metode rada, ili matematički koncepti kao takvi, kao i načela, principi i uputstva koji su sadržani u autorskom delu (oni se odnose na svako autorsko delo, ali je sasvim očigledno imajući u vidu prirodu ovog izuzetka da će njime najpre biti obuhvaćena pisana autorska dela).

Zakon dalje u članovima 28-30. ustanovljava osnovne elemente opšteg režima zaštite autorskih dela od nedozvoljenog emitovanja, koji se shodno odnose i na pisana dela. Od značaja je međutim i član 33. kojim se autoru daje pravo „da drugome zabrani ili dozvoli da njegovo delo koje je zabeleženo na nosaču zvuka, odnosno nosaču slike (kompakt disk, audio kaseta, video kaseta, filmska traka, optički disk, dijapozitiv) javno saopštava uz pomoć tehničkih uređaja za reprodukovanje zvuka, odnosno slike.“ Očigledno je da pod ovu situaciju spada i svako elektronsko emitovanje, odnosno reprodukovanje pisanih autorskih dela.

Autori onih dela koja za koja se, obzirom na njihovu prirodu, može očekivati da će biti umnožavana za lične nekomercijalne potrebe na nosače zvuka, slike i teksta (književna, muzička, filmska i dr.) imaju pravo na posebnu naknadu od uvoza, odnosno prodaje tehničkih uređaja i praznih nosača zvuka, slike i teksta za koje se opravdano može pretpostaviti da će biti korišćeni

[72] *Ibidem, č*lan 14.

za takvo umnožavanje.[73] U slučaju umnožavanja autorskih dela fotokopiranjem ili sličnom tehnikom, pored prava na naknadu iz stava 1. ovog člana autor ima pravo i na naknadu od pravnog ili fizičkog lica koje pruža usluge fotokopiranja uz naknadu.[74] Ovakav pravni režim, koji u praksi nailazi na različite osude zbog veličine naknade i načina naplaćivanja, očigledno je moguće primeniti i na pisana autorska dela, posebno u pogledu njihovog fotokopiranja, odnosno drugih oblika umnožavanja. Ipak, valja napomenuti da se ova odredba odnosi na one koji usluge fotokopiranja pružaju uz naknadu – dakle, bave se ovime kao profitnom delatnošću – i da se takvo rešenje ne može primeniti na fakultete i druge obrazovne i naučne ustanove koji fotokopiraju materijale različitih autora u obrazovne i naučnoistraživačke svrhe.[75] U prilog tom posebnom režimu govori i član 49. Zakona, prema kojem se za korišćenje pravilno citiranog dela čiji je izvod, odlomak upotrebljen kao ilustracija, potvrda ili referenca, ne mora plaćati autorska naknada, niti pribaviti dozvola autora (ovo korenspodira opisanom rešenju iz člana 10. Bernske konvencije).

Rešenje iz člana 10bis. Bernske konvencije razrađeno je i u ovom zakonskom tekstu. Tako, je moguće bez dozvole autora, a uz obavezu plaćanja autorske naknade, u sredstvima javnog obaveštavanja umnožavanje, stavljanje u promet primeraka, kao i drugi oblici javnog saopštavanja članaka koji su objavljeni u drugim sredstvima javnog obaveštavanja, pod uslovom da se ti članci odnose na tekuća ekonomska, politička ili verska pitanja, a da autor to nije izričito zabranio. Obaveza plaćanja naknade neće postojati ako se u ove svrhe u vidu pregleda više različitih komentara ili članaka, iskorišćavaju samo kratki odlomci iz komentara ili članaka.[76]

Pisana dela se dakle mogu, pod manje ili više sličnim uslovima u odnosu na ostale vrste i oblike autorskih dela, naći u elektronskoj formi i koristiti kao i u štampanom obliku. U tom

---

[73] Ovakva odredba nije neuobičajena u mnogim državama širom sveta. Razmatrajući je na primeru sudske prakse SAD, L.Lessig povlači paralelu između video-rekordera i pištolja: sudovi u SAD su naime najpre stali na stanovište da se svaki prodavac video-rekordera može smatrati odgovornim za kršenje autorskih prava koje počini kupac istog, time što mu je „omogućio“ da pribavi opremu za izvršenje krivičnog dela; ista takva odgovornost ne postoji kod prodavaca vatrenog oružja. (Lawrence Lessig, *Free Culture*, New York, 2004, str. 160) Verovatno i sami shvatajući ekstremnost i besmislenost ovakvih stavova, zakonopisci su potom počeli da „preventivno kažnjavaju“ prodavce sličnih tehnologija, koje se potencijalno mogu koristiti za kršenje autorskih prava, namećući im posebnu taksu već prilikom nabavke ovakvih porizvoda.

[74] Član 39, stavovi 1. i 5. Zakona.

[75] U tom smislu svakua eventualna nedoumica rešena je članom 55. Zakona: „Bez dozvole autora, a uz obavezu plaćanja autorske naknade, dozvoljeno je u državnim organima, obrazovnim institucijama i javnim bibliotekama umnožavanje, za potrebe nastave ili naučnog istraživanja, na papiru ili sličnom nosaču odlomaka iz publikacija putem fotokopiranja ili bilo kojeg oblika fotografske ili slične tehnike koja daje slične rezultate.“

[76] Član 56. Zakona.

smislu, razlike koje poznaje srpsko zakonodavstvo su minimalne a principi autorskog prava su dosledno sprovedeni bez obzira na to u kojoj formi se pisano autorsko delo koristi.

2.3.1.2 RAČUNARSKI PROGRAMI

Spasić navodi definiciju računarskih programa iz jednog starijeg zakonskog akta SAD, prema kojem oni predstavljaju „niz uputstava ili naloga koje treba upotrebiti neposredno ili posredno u računaru da se postigne određeni efekat“.[77] Danas većina građana računarske programe doživljava kao gotov proizvod koji im omogućava lakše obavljanje određenih poslova, ili neku vrstu zabave (npr. računarske igre). Međutim, računarski programi su u suštini ostali upravo ono što navedena definicija otkriva – niz *napisanih* komandi i uputstava u nekom računarskom jeziku, koje računar prepoznaje i izvršava. Ono što korisnik prepoznaje kao računarski program preko korisničkog interfejsa, samo je krajnji rezultat tog niza izvršenih komandi, od strane računara.

Kao što je već napomenuto, u članu 2. Zakona o autorskim i srodnim pravima, računarski programi su određeni kao vrsta pisanih autorskih dela, bez obzira na njihov pojavni oblik (kako stoji u Zakonu, „bez obzira na oblik izražavanja“) – u tom smislu je podjednako kažnjivo neovlašćeno raspolagati na bilo koji način skriptom računarskog programa, kao i mehanički kopirati CD/DVD na kojem se taj program nalazi u elektronskom obliku.[78]

Zakon je u tekstu koji sledi ipak škrt kada je reč o posebnim odredbama koje bi se odnosile samo na računarske programe. U članu 47. navedene su neke specifičnosti koje se vezuju za prirodu korišćenja računarskih programa. Tako je lice koje je „na zakonit način pribavilo primerak računarskog programa da, radi sopstvenog uobičajenog namenskog korišćenja programa, bez dozvole autora i bez plaćanja autorske naknade: smešta program u memoriju računara i pušta program u rad; otklanja greške u programu, kao i da vrši druge neophodne izmene u njemu koje su u skladu sa njegovom svrhom, ako ugovorom nije drukčije određeno; načini jedan rezervni primerak programa na trajnom telesnom nosaču; izvrši dekompilaciju

---

[77] .Spasić Ž Vidoje, *op.cit*, str. 69. U navedenom delu Spasić, sasvim pravilno, razlikuje računarski program kao napisani tekst programa i softver čiji je pojam širi – on se sastoji iz računarskog programa i različite dodatne dokumentacije, kao što je uputstvo za korišćenje programa, ambalaža, opis programa, i sl. *Ibidem.*

[78] Svrstavanje računarskih programa u pisana autorska dela nije originalnost srpskog Zakona o autorskim i srodnim pravima – slično rešenje primenjeno je u nizu zakonskih rešenja počev još od sredine osamdesetih godina prošlog veka (SAD, Japan, Velika Britanija, Nemačka, Francuska, nešto kasnije i Španija), dok je Evropska unija 1991. godine izdala direktivu kojom je računarske programe izjednačila sa književnim delima u smislu Bernske konvencije. Spasić Ž Vidoje, *op.cit*, str. 70.

programa isključivo radi pribavljanja neophodnih podataka za postizanje interoperabilnosti tog programa sa drugim, nezavisno stvorenim programom ili određenom računarskom opremom, pod uslovom da taj podatak nije bio na drugi način dostupan i da je dekompilacija ograničena samo na onaj deo programa koji je neophodan za postizanje interoperabilnosti.“ U pitanju su uobičajene radnje koje korisnici računarskih programa mogu (moraju) da vrše da bi ih koristili; u slučaju poslednje od navedenih radnji, Zakon izričito predviđa da se podaci dobijeni na takav način ne smeju saopštavati drugima ili koristiti za druge svrhe, posebno za stvaranje ili plasman drugog računarskog programa kojim bi se povredilo autorsko pravo na prvom, kao i da takve radnje može izvršiti neposredno lice koje je na zakonit način pribavilo primerak računarskog programa ili drugo stručno lice koje radi po njegovom nalogu.

Osim računarskih programa koji spadaju u uobičajeni, zakonski režim zaštite autorskih prava, postoje i licence koje dozvoljavaju različite drugačije režime korišćenja i prerade računarskih programa – u pitanju je tzv. „*open source software*“ (besplatan softver, ili softver otvorenog koda). O ovim pitanjima već je bilo reči u prethodnom tekstu.[79]

[79] Videti: Licence otvorenog sadržaja, deo 2.1.9 ove knjige, i Licence Kreativne zajednice, deo 2.1.10. ove knjige.

2.3.2. MUZIČKA DELAU SAJBER PROSTORU

Prema članu 2. Bernske konvencije, izraz „književna i umetnička dela“ obuhvata sve tvorevine iz književne, naučne i umetničke oblasti, bez obzira na način njihovog izražavanja, pa se između ostalih dela navode i *muzičke kompozicije s rečima i bez njih*.

Zakon o autorskim i srodnim pravima u članu 2 autorskim delom, u skladu sa Bernskom konvencijom, obuhvata i "muzička dela sa rečima ili bez reči".

Bernska konvencija u članu 2, tačci 3 posebno previđa zaštitu za *adaptacije i muzičke aranžmane*.[80]

U Bernskoj konvenciji i u našem Zakonu o autorskim i srodnim pravima posebno su izdvojena *dramsko muzička dela*. Dramska muzička dela se razlikuju od muzičkih dela po tome što u dramskom muzičkom delu muzika čini celinu sa dramskim delom i deo je scenskog nastupa.

Muzička autorska dela su orginalna autorska dela kompozitora, tekstopisaca, aranžera, i svih onih koji su prilikom stvaranja muzičkog dela uneli svoje intelektualno stvaralaštvo. Kod muzičkih dela potrebno je razlikovati samu muzičku kompoziciju od snimanja muzičkih dela. Muzičku kompoziciju čini sama kompozicija i tekst kompozicije (muzičko delo može biti kombinacije muzike i teksta ili sama muzika). Tako da imamo kao autore kompozitora, tekstopisca, aranžera, naravno i sve one druge koji su dali vidljiv i merljiv doprinos u stvaranju muzičkog autorskog dela.

Autor muzičkog dela pored prava koja imaju i svi drugi autori ima i pravo da reprodukuje svoje umetničko delo, da stvori izvedeno umetničko delo, da distribuira svoje muzičko delo i da javno izvodi svoje muzičko delo.

Pravo reprodukcije muzičkog dela obuhvata pravo da ga autor snimi na traci, kompakt disku, ili kao digitalni fajl u nekom od muzičkih formata (bio on analogni ili digitalni).Treba napomenuti da je napredak tehnologije danas omogućio vrlo jednostavno pretvaranje analognog u digitalni format i krajnje jednostavno i gotovo potpuno besplatno kopiranje i distriburanje muzičkih dela u sajber prostoru.

Pravo autora na distribuciju muzičkog dela obuhvata pravo na pravljenje i prodaju kopija muzičkog dela. On ovo pravo može preneti na izdavača, odnosno proizvođača recimo kompakt

[80] *Zakon o ratifikaciji Bernske konvencije za zaštitu književnih i umetničkih dela*, Sl. list SFRJ, 14/75 i Sl. list SFRJ – Međunarodni ugovori, 4/86.

diskova. Iz ovog prava proističe zabrana da bilo ko drugi bez dozvole autora muzičkog dela distribuira njegovo autorsko delo. Najčešći oblik kršenja prava autora muzičkog dela danas je neovlašćenja distribucija muzičkog dela. Svakoga dana u sajber prostoru se neovlašćeno postavljaju kopije mnogih muzičkog dela u digitalnog formata (mp3, flac, itd.) na raznim internet prezentacijama i omogućava se njihovo preuzimanje od strane neograničenog broja korisnika interneta.

Kao posebno pravo autora muzičkog dela postoji pravo javnog izvođenja muzičkog autorskog dela na koncertu i drugim javnim manifestacijama, emitovanje muzičkog autorskog dela na radiju, televiziji, kablovsko i satelitsko emitovanje. Muzičko delo ne sme biti javno izvođeno bez dozvole autora, odnosno udruženje autora muzičkih dela (organizacije za kolektivno ostvarivanje prava).

Članom 8. WIPO ugovora o autorskom pravu[81] predviđeno je da autori muzičkih dela, kao i autori književnih i umetničkih dela imaju isključivo pravo da dozvole bilo kakvo saopštenje javnosti svojih dela, *žičnim ili bežičnim putem,* uključujući i takvo činjenje dostupnim javnosti njihovih dela koje se vrši na takav način da pripadnici javnosti mogu da pristupe tim delima sa mesta i u vreme koje individualno odaberu, odnosno putem interneta.

Međunarodna pravna regulativa WIPO ugovorom o interpretacijama i fonogramima[82] posebno štiti prava interpretatora i prava proizvođača fonograma. Ovim aktom kao "interpretatori" se definišu glumci, pevači, muzičari, igrači i druga lica koja glume, pevaju, izvode, besede, igraju i interpretiraju ili na neki drugi način izvode književna i umetnička dela ili izraze folklora. Interpretatori imaju isključivo pravo da daju dozvolu u pogledu svojih interpretacija, za emitovanje i javno saopštavanje svojih nezabeleženih interpretacija, osim za slučajeve gde je interpretacija već emitovana, i za beleženje svojih nezabeleženih interpretacija. Oni imaju i prava na umnožavanje, na distribuciju, davanje u zakup i pravo činjeenja dostupnim zabeleženih interpretacija. Proizvođači fonograma, iraz "fonogram" označava zapis zvuka interpretacije ili drugih zvukova, ili predstavljanja zvukova zabeležen u drugom obliku zapisa od zapisa kinematografskom ili drugom audiovizuelnom delu, imaju pravo na umnožavanje, pravo na distribuciju, pravo na davanje u zakup i pravo na činjenja dostupnim javnosti svojih

[81] *Zakon o potvrđivanju WIPO ugovora o autorskom pravu*, SL. list SRJ – Međunarodni ugovori, 13/2002.
[82] *Zakon o potvrđivanju WIPO ugovora o interpretacijama i fonogramima*, SL. list SRJ – Međunarodni ugovori, 13/2002.

fonograma žičnim i bežičnim putem, na način koji omogućava da im publika može pristupiti sa mesta i u vreme koje ona individualno odabere.

2.3.3. AUDIO-VIZUELNA DELAU SAJBER PROSTORU

2.3.3.1. KINEMATOGRAFSKA DELA U UŽEM SMISLU

Bernska konvencija u već citiranom članu 2. kao vrstu autorskih dela navodi i „kinematografska dela s kojima su izjednačena dela izražena postupkom sličnim kinematografiji". U kasnijem tekstu Konvencije se kinematografska dela postavljaju u opšti okvir zaštite autorskih prava, uz neke izuzetke koji su razumljivi obzirom na njihove specifičnosti, dok se nosioci autorskih prava određuju prema pravu zemlje u kojoj je kinematografsko delo nastalo[83]. Zakon o autorskom i srodnim pravima navodi kao vrstu autorskog dela filmsko delo, i deli ga na kinematografska i televizijska dela. Otuda je V.Spasić sasvim u pravu kada napominje da postoji izvesna konfuzija između termina „kinematografsko delo" i „filmsko delo", obzirom da se pod prvim u početku podrazumevao sam sadržaj autorskog dela, dok je film bio samo medijum, nosač tog sadržaja.[84] Danas, u doba elektronskih komunikacija i elektronskih zapisa praktično svih autorskih dela, ova razlika gubi na značaju. Ipak, uobičajeni naziv filmska dela je ostao kao generički, i on obuhvata široki spektar igranih, dokumentarnih i animiranih filmova, kao i televizijskih emisija autorskog karaktera.

Filmovi kao ekvivalent užem značenju pojma kinematografskih ili filmskih dela, specifičan su proizvod koji sadrži više umetničkih elemenata, samim tim i više vrsta autorskih dela koja su ukomponovana u celinu. Tako se kod filma mogu sasvim jasno razdvojiti scenario kao pisano delo, muzička komponenta kao posebno autorsko delo, kao i slika kao zaseban element. Moguće je imati i druga autorska dela inkorporirana u ovu celinu – npr. posebna plesna koreografija, i sl. Otuda filmovi okupiraju posebnu pažnju zakonopisaca, a ni srpski Zakon nije izuzetak. U članu 11. Zakona o autorskim i srodnim pravima se izričito određuje da će se autorima filma smatrati pisac scenarija, režiser i direktor fotografije. Ukoliko je muzika bitan element filma, odnosno ukoliko je u pitanju tzv. muzički film, a komponovana je isključivo za potrebe stvaranja filmskog dela, onda će se i kompozitor smatrati koautorom filmskog dela. Ako

[83] Član 14bis. Konvencije.
[84] Spasić Ž Vidoje, *op.cit*, str. 79-80.

se radi o crtanom, odnosno animiranom filmu ili su crtež ili animacija bitni elementi filmskog dela, onda će se i glavni animator smatrati koautorom filmskog dela. Iako je moguće ugovorom o filmskom delu ustupiti imovinska prava na to delo proizvođaču filmskog dela, pisac scenarija i kompozitor filmske muzike, kao koautori filmskog dela zadržavaju pravo da svoje delo samostalno iskorišćavaju, odvojeno od filmskog dela, osim ako je u ugovoru o filmskom delu predviđeno drukčije.[85]

Filmska dela su pogodna za digitalizaciju, pa je otuda i filmsko delo obuhvaćeno rešenjima iz članova 33. i 39. Zakona. Članom 33. ustanovljeno je isključivo pravo autora da drugome zabrani ili dozvoli da njegovo delo koje je zabeleženo na nosaču zvuka, odnosno nosaču slike (kompakt disk, audio kaseta, video kaseta, filmska traka, optički disk, dijapozitiv) javno saopštava uz pomoć tehničkih uređaja za reprodukovanje zvuka, odnosno slike. Dalje, član 39. ustanovljava isti režim za filmska dela o kojem je bilo reči prilikom analize regulative za književna i srodna dela, a koji je izuzetno relevantan kada je reč o digitalizaciji filmskih dela: „Autori dela za koja se, s obzirom na njihovu prirodu, može očekivati da će biti umnožavana za lične nekomercijalne potrebe na nosače zvuka, slike i teksta (književna, muzička, filmska i dr.) imaju pravo na posebnu naknadu od uvoza, odnosno prodaje tehničkih uređaja i praznih nosača zvuka, slike i teksta za koje se opravdano može pretpostaviti da će biti korišćeni za takvo umnožavanje.“[86] Ova odredba, koja je kako je već rečeno prisutna (i kritikovana) u mnogim uporednim zakonodavstvima, upečatljivaje kada je reč o filmskim delima pre svega zato što veliki filmski studiji, uglavnom situirani u SAD, vode najglasniju kampanju protiv slobode interneta i internet komunikacije, koja se može zloupotrebiti za kršenje autorskih prava filmskih stvaralaca.[87]

Prema Zakonu, filmski producent, odnosno proizvođač videograma, jedini je ovlašćen da dozvoli (ili ne dozvoli) umnožavanje i distribuciju filmskog dela. Međutim, razvoj savremenih tehnologija i komunikacija učinio je mogućim da se ona mogu praktično umnožavati u svakom domaćinstvu, kao i pribavljati neautorizovane kopije na internetu. Zbog toga se pitanju te tzv. „piraterije“ posvećuje velika pažnja u filmskoj i muzičkoj industriji, kao i među proizvođačima

[85] Članovi 88. i 89. Zakona. Ugovorom o filmskom delu se jedno ili više lica obavezuju proizvođaču filmskog dela da stvaralački sarađuju na izradi filmskog dela, a za kasnije iskorišćavanje tog dela mogu dobiti određenu autorsku naknadu, koja se takođe ugovara (članovi 88. i 92. Zakona).
[86] Član 39, stav 1. Zakona.
[87] Videti naročito *supra*, deo o ACTA sporazumu.

računarskih programa. Kao što je već objašnjeno, svako premošćavanje zaštite kojom su nosači ovih dela obezbeđeni, njihovo neautorizovano kopiranje i stavljanje u promet odnosno činjenje dostupnim drugim licima na bilo koji način, predstavlja prekršaj, ili krivično delo u zakonodavstvima većine država.[88]

2.3.3.2. TELEVIZIJSKI I RADIO PROGRAMI

Bernska konvencija ne govori eksplicitno o televizijskim i radio programima kao o autorskim delima, već upotrebljava široki pojam „dela izražena postupkom sličnim kinematografiji“, u kojem bi definitivno trebalo prepoznati televizijske emisije bez obzira da li se radi o snimljenim emisijama ili programu koji se emituje uživo. Za razliku od tog teksta, televizijska dela se eksplicitno pominju u Zakonu o autorskom i srodnim pravima[89]. Televizijski i radio programi se u svakom slučaju moraju smatrati autorskim delima – činjenica da se radio programi ne pominju izričito prilikom nabrajanja specifičnih autorskih dela, im ne oduzima to svojstvo. Ovaj problem umnogome razrešava član 28. Zakona o autorskom i srodnim pravima, koji utvrđuje isključivo autorsko pravo da se dozvoli (odnosno zabrani) emitovanje autorskog dela, i pri tome emitovanje definiše kao „javno saopštavanje dela žičnim ili bežičnim prenosom radijskih ili televizijskih programskih signala namenjenih za javni prijem (radio-difuzija i kablovska difuzija)“. Radijski i televizijski program se dakle posmatraju kao načini izražavanja nekog drugog autorskog dela, pri tome ne isključujući mogućnost da se radijske emisije posmatraju i kao zasebna autorska dela, ako ispunjavaju kriterijume originalnosti koji se zahtevaju i za druge oblike autorskih dela.[90]

Analogno pravima filmskog producenta kod filmskih dela, Zakon predviđa pravo proizvođača emisije, koje se odnosi na električni, elektromagnetni ili drugi signal pretvoren u zvučni, vizuelni, odnosno zvučno-vizuelni sadržaj koji se emituje radi saopštavanja javnosti. U ova prava spadaju i dozvola za reemitovanje emisije, snimanje emisije na nosač zvuka i/ili slike,

[88] Na ovom mestu bi čini se bilo sasvim prikladno uputiti na zanimljivo poređenje koje L.Lessig pravi između internet deljenja fajlova sa autorskim sadržajem i prodavnica starih knjiga i ploča, efektno upoređujući drastično različite pravne režime pod kojima se nalaze:Lessig L., *op.cit*, str. 71-72.

[89] Član 2. Zakona.

[90] Do ovakvog zaključka se može doći tumačenjem člana 29. Zakona.

umnožavanje snimka, itd. Time se definitivno televizijski i radio programi zaokružuju u sistemu autorskog prava a posebnu pažnju bi trebalo posvetiti jednom od prava proizvođača emisije – interaktivno činjenje dostupnim javnosti svoje emisije žičnim ili bežičnim putem. Pravo proizvođača emisije između ostalog podrazumeva i dozvolu za *web casting*, emitovanje emisije preko interneta i to u realnom vremenu – uživo onda kada se emisija emituje i na radiju/televiziji, ili emitovanje snimka emisije (odložene verzije) u nekom kasnijem trenutku.[91] Ovo je jedan od osnovnih načina korišćenja, ali i mogućih zloupotreba odnosno neovlašćenih emitovanja, televizijskog i radio materijala – autorskih emisija – na internetu[92]. Međutim, pojam proizvođača emisije je važan i kod internet radio-stanica, koje svoj program emituju isključivo preko interneta. Internet radio ima svojih očiglednih prednosti, jer se može emitovati za ceo svet, bez obzira gde se slušalac nalazi, broj emitera nije ograničen brojem slobodnih frekvencija, i sl. Procene su da jedna petina građana SAD sluša onlajn radio stanice[93], dok je još 2004. godine ukupan broj korisnika na svetskom nivou bio 80 miliona, a u poslednjih nekoliko godina beleži rast od gotovo 50% godišnje.[94]

Mora se napomenuti da autorska prava koja važe u opštem režimu, ostaju identična i kada je reč o radiju i televiziji kao isključivom internet fenomenu – dakle, sve ono što je rečeno o „običnim medijima“ na način na koji su gledaoci i slušaoci tradicionalni navikli da ih konzumiraju, važi i za njihove internet verzije – autorska prava u internet svetu su i dalje zaštićena i svako neovlašćeno preuzimanje, ili bilo koji način neovlašćene distribucije, zabranjen je i kažnjiv.

---

[91] Videti: Spasić Ž Vidoje, *op.cit*, str. 117-118.

[92] Drugi načini bi se mogli smatrati kršenjem autorskih prava na drugim autorskim delima – npr. emitovanje ili činjenje dostupnim na drugi način filmskog dela koje je preuzeto (snimljeno) sa neke televizijske stanice.

[93] Izvor: *Online Radio Statistics*, Internet adresa: http://www.truemeasure.com/onlineStatistics.php, 01.06.2012.

[94] Lessig L., op.cit, str. 195; *Online Radio Statistics*, loc.cit.

2.3.4. GOVORNA DELAU SAJBER PROSTORU

Bernska konvencija u već citiranom članu 2 u okviru izraza „književna i umetnička dela“ obuhvata *predavanja, govore, besede i druga dela iste prirode*.U okviru Bernske konvencije veća pažnja je posvećena, kada su u pitanju govorna dela, jedino *političkimgovorima i govorima održanim u toku sudskih rasprava*. Članom 2bis ostavljeno je nacionalnim zakonodavstvima da delimično ili potpuno isključe iz zaštite predvišene članom 2 Bernske konvencije političke govore i govore održane u toku sudskih rasprava. Nacionalnim zakonodavstvima ostavljeno je da utvrde uslove pod kojima će predavanja besede i druga dela iste prirode koja su javno izrečena moći da budu reprodukovana putem štampe, emitovana putem radio-difuzije prenošena javnosti preko žica i da budu predmet javnog saopštavanjaukoliko je takvo korišćenje opravdano ciljem koji se ima postići obaveštavanjem. Mešutim i u ovim slučajevima ostavljeno je autoru isključivo pravo da svoja dela skupi u zbirke.

Naš Zakon o autorskim i srodnim pravima u članu 2, tačci 2 autorskim delom, u skladu sa Bernskom konvencijom, obuhvata i *govorna dela* (predavanja, govori, besede i dr.).

Za govorna dela predviđena su ista moralna i imovinska prava za autore, kao i za sva druga književna i umetnička dela.

Naravno da se govorna dela mogu pretvoriti u digitalnu formu, ali i tada autori zadržavaju sva prava koja im po zakonskim propisima pripadaju i samo oni mogu odbriti pretvaranje u digitalnu formu, distribuciju ili javno saopštavanje svog digitalnog govornog autorskog dela, osim u slučajevima kada je to drugačije regulisano za političke govore i govore održane u toku sudskih rasprava.

Preduslov orginalnosti predpostavlja se i kod govornih dela, tako da neki autori smatraju da predavanja koja se održavaju u nastavi, a zasnovana su na striktnom poštovanju određene literature ne predstavljaju izvorne intelektualne tvorevine i ne smatraju se autorskim delima.[95]

[95] Spasić Ž. Vidoje, *Autorska dela u digitalnom okruženju*, Pravni fakultet u Nišu, Niš, 2011, str. 71.

2.3.5. OSTALA AUTORSKA DELA U SAJBER PROSTORU

2.3.5.1. DELA LIKOVNE UMETNOSTI U SAJBER PROSTORU

Član 2. Bernske konvencije navodi dela iz oblasti crtanja, slikarstva, arhitekture, vajarstva, rezbarstva i litografije kao autorska umetnička dela koja su tim dokumentom zaštićena pod opštim režimom autorskih prava. Kada je reč o ovim delima u sajber prostoru, odnosno u digitalnoj formi, sasvim je izvesno da predmet autorskog prava mogu biti samo njihove reprodukcije, odnosno fotografije, a ne i sama dela. Otuda je od značaja i član 11bis. Bernske konvencije, koji autorima ostavlja isključivo pravo da daju saglasnost na, između ostalog, „radiodifuziju svojih dela ili njihovo saopštavanje javnosti bilo kojim sredstvom bežičnog prenosa znakova, zvukova ili slika“, odnosno „za saopštavanje javnosti putem zvučnika ili bilo kog drugog sličnog uređaja za prenos znakova, zvukova ili slika dela“... Iako zastarela i prevaziđena kada je reč o elektronskim komunikacijama i sajber prostoru, ova formulacija se može analogno upotrebiti i na savremene tehnologije „saopštavanja“. U članu 2, stav 2, tačka 6. Zakona o autorskim i srodnim pravima, dela likovne umetnosti su takođe izričito određena kao autorska dela.

Ono što je dakle specifično u smislu ove grupe autorskih dela jeste eventulani način njihovog izražavanja u elektronskom obliku – ono ne može biti takvo da se predstavlja kao original, jer ne poseduje trodimenzionalnost oblika niti mogućnost da se u bilo kojem trenutku zameni (slučajno ili namerno) za originalno delo. U ovim slučajevima postoji *samo jedan original koji ima umetničku vrednost*, a kopija ili prikaz (fotografija, 3D model) takvog dela biće upravo – samo kopija u elektronskoj, digitalnoj formi.[96] Manje ili više verne originalu, pa čak možda i identične, kopije ipak neće imati nikakvu posebnu umetničku vrednost. U tome je i razlika između npr. dela filmske, pozorišne i muzičke umetnosti u odnosu na ovu specifičnu kategoriju. Muzička numera se može sasvim verno preneti u elektronskom obliku i ne može biti reči o tome da li originalni snimak ima veću ili manju vrednost od elektronske kopije koja se protivpravno razmenjuje na internetu – original i kopija su u sadržinskom smislu identični. Kod dela likovne umetnosti to nije, niti može biti slučaj. Ipak, ono što je zajedničko ovim delima u sajber prostoru sa praktično svim ostalim autorskim delima, jeste mogućnost da se ona

[96] Videti: Bainbridge D., *op.cit*, str. 83; Vidoje Ž. Spasić, *op.cit*, str. 83.

protivpravno *prikažu* većem – praktično neograničenom – broju ljudi. Za mnoge će biti dovoljno da iz udobnosti svog doma pogledaju vernu reprodukciju neke slike u visokoj rezoluciji, nego da plate ulaznicu za galeriju koja to delo izlaže. U tom smislu, na ova dela se ne može primeniti odredba člana 37. Zakona o autorskim i srodnim pravima, prema kojoj je autor u prilici da zabrani izlaganje svog autorskog – umetničkog dela – osim ukoliko ga je otuđio, a pri otuđenju nije izričito insistirao na takvoj zabrani. Sa druge strane, u sajber prostoru, daleko veću relevantnost ima odredba člana 46. istog Zakona, koja onemogućava komercijalnu upotrebu umnoženih primeraka objavljenog dela – dakle, isključivo je dozvoljena lična (nikako javna!) i nekomercijalna upotreba. Otuda bi svako neautorizovano korišćenje umetničkog dela u sajber prostoru, koji je po po svojoj prirodi javan, predstavljalo kršenje autorskih prava za koje bi autor mogao da zahteva od prekršioca naknadu štete.

2.3.5.2. DELA ARHITEKTURE, PRIMENJENE UMETNOSTI, INDUSTRIJSKOG DIZAJNA U SAJBER PROSTORU

Dela arhitekture, primenjene umetnosti i industrijskog dizajne prema Bernskoj konvenciji takođe predstavljaju autorska dela. Članom 2. Bernske konvencije izričito se navode *dela iz oblasti arhitekture*, *dela primenjene umetnosti*, *planovi skice i plastična dela koja se odnose na arhitekturu*.

U Srbiji Zakon o autorskim i srodnim pravima, članom 2. je kao autorska dela izričito naveo u tačci 7. *dela arhitekture, primenjene umetnosti i industrijskog oblikovanja*, a u tačci 9. *planovi, skice, i makete*.

Član 51. našeg Zakona o autorskim i srodnim pravima predviđa da je dozvoljeno bez dozvole autora i bez plaćanja autorske naknade dvodimenzionalno umnožavanje, stavljanje u promet tako umnoženih primeraka, kao i *drugi oblici javnog saopštavanja dela koja se trajno nalaze izložena na ulicama, trgovima i drugim otvorenim javnim mestima*. Prema članu 57. istog Zakona, bez dozvole autora a uz obavezu plaćanja autorske naknade, dozvoljeno je trodimenzionalno umnožavanje dela koja su trajno izložena na ulicama, trgovima i drugim otvorenim javnim mestima, kao i stavljanje u promet tih primeraka, osim ako se primerak dela skulpture dobija otiskom iz originalnog kalupa iz kojeg je dobijen i primerak koji je trajno izložen na otvorenom javnom mestu ili iz kalupa koji je načinjen otiskivanjem sa primerka dela

skulpture; pravi nova građevina po uzoru na postojeću građevinu; proizvod oblikuje prema delu primenjene umetnosti.

Kada su u pitanju dela iz oblasti arhitekture podrazumeva se da se radi samo o orginalnim autorskim delima koja znači moraju imati orginalni dizajn i minimalni stepen kreativnosti. „Nije svako građevinsko delo autorsko delo. Naprotiv, samo mali broj objekata će se smatrati delom arhitekture i uživaće autorskopravnu zaštitu.“[97]

Iako neki autori smatraju da dela arhitekture ne mogu biti predmet interpretacije i ne mogu se pretvoriti u digitalnu formu koja bi imala upotrebnu vrednost, odnosno praktičnu primenu[98] to nije baš sasvim tačno jer je danas već moguće stvoriti trodimenzionalne modele objekata i omogućiti virtuelni obilazak tih objekata, ili čak boravak virtuelne ličnosti u tim objektima, a naravno planovi, skice i modeli arhitektonskih dela već se odvanodigitalizuju i često se koriste u sajber prostoru bez dozvola autora i na taj način se krše prava autora arhitekstonskih dela.

Dela primenjene umetnosti su umetnička dela (znači orginalna dela) koja *imaju primenu*, a mogu biti ručno proizvedena ili industrijski proizvedena. Praktična primena, predmeta za ličnu upotrebu, plakata, etiketa, ili drugih predmeta u stvari razlikuje ova umetnička dela od drugih vrsta umetničkih dela, a sa ostalim umetničkim delima ih spaja kreativnost i umetnička vrednost.

Dela primenjene umetnosti i industrijski crteži i modeli imaju svoje specifičnosti jer često nisu samo umetnička dela nego i industrijski proizvodi. Bernska konvencija u članu 2. tačka 7. ostavlja nacionalnim zakonodavtsvima da utvrde oblast primene zakona koja se odnosi na dela primenjene umetnosti i industrijske crteže i modele, kao i na uslove pod kojima će takva dela, crteži i modeli biti zaštićeni. Za dela koja su zaštićena isključivo kao crteži i modeli u zemlji porekla, može se u nekoj drugoj zemlji tražiti samo specijalna zaštita priznata u ovoj zemlji crtežima i modelima, međutim, ako takva specijalna zaštita nije priznata u ovoj zemlji, ova dela će biti zaštićena kao umetnička dela.

U pogledu sadržine prava autora u vezi sa delima primenjene umetnosti oni ne samo da imaju sva prava koja imaju i druga autorska dela već mogu imati i zaštitu na osnovu drugih propisa vezanih za industrijsku svojinu ili propisa vezanih za nelojalnu konkurenciju.

---

[97] Spasić Ž. Vidoje, *Autorska dela u digitalnom okruženju*, Pravni fakultet u Nišu, Niš, 2011, str. 83.
[98] *Ibidem*, str. 84.

Dela primenjene umetnosti baš zbog svoje prirode daleko su podložnija digitalnoj prirateriji od recimo dela arhitekture.

2.3.5.3. KARTOGRAFSKA DELA U SAJBER PROSTORU

Kartografska dela su definisana kao dvodimenzionalni prikazi površne zemlje ili njenog dela, nebeskih tela ili nebeskog svoda u umanjenoj meri, odnosno određenoj srazmeri.[99] Bernska konvencija navodi kartografska dela u ranije već više puta pomenutom članu 2, stav 1. kao jednu od oblika književnih i umetničkih dela, u daljem tekstu ovog dokumenta nema nijedne odredbe koja bi bliže odredila njihov pravni status. Zakon o autorskom i srodnim pravima, u članu 2, stav 2, tačka 8. takođe navodi geografske i topografske karte kao vrstu autorskog dela ali detaljnije o njima nema reči u tekstu. Obzirom na ovakve okolnosti, valjalo bi zaključiti da su ova autorska dela pod opštim režimom koji je ustanovljen pravnim sistemom, te da se na njih odnose sve one odredbe koje su najopštijeg karaktera i ustanovljene za sva autorska dela u celini.

Kada je reč o računarskim programima koji se pojavljuju u sajber okruženju u vezi sa kartografskim delima, daleko najveću pažnju do sada su izazvali Google programi: *Google Maps* i *Google Earth*. U pitanju su korisnički programi koji na jedan specifičan način približavaju geografske informacije pojedincima koji ih koriste.

Google Maps je naziv korisničkog programa koji služi predstavljanju kartografskih podataka, mapa praktično svih mesta na planeti. Ovaj program pre svega služi orijentaciji u urbanim delovima, prikazivanju puteva i objekata (kao i njihove udaljenosti, najkraćeg i/ili najbržeg puta, sredstava javnog prevoza, i sl.), objedinjujući na taj način praktično sve funkcije GPS sistema i mapa. Sam sistem je besplatan, ali trpi i određena ograničenja – mape koje se u programu prikazuju su stare od nekoliko meseci do nekoliko godina.[100] Ipak, ovaj popularni program je postao opšteprihvaćen pre svega zbog nekomercijalnog aspekta (korišćenje se ne naplaćuje), zbog mogućnosti da se kombinuju različita njegova svojstva (npr. moguće je pregledati teren u modu plana, ali i u modu geofizičke karte, korišćenjem satelitskih snimaka teritorije) kao i verzije koje je takođe besplatno moguće koristiti na mobilnim telefonima i tablet računarima. Kompanija *Google* je vlasnik autorskih prava na mapama koje se prikazuju, ili je

[99] *Ibidem*, str. 87.
[100] Prema podacima sa Wikipedie, satelitski snimci u programu su urađeni na samom začetku njegovog korišćenja i trenutno su stari preko pet godina. Internet adresa: http://en.wikipedia.org/wiki/Google_Maps, 01.06.2012.

zakupila njihovo korišćenje na određeni vremenski period od nosilaca autorskih prava[101]. Google Maps je besplatan za korisnike, ali komercijalna komponenta njegovog koriščenja se može uočiti u postojanju različitih internet oglasa, što je prepoznatljiv način funkcionisanja različitih proizvoda kompanije *Google*.

Ukoliko se analiziraju uslovi korišćenja programa, može se zaključiti da on potpada pod nekomercijalnu licencu, čije je korišćenje slobodno ali nije dozvoljeno za komercijalne svrhe, kao ni za dalju preradu i nadogradnju kako softvera tako i baze fotografija.[102] Uslovi korišćenja potpadaju pod jurisdikciju pravnog sistema SAD.

Kada je reč o korišćenju mapa u druge svrhe, *Google* je postavio dva osnovna ograničenja: nije moguće koristiti bilo koji konačni proizvod *Google Maps*-a (dakle, mapu ili njen deo, u bilo kojem obliku, rezoluciji i srazmeri) u komercijalne svrhe (kao što je dalja preprodaja, korišćenje u različitim publikacijama[103] ili drugim računarskim programima); drugo ograničenje se tiče nekomercijalne upotrebe – u tom slučaju je potrebno zadržati na samoj mapi pečat, logo, odnosno vodeni žig, koji će jasno označavati poreklo fotografije, tj. mape. Za pojedine namene *Google* ima drugačiju licencu, koja profesionalnim korisnicima može ponuditi integrisanje *Google Maps* programa u njihove (komercijalne) internet sajtove (*Google Maps API*).

Google Earth je program namenjen virtuelnom prikazu planete (globus) ali može imati iste, odnosno slične funkcije kao i *Google Maps* – dakle, prikazivati mape i satelitske snimke. U novije vreme, *Google* je proširio ovaj način posmatranja i na Mars, odnosno Mesec. Sve ono što je rečeno o funkcionalnosti (ali i zastarelosti snimaka) za *Google Maps*, može analogno važiti i za *Google Earth*.

Kada je reč o licenci, i ovde je situacija identična kao kod *Google Maps* programa. Komercijalna upotreba nije dozvoljena, a sam program je inače besplatan i može se nekomercijalno koristiti bez posebnih ograničenja. Za zahtevnije korisnike, u ponudi je

---

[101] Jedina država koja nije obuhvaćena ovih sistemom je Severna Koreja. Na njenom mestu, u programu stoji prazan prostor.

[102] Naravno, osim ovih ograničenja uslovi korišćenja sadrže i osvrt na bilo kakvu drugačiju nelegalnu upotrebu snimaka koje čine ovaj proizvod (npr. za ilegalno lociranje i praćenje ljudi, u svrhu ugrožavanja sigurnosti ili sa prevarnom namerom, i sl.).

[103] Osim ukoliko je reč o naučnoistraživačkom delu u kojem se proizvod koristi kao jedan od sporednih elemenata, pomoćno sredstvo vizuelizacije).

komercijalni program *Google Earth Pro*, koji nudi kvalitetnije prikaze i mape, a za koji naravno važe posebni uslovi korišćenja.

Verovatno najviše kontroverzi do sada izazvao je srodni program koji je moguće aktivirati uz *Google Maps* i *Google Earth* i koji se na njima zasniva, *Google Street View*. Ipak, ovaj program koji omogućava korisnicima da (besplatno) pregledaju ulice nekih od najvećih svetskih gradova zahvaljujući panoramskim snimcima koje je specijalno vozilo napravilo i koji su uklopljeni u celinu, nije se našao na meti vlasti različitih država ali i privatnih lica zbog kršenja autorskih prava, već zbog kršenja prava na privatnost ljudi koji su ne znajući za to, ili protiv svoje volje, usnimljeni prilikom stvaranja panoramskih snimaka i postali deo *Google Street View*-a.

2.3.5.4. FOTOGRAFIJE, PLANOVI, SKICE I MAKETE U SAJBER PROSTORU

Opšta pravila zaštite autorskog prava odnose se, na osnovu Bernske konvencije, prema članu 2. i na *dela iz oblasti fotografije s kojima su izjednačena dela izražena postupkom sličnim fotografiji*.

Naš Zakon autorskim i srodnim pravima takođe je članom 2. tačka 9. predvideo kao autorsko delo *planove, skice, makete i fotografije*.

Kada su u pitanju fotografije neophodno je napraviti razliku između *fotografija kao umetničkog dela* koju štiti Zakon o autorskim i srodnim pravima i *običnih fotografije* koje imaju zaštitu samo na osnovu opštih principa građanskog prava i propisa koji regulišu nelojalnu konkurenciju. Fotografija kao umetničko delo mora da poseduje izvestan stepen orginalnosti i kreativnosti koji je odvaja od obične fotografije, odnosno moraju da imaju određenu umetničku vrednost. Da bi postojao izvestan spepen orginalnosti i da bi se moglo tvrditi da je jedna fotografija umetničko delo neophodno je da je ona rezultat intelektualne, kreativne aktivnosti koja je toliko individualna da dve osobe, nezavisno jedna od druge, razumno je predpostaviti ne bi stvorile potpuno isti rezultat. Naravno da u praksi ipak nije uvek lako napraviti razliku između ove dve vrste fotografije.

Napredkom tehnologije omogućeno je jednostavne pretvaranje analogne fotografije u digitalnu fotografiju, skeniranjem ili fotografisanjem digitalnim fotoaparatom ili mobilnim telefonom, pa čak i njihova obradai izmena je vrlo jednostavna. Danas najveći broj fotografija

nastaje i ostaje samo u digitalnom obliku. Zbog ove specifičnosti fotografije su izuzetno podložne zloupotrebi u okviru sajber prostora.

Planovi, skice i makete mogu takođe biti autorska dela ukoliko zadovoljavaju potrebne kriterijume orginalnosti i kreativnosti. "To su autorske tvorevine iz različitih oblasti nauke ili umetnosti izražena u dvodimenzionalnom (planovi i skice) ili trodimenzionalnom obliku (plastična dela, makete i sl.)"[104].

Naravno da se i planovi, skice i makete mogu naći digitalizovani u sajber prostoru gde podležu istim oblicima zaštite kao i druga autorska dela.

2.3.5.5. DRAMSKA, KOREOGRAFSKA, PANTOMIMSKA DELA U SAJBER PROSTORU

Dramska, koreografska i pantomimska dela se zajednički nazivaju „pozorišnim delima“.[105] Njihova osnovna karakteristika jeste da su u pitanju dela namenjena scenskom izvođenju kod kojih se prepliće više elemenata izražavanja – muzika, pokret, tekst, igra. Vidoje Ž. Spasić, dosledno prateći domaću zakonsku odredbu, kao posebnu kategoriju ovih dela napominje i folklorna dela.[106]

Prema Bernskoj konvenciji, dramska, koreografska i pantomimska dela spadaju pod opštu definiciju pojma „književnih i umetnički dela“.[107] Autori dramskih, dramsko-muzičkih i muzičkih dela uživaju isključivo pravo da daju odobrenje za javno prikazivanje i izvođenje svojih dela, podrazumevajući javna prikazivanja i izvođenja svim sredstvima ili postupcima, kao i za javno prenošenje svim sredstvima prikazivanja i izvođenja svojih dela.[108] Ova odredba logično podrazumeva i prenošenje, odnosno reprodukcuju u celini ili delimično, izvođenja dramskih, koreografskih i pantomimskih dela u sajber prostoru. Takođe, prema članovima 12. i 14. Konvencije, autori uživaju isključivo pravo da daju odobrenje za adaptaciju, aranžmane i druge prerade svojih dela. To bi značilo da se ovakva dela, kao i ostali analizirani proizvodi

---

[104] Spasić Ž. Vidoje, *Autorska dela u digitalnom okruženju*, Pravni fakultet u Nišu, Niš, 2011, str. 87.
[105] Spasić Ž. Vidoje, *op.cit*, str. 71.
[106] *Ibidem*.
[107] Član 2, stav 1. Konvencije. Isto je i prema članu 2, stav 2, tačka 3. Zakona o autorskom i srodnim pravima Republike Srbije.
[108] Član 11. Konvencije.

intelektualnog i autorskog rada, ne mogu koristiti bez odobrenja autora niti u jednom obliku – za postavljanje, odnosno činjenje dostupnim u izvornom obliku – kao ni za dalju razradu, obradu ili bilo kakvu drugu preradu izvornog dela (i potonje postavljanje takvog dela u sajber prostor). Ni ova dela, kao ni druga koja su razmatrana u prethodnom tekstu, neće uživati zaštitu autorskog prava ukoliko su postala javno dobro (član 18. Konvencije).

Kada je reč o dramskim i dramsko-muzičkim delima, u pitanju su dela koja sadrže tekst i muziku, a koja su namenjena (ili prilagođena) scenskom izvođenju. Kada je u pitanju oblast autorskog prava, trebalo bi napomenuti da se svaka muzička numera, nezavisno od teksta koji se eventualno izgovara u delu, smatra posebnim autorskim delom, ali da su oni zajednički obuhvaćeni pravom na emitovanje, odnosno prikazivanje dela, koje pripada autoru dela u celini. U sajber prostoru, može se govoriti o nekoliko apekata autorskih prava u vezi sa ovim delima: prenošenje ili reprodukcija dela, objavljivanje teksta ili muzike, delimično ili u celini, odnosno pojedinih muzičkih numera, bilo kakvih audio ili video zapisa ovih dela bez obzira na način i modalitet njihovog izvođenja.[109] Sva ova prava pripadaju nosiocu autorskog prava na delo u celini, i mogu se realizovati isključivo uz njegovo odobrenje. Isto se odnosi i na umnožavanje i distribuciju dela u celini, ili njegovih pomenutih segmenata.

Koreografska i pantomimska dela su specifična u grupi tzv. „pozorišnih dela“ pre svega zato što se ne moraju nužno scenski izvoditi, pa su samim tim najčešće izdvojena u uporednim propisima kao posebna vrsta autorskih dela.[110] Dok se pantomimska dela izvode pokretom uz eventualnu muzičku podlogu, koreografska dela su raznovrsnija i njima se, osim baleta koji je najčešći oblik ovih dela, smatrati i narodni, folklorni plesovi i igre. Kod baleta postoji sinteza teksta, pokreta i muzike u jednom autorskom delu, dok se kod ostalih uglavnom kombinuju muzika i pokreti.[111] Kao i u prethodnim slučajevima, ova dela su zaštićena od bilo koje vrste reprodukcije i/ili adaptacije bez odobrenja autora, u sajber prostoru pomoću audio-video snimaka, isto kao i kao i ostala pozorišna dela.

---

[109] Npr. podjednako će se smatrati kršenjem autorskog prava stavljanje snimka na internet zvaničnog izvođenja dela za koje je autor dao odobrenje (ali ne postoji odobrenje za njegovo dalje prenošenje i distribuciju) ili stavljanje snimka na internet tog dela u nečijem privatnom – neautorizovanom – izvođenju.

[110] Spasić Ž Vidoje, *op.cit*, str. 74.

[111] *Ibidem*.

2.3.6. ZBIRKE AUTORSKIH DELA I PODATAKA U SAJBER PROSTORU

Bernska konvencija za zaštitu književnih i umetničkih dela u članu 2. tačka 5. predviđa poseban oblik zaštite za *zbirke književnih ili umetničkih dela kao što su enciklopedije i antologije koje prema izboru i rasporedu sadržine predstavljaju intelektualne tvorevine*, naravno ova zaštita ne sme da proizvede bilo kakvu štetu za prava autora na svako od tih dela koja čine sastavni deo ovih zbirki.

Naš Zakon o autorskim i srodnim pravima u članu 5. nešto detaljnije određuje kada se *zbirka* ima smatrati autorskim delom. To su slučajevi kada se radi o *enciklopedijama, zbornicima, antologijama, izabranim delima, muzičkim zbirkama, zbirkama fotografija, grafičkim mapama, izložbama i sl.* pod uslovom da se radi o originalnoj duhovnoj tvorevini autora. Autorskim delom se smatra i *zbirka narodnih književnih i umetničkih tvorevina, kao i zbirka dokumenata, sudskih odluka i slične građe, baza podataka, bez obzira da li je u mašinski čitljivoj ili drugoj formi*koja s obzirom na izbor i raspored sastavnih delova ispunjava uslov da je orginalna duhovna tvorevina autora. U našem Zakonu o autorskim i srodnim pravima, a u skladu sa Bernskom konvencijom za zaštitu književnih i umetničkih dela, predviđeno je da zaštita zbirke ni na koji način ne ograničava prava autora dela koja su sastavni deo zbirke.

Obično se autorom zbirke smatra urednik, pa njemu pripadaju imaovinska i moralna prava koja proističu iz autorskog prava. "Međutim ukoliko je zbirka sastavljena od autorskih dela koja su u roku trajanja pravne zaštite, a autor zbirke nije autor i pojedinih dela, onda nastaje autorskopravni odnos analogan odnosu između izvornog i izvedenog dela, sa svim pravnim posledicama koje iz toga proističu. Dakle autori dela (sastavnih elemenata zbirke) imaju svoja zasebna ovlašćenja, nezavisno od prava autora zbirke. U tom smislu, autor zbirke mora, pre svega, da zatraži saglasnost autora sastavnih delova. Takođe, autori sastavnih delova imaju pravo da zahtevaju da njihova imena budu naznačena prilikom korišćenja zbirke. Osim toga, autor dela koje je sastavni deo zbirke, može vršiti svoja ovlašćenja na zaštiti integriteta dela, suprotstavljanje nedostojnom iskorišćenju dela, kao i pravo pokajanja."[112]

[112] Spasić Ž Vidoje, *Autorska dela u digitalnom okruženju*, Pravni fakultet u Nišu, Niš, 2011, str. 63.

Sve vrste zbirki autorskih dela mogu biti digitalizovane i na njih se po pitanju ostvarivanja prava odnosi sve ono već rečeno za zaštitu svih ostalih autorskih dela u sajber prostoru.

Najednostavnija definicija baza podataka je da su to organizovani skupovi (zbirke) podataka. Stvaranje baza podataka ima za svoj cilj da omogući lako korišćenje, pregledanje, pretraživanje, prenošenje, upoređivanje, sortiranje, i menjanje podataka. Danas je najveći broj baza podataka u potpunosti digitalizovan i dostupan u sajber prostoru. Digitalizovane baze podataka su sastavljene od određenog broja zapisa, a svaki zapis sastavljen je od određenog skupa elemenata (podataka). Jedna od bitnih karakteristika baza podataka je da one obuhvataju podatke, materijale i/ili dela koja čine zbirku, a tako su odabrani, povezani i uređeni da čine intelektualnu tvorevinu i novo autorsko delo.[113]

Pravna zaštita baza podataka moguća je u okviru pravnih propisa *sui generis*, i u okviru propisa kojima se štite autorska i srodna prava i u okviru propisa kojima se regulišu pitanja nelojalne konkurencije.

Sui generis propisi su propisi koji se donose kada postoji posebna situacija koja se ne može podvesti pod već postojeće propise. Baze podataka obiluju specifičnostima i stoga mnogi smatraju da se one ne mogu kvalitetno zaštiti korištenjem postojećih pravnih instituta pa je potrebno doneti posebne propise – sui generis propise radi zaštite autora baza podataka. Jedan takav pripis donet od strane Evropske unije je Direktiva Evropske unije 96/9/EC o pravnoj zaštiti baza podataka. Ona definiše u članu 1. bazu podataka kao "zbirku nezavisnih dela, podataka ili drugih materijala uređenih na sistematičan ili metodičan način, koja je pojedinačno dostupna elektronskim ili drugim putem."[114] Isključiva prava autora prema Direktivi 96/9/EC su 1. privremeno ili stalno umnožavanje na bilo koji način ili u bilo kom obliku, u celini ili delimično; 2. prevođenja, prilagođavanja, priređivanja ili svakog drugog menjanja; 3. bilo koji oblik distribucije javnosti baze podataka ili njene kopije; 4. bilo koje vrste komunikacije, javnog prikazivanja ili javnog izvođenja; i 4. umnožavanja, distribucije, ili bilo koja vrsta komunikacije, javnog prikazivanja ili javnog izvođenja prevedene, prilagođene, priređene ili na bilo koji način menjane baze podataka. Članom 7 Direktive 96/9/EC predviđeno je *sui generis* pravo autora baza

[113] Drakulić Mirjana, *Osnovi kompjuterskog prava*, DOPIS, Beograd, 1996, str. 343.
[114] *Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases*, Official Journal L 077 , 27/03/1996, pp. 24

podataka u smislu sprečavanja ekstrakcije i/ili ponovnog iskorištavanja celine ili značajnog dela baze podataka u kvalitativnom i/ili kvantitativnom smislu. Pod "ekstrakcijom" se ima smatrati stalni ili privremeni prenos cele baze podataka ili značajnog dela baze podataka u drugi medij na bilo koji način u bilo kom obliku. Pod "ponovnim iskorištavanjem" će se smatrati svaki oblik činjena dostupnim javnosti cele baze ili bitnog njenog dela distribucijom, iznajmljivanjem on-line ili drugim oblikom prenosa. Ovaj član Direktive 96/9/EC stavom 4. predviđa da se ovaj vid zaštita primenjuje nezavisno od podobnosti sadržaja baze podataka da bude zaštićena kao autorsko delo. Članom 9. predviđena je mogućnost da nacionalna zakonodavstva utvrde zuzetke od primene sui generis pravila u slučajevima: 1. ekstrakcije za privatne svrhe sadržaja ne elektronske baze podataka; 2. u slučaju ekstrakcije u svrhu ilistracije nastave ili naučnog istraživanja, uz naznaku izvora i u meri koja je neophodna za ne komercijalnu svrhu upotrebe; i 3. u slučaju ekstrakcije ili ponovnog korišćenja za potrebe javne bezbednosti, upravnog ili sudskog postupka.

Pored zaštite putem propisa koji štite autorska i srodna prava i putem propisa sui generis autori baze podataka se mogu štititi i nacionalnim propisima vezanim za nelojalnu konkurenciju. Ovi propisi ne zamenjuju pomenute dve vrste propisa već nadopunjuju te propise i omogućavaju autorima baza podataka specifični vid zaštite u slučajevima neovlašćenog ekstrahovanja većeg ili manjeg dela sadržaja iz baza podataka sa ciljem postizanja komparativne prednosti na tržištu.

2.4. AUTORSKA PRAVA I INTERNET DOMENI

Da bi računar pristupio internetu potrebno je da se „registruje“ – dobije svoju jedinstveno IP adresu, lokaciju na internetu. IP (eng. *Internet Protocol*) adrese su zapravo sačinjene od niza cifara koje su podeljene u grupe, prema unapred utvrđenim pravilima (npr. 192.168.0.0). Ukucavanjem IP adrese dolazi se do sadržaja internet prezentacije koja se nalazi na tom računaru. Broj kombinacija cifara je praktično neograničen. Međutim, budući da je ovaj način pristupanja internet sajtovima jako komplikovan korisnicima, koji bi morali da pamte nizove za svaki pojedinačni sajt koji žele da otvore, postoji DNS sistem (eng. *Domain Name System*) koij prevodi znake domena (imena internet sajtova) u numeričke oblike. To praktično znači da se adresa koju korisnik ukucava kao alfanumeričku – npr. www.comparativelaw.info – izražava u odnosu na traženi računar u numeričkom smislu, kao njegova IP adresa, pa računar „reaguje“ i prenosi korisniku sadržaj koji se nalazi na traženoj adresi.

IP adrese su jedinstvene – ne mogu postojati dve iste u istom trenutku. Ne mogu postojati ni dva ista internet domena - u protivnom, postojala bi zabuna kako kod korisnika koji ne bi znao koji od sajtova sa istim imenom zapravo želi, tako i kod DNS-a koji ne bi mogao da prevede naziv u određenu numeričku adresu, jer bi imao nekoliko mogućih opcija na raspolaganju. Ovako grubo objašnjen, sistem dodeljivanja naziva internet domena u praksi je izazvao mnoge probleme i otvorio pitanja odnosa autorskih prava i prava na internet domen. Ovo pitanje je naročito aktuelizovano početkom XXI veka, kada je internet naglo ušao u opštu upotrebu i dobio globalne razmere. U osnovi problema jeste dilema da li vlada potpuna sloboda izdavanja Internet domena, ili moraju postojati neka ograničenja koja bi išla u prilog određenim kompanijama i institucijama[115], koja bi imale „pravo prethodnog izbora“? Šta bi se desilo kada bi neko lice registrovalo (zakupilo) internet domen www.samsung.com? Svaki korisnik koji želi da pogleda najnovije proizvode će, direktno ili preko pretraživača, naići među prvima na ovu adresu. Ukoliko međutim ona ne pripada kompaniji Samsung, može se desiti da se kod korisnika stvori zabuna da su na internet sajtu koji su tražili, ili mogu odustati od daljeg traganja, i otići na

[115] Ovo se naročito odnosi i na najvažnije državne institucije. Npr, u Srbiji je sve do promene .yu domena u .rs domen, postojao domen www.vlada.yu. Uprkos činjenici da bi to bio jedan od prvih izbora pretraživača kada bi korisnik ukucao samo reč „vlada“ (misleći na Vladu Republike Srbije), u pitanju nije bila prezentacija Vlade RS, već privatna prezentacija fizičkog lica. Citirano prema: Prlja Dragan, Reljanović Mario, *Pravna informatika*, Beograd, 2010, str. 140.

internet prezentaciju neke druge firme koja ima slične proizvode. Pitanje posedovanja odgovarajućeg internet domena postalo je pitanje prestiža, praktične potrebe i imidža svake kompanije. Toga su postali svesni i u zemlji u kojoj se internet razvio, SAD, pa su domeni u početku davani u zakup bez ikakvih ograničenja. Kada se pitanje slobode zakupa konačno postavilo, različite verzije domena koje su kompanije mogle upotrebljavati u budućnosti su već bile zauzete i bile su prodavane tim kompanijama, ponekad i za neverovatne iznose[116]. Ovo je bilo moguće činiti pre svega zbog toga što u najranijoj fazi razvoja Interneta nije postojalo nikakvo ograničenje prilikom registrovanja domena – niko nije mogao predvideti njihovu komercijalnu vrednost u bliskoj budućnosti.[117]

Poseban problem postoji kada nije u pitanju „investiranje" u neki brend i zakupljivanje domena sa ciljem preprodaje, već kada firma ili pojedinac zakupe internet domen sa ciljem da zaista promoviše sebe ili svoju delatnost, profitnu ili neprofitnu. Oni zakupljuju domen koji može ličiti na neki koji bi koristila velika kompanija, daleko poznatija od one koja domen drži u svom posedu ili zakupu. Prvi takav primer karakterističan je po tome što se novinar koji je zakupio domen nije vodio lukrativnim ciljevima već je želeo da skrene pažnju na ovaj zanimljivi tehničko-pravni problem. Novinar američkog lista *Wired* je zakupio domen www.mcdonalds.com i napisao članak o tome još 1994. godine. Mc Donald's je tužio novinara, ali je izgubio spor.[118] Tako je šira javnost saznala za mogućnost da je (u to vreme bilo) sasvim legalno da se na internetu zauzmu domeni velikih svetskih kompanija.

Jedan od do sada najpoznatijih primera ove vrste jeste američki slučaj *Nissan protiv Nissana*.[119] Ukratko, gospodin Nissan – koji je rođen sa tim prezimenom – registrovao je domene www.nissan.com i www.nissan.net radi prezentacije svoje firme koja se bavi prodajom računara, Nissan Computers. Nakon što nije želeo da ustupi ili proda svoje domene velikoj kompaniji sa istim nazivom koja se bavi proizvodnjom automobila, Nissan automobili su pred američkim sudom tužili Nissan Computers, tražeći da im se dodele pomenuti domeni. Sud je to, u više navrata i na više instanci, odbio.

---

[116] Ovaj fenomen je u Velikoj Britaniji, krajnje maštovito, nazvan *cybersquatting*. Graham J.H. Smith, *Internet Law and Regulation*, London, 2002, str. 78.

[117] Trebalo bi skrenuti pažnju da se ovde ne misli na domene koji samo na prvi pogled podsećaju na imena velikih kompanija, kao što je npr. slučaj sa www.mircosoft.com domenom. Oni po pravilu služe za vršenje internet prevara, i o njima će više biti reči u delu o visokotehnološkom kriminalu.

[118] *Ibidem*, str. 91-92.

[119] Hronološka verzija događaja u ovom slučaju, ispričana iz ugla tuženog, zajedno sa svim relevantnim sudskim odlukama, može se naći na Internet adresi: http://www.digest.com/Big_Story.php, 01.08.2010.

Dakle, postoje različite situacije u kojima se postavlja pitanje postoji li pravo na određeni internet domen, koje bi proisteklo iz registrovane firme, odnosno žiga? Uporedna rešenja su različita, ali ono što je sasvim jasno jeste da internet domeni *ne spadaju u domen autorskih prava niti prava intelektualne svojine*. Internet domeni imaju dodirnih tačaka sa ovom problematikom samo kada se njihovom upotrebom može uticati na kršenje autorskih prava i prava intelektualne svojine, ali ona sama ne mogu biti subjekat takvih prava.[120]

U američkom pravu je nastalo specifično rešenje problema ove vrste, koje su kasnije preuzele i neke druge države, npr. Hrvatska i Srbija: postoji period koji se naziva *trade mark landrush*, kada centralno telo za dodeljivanje nacionalnih domena ne izdaje domene sa imenima onih preduzeća koja imaju *registrovanu firmu, odnosno žig (trade mark)* u toj državi. Drugim rečima, preneto na primer .rs domena, to bi značilo da Samsung, budući da ima registrovano preduzeće u Srbiji, ima „pravo prečeg zakupa" domena www.samsung.rs. Period u kojem vlasnik firme, odnosno žiga, može da iskoristi ovo pravo se razlikuje u različitim državama. U Srbiji je ono trajno, dok god traje registracija žiga, pa se takvi domeni ponekad nazivaju „zaštićenim domenima" – ovaj naziv ne bi trebalo shvatatti bukvalno, jer je on proistekao iz naziva „zaštićeni žig". Žig je, kao osnova vizuelnog prepoznavanja neke kompanije, zaštićen autorskim pravom – niko se ne sme služiti nekim žigom bez odobrenja njegovog vlasnika. Otuda, prema srpskom rešenju, svako ko ima zaštićeni žig ima i pravo na domen koji će sadržati ime registrovane firme. Ovo važi i za pojedince, tj. fizička lica – dakle, nije potrebno imati firmu da bi se neki žig registrovao i samim tim steklo pravo na upotrebu istog internet domena.[121] Osim ove situacije, za registrovanje domena važi pravo prvenstva u vremenu – ko prvi podnese zahtev za registraciju određenog domena, moći će da ga zakupi.[122]

Prema članu 16. *Pravilnika o arbitražnom postupku za rešavanje sporova povodom registracije .rs domena*[123], arbitražno veće može doneti odluku o prestanku ili prenosu spornog Internet domena sa registranta (lica koje je zakupilo domen) na tužioca, ukoliko se dokaže sledeće:

---

[120]Graham J.H. Smith, *op.cit*, str. 89-90.

[121] U Srbiji o ovim pitanjima brine Registar nacionalnog Internet domena Srbije – RNIDS. Internet adresa: http://www.nic.rs, 01.08.2010.

[122] U Srbiji se domeni zakupljuju na period jedne do deset godina, s tim što se po isteku tog perioda domen može ponovo registrovati – naravno, prednost uvek ima prethodni registrant. Citirano prema: Prlja Dragan, Reljanović Mario, *op.cit*, str. 142.

[123] Tekst Pravilnika može se naći na Internet adresi: http://www.nic.rs/files/list0031.pdf, 01.06. 2012.

- da je sporni domen identičan ili bitno sličan zakonom zaštićenom znaku, poslovnom ili trgovačkom imenu tužioca za istu ili sličnu vrstu robe ili usluga, ili ako ta sličnost može da stvori zabunu i dovede u zabludu učesnike u prometu;
- da registrant nema pravo i legitiman interes da koristi sporni domen – ovo je situacija kada registrant nije zakupio domen sa namerom da ga koristi u poslovne svrhe, već iz nekog drugog razloga, a naročito iz razloga kasnije preprodaje, ili samo da bi sprečio drugo lice da ga koristi;
- da je registrant domen registrovao i koristio protivno načelu savesnosti, poštenja i dobrih poslovnih običaja – ovo će se desiti ako neko zakupi domen koji podseća na naziv konkurentske firme i na njemu objavljuje netačne podatke o njenom poslovanju, ponudi, i sl; ovakva situacija će postojati naročito i kada se domen zakupi da bi se koristili firma, odnosno žig koji su slični nekom zaštićenom znaku, kako bi se privukli korisnici i stvorila zabuna o poreklu robe u pitanju[124].

Problemi se nastavljaju ako je reč o globalnim internet domenima. Žig i firma su po pravilu registrovani na nacionalnom nivou; internet sa druge strane ne poznaje nacionalna ograničenja. Ovde se priča širi sa naziva internet domena i ulazi u polje reklamiranja – različite kompanije mogu imati iste ili slične žigove registrovane u različitim državama, a reklamirati svoje proizvode u celom svetu putem novina, satelitske televizije, i sl. Tada se sasvim opravdano može očekivati da potencijalni potrošači neće razumeti da se radi o različitim kompanijama, koje osim zajedničkog imena, firme i/ili žiga – dakle, vizuelnog utiska koji stvaraju kod klijenata ili potrošača, nemaju zapravo ništa zajedničko. Kako G.J.H. Smith pravilno primećuje, ovaj problem nije nov ali se sada postavlja u novom, daleko komplikovanijem kontekstu, obzirom da se sa pojavom interneta neka reklama može učiniti trenutno dostupnom i svim državama sveta, 24 časa dnevno, potencijalno neograničenom broju korisnika, a da pri tome nema fizičke manifestacije, odnosno fizičkog oblika te reklame čiji bi se promet mogao zabraniti, ili bar ograničiti, u zemljama u kojima ona krši pravo na korišćenje registrovanog žiga.[125] Jedno od rešenja koje je sasvim logično, jeste šire registrovanje firme i žiga, koje bi obuhvatilo više zemalja istovremeno.

[124] Videti i član 17. istog Pravilnika.
[125] Graham J.H. Smith, *op.cit*, London, 2002, str. 74.

Drugo, koje mogu u praksi da primenjuju samo velike i bogate kompanije, jeste da se žigovi i/ili firme registruju u svakoj državi sveta pojedinačno.[126]

[126] *Ibidem*. Interesantno je da ni ovaj autor nema definitivan odgovor na pitanje kako bi se najefikasnije mogla obezbediti potpuna zaštita firme ili žiga, i predlaže fokusiranje manjih kompanija na najvažnija tržišta za njihovo poslovanje, na kojima bi ih štitili. Ovo bi ipak u praksi dovelo do toga da se kompanija koja se razvija i osvaja nova tržišta, potencijalno morala u budućnosti na svakome od njih pojavljivati sa novim imenom i vizuelnim identitetom zato što svoji originalni nije zaštitila na vreme, što je dosta nepraktično i ne pogoduje firmama koje pretenduju da stvore svetski poznate brendove.

3. ZAŠTITA ELEKTRONSKIH PODATAKA I PRAVO PRIVATNOSTI U SAJBER PROSTORU

3.1. ZAŠTITA ELEKTRONSKIH PODATAKA

3.1.1. ZAŠTITA PODATAKA U RAČUNARSKIM SISTEMIMA I MREŽAMA

Internet funkcioniše, uprošćeno gledano, kao velika (svetska) računarska mreža. Otuda se na pravila ponašanja na internetu mogu primeniti opšta pravila o zaštiti podataka koja važe i u svakoj drugoj računarskoj mreži, ali uvek imajući u vidu specifičnosti koje delovanje na internetu ima.

Zaštita podataka može biti okrenuta pitanjima funkcionalnog karaktera, kao što su: a) ograničavanje raspolaganja određenim vrstama podataka, b) obaveza davanja informacija nedržavnih subjekata državnim organima i organizacijama i v) obaveštavanje građana o podacima koji se o njemu prikupljaju i u koju svrhu.[127] Zaštita podataka dakle obuhavta situacije u kojima se informacije koje pripadaju građanima i/ili državnim i nedržavnim ustanovama, službama i organima, razmenjuju na određeni način, ili se jednostavno čine dostupnim određenim ili svim korisnicima interneta. U širem smislu, izučavanje zaštite podataka na internetu može obuhvatiti i zakonska rešenja koja se tiču postojanja određenih organa koja se staraju o primeni propisa o zaštiti podataka. Podaci o kojima je ovde reč mogu biti kako podaci o ličnosti, tako i podaci koji se odnose na funkcionisanje pravnih lica ili državnih organa i institucija, a zaštita podrazumeva dvostruku aktivnost: sa jedne strane, ne smeju se učiniti javnim podaci koji nisu kao takvi određeni propisima; sa druge strane, to je problem obezbeđivanja integriteta računara i računarskih sistema u kojima se nalaze podaci koji su postavljeni na internet u nekom restriktivnom obliku (za strogo određeni broj korisnika koji imaju interes da u njih imaju uvid i sa njima dalje raspolažu). Karakteristično je, a i razumljivo da se pravna doktrina prevashodno bavi

[127] Prlja Dragan, Reljanović Mario, *Pravna informatika, op.cit*, str. 87.

pravnim regulisanjem zaštite privatnosti i podataka, dok se područje bezbednosti sistema manje razmatra. Međutim, ostvarivanje bezbednosti sistema podrazumeva između ostalog i regulisanje i propisivanje obaveznih standarda i normativa koje bi primenjivali tehnički izvršioci (npr. zavodi za informatiku i kompjuterski centri), nezavisno od proizvođača računarskih sistema i programske opreme. Mere koje imaju za cilj obezbeđenje sistema primenjuju se radi ostvarivanja različitih ciljeva bezbednosti i sigurnosti kompjuterizovanih informacionih sistema, i same po sebi mogu biti raznovrsne, između ostalog: a) mere radi obezbeđenja bezbednosti iintegriteta tehničkih komponenata kompjuterskog sistema (tj. hardvera), tj. postrojenja, opreme, terminala, konzola i slično, b) mere radi obezbeđenja bezbednosti i integriteta programskih komponenti sistema (tj. softvera), tj. programa, datoteka, banaka podataka itd., v) mere fizičkog obezbeđenja prostorija, zgrada, vozila i slično, od slučajnog ili namernog oštećenja, g) mere koje doprinose održavanju i povećanju standarda u profesionalnoj obučenosti osoblja, d) mera održavanja i unapređenja standarda „redovne operativne procedure" itd.

„Bezbednost kompjuterskog sistema predstavlja *kišobran* koji štiti hardverske i softverske elemente organizacije, kao i podatke i informacije koje se kompjuterom obrađuju od zloupotrebe, prevare, pronevere, sabotaže, namernog ili slučajnog oštećenja, kao i od prirodnih nepogoda.“[128]

3.1.2. PRAVNI OKVIRI ZAŠTITE

Posebna regulativa koja se bavi problemom zaštite podataka na internetu i u elektronskim komunikacijama uopšte, javila se kao odgovor na neadekvatnost postojeće pravne zaštite u državama. Izuzetni razvoj računara i široka upotreba računarskih sistema doveli su do digitalizacije podataka u gotovo svim sferama koje kontroliše država – u mnogim zemljama danas je moguće i potpuno uobičajeno da se najrazličitije potvrde, uverenja i druga dokumenta, pa čak i neke vrste isprava poput saobraćajnih i vozačkih dozvola, zatraže putem interneta korišćenjem postojećih baza podataka o građanima. „Prvi konkretni oblici zakonodavne regulative zaštite podataka u kompjuterizovanim informacionim sistemima javljaju se pre tridesetak godina - prvi posebni zakon koji neposredno reguliše pitanje zaštite podataka donela je 1970. godine u Nemačkoj savezna država Hese. U svetu je danas na snazi veći broj raznih zakona koji regulišu materiju zaštite podataka, odnosno prava privatnosti. Po pravilu, ova oblast se

[128]Van Duyn J. A., *The Human Factor in Computer Crime*, Los Angeles, 1985, str. 4. Preuzeto iz: Prlja Dragan, Reljanović Mario, *Pravna informatika, op.cit*, str.88.

reguliše posebnim zakonima, odnosno, ukoliko je država federalnog tipa, i posebnim zakonima federalnih jedinica (npr. u Nemačkoj, SAD, Kanadi, itd.).Međutim, interesantno je istaći da je pitanje zaštite podataka u nekim zemljama regulisano neposredno i ustavima tih zemalja.“[129]

Ako se posmatraju strana zakonodavstva, mogu se jasno izdvojiti dva sistema zakonskog regulisanja ovog pitanja. U tom smislu, može se uslovno razlikovati zakonodavna regulativa prava privatnosti karakteristična za anglosaksonske pravne sisteme, od zakonodavne regulative o zaštiti podataka evrokontinentalnih pravnih sistema. U širem smislu posmatrano, naravno, može se reći da je reč o dve strane jedne iste medalje.[130]

„Ukoliko se pri određivanju osnovnih institucija zakonodavne regulative i mehanizama pravne zaštite polazi sa stanovišta „privatnopravne“ zaštite (ličnih prava i sloboda pojedinca), rezultat će, po pravilu, biti pravna zaštita prava na privatnost, odnosno donošenje „zakona o privatnosti“, kao što je slučaj s većinom zemalja anglosaksonske pravne tradicije (npr. SAD, većina kanadskih provincija itd.), gde je ova oblast regulisana zakonom čije se sprovođenje, u suštini, ostvaruje preko sudova po osnovu „lične inicijative“. Interesantno je, međutim, napomenuti da Velika Britanija, kao zemlja s najjačom anglosaksonskom tradicijom, nije pitanju zaštite podataka pristupila sa stanovišta tradicije svog pravnog sistema. Tako, Zakon o zaštiti podataka Velike Britanije (*Data Protection Act*, 1984), između ostalog, predviđa obrazovanje „registrara za zaštitu podataka“, tj. posebnog „matičara za vođenje evidencije o zaštiti podataka“, koga imenuje Kruna i koji je praktično nezavisan od vlade. Registrar je organ za zaštitu podataka s ovlašćenjima sličnim ovlašćenjima „poverenika parlamenta“, odnosno ombudsmana. Registrar vrši registraciju svih korisnika kompjuterizovanih informacionih sistema za obradu ličnih podataka, kako u javnom, tako i u privatnom sektoru. Uslovi u vezi s pristupanjem *Evropskoj konvenciji za zaštitu pojedinaca u odnosu na automatsku obradu ličnih podataka* (1981) bili su razlog što je Velika Britanija donela ovaj Zakon. Po svojoj strukturi, a posebno po svojoj sadržini, britanski Zakon o zaštiti podataka sledi evrokontinentalne, a ne anglosaksonske modele.

S druge strane, ukoliko se pri određivanju osnovnih institucija zakonodavne regulative i mehanizama pravne zaštite polazi sa stanovišta imperativnog ostvarivanja načela zakonitosti i pružanja „javnopravne“ zaštite pojedincu i građanima u odnosu na podatke o njima u

---

[129] *Ibidem*.

[130] Čok Vida, Lilić Stevan, VranjanacDušan, *Zaštitaličnihpodatakaukompjuterizovaniminformacionimsistemima - Komparativno-pravnaanaliza,* naučno-istraživačkiprojekt, Institutzauporedniopravo, Beograd, 1987.

kompjuterizovanim informacionim sistemima – rezultat će, po pravilu, biti donošenje zakona o „zaštiti podataka“. Takav je slučaj s većinom zemalja evrokontinentalnog pravnog sistema – Francuskom, Nemačkom, Švedskom itd. i, kao što je istaknuto, Velikom Britanijom. Francuski zakon kojim je regulisana oblast zaštite podataka donet je 1978. godine i nosi naziv Zakon o informatici, evidencijama i slobodama. U oblasti zaštite podataka, može se reći da je francuski zakon, pre svega, iz razloga osnivanja posebnog organa za zaštitu podataka, prototip zakonodavnog akta „javno-pravnog“ karaktera. Zakonom je, između ostalog, formirano i posebno telo s regulativnim, kontrolnim i nekim drugim ovlašćenjima - Nacionalna komisija za informatiku i slobode, tzv. CNIL. „Ovim Zakonom obrazuje se i CNIL s obeležjima jednog novog nezavisnog administrativnog tela, koje se, sa svojstvom pravnog lica, nalazi u sastavu države - iako nema ni hijerarhijskih, ni starateljskih ovlašćenja i podleže samo sudskoj kontroli.“[131]

Svakako, ne mogu se isključiti ni neke specifične situacije, kao što je, recimo, slučaj sa Japanom. Polazeći od posebnih okolnosti pod kojima je ova zemlja, takoreći iz feudalnog sistema postala supersila postindustrijskog društva, i pitanja zakonodavne regulative ipravnih mehanizama zaštite podataka imajusvoje osobenosti. U tom smislu, karakteristično je da Japan nije doneo poseban zakon o zaštiti podataka (niti o zaštiti prava na privatnost), već je ustanovljen jedan poseban sistem „decentralizovane kontrole“ u vezi sa zaštitom podataka koju svako ministarstvo posebno sprovodi u svom resoru.“[132]

Kako se razlikuju zakonodavni principi prema kojima se štite podaci nu sajber prostoru, tako postoji i razlika kada je reč o organima i institucijama koje su zakonom određene da se staraju o primeni navedenog zakonodavstva. Iako se uglavnom posebnim zakonima uvode i specifični organi koji bi imali ovu nadležnost, u uporednom zakonodavstvu vlada izražena raznolikost njihovog ustrojstva, ovlašćenja, sastava.

„U pojedinim zemljama, organ za zaštitu podataka obrazovan je kao inokosni (individualni) organ i različito je nazvan. Tako, na primer, individualni organ za zaštitu podataka određen je kao „komesar za zaštitu privatnosti“ (Kanada), odnosno „poverenik za zaštitu ličnih podataka“ (Nemačka), „registrar za zaštitu podataka" (Velika Britanija) itd. U saveznim

[131] MaislHerbert, *Etat de la Legislation Française et Tendences de la Jurisprudence Relatives à la Protection des donnees Personnalles*, Revue Internationale de Droit Comparé, No. 3, 1987, str. 581.
[132]Prlja Dragan, Reljanović Mario, *Pravna informatika, op.cit*, str. 90-91.

(federalnim) državama, recimo u Nemačkoj, pored „saveznog poverenika za zaštitu podataka“, postoje još i odgovarajući „zemaljski poverenici za zaštitu podataka“ u pojedinim saveznim zemljama.

Nasuprot ovom rešenju, druge zemlje koje su obrazovale poseban organ za zaštitu ličnih podataka ustanovile su ga u kolegijalnom obliku. I ovi kolegijalni organi kojima je poverena zaštita ličnih podataka razlikuju se kako po nazivima i strukturi, tako i po nadležnostima i ovlašćenjima. Tako, na primer, ovaj kolegijalan organ obrazovan je kao Komisija za zaštitu ličnih podataka (Austrija), Ured za zaštitu privatnosti (Belgija), Komisija za zaštitu podataka (Švedska), Nacionalna komisija za informatiku i slobode – tzv. CNIF (Francuska), Računarski odbor (Island). Za rukovodioca, odnosno predsednika ovih kolegijalnih organa (kao i za inokosni organ), po pravilu se traži odgovarajuća stručna, pre svega, pravna kvalifikacija, kao i poznavanje problematike prava i sloboda građana, odnosno zaštite podataka.“[133]

3.1.4 KONVENCIJA SAVETA EVROPE O ZAŠTITI LICA O ODNOSU NA AUTOMATSKU OBRADU PODATAKA I ZAKON O SLOBODNOM PRISTUPU INFORMACIJAMA OD JAVNOG ZNAČAJA REPUBLIKE SRBIJE[134]

Savet Evrope doneo je u januaru 1981. godine, u Strazburu, Konvenciju o zaštiti lica u odnosu na automatsku obradu ličnih podataka. Namera Konvencije je da zemlje potpisnice usklade svoja nacionalna zakonodavstva s osnovnim načelima i preporukama sadržanim u ovom dokumentu. Poštujući vladavinu prava, ljudska prava i osnovne slobode, Konvencija je imala za cilj da poveže svoje članice, da proširi zaštitu osnovnih prava i sloboda pojedinca, naročito prava na privatnost, kada je reč o automatskoj obradi ličnih podataka. Državama je prepuštena inicijativa da se u postupku regulisanja ove materije opredele u pogledu sadržaja, dometa i obuhvata zaštite ličnih podataka, uz mogućnost iskazivanja određenih specifičnosti, Pri tome, svaka država mora da se pridržava utvrđenih načela.

Jedno od osnovnih načela zaštite ličnih podataka jeste načelo zakonitosti i nepristrasnosti. Ono podrazumeva da se lični podaci prikupljaju, obrađuju i koriste na zakonom propisan način, što znači da zaštita ličnih podataka treba da obuhvati mere ipostupke kojima se sprečava

[133] *Ibidem*.
[134] Preuzeto iz: *Ibidem*, str. 91-93.

nezakonito prikupljanje, obrada, čuvanje, korišćenje, razmena i iznošenje podataka o ličnosti iz zemlje. To, takođe, podrazumeva da se podaci o ličnosti prikupljaju, obrađuju i koriste nepristrasno i na način kojim se ne vređa lično dostojanstvo čoveka.

Propisi kojima se reguliše zaštita podataka o ličnosti treba da sadrže i odredbe zasnovane na načelu tačnosti podataka. Ovim načelom određuje se kvalitet podataka o ličnosti i obaveza lica, zaduženih za prikupljanje i obradu ličnih podataka, da vrše proveru tačnosti, ažurnosti i potpunosti podataka, kao i njihove zasnovanosti na verodostojnim izvorima. Načelo podrazumeva i odgovornost lica zaduženih za vođenje evidencija, kataloga, zbirki podataka o ličnosti za netačno, neažurno i nepotpuno prikupljanje, obradu i korišćenje podataka o ličnosti.

Prava lica o kojima se prikupljaju i obrađuju podaci da budu obavešteni u kojim zbirkama se nalaze podaci koji se na njih odnose, koji su to podaci, ko ih obrađuje, u koje svrhe i po kom osnovu, kao i ko su korisnici tih podataka, sadržano je u načelu utvrđivanja namene. Ovo načelo podrazumeva i da obaveza obrade i čuvanja ličnih podataka prestaje po prestanku potrebe za koju su podaci prikupljeni i obrađeni, odnosno po isteku, zakonom ili pismenom saglasnošću lica, određenog trajanja zbirke ličnih podataka.

Načelo dostupnosti podataka, u kome je sadržano pravo lica o kome se vode podaci da bude obavešteno o postojanju zbirke ili druge evidencije s ličnim podacima, pravo da može da ima uvid u svoje lične podatke, da može da traži ispravku netačnih podataka koji se na njega odnose, brisanje podataka ako njihova obrada nije u skladu sa zakonom ili ugovorom, zabranu korišćenja netačnih, neažurnih i nepotpunih podataka koji se na njega odnose, odnosno zabranu korišćenja tih podataka ako se ne koriste u skladu sa zakonom ili ugovorom.

Prava određena načelom utvrđivanja namene i načelom dostupnosti podataka licu o kome su prikupljeni i obrađeni podaci mogu biti ograničena i mogu se koristiti u obimu koji je neophodan za zaštitu bezbednosti zemlje, javne bezbednosti, monetarnih interesa države ili za suzbijanje krivičnih dela, kao i prava i sloboda drugih. To su slučajevi u kojima se izuzetno, u skladu s članom 9. Konvencije, a takođe i u skladu s načelima utvrđenim u smernicama za regulisanje dosijea s kompjuterizovanim ličnim podacima, zakonom mogu ograničiti prava lica o kome su prikupljeni i obrađeni podaci i utvrditi odgovarajući oblici zaštite.

Zbog potrebe da se određeni lični podaci prikupljaju, obrađuju i koriste u posebnom režimu, za ove podatke, kao posebnu kategoriju podataka, propisujuse, u skladu sa načelom nediskriminacije, odnosno načelom zabrane diskriminacije, i posebna pravila. Tu posebnu

kategoriju podataka čine lični podaci o rasnom poreklu, nacionalnoj pripadnosti, religioznim i drugim uverenjima, političkim i sindikalnim opredeljenjima i seksualnom životu. Ova vrsta podataka može se prikupljati, obrađivati i davati na korišćenje samo uz pismenu saglasnost lica na koje se odnose i pod uslovima koji su propisani zakonom. Takođe i lični podaci o zdravstvenom stanju i osuđivanosti lica mogu se prikupljati, čuvati i davati na korišćenje samo u skladu sa zakonom. Izuzeci od ovog načela mogu biti regulisani zakonom, i to u okviru limita koji je određen Međunarodnom poveljom o ljudskim pravima i drugim relevantnim dokumentima u oblasti zaštite ljudskih prava i sprečavanja diskriminacije.

Navedeni izuzeci, odnosno odstupanja od proklamovanih načela, u skladu su s načelom odobrenja za izuzimanje, pod uslovom da su takva odstupanja izričito predviđena zakonom ili drugim propisom donetim u skladu s unutrašnjim pravnim sistemom koji jasno precizira njegova ograničenja i utvrđuje odgovarajuće oblike zaštite.

U skladu s načelom bezbednosti, zakonom treba regulisati i mere i postupke koje lice zaduženo za evidencije i zbirke ličnih podataka treba da preduzme radi zaštite tih zbirki, kako od prirodnih opasnosti, od slučajnih gubitaka i uništenja, tako i od rizika koji može nastati delovanjem ljudskog faktora, kao što su neovlašćeni pristup podacima, zloupotreba podataka ili zaraza kompjuterskim virusima.

Polazeći od načela slobodnog protoka, razmene i iznošenja ličnih podataka iz zemlje, koji su automatski obrađeni ili prikupljeni radi takve obrade, odnosno načela prekogranične razmene informacija, nacionalnim zakonom treba predvideti uslove za prekograničnu razmenu informacija i mere zaštite privatnosti. Neopravdana zabrana protoka informacija ne može se predvideti, osim ukoliko to ne zahteva zaštita privatnosti ili poštovanje načela uzajamnosti.

Imajući u vidu značaj pitanja zaštite ličnih podataka, u zakonima kojima se reguliše zaštita podataka o ličnosti treba posvetiti posebno poglavlje ostvarivanju nadzora, odnosno treba, u skladu s unutrašnjim pravnim sistemom, utvrditi organ koji će biti nadležan za primenu odredaba zakona i poštovanje načela na koje se te odredbe odnose. Načelo ostvarivanja nadzora, pored navedenog, podrazumeva i detaljnu razradu prava nadležnog organa i mera koje može preduzeti u vršenju nadzora. U domen prava nadležnog organa spada pravo da može da pregleda zbirke ličnih podataka i dokumentaciju vezanu za prikupljanje, obradu, čuvanje, prenošenje i korišćenje podataka o ličnosti, a takođe i da može da kontroliše mere ipostupke koje zaduženo lice preduzima u cilju zaštite ličnih podataka, kao i da ostvaruje nadzor nad prostorijama i

opremom, s aspekta ostvarivanja zaštite zbirki ličnih podataka. Nadležni organ treba da ima i ovlašćenje da zabrani prikupljanje, obradu, korišćenje i prenošenje podataka o ličnosti, ako smatra, odnosno utvrdi da za to nisu ispunjeni propisani uslovi. U domen mera koje nadležni organ može preduzeti, koje treba regulisati zakonom, spada pravo da može narediti otklanjanje uočenih nepravilnosti u zaštiti, brisanje podataka koji nisu uspostavljeni ili koji se ne koriste po zakonu, kao i izmenu ili zabranu korišćenja podataka o ličnosti kada utvrdi da su povređena lična prava lica čiji su podaci obrađeni.

U skladu s potrebom da se naglasi odgovornost svih subjekata koji učestvuju u prikupljanju, obradi, korišćenju i zaštiti ličnih podataka, a za slučaj povrede odredaba koje se tiču sprovođenja osnovnih načela na kojima se zasniva zaštita ličnih podataka, nacionalnim zako nomtreba obavezno predvideti i kaznene odredbe, krivične, prekršajne ili druge kazne, što zavisi od pravnog sistema same države.

U zakonodavstvu Srbije, kada se radi o informacijama od javnog značaja, posebnu ulogu ima Zakon o slobodnom pristupu informacijama od javnog značaja (2004).[135] Ovim zakonom uređuju se prava na pristup informacijama od javnog značaja kojima raspolažu organi javne vlasti, radi ostvarenja i zaštite interesa javnosti da zna i ostvarenja slobodnog demokratskog poretka i otvorenog društva. Radi ostvarivanja prava na pristup informacijama od javnog značaja kojima raspolažu organi javne vlasti, ovim zakonom ustanovljava se Poverenik za informacije od javnog značaja, kao samostalan državni organ, nezavisan u vršenju svoje nadležnosti.

Informacija od javnog značaja, u smislu ovog zakona, jeste informacija kojom raspolaže organ javne vlasti, nastala u radu ili u vezi sa radom organa javne vlasti, sadržana u određenom dokumentu, a odnosi se na sve ono o čemu javnost ima opravdan interes da zna. Da bi se neka informacija smatrala informacijom od javnog značaja nije bitno da li je izvor informacije organ javne vlasti ili koje drugo lice, nije bitan nosač informacija (papir, traka, film, elektronski mediji i sl) na kome se nalazi dokument koji sadrži informaciju, datum nastanka informacije, način saznavanja informacije, niti su bitna druga slična svojstva informacije.

Organ javne vlasti u smislu ovog zakona su: 1) državni organ, organ teritorijalne autonomije, organ lokalne samouprave, kao i organizacija kojoj je povereno vršenje javnih

[135]Službeni glasnik RS, 120/2004.

ovlašćenja (u daljem tekstu: državni organ); 2) pravno lice koje osniva ili finansira u celini, odnosno u pretežnom delu državni organ.

Svako ima pravo da mu bude saopšteno da li organ vlasti poseduje određenu informaciju od javnog značaja, odnosno da li mu je ona inače dostupna. Svako ima pravo da mu se informacija od javnog značaja učini dostupnom tako što će mu se omogućiti uvid u dokument koji sadrži informaciju od javnog značaja, pravo na kopiju tog dokumenta, kao i pravo da mu se, na zahtev, kopija dokumenta uputi poštom, faksom, elekronskom poštom ili na drugi način.

Kada organ vlasti ne poseduje dokument koji sadrži traženu informaciju, proslediće zahtev Povereniku i obavestiće Poverenika i tražioca o tome u čijem se posedu, po njegovom znanju, dokument nalazi. Po prijemu zahteva Poverenik proverava da li se dokument koji sadrži traženu informaciju na koju se zahtev odnosi nalazi u posedu organa vlasti koji mu je prosledio zahtev. Ako utvrdi da se dokument ne nalazi u posedu organa vlasti koji mu je prosledio zahtev tražioca, Poverenik će dostaviti zahtev organu vlasti koji taj dokument poseduje, osim ako je tražilac odredio drugačije, i o tome će obavestiti tražioca ili će tražioca uputiti na organ vlasti u čijem posedu se nalazi tražena informacija. Način postupanja odrediće Poverenik u zavisnosti od toga na koji će se način efikasnije ostvariti prava na pristup informacijama od javnog značaja. Ako Poverenik dostavi zahtev organu vlasti, rok počinje da teče od dana dostavljanja. Na postupak pred organom vlasti primenjuju se odredbe zakona kojim se uređuje opšti upravni postupak, a koje se odnose na rešavanje prvostepenog organa, osim ako je ovim zakonom drugačije određeno.

U roku od tri meseca od okončanja fiskalne godine, Poverenik podnosi Narodnoj skupštini godišnji izveštaj o radnjama preduzetim od strane organa vlasti u primeni ovog zakona, kao i o svojim radnjama i izdacima. Pored ovog izveštaja Poverenik podnosi Narodnoj skupštini i druge izveštaje, kada oceni da je to potrebno.

3.2 PRAVO NA PRIVATNOST NA INTERNETU

3.2.1 PRIVATNOST I ZAŠTITA LIČNIH PODATAKA

I pored brojnih pokušaja da se utvrdi jedinstvena definicija koja se odnosi na *pravo na privatnost,* sam pojam ostao je relativno neodređen. Jednu od ranijih definicija ovog prava formulisala je američka jurisprudencija krajem XIX veka kao „pravo da se bude ostavljen na miru“ (eng. *right to be left alone*). Često se ističe da je, zajedno s prvim uređajima informatičke tehnologije (telefonom, telegrafom itd.), nastala i savremena koncepcija „prava na privatnost“ (eng. *right to privacy*). Ova koncepcija privatnosti izneta je još krajem prošlog veka, u čuvenom radu „Pravo na privatnost" američkih sudija Semjuela Vorena (*Samual Warren*) i Luisa Brandajsa (*Louis Brandais*).[136]

Savremena pravna teorija pravo na privatnost posmatra sa tzv. aktivnog stanovišta. Prednost definicija privatnosti koje polaze od kontrole informacija jeste u tome što omogućavaju da se jasno identifikuje interes koji je u pitanju (npr. pri vršenju elektronskog nadzora i praćenja). Interes koji se javlja kod prava privatnosti predstavlja interes samoodređivanja sopstvene komunikacije sa drugima i odražava želju pojedinca i grupa da saopštavaju informacije o sebi kako nađu za shodno i kome nađu za shodno.[137]Savremeni koncept prava na privatnost ličnog i porodičnog života obuhvata složeno ljudsko pravo, koje se može posmatrati iz nekoliko aspekata: kao privatnost doma, prepiske, komunikacije, intimnog i porodičnog života. Različite su posledice postojanja i praktikovanja ovog prava: privatni život svakog pojedinca, posebno onaj deo koji se odvija u njegovom domu, zaštićen je od bilo kakvog (neodobrenog) uvida javnosti; čak i kada je reč o javnim ličnostima koje su uvek pod budnim okom javnosti i medija, granice su jasno povučene i ne mogu se prelaziti. Dom kao takav je zaštićen od neovlašćenog upada drugih lica, kao i predstavnika državnih vlasti i organa, osim u slučajevima koji su detaljno i jasno

[136] WarrenSamuel, BrandaisLouis, *The Right to be Left Alone*, Harvard Law Review, 1890. (G.L. Simons, *Privacy on the Computer Age,* str. 14).

[137] SchaferArthur, *Privacy - A Philosophical Overview*, *Aspects of Privacy Law*, Edited by Dale Gibson, Toronto, 1980, str. 9.

uređeni zakonom. Isti je slučaj i sa prepiskom, odnosno u novije vreme aktuelnom komunikacijom putem telefonskih i elektronskih uređaja. Zabranjeno je prisluškivati, ometati i presretati komunikaciju pojedinca ili grupe sa drugim pojedincima ili grupama – to je ustavni princip koji se mora poštovati i koji trpi mali broj zakonskih izuzetaka, povezanih za vršenje istražnih radnji povodom krivičnih dela. Sa druge strane, postoji i zaštita pojedinca i grupa od uvida drugih pojedinaca u njihov privatni i porodični život. Država je, dakle, u specifičnom položaju – ona se uzdržava od narušavanja prava na privatnost, ali istovremeno i štiti građane od takvog ugrožavanja prava od strane nedržavnih subjekata, pojedinaca i organizacija.[138]

Razvoj elektronskih komunikacija dakle donose niz mogućnosti da se pravo na privatnost ugrozi, odnosno prekrši. Mnogi postupci koje pojedinci ili organizacije čine, a koji bi se mogli podvesti kao kršenje prava na privatnost, ne spadaju u dela visokotehnološkog kriminala; zapravo, ona još uvek ne spadaju ni u kažnjive ili zabranjene vrste ponašanja. Pravo na privatnost se međutim može kršiti upotrebom elektronskih uređaja komunikacije na dva osnovna načina. Prvi je kršenje zakona od strane pojedinaca, grupa ili organizacija, kao i drugih državnih i nedržavnih tela; drugi je kršenje od strane policije i drugih nadležnih organa u istraživanju krivičnih dela visokotehnološkog kriminala.

3.2.2 OPASNOSTI PO PRIVATNOST LIČNOSTI NA INTERNETU[139]

Najdrastičniji oblik narušavanja privatnosti korišćenjem elektrosnkih komunikacija je krađa identiteta neke osobe sa ciljem sticanja materijalne ili druge koristi (eng. *phishing*). Ovo će se dogoditi kada neko neoprezno upotrebljava svoje lične podatke, kao što su matični broj, broj kreditne kartice, različite šifre i pin kodovi koje omogućavaju pristup privatnim podacima tog lica. Kada se jednom njegovi privatni podaci kompromituju, odnosno postanu dostupni drugom licu koje inače nema autorizaciju da im pristupi, mogu se upotrebiti za različite protivpravne svrhe. Lice koje je došlo do privatnih podataka predstavlja se kao osoba čije je podatke nelegalno pribavilo i npr. zaključuje elektronske ugovore, kupuje u *online* prodavnicama, vrši transfer novca sa kreditne kartice, i sl.

---

[138] Videti: Reljanović Mario, *Odnos prava na privatnost i pojedinih aspekata visokotehnološkog kriminala*, u: Komlen-Nikolić Lidija et alia, *Suzbijanje visokotehnološkog kriminala*, Beograd, 2010, str. 201-213.

[139] Videti: Prlja Dragan, Reljanović Mario, *Pravna informatika, op.cit*, str. 82-83.

Moguće je zamisliti i druge oblike narušavanja privatnosti lica, koji u većini slučajeva nisu određeni kao kažnjivi, kao što je korišćenje tuđih podataka ili lika bez namere da se preuzme identitet lica; korišćenje podataka koje osoba ostavi na internetu u reklamne svrhe. Svi ovi postupci spadaju u narušavanje prava na privatnost lica, kao i drugih ličnih prava. Treba primetiti da se oni ipak značajno razlikuju u načinu izvršenja i ostvarenoj koristi, kao i društvenoj opasnosti koju nose od klasičnih krivičnih dela. Kako npr. okarakterisati predstavljanje pod tuđim likom? Ovo je pitanje koje do danas nije rešeno u zakonodavstvima, kako u Srbiji tako i u drugim državama. Očigledno je da krađa tuđeg lika sama po sebi ne povlači posledice koje bi bile društveno opasne – osim ukoliko se neko lice ne služi tuđim likom da bi izvršilo neko drugo krivično delo (npr. pedofili se na internetu često predstavljaju kao deca, kako bi zadobili poverenje svojih potencijalnih žrtava). Međutim, uzimanje tuđih fotografija i pravljenje izmišljenih profila kako bi se ostvarila popularnost u određenoj socijalnoj mreži, svakako predstavlja narušavanje privatnosti lica čije se fotografije koriste.

Elektronsko plaćanje, *online* kupovina ili samo posećivanje nekih specijalizovanih sajtova mogu takođe biti zloupotrebljeni, i to u marketinške svrhe. Na osnovu podataka koje neko lice na taj način ostavi, može se rekonstruisati čitav njegov privatni život, navike, bračni status, da li ima kućnog ljubimca, i sl. Poznati su primeri da su osobe koje su kupovale određene proizvode na internetu, počele da dobijaju neželjenu elektronsku poštu – reklame za istovrsne proizvode. Ukoliko danas postavite slike sa putovanja na neku društvenu mrežu i na njima odredite lokaciju na kojoj su snimljene (eng. *geotaging*) postoji veoma velika mogućnost da će vas prilikom neke od sledećih poseta tom sajtu „sačekati“ niz oglasa – reklama upravo za putovanja na lokaciju koju ste posetili, ili lokacije koje su kulturno, istorijski ili na drugi način povezane. Postavlja se pitanje da li je ovo legalno? Nažalost, uslovi korišćenja različitih društvenih mreža i drugih servisa koji se nalaze na internetu a koje korisnici po pravilu „u dobroj veri“ prihvataju bez čitanja, uvek sadrže i klauzule o korišćenju ličnih podataka koje korisnik ostavi na tim sajtovima u najrazličitije svrhe, najčešće upravo radi modeliranja oglasa koji će se pojaviti na stranama koje pregleda u skladu sa njegovim navikama, doživljajima, obrazovanjem, interesovanjima, i sl. Iako je ovo, formalnopravno govoreći, ipak iskorak u dobrom pravcu u odnosu na situaciju koja je postojala ranije a koja se i danas često može iskusiti (naročito u državama poput Srbije u kojima ne postoji razvijena svest i kutura čuvanja podataka o ličnosti a sankcije po pravilu izostaju) kada

su kompanije koje dođu do ličnih podataka korisnika iste prodavale dalje radi reklamiranja, ili vršenja još drastičnijih kriminalnih radnji.[140]

3.2.3 ISTRAŽIVANJE DELA VTK I PRIVATNOST LIČNOSTI[141]

Osnovno pitanje kod vršenja istražnih radnji u pretkrivičnom postupku, kao i za vreme izvođenja dokaza u toku krivičnom postupka, bilo je koliko se može zadirati u privatnost građana, tako da se uspostavi adekvatan balans između pronalaženja i procesuiranja izvršioca krivičnog dela, a da se na taj način ne ugroze ni njegova prava, kao ni prava trećih lica. Ovo pitanje dobilo je novu dimenziju kada se otpočelo sa istraživanjem dela visokotehnološkog kriminala. Kako se klasične mere i istražne radnje, klasični standardi invazije privatnosti pojedinca, mogu upotrebiti kada je reč o virtuelnom svetu? Veoma brzo je postalo očigledno da dela počinjena putem računara i na računarskim mrežama uopšte nije lako ni percipirati, a da se tragovi o njihovom postojanju lako i efikasno uklanjaju od strane počinilaca, ali i delovanjem mnoštva drugih faktora. Samim tim, morala su se razviti specifična ovlašćenja istražnih organa, a pre svega policije, prilikom sprovođenja istražnih radnji. U savremenoj teoriji prevoladava stanovište da je obim ovih ovlašćenja još uvek neodređen i da će tek praksa pokazati kako će se ona dalje razvijati.[142]

Evropska konvencija o visokotehnološkom kriminalu navodi određene procesne (istražne) radnje koje se mogu izvršavati prilikom istraživanja dela visokotehnološkog kriminala. U ove radnje, između ostalih, spadaju: hitna zaštita sačuvanih računarskih podataka, hitna zaštita i delimično otkrivanje podataka u saobraćaju, izdavanje naredbe o predaji, kao i zaplena i pretraživanje sačuvanih računarskih podataka, prikupljanje podataka o saobraćaju u realnom vremenu, presretanje poruka. Ova Konvencija u članu 15. naglašava: „Svaka Strana ugovornica treba da obezbedi da uspostavljanje, sprovođenje i primena ovlašćenja i postupaka navedenih u ovom odeljku, podleže uslovima i ograničenjima predviđenim domaćim pravom, koje mora da omogući odgovarajuću zaštitu ljudskih prava i sloboda, uključujući i prava koja proizilaze iz

[140] Npr. poznat je slučaj prodaje podataka o kućnim adresama porodica koje su uplaćivale turističke aranžmane preko *online* prodaje. U ovom slučaju, njihovi domovi bili su izloženi provalnim krađama, a izvršioci su znali da su oni prazni – vlasnici su bili na putovanjima. *Ibidem.*

[141] Preuzeto iz: *Ibidem*, str. 83-86.

[142] DrozdovaEkatarina A, *Civil Liberties and Security in Cyberspace*, u: Abraham D.Sofaer, Seymour E.Goodman (ed.), *The Transnational Dimension of Cyber Crime and Terrorism*, Hoover Press, 2001, str. 204.

obaveza koje je Strana ugovornica preuzela na osnovu Konvencije Saveta Evrope o zaštiti ljudskih prava i osnovnih sloboda iz 1950. godine, Međunarodnog pakta Ujedinjenih nacija o građanskim i političkim pravima iz 1966. godine i ostalih važećih međunarodnih dokumenata o ljudskim pravima, i koje će da sadrži načelo proporcionalnosti. Ti uslovi i ograničenja mogu, u zavisnosti od vrste ovlašćenja ili postupaka o kojima se radi, između ostalog, da obuhvate sudsku ili drugu vrstu nezavisne kontrole, na osnovu kojih se opravdava primena i ograničenje obima i trajanja tih ovlašćenja ili postupaka. U meri u kojoj je to u skladu sa javnim interesom, a naročito sa pravilnom primenom prava, svaka Strana ugovornica treba da razmotri posledice ovlašćenja i postupaka iz ovog odeljka na prava, odgovornosti i opravdane interese trećih strana.“ Time se jasno šalje poruka da se mora postaviti granica između novih istražnih ovlašćenja i garantovanih ljudskih prava i sloboda, kao i da u slučaju sukoba ovih dvaju vrsta normi, očuvanje ljudskih prava i sloboda građana ima prioritet.

Smernice za saradnju između organa za sprovođenje zakona i Internet provajdera u borbi protiv visokotehnološkog kriminala, koje je objavio Savet Evrope 2008. godine[143], smatraju da su Internet provajderi (eng. *Internet Service Provider*, ISP) i policijsko-tužilački istražni organi osnova na kojoj počiva sistem za otkrivanje i istraživanje ove vrste krivičnih dela. Otuda je za svaku državu važno da njihov odnos reguliše na način koji bi omogućio nadzor nad saobraćajem na Internetu, ali istovremeno garantovao zaštitu svih prava korisnika računara, odnosno svetske mreže. Čak se zaštita privatnosti podataka u saobraćaju posebno pominje kao jedan od ciljeva kojima efikasna saradnja mora težiti.[144] Od drugih načina sprečavanja zloupotreba ovakvih postupaka, Smernice izričito preporučuju da se svaki nalog koji potiče ot tužilaštva ili policije može dostaviti isključivo u dokumentovanom obliku (napismeno), a u ekstremno hitnim slučajevima kada je moguć samo usmeni dogovor, dokumentacija mora biti naknadno dostavljena, bez odlaganja. Zahtevi moraju biti jasni i nedvosmisleni, odnosno precizni i

---

[143] *Guidelines for the cooperation between law inforcement and Internet service providers against cybercrime*; dokument je usvojen na globalnoj konferenciji o saradnji protiv visokotehnološkog kriminala u organizaciji Generalnog direktorata za ljudska prava i pravne poslove Saveta Evrope, 1. i 2. aprila 2008. godine. Smernice ne predstavljaju obavezujući dokument i cilj njihovog stvaranja je pre svega edukacija pripadnika policije i tužilaštva kada je reč o istraživanju dela visokotehnološkog kriminala. Mogu se, između ostalog, pronaći i na Internet adresama http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/567_prov-d guidelines_provisional2_3April2008_en.pdf i http://www.ifap.ru/library/book294.pdf, 01.07.2012.

[144] *Guidelines for the cooperation between law inforcement and Internet service providers against cybercrime*, tačke 14. i 15.

usmereni samo na one podatke koji su nužno neophodni radi sprovođenja istražnih radnji. Takođe, svi podaci koje ISP dostave istražnim organima moraju biti poverljivi i upotrebljavati se samo za svrhe zbog kojih su prikupljeni.[145]

Uporednopravna rešenja se zasnivaju na ovim principima.[146] Uspostavljen je princip proporcionalnosti mera koje će se preduzeti i težine krivičnog dela u pitanju, tako da se invazivne mere ne primenjuju na lakše oblike dela, kao ni u slučajevima kada ne mogu imati racionalnu svrhu. U onim slučajevima kada se mogu preduzeti sa realnim očekivanjima da će dovesti do otkrivanja krivičnog dela ili omogućiti njegovo procesuiranje, primenjuju se različita ograničenja. Tako npr. u Belgiji i Mađarskoj vlasnik podataka ili administrator sistema mora biti obavešten o tome koji su podaci kopirani u toku istrage; podaci koji se nalaze na računarskim mrežama će se kopirati samo ako postoji realna opasnost da će u protivnom biti trajno izbrisani; u svakom slučaju, kopiraće se samo oni podaci koji su nužni za sprovođenje krivičnog postupka – ovaj standard «minimuma uzurpiranja privatnosti» nalazimo i u drugim zemljama, npr. u Estoniji, Španiji, kao i u Austrijskom Zakoniku o krivičnom postupku. Takođe, u Belgiji, Austriji i Finskoj postoji standard tajnosti preuzetih podataka i njihove upotrebe samo u svrhe sprovođenja istrage i krivičnog postupka. Postoje i druga specifična ograničenja – npr. nemački Zakonik o krivičnog postupku predviđa da ove podatke mogu pregledati samo tužioci, ali ne i policijski organi. Dalje, dokazi koji se nalaze na računaru se mogu prihvatiti u postupku protiv određenog lica ukoliko tužilac može da dokaže da je računar radio normalno u vreme njegove zaplene, odnosno da se to lice zaista koristilo nedozvoljenim sadržajem sa računara (audio i video zapisi, dokumenti, štetni programi i sl.), kao i da se sadržina hard diska i ostalih nosača informacija na računaru nije promenila od trenutka njegove zaplene do trenutka izvođenja dokaza. U suprotnom, vršenje alternacija na računaru se smatra kontaminacijom dokaza. Ovakvo rešenje postoji npr. u kiparskom zakonodavstvu (Zakon o dokazima i Zakon o krivičnom postupku), kao i u Ujedinjenom kraljevstvu (Zakon o policiji i dokazima u krivičnom postupku i policijski Vodič kroz dobru praksu pri sakupljanju računarskih dokaza). Za pretraživanje prostorija (stana, poslovnog prostora) se uglavnom traže isti uslovi kao kod bilo kog drugog krivičnog dela –

[145] *Ibidem*, tačke 25-28. i 32. Navedeno prema: Reljanović Mario, *op.cit*, str. 211.

[146] Pri istraživanju nacionalnih zakonodavstava o procesnim odredbama koje mogu ugroziti ili ograničiti pravo na privatnost ličnosti, korišćeni su podaci objavljeni u analizi za Evropsku komisiju: Lorenzo Valeri, *et alia*, *Handbook of Legal Procedures of Computer and Network Misuse in EU Countries* (2006), kao i u nacionalnim izveštajima država upućenim Savetu Evrope koji se mogu naći na Internet adresi: http://www.coe.int/cybercrime, 01.08.2010.

policija može pristupiti pretraživanju (pretresu) sa sudskim nalogom, a bez njega samo u slučaju da postoje osnove sumnje da je u tim prostorijama neko krivično delo izvršeno u bliskoj prošlosti, trenutno je u izvršenju ili će se izvršiti u bliskoj budućnosti.[147] Krivično delo u pitanju mora biti teže prirode, s tim što različita zakonodavstva postavljaju različite uslove kada će se ono tako posmatrati. Kada je reč o prisluškivanju komunikacija i presretanju podataka, takođe se može povući paralela sa „klasičnim" istražnim metodama – obavezno je odobrenje suda (u Finskoj je npr. u pitanju viši sud) i ove radnje mogu trajati ograničeno vreme. U Estoniji je npr. izričito naglašeno da tzv. „Internet monitoring" nije svakodnevna policijska aktivnost, i da se može vršiti samo u slučajevima kada postoje osnovi sumnje da se određene komunikacije koriste za vršenje dela visokotehnološkog kriminala. Francuski Zakon o krivičnom postupku (član 100.) postavlja i dodatni uslov za presretanje podataka – informacije koje će se na ovaj način prikupiti, moraju biti posebno značajne za istraživanje krivičnog dela. Nemački Ustav (Osnovni zakon) štiti prava građana na privatnost u komunikaciji – otuda se presretanje može vršiti samo za izvesna krivična dela od naročitog značaja (ugrožavanje nacionalne bezbednosti, terorizam i sl.) dok se za sva ostala dela mora pribaviti nalog suda, ili tužioca u hitnim slučajevima. U Poljskoj je presretanje podataka i osluškivanje elektronskih komunikacija moguće samo za dela koja su izričito navedena u Zakonu o policiji i Zakonu o krivičnom postupku, a dela visokotehnološkog kriminala mogu biti predmet ovakvih mera samo ako se dokaže da su ona bila jedna od faza izvršenja nekog složenijeg, težeg krivičnog dela.

U nizu zemalja ne postoje posebne odredbe za istraživanje dela visokotehnološkog kriminala: Italija (sa nekoliko izuzetaka), Belgija, Portugal, Estonija, Holandija, Letonija, Litvanija, Slovenija, Luksemburg, Poljska, itd. U ovim državama se krivična dela povezana sa upotrebom računara istražuju i procesuiraju na osnovu ekstenzivnog tumačenja postojećih odredbi o istražnim i drugim radnjama. U svakom pojedinačnom slučaju su tužioci ili sudije ti koji određuju šta se može sprovesti kao istražna radnja kao i koji dokazi mogu biti prihvaćeni u toku postupka. Ipak, osnovni zaključak koji se nameće jeste da su sudovi prihvatili sve specifičnosti u postupku dokazivanja dela visokotehnološkog kriminala kao nužno potrebne, kao i da su elektronski dokazi uobilajena pojava u ovakvim postupcima. To istovremeno znači da se oni moraju prikupljati sa posebnom pažnjom i da moraju i za njihovo pribavljanje važiti isti

[147] U Nemačkoj i u tom slučaju policija mora pribaviti nalog, ali ne od suda nego od tužioca (član 105. Zakonika o krivičnom postupku).

standardi poštovanja ljudskih prava, naročito prava na privatnost, kao i ostala materijalna i procesna ograničenja zapisana u nacionalnim zakonima.[148]

Zakon o zaštiti podataka o ličnosti[149] daje odgovore na neka od pitanja koja mogu biti značajna kada je reč o problemima sa prikupljanjem i pretraživanjem podataka u procesu vršenja ispitivanja, odnosno istrage od strane nadležnih državnih organa. Podatkom o ličnosti smatra se *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); pismeni oblik podrazumeva i bilo koji način elektronskog ispisa, odnosno čuvanja podatka.

Obrada podataka je svaka radnja preduzeta u vezi sa podacima kao što su: prikupljanje, beleženje, prepisivanje, umnožavanje, kopiranje, prenošenje, pretraživanje, razvrstavanje, pohranjivanje, razdvajanje, ukrštanje, objedinjavanje, upodobljavanje, menjanje, obezbeđivanje, korišćenje, stavljanje na uvid, otkrivanje, objavljivanje, širenje, snimanje, organizovanje, čuvanje, prilagođavanje, otkrivanje putem prenosa ili na drugi način činjenje dostupnim, prikrivanje, izmeštanje i na drugi način činjenje nedostupnim, kao i sprovođenje drugih radnji u vezi sa navedenim podacima, bez obzira da li se vrši automatski, poluautomatski ili na drugi način.

Obrada podataka nije dozvoljena u sledećim slučajevima: ako fizičko lice nije dalo pristanak za obradu, odnosno ako se obrada vrši bez zakonskog ovlašćenja; ako 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; ako svrha obrade nije jasno određena, ako je izmenjena, nedozvoljena ili već ostvarena; ako je lice na koje se podaci odnose određeno ili odredivo i nakon što se ostvari svrha obrade; ako je način obrade nedozvoljen; ako je podatak koji se obrađuje nepotreban ili nepodesan za ostvarenje svrhe obrade; ako su broj ili vrsta podataka koji se obrađuju nesrazmerni svrsi obrade; ako je podatak neistinit i nepotpun, odnosno kada nije zasnovan na verodostojnom izvoru ili je zastareo. Kada se ova odredba posmatra iz

[148]Navedeno prema: Reljanović Mario, *op.cit*, str. 211-213.
[149] Službeni glasnik RS, 97/08. Navedeno prema: Prlja Dragan,Reljanović Mario, *Pravna informatika, op.cit*, str. 94-96.

aspekta obrade elektronskih podataka, ovo može značiti da se podaci o ličnosti mogu prikupljati (isto važi i za njihovo obrađivanje, analizu, čuvanje, izmenu, uništavanje, itd.) samo ukoliko: se poštuje predviđena zakonska procedura (kako u pogledu nadležnosti organa koji ih prikuplja, tako i u pogledu koraka koje zakon definiše); postoji realan osnov za njihovo prikupljanje (inače postoji zloupotreba ovlašćenja od strane organa koji ih prikuplja); se prikupljanje vrši u onom obimu koji je nužno potreban radi izvršenja istražnih radnji i pri tome se koriste najmanje invazivna sredstva. Ovo praktično znači da će se lice koje vrši prikupljanje podataka na način predviđen zakonom, uzdržati od svakog *uvida u podatke, njihovog kopiranja, drugog načina distribuiranja ili druge vrste analize*, u situaciji kada je sasvim jasno da se podaci u pitanju ne mogu odnositi na predmet njegovog postupanja.

Ova pravila imaju svoj praktičan značaj, naročito u situacijama vršenja istrage, ili neke druge vrste ispitnog postupka. U praksi bi ovo npr. značilo da, ukoliko je poznato da je neko lice sa svog privatnog naloga elektronske pošte vršilo komunikaciju sa drugim licem na način koji predstavlja kršenje nekog propisa (npr. odajući poslovne tajne), lice koje vrši uvid u podatke može lako pregledati elektronsku poštu prema adresi primaoca poruka i izolovati samo te poruke za dalju obradu. Onog trenutka kada pronađe elektronsku poštu koju je tražilo, to lice neće ići u dalju pretragu, npr. ostalih adresa primaoca, ili drugih naloga elektronske pošte koji se nalaze na tom računaru. Izuzetak od ovoga se može dogoditi kada se *osnovano sumnja* da postoji slična komunikacija sa drugim licima, ili da je korišćen i neki drugi nalog elektronske pošte za nedozvoljenu komunikaciju. Jako je teško u datom trenutku proceniti da li su se stekli uslovi za dalje ispitivanje elektronskih podataka na računaru ili drugom nosaču, kada lice koje vrši pretragu nađe one podatke za kojima je tragalo, odnosno one podatke za koje je unapred znalo ili sumnjalo da postoje. U svakom slučaju, ukoliko se prilikom pretrage računara ili drugog uređaja dođe do ličnih podataka koji očigledno ne mogu imati nikakve veze sa predmetom istrage, lice koje vrši pretraživanje dužno je da se uzdrži od njihovog pregleda i analiziranja. Npr, ukoliko se pomenutim pregledom elektronske pošte dođe do medicinskih podataka ili podataka o seksualnom opredeljenju lica, oni se ne mogu dalje pregledati i analizirati, kao ni upotrebiti na bilo koji drugi način, jer ne predstavljaju relevantne činioce u postupku koji se vodi protiv lica.

Izuzetak od različitih ograničenja ove vrste postoji ukoliko lice, nakon što je obavešteno o obradi podataka da svoj pristanak na uvid u sve podatke bez izuzetka. Ipak, i tada postoje izuzeci koja se odnose na naročito osetljive podatke: one koji otkrivaju nacionalnu pripadnost, rasu, pol,

jezik, veroispovest, pripadnost političkoj stranci, sindikalno članstvo, zdravstveno stanje, primanje socijalne pomoći, žrtvu nasilja, osudu za krivično delo i seksualni život. Oni se mogu obrađivati samo uz prethodni pristanak lica, i to u skladu sa relevantnim zakonskim propisima koji takvu obradu dozvoljavaju. Lice čiji se podaci koriste u svakom slučaju ima pravo da bude obavešteno koji podaci o njemu (njoj) se koriste, sa kojom svrhom i na koji način, a u slučaju da smatra da je neko njegovo pravo povređeno prilikom uvida, prikupljanja i obrade ličnih podataka, lice se može žaliti Povereniku za informacije od javnog značaja i zaštitu podataka o ličnosti. Kršenje propisa o zaštiti podataka o ličnosti osnov je za prekršajnu odgovornost.

4. ELEKTRONSKO POSLOVANJE U SAJBER PROSTORU

4.1. POJAM ELEKTRONSKOG POSLOVANJA

Elektronska trgovina (eng. *electronic commerce*,ili *e-commerce*) se razvijala paralelno sa razvojem informaciono-komunikacionih tehnologija. Tokom sedamdesetih godina otpočelo se sa elektronskim plaćanjima. Tokom osamdesetih godina razvile su se elektronske komunikacije. Tokom devedesetih godina pojavljuje se pojam elektronske trgovine u široj upotrebi i označava obavljanje raznih vrsta poslovnih transakcija elektronskim putem. Ovaj termin obuhvatao je pre svega: prodaju dobara i usluga, elektronski prenos sredstava, komercijalne aukcije, itd. Nakon 2000. godine možemo konstatovati da dolazi do masovne proizvodnje i distribucije elektronskih proizvoda i usluga, a tako i kupovine i prodaje proizvoda, usluga i informaciija putem globalne računarske mreže (Interneta), pa se pored elektronske trgovine javlja i novi pojam „Internet trgovina“. Internet trgovina je uži pojam, a ne sinonim za elektronsku trgovinu. Širi pojam od elektronske trgovine i Internet trgovine je pojam „elektronskog poslovanja“ koji se može definisati i kao obavljanje poslovnih operacija primenom savremene elektronske tehnologije.

Pojam „elektronsko (digitalno) poslovanje“ obuhvata *on-line komunikacije,poslovne transakcije, trgovinu, pružanje servisnih i finansijskih usluga i sve ostale akcije i radnje koje prate poslovanje za čiju realizaciju je neophodna računarska mreža*, npr. Internet. Ovaj oblik poslovanja sposoban je da eliminiše problem vremenske razlike i geografske udaljenosti između poslovnih partnera vezan za naručivanje, isporuku i plaćanje robe ili usluga. Pored toga granice poslovanja se proširuju na robe i usluge koje do pojave ovog tip poslovanja nisu ni postojale, odnosno na elektronske robe i usluge. Elektronske poslovne transakcije generalno se mogu podeliti na one između dva pravna lica (*business to business*, B2B) i one između pravnog lica i pojedinaca (*business to individuals*, B2I). Bez obzira ko se u ovim transakcijama nalazi u ulozi prodavca, odnosno kupca, može očekivati poboljšanje svog statusa u odnosu na klasično poslovanje. Ponuđači roba i usluga kreirajući strategiju nastupa koja se bazira na elektronskom poslovanju kreiraju strategiju globalnog nastupa koji će dovesti do smanjenja troškova, povećanja konkurentnosti, boljeg prilagođavanja robe potrebama kupaca, a što bi sve trebalo da dovede do

povećanja ukupne sposobnosti poslovanja. S druge strane, potrošači biraju kvalitetniju robu prilagođeniju njihovim potrebama, po manjim cenama uz povećani standard usluga.[150]

Neki naši autori smatraju da se elektronsko poslovanje može klasifikovati u nekoliko oblasti: elektronsku trgovinu, elektronsko plaćanje, elektronske komunikacije, elektronsku proizvodnju i elektronsku distribuciju.[151]

Početak elektronske trgovine vezuje se za kraj sedamdesetih godina, kada je nastala prva ideja o *on-line shoping*-u. Početkom osamdesetih su prvi put počele prodaje korišćenjem računarskih mreža; bile su to B2B mreže u Velikoj Britaniji i SAD. Međutim, prekretnicu u omasovljavanju elektronske kupovine i uvođenju B2I kao dominantnog oblika, imala je pojava prvog *Internet browser*-a 1994. godine. U pitanju je bio Netscape Navigator, koji je omogućio svakom korisniku Interneta da pretražuje prve sajtove i komercijalne prezentacije. Interesantno je da je već ta prva verzija softvera imala SSL enkripciju, odnosno sistem zaštite od prevara. Veliki prodajni lanci brzo su prihvatili ovu vizionarsku ideju i otpočeli dve nove vrste aktivnosti – *on-line banking* i *e-commerce*. Pizza Hut, lanac picerija iz SAD, prvi je omogućio prodaju proizvoda preko Interneta. Za njime su krenuli i drugi industrijski i prodajni lanci, i elektronska trgovina ubrzo nije bila ograničena samo na velike korporacije, naprotiv – neke od prvih ideja *on-line* prodaje imale su lokalni domašaj i odnosile su se na prodaju cveća i pretplatu na elektronska izdanja različitih novina. Tokom iste godine, naglo se razvijaju i modeli prodaje automobila preko Interneta, kao i pornografska industrija. Već sledeće godine počinju da rade dve Internet radio-stanice i kreće sa radom jedan od najvećih sajtova kada je reč o *e-bussiness*-u uopšte, eBay. Otada, pa sve do danas, elektronska trgovina u svetu beleži konstantni godišnji rast. U SAD je u 2010. godine predviđen rast prodaje putem Interneta od 7%, tako da će samo u ovoj zemlji ukupna vrednost elektronske kupoprodaje biti oko 170 milijardi dolara, a do 2014. se predviđa skok na 250 milijardi dolara[152].

Upotreba digitalnih uređaja u elektronskoj trgovini omogućava izvršavanje klasičnih poslovnih zloupotreba kao što su prevare, finansijske malverzacije ili izbegavanja plaćanja poreza na nov način, koji je potrebn je posebno regulisati, jer se pravila i kontrolni mehanizmi

---

[150] DrakulićMirjana i DrakulićRatimir, *Pravna regulacija e-poslovanja*, Internet adresa: http://www.e-trgovina.co.yu/pravo/regulacija1.html, 17.08.2009.

[151] Bjelić Predrag, *Elektronsko trgovanje – elektronsko poslovanje u međunarodnoj trgovini*, Beograd, Institut za međunarodnu trgovinu i privredu, 2000, str. 4.

[152] *US On-line Retail Forecast, 2009 To 2014*, Internet adresa: http://techcrunch. com/ 2010/ 03/ 08/forrester-forecast-online-retail-sales-will-grow-to-250-billion-by-2014, 02.08.2010.

klasičnog poslovanja ne mogu primeniti.[153] U međuvremenu, sistem zaštite i praćenja pošiljki koje su poručene preko Interneta se značajno razvio, što je omogućilo i brisanje bilo kakvih ograničenja u *on-line* kupovini širom sveta – i Srbija se polako ali sigurno kreće ka onoj grupi zemalja u koje je moguća dostava robe kupljene *on-line* bilo gde u svetu.[154]

Elektronsko poslovanje ne priznaje državne granice što komplikuje naplatu poreza u mnogim zemljama širom sveta. Kada se tome doda tzv. „elektronski keš" koji je osnovni oblik plaćanja kod ovog poslovanja problem postaje veoma kompleksan, jer tehničke mogućnosti dozvoljavaju gotovo momentalni prenos gotovine sa jednog računa na drugi, iz jedne zemlje u drugu, bez evidentiranja prenosa. Pored toga, mnogi kupci i prodavci posluju samo sa svojih elektronskih adresa koje se nalaze na besplatnim serverima i ne sadrže podatke o njihovim fizičkim adresama. Kako je elektronsko poslovanje donelo i neke proizvode koje nemaju fizičke karakteristike (na primer, softver) i koji se isporučuju samo u elektronskom obliku na elektronske adrese postavlja se pitanje kako se oni mogu oporezovati.[155]

4.2. PRAVNA PITANJA ELEKTRONSKOG POSLOVANJA

Ekspanzija elektronskog poslovanja otvorila je niz novih pitanja koja je trebalopravno regulisati. Sklapanje elektronskih ugovora zahtevalo je precizno definisanje utvrđivanja verodostojnosti elektronskih poruka i autentičnosti elektronskih komunikacija, a takođe je zahtevalo i definisanje procesnih pravila pri sklapanju elektronskih ugovora. Mnogobrojne zloupotrebe elektronskih podataka, lažno predstavljanje na internetu, elektronske prevare, elektronske sabotaže, unošenje virusa u računarske sisteme,neovlašćeno menjanje elektronskih podataka, linkovanje bez predhodne dozvole, i mnoge druge nedozvoljene radnje prilikom elektronske trgovine zahtevale su da bude pravno regulisane. Neisporučivanje naručenih dobara preko mreže, nedovoljan kvalitet isporučene robe, i mnogi drugi načini nanošenja štete

---

[153] Dimitrijević,Predrag,*Pravo informacione tehnologije - osnovi kompjuterskog prava*, SVEN, Niš, 2009, str. 177.

[154] Ovaj put za Srbiju bio bi sasvim sigurno kraći i jednostavniji, da naša zemlja dugo nije bila poznata po masovnom korišćenju ukradenih podataka o platnim karticama, naročito u periodu omasovljavanja korišćenja računara i Interneta krajem devedesetih godina prošlog, i početkom novog veka. Velike kompanije koje se bave prometom *on-line* transakcija, kao što je PayPal sistem, zbog toga dugo vremena nisu želele da zvanično dođu na srpsko tržište i omoguće elektronsko plaćanje i njenim rezidentima pod istim uslovima kao svugde u svetu, dok su veliki sajtovi specijalizovani za *on-line* prodaju robe, odbijali da Srbiju uvrste među zemlje u koje je moguća isporuka, ili su za isporuku naplaćivali izuzetno velike iznose koji su po pravilu premašivali iznose narudžbina.

[155] Drakulić,Mirjana, DrakulićRatimir, *loc.cit*, Internet adresa: http://www.e-trgovina.co.yu/pravo/regulacija1 .html, 02.08.2010.

potrošačima pri elektronskom poslovanju zahtevali su da pravne norme na najbolji mogući način zaštite sve veći broj potrošača koji robe nabavljaju putem virtuelnih prodavnica, a plaćanja vrše elektronskim putem. Posebno značajna pitanja su zaštite patenata, poslovnih tajni, pitanja plaćanja poreza i pitanja nadležnosti prilikom vođenja sporova, a naravno i ona moraju biti pravno regulisana u okviru nacionalnih zakonodavstava, kao i na međunarodnom nivou.

Prve korake u pravnom regulisanju područja elektronskog poslovanja načinile su međunarodne organizacije, pre svega Ujedinjene nacije i Evropska unija. Komisija Ujedinjenih nacija za međunarodno trgovačko pravo (UNCITRAL) usvojila je Model zakona kojim se reguliše elektronsko poslovanje 1996.g, a Model zakona o elektronsom potpisu 2001.g. Evropska unija je 1997. godine usvojila „Evropsku inicijativu u oblasti elektronskog poslovanja", 1999. godine je usvojila Direktivu o elektronskom potpisu,[156] a 2000. godine je usvojila i Direktivu o elektronskoj trgovini.[157]

Nakon što su međunarodne organizacije utvrdile osnove pravnog regulisanja i na nacionalnim nivoima su počeli da se donose pravni propisi koji regulišu pitanja elektronske trgovine.

Pored zakonodavstva koje direktno reguliše pitanja vezana za elektronsko poslovanje kao što su pitanja: elektronskog potpisa, elektronskog ugovora, elektronskog dokumenta, itd. za područje elektronskog poslovanja od izuzetnog su značaja i drugi pravni propisi koji regulišu pitanja iz oblasti zaštite intelektualne svojine, zaštite podataka, zaštite privatnosti, zaštite potrošača, oporezivanja, itd.[158]

4.3. PRAVNA REGULATIVA ELEKTRONSKOG POSLOVANJA U SRBIJI

U Srbiji su u predhodnom periodu doneti pravni propisi koji regulišu pojedina pitanja elektronskog poslovanja.

Zakonski propisi koji omoguićuju elektronsko poslovanje su: Zakon o elektronskom potpisu[159], Zakon o elektronskoj trgovini[160], i Zakon o elektronskom dokumentu[161].

---

[156] *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures*, Official Journal of the European Communities, L 13/2000.

[157] *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)*, Official Journal of the European Communities, L 178/2000.

[158] Efraim Turban, at all, *Electronic Commerce : A Managerial Perspective*, New Jersey, 2000, pp. 342

[159] Službeni glasnik RS, 135/2004.

Podzakonski propisi koji omogućuju elektronsko poslovanje su: Pravilnik o tehničko-tehnološkim postupcima za formiranje kvalifikovanog elektronskog potpisa i kriterijume koje treba da ispune sredstva za formiranje kvalifikovanog elektronskog potpisa[162], Pravilnik o bližim uslovima za izdavanje kvalifikovanih elektronskih sertifikata[163], Pravilnik o Regitru sertifikacionih tela za izdavanje kvalifikovanih elektronskih sertifikata u Republici Srbiji[164], Pravilnik o načinu podnošenja poreske prijave elektronskim putem[165], Odluka o elektronskom načinu obavljanja platnog prometa[166], Odluka o elektronskom potpisivanju dokumenata koje banke dostavljaju Narodnoj banci Srbije[167], Pravilnik o načinu postupanja sa elektronskim ponudama i načinu sprovođenja elektronske licitacije u postupcima javnih nabavki[168].

4.3.1 ZAKON O ELEKTRONSKOM POTPISU

Zakon o elektronskom potpisu donet je 2004. godine, i to je prvi propis u Srbiji koji se bavi nekim od aspekata elektronske trgovine, elektronskog poslovanja, i sl. Tek 2009. godine korpus najvažnijih zakona u ovoj oblasti je kompletiran donošenjem i druga dva pomenuta zakona. Njime se uređuju upotreba elektronskog potpisa (eng. *electronic signature*) u pravnim poslovima i drugim pravnim radnjama, poslovanju, kao i prava, obaveze i odgovornosti u vezi sa elektronskim sertifikatima. Njegove odredbe se primenjuju na opštenje organa, opštenje organa i stranaka, dostavljanje i izradu odluke organa u elektronskom obliku u upravnom, sudskom i drugom postupku pred državnim organom – ako je zakonom kojim se uređuje taj postupak propisana upotreba elektronskog potpisa. Potencijalna primena elektronskog potpisa bi mogla da obuhvati celokupnu državnu upravu, lokalnu samoupravu, kao i sudstvo.

Zakon o elektronskom potpisu uvodi nekoliko novih pojmova u srpski pravni sistem:

- „Elektronski dokument“ - dokument u elektronskom obliku koji se koristi u pravnim poslovima i drugim pravnim radnjama, kao i u upravnom, sudskom i drugom postupku pred državnim organom;

---

[160] Službeni glasnik RS, 41/2009.
[161] *Zakon o elektronskom dokumentu*, Službeni glasnik RS, 51/2009.
[162] Službeni glasnik RS, 26/2008.
[163] Službeni glasnik RS, 26/2008.
[164] Službeni glasnik RS, 26/2008.
[165] Službeni glasnik RS, 127/2003.
[166] Službeni glasnik RS, 57/2004.
[167] Službeni glasnik RS, 28/2009 i 47/2009.
[168] Službeni glasnik RS, 50/2009.

- „Elektronski potpis“ - skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa elektronskim dokumentom i koji služe za identifikaciju potpisnika;
- „Kvalifikovani elektronski potpis“ - elektronski potpis kojim se pouzdano garantuje identitet potpisnika, integritet elektronskih dokumenata, i onemogućava naknadno poricanje odgovornosti za njihov sadržaj, i koji ispunjava uslove utvrđene zakonom;
- „Elektronski sertifikat“ – elektronski dokument kojim se potvrđuje veza između podataka za proveru elektronskog potpisa i identiteta potpisnika;
- „Kvalifikovani elektronski sertifikat“ – elektronski sertifikat koji je izdat od strane sertifikacionog tela za izdavanje kvalifikovanih elektronskih sertifikata i sadrži podatke predviđene zakonom;
- „Korisnik“ - pravno lice, preduzetnik, državni organ, organ teritorijalne autonomije, organ lokalne samouprave ili fizičko lice kome se izdaje elektronski sertifikat;
- „Sertifikaciono telo“ - pravno lice koje izdaje elektronske sertifikate.[169]

Elektronski potpis, dakle, služi za identifikaciju potpisnika. On mora osigurati najmanje dve stvari: pokazati da je osoba koja se navodi kao potpisnik taj potpis zaista i stavila, kao i da sadržina dokumenta odgovara sadržini koja je postojala u trenutku potpisivanja. Ovo su dva problema koja od samog nastanka prate elektronski potpis, a koja su direktno vezana za pitanje sigurnosti. Da bi se bolje razumelo kako se elektronski potpis koristi, može se povući paralela sa klasičnom kriptografijom iz prošlosti: nije bilo neobično, naročito u doba ratova, da se poverljivi vojni ugovori prenose putem telegrafa, šifrirani. Strana koja inicira dogovor bi poslala ponudu, a druga strana bi se sa njom složila i na taj način zaključila punovažan ugovor. I ponuda i odgovor na ponudu slati su u kriptovanoj – šifriranoj formi, kako neprijatelj ne bi otkrio njihovu sadržinu. Ključ za čitanje ovih poruka imaju obe strane, ali ne i neprijatelj, tako da ga one mogu koristiti za dešifriranje i otkrivanje pravog značenja dolazećih poruka. Isti princip, ali na daleko naprednijem tehnološkom nivou, koristi se kod elektronskog potpisa: potpis se „šifrira“, a dešifrovanje se vrši pomoću elektronskog sertifikata.

„Običan“ elektronski potpis može se sresti u svakodnevnom radu, i mogu ga napraviti svi korisnici računara uz pomoć odgovarajućeg softvera. To je jednostavna oznaka kojom se potvrđuje autorstvo nad nekom elektronskom slikom, porukom, i sl. Međutim, ovaj potpis se lako može falsifikovati, kopirati, i zatim (zlo)upotrebiti. Zato se kao jedina pouzdana verzija elektronskog potpisa javlja „kvalifikovani elektronski potpis“, koji se u stranoj literaturi još naziva i „digitalni potpis“ (eng. *digital signature*). U pitanju je potpis koji je nastao poštovanjem

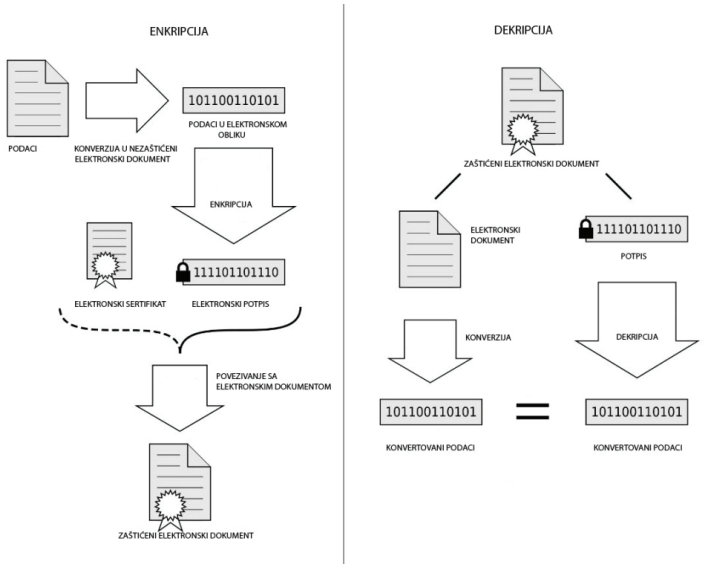
[169] Član 2. Zakona o elektronskom potpisu.

određenih procedura i protokola, kao i upotrebom odgovarajućeg softvera. Kvalifikovani elektronski potpis ne mora fizički odgovarati potpisu lica – izraz potpis se koristi kao oznaka nečeg jedinstvenog, prema čemu se nepobitno može ustanoviti identitet. Otuda se osim izraza elektronski potpis ponekad koriste i izrazi „digitalni otisak prsta“ (eng. *digital fingerprint*), ili klasičnim jezikom „šifrovana poruka“.

Razlika između pouzdanog i nepouzdanog elektronskog potpisa je dakle u kvalitetu zaštite, odnosno informaciji koju on u sebi nosi. Ako se posmatra kao šifrirani tekst, onda se njegova autentičnost može (i mora) utvrditi dešifriranjem. Opet zamislimo da je u pitanju klasičan oblik komunikacije između prijateljskih trupa u ratu. Kada dobiju šifriranu poruku, vojnici pristupaju njenom dešifriranju, koristeći unapred utvrđena pravila, odnosno tabele za šifriranje i dešifriranje, koje su zajedničke za obe strane – i pošiljaoca i primaoca. Ukoliko se dešifriranjem dobije smislena poruka, dobija se i potvrda njene autentičnosti. U digitalnom svetu, pomenuti „alat“ za dešifriranje naziva se „elektronski sertifikat“. Kao što smo već pokazali, elektronski sertifikat je elektronski dokument kojim se potvrđuje veza između podataka za proveru elektronskog potpisa i identiteta potpisnika; da bi bio pouzdan, elektronski sertifikat mora biti „kvalifikovan“ – izdat od strane sertifikacionog tela za izdavanje kvalifikovanih elektronskih sertifikata, kao i da sadrži podatke predviđene Zakonom o elektronskom potpisu. Kvalifikovani elektronski sertifikat mora da sadrži: oznaku o tome da se radi o kvalifikovanom elektronskom sertifikatu; skup podataka koji jedinstveno identifikuje pravno lice koje izdaje sertifikat; skup podataka koji jedinstveno identifikuje potpisnika; podatke za proveru elektronskog potpisa, koji odgovaraju podacima za izradu kvalifikovanog elektronskog potpisa a koji su pod kontrolom potpisnika; podatke o početku i kraju važenja elektronskog sertifikata; identifikacionu oznaku izdatog elektronskog sertifikata; kvalifikovani elektronski potpis sertifikacionog tela koje je izdalo kvalifikovani elektronski sertifikat; ograničenja vezana za upotrebu sertifikata, ako ih ima.

Elektronske sertifikate izdaje sertifikaciono telo, koje može biti bilo koje pravno lice koje se u skladu sa zakonom registruje za obavljanje ovakve delatnosti. Nadležno ministarstvo vodi jedinstveni registar svih sertifikacionih tela, a ona moraju ispuniti niz tehničkih i personalnih zahteva koji su detaljnije opisani samim Zakonom o elektronskom potpisu (član 18. Zakona). Sertfikate može izdavati i organ državne uprave.

Shematski prikazano, kvalifikovani elektronski potpis i kvalifikovani elektronski sertifikat funkcionišu na sledeći način[170]:



Ukupno gledano, značaj donošenja ovog Zakona je izuzetan, kada je reč o elektronskoj komunikaciji. Elektronskom dokumentu se ne može osporavati punovažnost ili dokazna snaga, samo zato što je u elektronskom obliku, osim u onim slučajevima kada zakon zahteva svojeručni potpis kao obaveznu formu. Ovo je dakle propis koji omogućava uvođenje elektronskih dokumenata u svakodnevni pravni promet, bez bojazni o njihovoj originalnosti i validnosti.

4.3.2 ZAKON O ELEKTRONSKOJ TRGOVINI

Zakon o elektronskoj trgovini je donela je Narodna skupština republike Srbije 29. maja 2009. godine. Ovaj Zakon stvorio je pravni osnov za izjednačavanje elektronskih oblika poslovanja sa klasičnim neposrednim oblikom, što omogućuje značajnu konkurentsku prednost privredi i organima državne uprave. Područje elektronske trgovine do sada nije bilo zakonski regulisano, što je predstavljalo veliku prepreku u opštem privrednom razvoju Srbije. Zakon o elektronskoj trgovini predstavlja potpunu novinu u našem zakonodavstvu, jer se prvi put pravno

[170] Izvor: Internet adresa: http://en.wikipedia.org/wiki/Electronic_signature, 02.08.2010.

uređuje oblast prometa robe i usluga koji se obavlja preko elektronskih mreža, a naročito preko Interneta. Cilj zakona jeste obezbeđivanje pravne sigurnosti za sve učesnike u elektronskoj trgovini, tako što se propisuju obaveze i odgovornosti učesnika u komercijalnim aktivnostima koje se pružaju na Internetu. Uz pomenuti, tu su i zakoni o elektronskom potpisu i elektronskom plaćanju, tako da je donošenjem ovog zakona zaokružen pravni okvir za funkcionisanje elektronskog poslovanja u Srbiji.

Kada je u pitanju poslovanje pravnih lica, jedna od najznačajnijih novina koju zakon uvodi u naš pravni sistem jeste pravni institut ugovora u elektronskom obliku, i to zato što su način zaključivanja ugovora i uslovi za njegovu punovažnost od ključnog značaja za svaki promet koji se obavlja preko Interneta. U pogledu verifikacije identiteta učesnika u prometu preko Interneta, veoma je važan i ranije donet Zakon o elektronskom potpisu, koji može biti i uslov punovažnosti ugovora u elektronskom obliku. Upisom prvih sertifikacionih tela za izdavanje kvalifikovanih elektronskih sertifikata, stvoreni su svi uslovi za primenu elektronskog potpisa u praksi. Donošenjem Zakona o elektronskoj trgovini napravljen je krupan korak u pravcu regulisanja elektronske trgovine, odnosno kupovina robe i usluga preko sajtova domaćih firmi koje ih prodaju i preko Interneta, gde se može plaćati platnim karticama.

Ugovor u elektronskoj formi Zakon jednostavno definiše kao ugovor koji pravna i fizička lica zaključuju, šalju, primaju, raskidaju, otkazuju, kome pristupaju i koji prikazuju elektronskim putem uz korišćenje elektronskih sredstava. U pitanju je dakle ugovor čije su *sadržina i forma* identične onoj koju određuju drugi, posebni propis (npr. Zakon o obligacionim odnosima). Svaki ugovor zaključen u elektronskoj formi mora poštovati zakonom određene norme da bi bio validan i izvršiv – ovo se odnosi na njegovu sadržinu (bitne elemente ugovore, zabranjene predmete ugovaranja, i sl.) ali i na njegovu formu – način pregovaranja, ponudu i odgovor na ponudu, i sl; pored toga, ugovor u elektronskom obliku izjednačen je sa drugim ugovorima koji se zaključuju u pisanoj formi. Ono što ga razlikuje od „običnih“ ugovora jeste *način zaključenja*, odnosno *sredstva elektronske komunikacije* kao isključivi alati koji se koriste prilikom procedure zaključenja ugovora.

Da bi neko pravno lice moglo da obavlja poslove elektronske prodaje, mora se registrovati kao i svaki drugi privredni subjekat. Moguće je zamisliti i situaciju, koja se po pravilu često i dešava, da preduzeće kao dopunski način prodaje svojih proizvoda nudi elektronsku trgovinu, pored klasične distribucije, i prodaje koja se vrši u prodajnim objektima. Bitno je napomenuti i da

se Zakon, prema izričitoj odredbi iz člana 2, ne primenjuje na zaštitu podataka, oporezivanje, zastupanje stranaka i zaštitu njihovih interesa pred sudovima, kao ni na igre na sreću sa novčanim ulozima, uključujući lutrijske igre, igre u kazinima, kladioničke igre i igre na sreću na automatima. Kod ovih pitanja važi regulativa koja je data u posebnim zakonskim tekstovima.

Kada je reč o vrstama ugovora koji se mogu zaključiti u elektronskoj formi, Zakon sadrži odredbu kojom isključuje neke oblike pravnih poslova, koji se pre svega zbog svoje naročite važnosti, i dalje mogu zaključiti samo u klasičnoj pisanoj formi. To su ugovori koji se odnose na:

1) pravne poslove kojima se vrši prenos prava svojine na nepokretnosti ili kojima se ustanovljavaju druga stvarna prava na nepokretnostima;
2) izjave stranaka i dugih učesnika u postupku za raspravljanje zaostavštine, formu zaveštanja, ugovore o ustupanju i raspodeli imovine za života, ugovore o doživotnom izdržavanju i sporazume u vezi sa nasleđivanjem, kao i druge ugovore iz oblasti naslednog prava;
3) ugovore o utvrđivanju imovinskih odnosa između bračnih drugova;
4) ugovore o raspolaganju imovinom lica kojima je oduzeta poslovna sposobnost;
5) ugovore o poklonu;
6) druge pravne poslove ili radnje, za koje je posebnim zakonom ili na osnovu zakona donetih propisa, izričito određena upotreba svojeručnog potpisa u dokumentima na papiru ili overa svojeručnog potpisa.[171]

Zakonom o elektronskoj trgovini se dalje definišu obavezni podaci i obaveštenja pre zaključivanja ugovora, dostupnost ugovora, potvrda prijema, vreme zaključenja ugovora, odgovornost pružaoca usluga, privremeno i trajno skladištenje podataka. Obzirom da se elektronska trgovina obavlja po principu masovnosti, ugovori koji se na ovaj način zaključuju su formularni. Oni moraju sadržati dovoljno podataka, kako ne bi doveli kupca u zabludu o predmetu koji kupuje, njegovim svojstvima, ceni, ili nekom drugom bitnom elementu pravnog posla kupoprodaje. Stoga je prodavac (kao pružalac usluga) dužan da potencijalnom kupcu (korisniku usluga), pre zaključenja ugovora o pružanju usluga, obezbedi na jasan, razumljiv i nedvosmislen način podatke i obaveštenja o postupku koji se primenjuje kod zaključivanja ugovora, ugovornim odredbama, opštim uslovima poslovanja (ako su sastavni deo ugovora), jezicima na kojima ugovor može biti zaključen, kodeksima ponašanja u skladu sa kojima postupaju pružaoci usluga i kako se ti kodeksi mogu pregledati elektronskim putem, kao i da obezbedi tehnička sredstva za prepoznavanje i ispravljanje pogrešnog unosa podataka u poruku pre njene predaje ili slanja. Pružalac usluga je dalje dužan da obezbedi da tekst ugovora i odredbe

[171] Član 10. Zakona.

opštih uslova poslovanja koje su sastavni deo ugovora zaključenih u elektronskoj formi budu dostupni korisnicima usluga na način koji omogućava njihovo skladištenje, ponovno korišćenje i reprodukovanje, kao i da bez odlaganja, elektronskim putem, posebnom elektronskom porukom, potvrdi prijem elektronske poruke koja sadrži ponudu ili prihvat ponude za zaključenje ugovora.[172] Ove odredbe primenjuju se na ugovore koji su sačinjeni i zaključeni *on-line*, ali ne i na ugovore koji su *zaključeni razmenom elektronske pošte*, ili drugim oblikom lične komunikacije dva ili više lica! Ovakvo rešenje ima smisla pre svega zato što se prilikom *on-line* kupovine pristupa prethodno određenim modelima ugovora, sa malo ili nimalo prostora za izmenu istih. Kod direktne komunikacije, lica koja imaju nameru zaključenja ugovora će u prepisci razmeniti sve one informacije koje smatraju relevantnim, i sami uticati na uslove zaključenja ugovora i njegovu sadržinu – on dakle u ovom slučaju neće biti unapred pripremljen i ponuđen potencijalnom kupcu po principu „uzmi ili ostavi".

Vreme zaključenja ugovora je takođe jedan od bitnih elemenata svakog pravnog posla. Ugovor u elektronskoj formi smatra se zaključenim onog časa kada ponuđač primi elektronsku poruku koja sadrži izjavu ponuđenog da prihvata ponudu. Ponuda i prihvat ponude, kao i druge izjave volje učinjene elektronskim putem, smatraju se primljenim kada im lice kome su upućene može pristupiti.[173]

4.3.3 ZAKON ELEKTRONSKOM DOKUMENTU

Zakon o elektronskom dokumentu donela je Narodna skupština Srbije 8. jula 2009. godine. Ovaj zakon definiše proceduru postupanja sa elektronskim dokumentom, prijem takvog dokumenta, izdavanje potvrde o prijemu, kao i način čuvanja duplikata. Cilj zakona je da takav zapis dobije punu pravnu snagu i važnost. Pre donošenja Zakona o elektronskom dokumentu i Zakona o elektronskoj trgovini postojao je samo Zakon o elektronskom potpisu, koji je dokumentu sa elektronskim potpisom davao isti status koji ima papirini dokument. Međutim, nisu bile uređene procedure postupanja sa takvim dokumentom, pa je bilo neophodno donošenje Zakona o elektronskom dokumentu.

Elektronski dokument jeste skup podataka sastavljen od slova, brojeva, simbola, grafičkih, zvučnih i video zapisa sadržanih u podnesku, pismenu, rešenju, ispravi ili bilo kom

[172] Članovi 12-14. Zakona.
[173] Član 15. Zakona.

drugom aktu koji sačine pravna i fizička lica ili organi vlasti radi korišćenja u pravnom prometu ili u upravnom, sudskom ili drugom postupku pred organima vlasti, ako je elektronski izrađen, digitalizovan, poslat, primljen, sačuvan ili arhiviran na elektronskom, magnetnom, optičkom ili drugom mediju.[174]

Dakle, elektronskim dokumentom se smatra onaj dokument koji je napisan u elektronskom formatu i potpisan elektronskim potpisom, *za potrebe korišćenja u pravnom prometu ili nekom postupku*. Obzirom da se u kancelarijskom poslovanju pod dokumentom u klasičnom smislu smatraju dokumenti u papirnoj formi, tj. oni koji sadrže pisane i eventualno grafičke zapise, mora se odmah napomenuti da elektronski dokument može imati značajno širu sadržinu, kao što su i video i zvučni zapisi; pod pojam elektronskog dokumenta se mogu podvesti i druge kategorije zapisa, kao što su npr. računarski programi. Svaki dokument u klasičnoj formi može se prevesti u elektronsku formu (npr. skeniranjem, prekucavanjem, i sl.)[175]. Ukoliko se to uradi na način koji garantuje njegovu autentičnost i u skladu sa zakonskom procedurom, kao i ukoliko relevantnim zakonom nije drugačije određeno, klasična i elektronska forma nekog dokumenta imaju istu važnost u pravnom prometu i svim vrstama postupaka pred državnim organima i sudovima.

Prema Zakonu o elektronskom dokumentu, elektronski dokument se ne može upotrebljavati u sledećim pravnim poslovima:

1) pravne poslove kojima se vrši prenos prava svojine na nepokretnosti ili kojima se ustanovljavaju druga stvarna prava na nepokretnostima;
2) izjave stranaka i dugih učesnika u postupku za raspravljanje zaostavštine, formu zaveštanja, ugovore o ustupanju i raspodeli imovine za života, ugovore o doživotnom izdržavanju i sporazume u vezi sa nasleđivanjem, kao i druge ugovore iz oblasti naslednog prava;
3) ugovore o utvrđivanju imovinskih odnosa između bračnih drugova;
4) ugovore o raspolaganju imovinom lica kojima je oduzeta poslovna sposobnost;
5) ugovore o poklonu;
6) druge pravne poslove ili radnje, za koje je posebnim zakonom ili na osnovu zakona donetih propisa, izričito određena upotreba svojeručnog potpisa u dokumentima na papiru ili overa svojeručnog potpisa.[176]

U Zakonu o elektronskom dokumentu unete su i odredbe o vremenskom žigu jer je prema Uredbi o kancelarijskom poslovanju i Zakonu o upravnom postupku bitno vreme stizanja

[174] Član 2. Zakona.
[175] Zakonski izraz za prevođenje u elektronsku formu je digitalizacija – prenošenje dokumenata iz drugih oblika u elektronski oblik (član 3, tačka 1. Zakona).
[176] Član 4, stav 3. Zakona.

dokumenata. Vremenski žig je zvanično vreme pridruženo elektronskom dokumentu ili grupi elektronskih dokumenata, kojim se potvrđuje sadržaj elektronskog dokumenta u to vreme odnosno sadržaj svakog dokumenta u grupi. Elektronske sertifikate za potpisivanje vremenskog žiga izdaje sertifikaciono telo upisano u evidenciju, odnosno registar kod nadležnog organa, u skladu sa zakonom kojim se uređuje elektronski potpis. Vremenski žig pridružuje se elektronskom dokumentu na osnovu zahteva za formiranje vremenskog žiga. Zahtev za formiranje vremenskog žiga sadrži određene podatke iz sadržaja elektronskog dokumenta, odnosno elektronskog potpisa. Struktura podataka vremenskog žiga sadrži: identifikator izdavaoca vremenskog žiga; serijski broj vremenskog žiga; vreme formiranja vremenskog žiga; objekat za formiranje vremenskog žiga; elektronski potpis strukture podataka vremenskog žiga; identifikator algoritma za elektronski potpis vremenskog žiga; identifikator elektronskog sertifikata putem koga se može verifikovati elektronski potpis vremenskog žiga. Vreme koje je sadržano u vremenskom žigu odgovara trenutku formiranja tog žiga, sa razlikom manjom od jedne sekunde, u odnosu na UTC (eng. *Universal Time Coordinate*) vremensku skalu.[177]

Elektronski dokument izrađuje se primenom bilo koje dostupne i upotrebljive računarske tehnologije, ako zakonom nije drugačije određeno. Ovo praktično znači da se elektronski dokumenti formiraju primenom niza korisničkih programa koji su dostupni na svakom kućnom ili poslovnom računaru, kao što su npr. *MOWord*, *MOExcel*, *Adobe Reader*, itd. Sadržina fajla, ili grupe fajlova koja na ovaj način nastane nije presudna za kvalifikovanje tog fajla ili grupe fajlova kao elektronskog dokumenta – bitna je njihova svrha, zbog koje su nastali i/ili kako se mogu upotrebiti. Tako će se elektronskim dokumentom smatrati svaki fajl koji npr. predstavlja ugovor, ispravu, odluku državnog organa u upravnom postupku. Ali se elektronskim dokumentom može smatrati i svaki elektronski oblik informacije koja se može iskoristiti u nekom od sudskih postupaka, npr. kao digitalni (elektronski) dokaz – u ovom slučaju, to mogu biti fotografije, različiti oblici elektronske komunikacije, i sl. Elektronski dokument mogu biti i drugi elektronski fajlovi koji nastanu kao proizvod delovanja nekog državnog organa u postupku – npr. elektronski snimak (audio, video, ili oba) glavnog pretresa na suđenju. Zbog svega ovoga, Zakon razlikuje unutrašnju i spoljnu formu prikaza elektronskog dokumenta – unutrašnja forma se odnosi na tehničko-programsku formu zapisivanja njegove sadržine (misli se na format zapisa – npr. .jpeg,

[177] Članovi 14-19. Zakona.

.doc, .mp3 i tehničke pretpostavke za njegov nastanak i reprodukciju – odgovarajuće korisničke programe); spoljna forma se odnosi na percepciju sadržine tog elektronskog dokumenta u spoljašnjem svetu – da li je u pitanju zvučni dokument, video snimak, pisani dokument, grafički dokument, fotografija, itd.

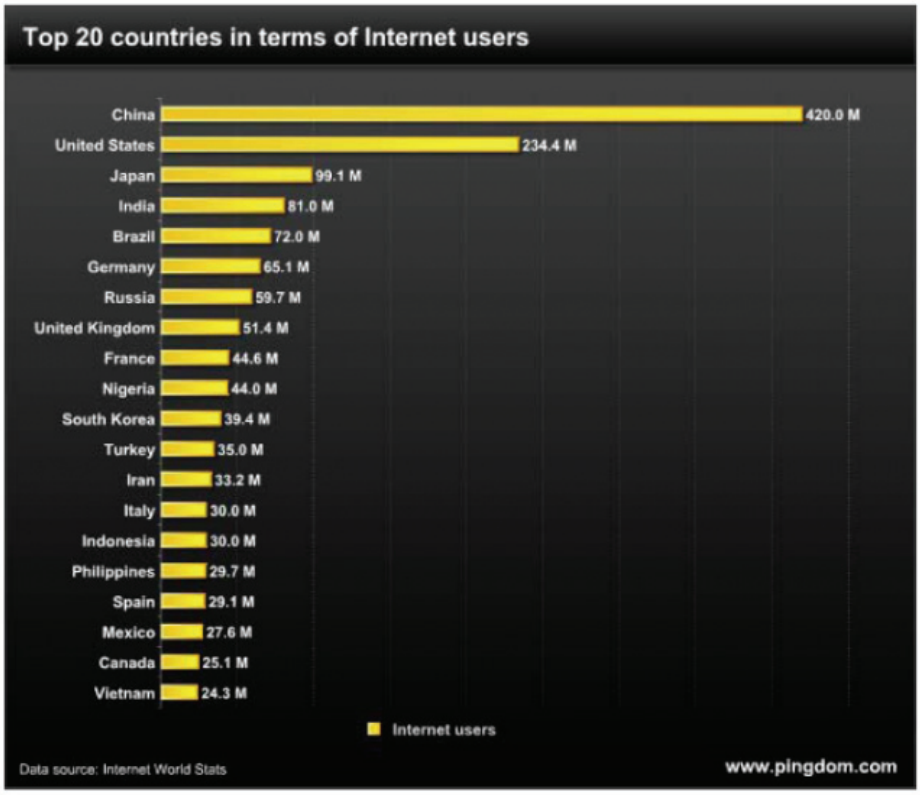
Kao što je već naomenuto, svaki elektronski dokument može biti originalni ili kopija. Originalni je onaj koji je izvorno nastao u elektronskom obliku, dok je kopija dokument koji je nastao digitalizacijom izvornog dokumenta čija forma nije elektronska. Da bi kopija imala istu pravnu snagu kao izvorni dokument, digitalizaciju mora da obavi organ vlasti u vršenju svojih nadležnosti i ovlašćenja, odnosno pravno lice ili preduzetnik u obavljanju svojih delatnosti, a istovetnost sa izvornim dokumentom kvalifikovanim elektronskim potpisom mora da potvrdi ovlašćeno lice organa vlasti, odnosno ovlašćeno lice pravnog lica, ili preduzetnik. Ovo je potpuno logično rešenje kada se ima u vidu obezbeđivanje sigurnosti u pravnom prometu – nije dovoljno jednostavno prekucati neki izvorni dokument, već se moraju primeniti sve one mere zaštite o kojima je bilo reči kod elektronskog potpisa i elektronske trgovine. Obzirom na značaj zaštite elektronskih dokumenata, Zakon tome posvećuje posebnu odredbu: „U obavljanju poslova sa elektronskim dokumentima primenjuju se odgovarajući tehnološki postupci i oprema koji obezbeđuju zaštitu tih dokumenata, u skladu sa zakonom kojim se uređuje arhivska građa, propisima o kancelarijskom poslovanju i međunarodnim standardima iz oblasti upravljanja dokumentima.“[178]

[178] Član 13. Zakona.

5. VISOKOTEHNOLOŠKI KRIMINAL U SAJBER PROSTORU

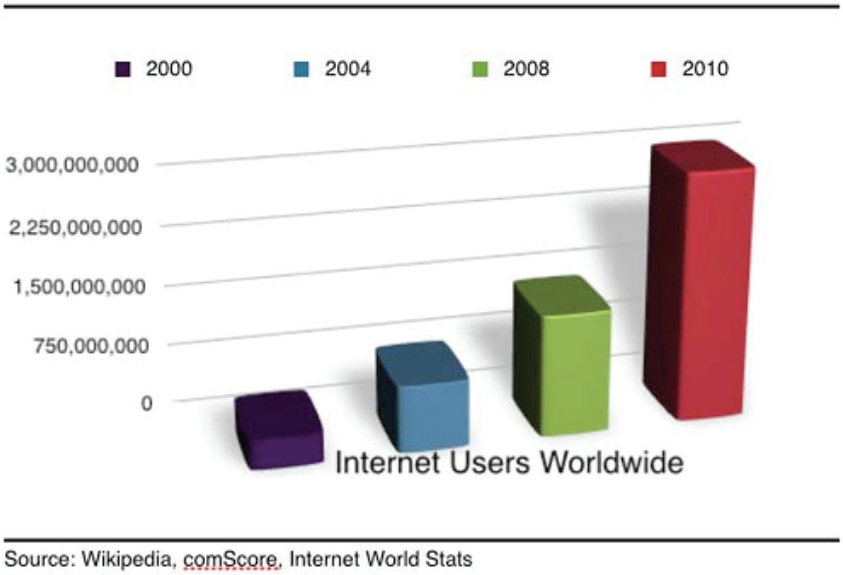
5.1 OSNOVNE NAPOMENE

Teško je zamisliti bilo koju kompaniju ili domaćinstvo bez računara. U poslednje dve decenije, a naročito u XXI veku, računari su doživeli izuzetnu ekspanziju i koriste se kako za poslovne tako i za svakodnevne potrebe ljudi, ali i edukaciju i zabavu. Računarske mreže koje su se razvile u istom periodu definitivno su učinile mnoge poslove jednostavnijim, naročito kada je reč o iznalaženju informacija, deljenju iskustava, prenosu zvuke i slike, itd. Najpoznatija računarska mreža svakako je internet, tzv. svetska mreža. Ekspanzija korišćenja interneta je očigledna – naročito je vidljiva u državama koje tek „otkrivaju“ internet, kao što je slučaj sa mnogoljudnim državama Azije, posebno Indijom i Kinom. Samo njihov udeo u korišćenju interneta je od 2005. godine narastao nekoliko desetina puta, što je ukupan broj korisnika drastično povećalo. Popularnost interneta naročito je skočila pojavom tzv. društvenih mreža, među kojima je trenutno najpopularnija Facebook. Iako imaju mnogo pozitivnih aspekata, ovakve mreže su često idealna prilika za vršenje prevara, naročito za krađu privatnih podataka i identiteta neopreznih korisnika, o čemu će više reči biti u daljem tekstu. Visokotehnološki kriminal (u daljem tekstu: VTK) jeste proizvod ovakve tehnološke revolucije koja još uvek traje, a u kojoj su visoke tehnologije postale dostupne najširem krugu korisnika.

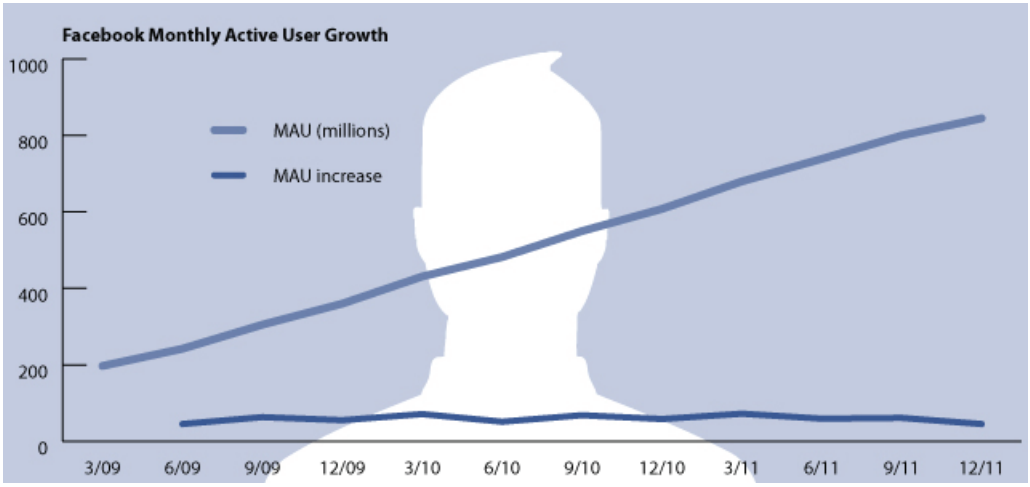


Korisnici interneta po državama u 2010. godini.[179]

[179] Izvor: http://aykuticoz.wordpress.com/category/bilgi-teknolojileri/, 01.07.2012.



Broj korisnika interneta u periodu 2000-2010. godina [180]



Porast broja korisnika Facebook-a u periodu 2009-2011. godina [181]

[180] Izvor: http://thinkeextension.com/eextension/philippines-government-commits-to-eextension/, 01.07.2012.

[181] Izvor: http://www.clickdex.com/facebook-wants-all-two-billion-internet-users-but-growth-rates-are-slowing/#.T917OpE2crA, 01.07.2012. MAU = Montly Active Users – korisnici Facebook-a koji se pojavljuju na ovoj socijalnoj mreži makar jednom mesečno, ili češće (broj takvih korisnika na kraju 2011. godine prevazišao je 800 miliona).

Nije teško pretpostaviti da je ovakav razvoj događaja zahtevao i određenu zaštitu, jer su se uporedo javili i oni pojedinci koji su u razvoju računarskih tehnologija i računarskih mreža videli dobru priliku da protivpravno deluju, radi sticanja imovinske koristi ili iz drugih povoda. Period samodovoljnosti računara, kada su oni funkcionisali izolovano od ostalih, brzo je prevaziđen. Uostalom, takva koncepcija bila je protivna samoj prirodi njihovog razvoja – bilo je sasvim očigledno da pojedinačni računari mogu da postignu mnogo, ali da grupe računara umrežene radi obavljanja određenih operacija ili jednostavno razmene informacija – imaju daleko veći stepen korisnosti. Deljenje podataka tako je postalo uobičajeno za lokalne mreže računara, a ubrzo i za *World Wide Web*, internet. Danas svaka kompanija, a često i pojedinci udruženi radi ispunjavanja određenih potreba ili jednostavno zabave, imaju svoje interne mreže, kao i istovremeni pristup svetskoj mreži. Računari su dostupni praktično svim slojevima društva, što se uglavnom može reći i za internet konekcije. Sam internet nudi mnogo načina da se korisnici edukuju i ovladaju osnovnim ali i naprednim funkcijama računara. Ovakav pristup je istovremeno revolucionaran, izuzetan sa stanovišta razvoja ljudske civilizacije koja po prvi put u istoriji može „na jednom mestu“ da nađe celokupno svoje znanje, iskustvo i dostignuća, ali je i opasan jer na internetu vrebaju različite zamke za neiskusne, lakoverne, pa čak i one koji znaju ponešto o zaštiti svoje privatnosti i finansija.

Većina korisnika interneta ima određeni cilj zašto to čini – slušanje muzike, dopisivanje sa prijateljima, iznalaženje različitih informacija, elektronska kupovina ili elektronsko bankarstvo – mogućnosti su veoma različite i raznovrsne. Ipak, svi takvi korisnici imaju i jednu zajedničku karakteristiku, u ispunjavanju svojeg cilja boravka na internetu nemaju dovoljno pažnje, vremena ili volje da se valjano zaštite i upoznaju sa mogućim neprilikama koje ih mogu zadesiti ako lakoverno ili nedovoljno ozbiljno ulaze u različite vrste transakcija ili komunikacija. Činjenica je da se mnoga klasična krivična dela mogu počiniti na internetu, kao i da se pribavljanjem informacija o korisnicima može pripremiti ili omogućiti izvršenje gotovo svih krivičnih dela protiv života i fizičkog integriteta, imovine, autorskih prava, kao i mnoga druga. Pored njih, postoje i krivična dela čiji su pojava i razvoj vezani isključivo za razvoj elektronskih komunikacija i interneta. Reč je o širokoj paleti ponašanja koja mogu biti i bezazlena, ali mogu voditi i najtežim krivičnim delima.

„Posledica ovakve ekspanzije bilo je rađanje globalnog talasa krivičnih dela koja su povezana sa računarskim tehnologijama. 1998. godine se desio prvi masovni napad na Internetu,

kada je u mrežu ubačen samoreplicirajući program koji uništava podatke na računarima i širi se samostalno po mreži (tzv. „crv“, eng. *worm*) koji je napravio veliku štetu i praktično uništio gotovo trećinu Internet sadržaja u SAD. Iste godine uhapšen je Robert Moris, (SAD) i osuđen je na 400 sati dobrovoljnog rada i 10.000 dolara. U periodu od juna do avgusta 1994 u osamnaest upada Vladimir Levin iz Petrograda izvukao je preko 10 miliona dolara iz sistema Citibank. Naredne godine je uhapšen u Londonu, 1997. je izručen američkim vlastima, a u avgustu 1997.g. je osuđen na 36 meseci zatvora i kaznu od 250.000 dolara. Kevin Mitnik u SAD je uhapšen i osuđen 1995.g. za falsifikovanje 20.000 brojeva kreditnih kartica. Čak su i pet gospođa starijih od 50 godina, službenici Zavoda za penzije u Francuskoj prebacile na svoje račune 6 miliona franaka kao penzije za osobe koje su već odavno umrle. U sledećim godinama gotovo da nije bilo Internet prezentacije važnije vladine institucije u SAD, multinacionalne korporacije, međunarodne organizacije i sl. koji nije „hakovan“ (eng. *hacked*) – čiji sadržaj nije izbrisan, zamenjen nekim drugim sadržajem, ili sklonjen na izvesno vreme sa Interneta, tako što bi neka osoba (osobe) neovlašćeno pristupile računaru-serveru, na kome se čuvaju podaci tih sajtova.[182] Uporedo sa ovim, ponekad čak i simpatičnim i naivnim pokušajima da se skrene pažnja na određeni problem ili da se izrazi protest zbog postupanja neke države ili organizacije, nastale su i prve ozbiljnije finansijske prevare, naročito nakon pojave elektronskog bankarstva polovinom devedesetih godina prošlog veka i početkom korišćenja platnih kartica putem Interneta. Na taj način su stvorene pretpostavke za rađanje modernog visokotehnološkog kriminala.[183] Organizovani kriminal, odnosno terorističke grupe, pornografske i pedofilske mreže, ilegalni trafiking oružja, narkotika, ljudi, uznapredovali su u korišćenju savremenih tehnologija. Šteta načinjenja od strane sajberkriminala u 2006. godini iznosila je oko 200 milijardi evra.“[184]

---

[182] 2003. godine pušten je do sada najdestruktivniji crv do sada, tzv. „Safirni crv”, koji je u roku od deset minuta zarazio 90% računarskih sistema na planeti koji nisu imali (adekvatnu) zaštitu. Prema rečima Davida Perry-a, direktora sektora za obrazovanje kompanije Trend Micro koja se bavi bezbednošću računara, napadi na računarske mreže postaju sve sofisticiraniji i teži za uočavanje i odbranu, ali i sve više okrenuti lukrativnoj dimenziji ove aktivnosti. Izvor: Michael Coren, *Cyber-crime bigger threat then cyber-terror*, CNN International, 24.01.2005. (http://www.cnn.com/2005/TECH /Internet/01/18/cyber.security, 01.08.2010.)

[183] Koliko je „moderni” visokotehnološki kriminal opasan, može se videti iz napada koji se desio u februaru 2007. godine, kada su simultano napadnuto – sa ciljem potpunog onesposobljavanja – šest od trinaest tzv. „root servera” na Internetu. Da su uspeli u svojoj nameri, Internet bi kao takav u potpunosti prestao da funkcioniše. Na sreću, samo su dva servera pretrpela značajnije posledice. (Izvor: http://www.crime-research.org/articles/threat-ti-Internet, 03.10.2007.). Zanimljivu priču o «tradicionalnom» visokotehnološkom kriminalu videti na Internet adresi: http://cybercrime.planetindia.net/intro.htm, 01.08.2010.

[184] Prlja Dragan, Reljanović Mario, *Pravna* informatika, Beograd, 2009, str. 46-47.

Na ovaj način se mogu uočiti i neke pravilnosti koje se vezuju za definisanje visokotehnološkog kriminala (eng. *cybercrime*). Naime, korišćenje računara i računarskih mreža je jedinstvena komponenta koja povezuje sva ilegalna ponašanja. Ovaj element ipak treba shvatiti relativno, jer poslednjih nekoliko godina teškoće nastaju kada se uzme u obzir da se mobilnim telefonima nove generacije može nesmetano pristupiti internetu i praktično počiniti veći broj krivičnih dela. VTK nije više karakteristika korišćenja računara, već korišćenja bilo kojeg oblika novih tehnologija i elektronske komunikacije. Broj dela koja se na ovaj način mogu počiniti je jako velike, a ona sama su veoma raznovrsna. Ovde ćemo se zadržati na podeli koja je od značaja za korišćenje interneta kao sredstva elektronske komunikacije pri izvršenju takvih dela.

Kada je reč o počinocima ovih dela, mora se napomenuti da raznolikost dela prati i raznolikost motiva, načina, kao i profila ličnosti koji se bave nekim od oblika VTK. Ovim oblikom kriminala se bave kako pedofili, tako i „obični" prevaranti, ali i računarski stručnjaci koji upadima u računare i računarske sisteme takođe ostvaruju različite ciljeve – dok je nekima u prvom planu materijalna korist od takvog kriminala, drugi žele da ostave neku političku poruku, ili jednostavno da se dobro zabave. Kršenje autorskih prava se takođe može vršiti iz najrazličitijih motiva, počev od preprodavaca tuđih intelektualnih proizvoda, pa do onih koji se širenjem besplatnih sadržaja bore za jednakost na internetu a protiv preskupih proizvoda muzičke, filmske i programske industrije.

„Zlonamerni učinioci kompjuterskih delikata najčešće su motivisani koristoljubljem, a smatra se da podaci iz prakse ukazuju na određeni skup osobina koje čine njihov kriminalni profil. Oko 80% delinkvenata čini delo prvi put, a 70% je zaposleno više od pet godina u oštećenom preduzeću; njihovo starosno doba je u proseku između 19 i 30 godina, pretežno su muškog pola, veoma su inteligentni; imaju uglavnom više godina radnog iskustva i važe kao savesni radnici koji prilikom obavljanja radnih zadataka ne prouzrokuju nikakve probleme, često su tehnički kvalifikovaniji nego što to zahteva radno mesto na koje su raspoređeni; ovi učinioci sebe po pravilu ne smatraju kradljivcima ili uopšte kriminalcima, već samo pozajmljivačima."[185]

[185] *Ibidem*, str. 48.

5.2 KRIVIČNA DELA VTK

5.2.1 Pojmovi iz Krivičnog zakonika vezani za dela VTK[186]

Postoji niz karakterističnih svojstava koji dela VTK izdvajaju od „klasičnih" krivičnih dela. Ove specifičnosti su stvorile značajne poteškoće zakonodavcima država, jer je pre svega trebalo prepoznati koja dela mogu da potpadaju pod ovu vrstu, a potom i rešiti čitav niz procesnih i forenzičkih specifičnosti. Dela VTK se uvek vrše korišćenjem savremenih, elektronskih tehnologija i sredstava elektronskih komunikacija; samim tim, veoma je teško percipirati mesto i vreme izvršenja – neka dela ostavljaju trajne ili kontinuirane posledice (npr. nemogućnost pristupa određenim elektronskim podacima), dok se neka svode na vršenje običnih krivičnih dela ali uz korišćenje specifične tehnologije, odnosno metoda izvršenja (prevare, falsifikovanja, i sl.). Takođe, svaki korisnik računara ili drugog uređaja pogodnog za izvršenje dela, može to učiniti iz jedne države dok se oštećena strana nalazi u nekoj drugoj državi, možda i na drugom kraju planete – element inostranosti se uobičajeno pojavljuje u daleko većem procentu kod dela VTK nego što bi se mogao pojavljivati u bilo kojem drugom krivičnom delu.

Zakonodavci su u tom smislu morali da budu inovativni, kako bi se nove situacije podvele pod klasične institute krivičnog prava. Pri tome, terminologija koju koriste je slična ili identična, ali postoje i različite specifičnosti koje su proizvod uticaja tradicije nacionalnog krivičnog prava.

Krivični zakonik Srbije objašnjava sledeće termine, koji se koriste u zakonskom tekstu:

„*Računarskim podatkom* se smatra predstavljena informacija, znanje, činjenica, koncept ili naredba koji se unosi, obrađuje ili pamti ili je unet, obrađen ili zapamćen u računaru ili računarskoj mreži.

Računarskom mrežom smatra se skup međusobno povezanih računara koji komuniciraju razmenjujući podatke.

Računarskim programom smatra se uređeni skup naredbi koji služe za upravljanje radom računara, kao i za rešavanje određenog zadatka pomoću računara.

Računarski virus je računarski program ili neki drugi skup naredbi unet u računar ili računarsku mrežu koji je napravljen da sam sebe umnožava i deluje na druge programe ili

[186] Istraživanje preuzeto iz: Prlja Dragan, Reljanović Mario, *Visokotehnološki kriminal – uporedna iskustva*, Strani pravni život 3/2009, str. 161-184.

podatke u računaru ili računarskoj mreži dodavanjem tog programa ili skupa naredbi jednom ili više računarskih programa ili podataka."[187]

Evropska konvencija o visokotehnološkom kriminalu[188] sadrži različite definicije nekih od ovih pojmova pojmova:

„a) „računarski sistem" označava svaki uređaj ili grupu međusobno povezanih ili zavisnih uređaja, od kojih jedan ili više njih, na osnovu programa, vrši automatsku obradu podataka;

b) „računarski podatak" označava svako predstavljanje činjenica, informacija ili koncepata u obliku koji je podesan za njihovu obradu u računarskom sistemu, uključujući i odgovarajući program na osnovu koga računarski sistem obavlja svoju funkciju;

v) „davalac usluge" označava:

i. svaki javni ili privatni subjekt koji korisnicima svoje usluge pruža mogućnost komuniciranja preko računarskog sistema, i

ii. svaki drugi subjekt koji obrađuje ili čuva računarske podatke u ime takve komunikacione usluge ili korisnika takve usluge.

g) „podatak o saobraćaju" označava svaki računarski podatak koji se odnosi na komunikaciju preko računarskog sistema, proizvedenu od računarskog sistema koji je deo lanca komunikacije, a u kojoj su sadržani podaci o poreklu, odredištu, putanji, vremenu, datumu, veličini, trajanju ili vrsti predmetne usluge." [189]

---

[187] Član 112, stavovi 17-20. Krivičnog zakonika, Sl.glasnik RS, 85/05, 72/09.

[188] Konvencija je usvojena 2001. godine (Konvencija 185 Saveta Evrope). Konvencija je otvorena za potpisivanje i prema državama koje nisu članice Saveta Evrope.Za njeno stupanje na snagu bilo je potrebno najmanje pet ratifikacija, od toga najmanje tri od strane država-članica Saveta Evrope, što se i dogodilo 1. jula 2004. godine. Do sada je potpisalo 46 zemalja, a ratifikovalo 30.Dodatni protokol uz Konvenciju, koji se bavi inkriminisanjem akata rasističke i ksenofobične prirode počinjenih putem računarskih sistema, donet je 2003. godine. Dodatni protokol je stupio na snagu nakon što ga je ratifikovalo pet država, 1. marta 2006. godine. Srbija je ratifikovala Konvenciju i Dodatni protokol 2009. godine: Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu, Službeni glasnik RS 19/09. Tekst Konvencije i ostali bitni podaci mogu se naći na Internet adresi: http://conventions.coe.int/Treaty/ Commun/QueVoulezVous.asp?NT=185&CL=ENG, 01.07.2012. Ciljevi Konvencije su, pre svega harmonizacija između nacionalnih zakonodavstava kada je reč o materijalnopravnim odredbama u oblasti visokotehnološkom kriminala; uvođenje adekvatnih instrumenata u nacionalna zakonodavstva kada je reč o procesnim odredbama, kako bi se stvorila osnova za istraživanje i procesuiranje ovih krivičnih dela; ustanovljavanje brzih i efikasnih institucija i procedura međunarodne saradnje. *Convention on Cybercrime – Explanatory Report*, str. 4-5 (tekst dostupan na Internet adresi: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm, 01.07.2012).

[189] Član 1 Konvencije o visokotehnološkom kriminalu, Službeni glasnik RS 19/09.

Austrijski Krivični zakonik u članu 74. daje definicije najvažnijih pojmova. Među njima je i definicija računarskog sistema kao „jednog ili više kombinovanih uređaja koji služe automatskoj obradi podataka". Isti član upozorava da je pojam računarskog programa istovetan pojmu podatka, u smislu tog Zakona. Član 6. poglavlja III Finskog Krivičnog zakona pod podacima podrazumeva „svaki dokument, ... audio i video snimak, kao i svaki drugi snimak koji se može obraditi"... Svaki takav podatak se može koristiti i kao dokazno sredstvo u krivičnom postupku. Zakon 161/2003 Rumunije u članu 35. daje precizne definicije računarskog sistema, automatske obrade podataka, računarskog podatka, računarskog programa, provajdera usluga, podatka o saobraćaju, podatka o korisniku, merama bezbednosti i pornografskog materijala sa maloletnim licem. Italijansko zakonodavstvo je nešto siromašnije – postoje definicije računarskog dokumenta (podatka) i podatka o saobraćaju. U mnogim zakonodavstvima koja ne sadrže posebne definicije, kao što je npr. litvansko, ova praznina popunjena je ratifikacijom Konvencije o visokotehnološkom kriminalu, čije se definicije u praksi direktno primenjuju.

Dela VTK uvedena su srpski pravni sistem Krivičnim zakonom Srbije iz 2005. godine, koja su u Glavi 27 predviđena kao „krivična dela protiv računarskih podataka" (čl. 298-304). Osim toga, Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala[190] u Okružnom javnom tužilaštvu u Beogradu (sada Više javno tužilaštvo u Beogradu) 2005. godine je osnovano posebno odeljenje za borbu protivvisokotehnološkog kriminala. Visokotehnički kriminal u smislu ovog zakona predstavlja vršenje krivičnih dela kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku.Cilj donošenja Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala je da se otkriju i krivično gone počinioci krivičnih dela protiv bezbednosti računarskih podataka određena krivičnim zakonom; i počinioci krivična dela protiv intelektualne svojine, imovine i pravnog saobraćaja kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku.

U posebnom odeljku**,** Krivični zakon definiše izraze koji se koriste u zakonu, a u okviru toga daje zakonske definicije koje se odnose na kompjuterska krivična dela. U tom smislu,

[190] *Zakon o organizacijii nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala*, Službeni glasnik RS, 61/2005.

„računarski podatak“ je predstavljena informacija, znanje, činjenica, koncept ili naredba koja se unosi, obrađuje ili pamti ili je uneta, obrađena ili zapamćena u računaru ili računarskoj mreži. „Računarska mreža“ je skup međusobno povezanih računara koji komuniciraju razmenjujući podatke. „Računarski program“ je uređeni skup naredbi koji služe za upravljanje radom računara, kao i za rešavanje određenog zadatka pomoću računara. „Računarski virus“ je računarski program ili neki drugi skup naredbi unet u računar ili računarsku mrežu, koji je napravljen da sam sebe umnožava i deluje na druge programe ili podatke u računaru ili računarskoj mreži dodavanjem tog programa ili skupa naredbi jednom ili više računarskih programa ili podataka. „Ispravom“ se smatra svaki predmet koji je podoban ili određen da služi kao dokaz kakve činjenice, koja ima značaj za pravne odnose, kao i računarski podatak, dok je „pokretna stvar“ svaka proizvedena ili sakupljena energija za davanje svetlosti, toplote ili kretanja, telefonski impuls, kao i računarski podatak i računarski program.

5.2.2 Klasifikacija krivičnih dela VTK

Veoma je teško, ponekadi necelishodno, praviti klasifikacije dela VTK. Ovo pre svega zato što su ova dela izuzetno raznovrsna, kako je već napomenuto. Zapravo, koliko god zakonodavac bio dalekovid i maštovit prilikom inkriminisanja, velika je šansa da će brzi razvoj računarskih tehnologija i elektronskih komunikacija (i zloupotrebe istih) izroditi neko delo koje nije obuhvaćeno postojećom klasifikacijom. Takođe, postoje dela koja su inkriminisana kao prekršaji ili krivična dela u pojedinim zakonodavstvima, dok su u drugim sasvim legalna (npr. tzv. *spam*-ovanje, slanje neželjene elektronske pošte većem broju korisnika). Zbog toga postoji nekoliko klasifikacija, koje se razlikuju prema određujućem elementu dela na osnovu kojeg je podela izvršena. Npr. aktuelne su podele prema zaštićenom (ugroženom) objektu, koje obuhvataju dela VTK usmerena protiv pojedinca (usmereni na njegovu ličnost ili na njegovu imovinu), protiv organizacije (neovlašćen pristup računaru ili računarskoj mreži, izmena podataka, kršenje autorskih prava, i sl.) i protiv društva u celini (falsifikovanje, prevare, kockanje, dečija pornografija, trgovina ljudima, i sl.).[191] M.Ngafeeson daje kratak pregled prvih normativnih regulisanja i stručnih istraživanja dela VTK u SAD – interesantno je primetiti kako

[191] Sidhartha Roy, *Cyber Crimes*, http://www.articlesbase.com/cyber-law-articles/cyber-crimes-539363.html, 01.07.2012. P.Mali daje sličnu podelu dela VTK na dela protiv pojedinaca, dela protiv imovine, dela protiv organizacija i dela protiv društva u celini (Prashant Mali, *Classification Of Cyber Crimes*, http://www.lawyersclubindia.com/articles/Classification-Of-CyberCrimes--1484.asp, 01.07.2012.).

su u početku zakonski tekstovi i naučne analize jednostavno nabrajale postupke koji su se u tom trenutku činili značajnim za ovu oblast. Kako su se problemi usložnjavali, stvorila se i potreba za drugačijim pristupom i podelom sve raznovrsnijih akata na određene grupe dela.[192]

Praktičniji, iako zasigurno nepregledniji, jeste pristup kojim se ne vrši podela tako da svako delo pripada samo jednoj isključivoj grupi, već se dela grupišu na osnovu samo nekih zajedničkih karakteristika. U tom smislu, može se govoriti o sledećim grupama krivičnih dela visokotehnološkog kriminala[193]:

1) Krivična dela protiv računara i računarskih sistema u užem smislu.

Ovo je najšira grupa dela, koja se konstantno umnožavaju zahvaljujući mašti počinilaca ali i stalnom usložnjavanju i izmenama računara, njihovih karakteristika, funkcija, potencijala, načina povezivanja i sl.

Konvencija o visokotehnološkom kriminalu Saveta Evrope ovu grupu naziva „Krivična dela protiv poverljivosti, integriteta i dostupnosti računarskih podataka i sistema“, i u nju svrstava sledeća dela:

Nelegalni pristup informacijama sadržanim na računaru ili računarskom sistemu, u nameri da se te informacije prisvoje, izmene ili unište. Za ovo delo se dakle traži *namera*, tako da je državama-potpisnicama ostavljena mogućnost da inkriminišu samo posebne radnje koje dovode do ilegalnog pristupa nekom računaru ili mreži. Tipičan primer ovakvog dela je postavljanje „trojanaca“ u nečiji računar. „Trojanci“ (eng. *trojans*) se ispoljavaju pre svega kao forma nenasilnog preuzimanja kontrole nad tuđim računarom, čega vlasnik računara najčešće nije svestan. „Trojanac“ ne može sam da se aktivira, već to *čini korisnik računara koji je napadnut* u ubeđenju da instalira autorizovan program, ili neku drugu aplikaciju za rad na računaru (otud analogija sa Trojanskim konjem).[194] Slično „trojancima“ deluju i „logičke bombe“, štetni programi poput virusa, ali bez mogućnosti samostalnog izvršavanja, sve dok ne dobiju komandu od korisnika napadnutog računara koja se najčešće sastoji u pokretanju određenog programa.

---

[192] Ngafeeson Madison, *Cybercrime Classification: A Motivational Model*, The University of Texas-Pan American, str. 3-4. Ovaj autor predstavlja takođe zanimljiv pristup podeli dela VTK, i to prema motivaciji počinilaca.

[193] Podela preuzeta iz: Reljanović Mario, *Visokotehnološki kriminal – pojam, regulativa, iskustva*, Strani pravni život 3/2007, str. 75-98.

[194] Više o „trojancima“ na internet stranici: http://en.wikipedia.org/wiki/Trojan_horse_(computing), 01.07.2012.

Nelegalno presretanje privatnih podataka koji se prenose na bilo koji način između dva računara (ili mreže). Ovde Konvencija ostavlja mogućnost državama da ovako definisano delo ograniče postojanjem namere. Kao i u prethodnom slučaju, ova činjenica je bitna pre svega zbog mogućnosti da neko bez svog znanja, ili bar bez ikakve namere, dođe u posed tuđih podataka na računarskoj mreži.

Izmena podataka na računaru, u smislu namernog potpunog ili delimičnog oštećenja, brisanja, promene sadržine, kompresije i bilo kog drugog načina izmene originalnih podataka. Ovo delo možda na prvi pogled izgleda slično *nelegalnom pristupu*, ali se mora shvatiti pre svega kao njemu komplementarno: nelegalni pristup (u nameri da se izmene podaci) omogućava izvršenje samog dela izmene podataka. I ovde Konvencija ostavlja mogućnost sužavanja dometa inkriminacije – države mogu izmenu podataka smatrati krivičnim delom samo ako je pričinjena veća šteta. Postupci opisani u delu nelegalnog pristupa, kao što su „trojanci" i „logičke bombe", zapravo za krajnji cilj imaju izmenu podataka na računaru, ili njihovo slanje autoru štetnog programa (radi dalje zloupotrebe, najčešće preuzimanja identiteta napadnutog računara).

Na delo izmene podataka nadovezuje se *upad u računarsku mrežu*, koji je na potpuno isti način definisan, ali se odnosi na sistem računara čiji se rad onemogućava ili menja nelegalnim pristupom i izmenom podataka na mreži. Ovo delo se sreće u mnogim nacionalnim zakonodavstvima kao „*uskraćivanje usluga"* (misli se na usluge odgovarajuće računarske mreže zbog nelegalnog upada u njene podatke).

Zloupotreba uređaja je specifično delo koje veoma dobro oslikava sa kakvim se problemima mogu nacionalni zakonodavci ili međunarodna zajednica susresti u pokušajima da definišu sva dela visokotehnološkog kriminala. Zloupotreba uređaja je složeno krivično delo, koje pokušava da pomiri načelo *nulla crimen, nulla poena, sine lege* i faktičko „bujanje" najrazličitijih krivičnih dela koja su vezana za savremene tehnologije. Zato generalnom odredbom države-potpisnice preuzimaju na sebe obavezu da kazne svaku namernu ilegalnu proizvodnju, posedovanje, upotrebu ili nabavku, prodaju kao i svaki drugi oblik distribucije i činjenja dostupnim nekome ko na to inače nema prava bilo kog „uređaja", pod kojim se podrazumevaju i računarski programi, kao i bilo koji oblik podataka pomoću kojih se mogu izvršiti krivična dela navedena u prethodnim članovima Konvencije. Imajući u vidu revolucionarnost, a verovatno i neodređenost ove odredbe, pisci Konvencije ipak dopuštaju državama da stave rezervu na ovaj član, osim kada je reč o prodaji ili drugom obliku distribucije

lozinki ili drugih računarskih podataka pomoću kojih se mogu počiniti navedena dela. Na ovaj način se «uređaji» možda i nepravedno stavljaju u drugi plan, ali se i državama ostavlja da same odrede domašaj pomenutog principa da nema kažnjavanja bez (jasno) inkriminisanog krivičnog dela.

Ovakav pokušaj Saveta Evrope je u svakom slučaju u skladu sa rastućom opasnošću od visokotehnološkog kriminala, a istovremeno zadovoljava i kriterijume koje smo naveli – na generički način sažeti veliku grupu protivpravnih radnji u nekoliko složenih krivičnih dela, čije su inkriminacije dovoljno precizne da mogu poslužiti nacionalnim zakonopiscima, a istovremeno ostavljaju dovoljno slobode budućoj praksi da odredi granice njihovog domašaja bez stvaranja pravne nesigurnosti. Ovo se možda ne može primeniti i na pojam „uređaja“, ali je više nego jasno da se u ovom slučaju radi o maštovitom pristupu sa ciljem da se pravo približi realnosti i da se na neki način premosti očigledna razlika između dinamike razvoja pravnih akata i tehničko-tehnoloških mogućnosti za njihovo kršenje, koja sada postoji.

Krivični zakonik predviđa sledeća krivična dela protiv bezbednosti računarskih podataka:

Oštećenje računarskih podataka i programa (čl. 298). Ko neovlašćeno izbriše, izmeni, ošteti, prikrije ili na drugi način učini neupotrebljivim računarski podatak ili program, kazniće se novčanom kaznom ili zatvorom do jedne godine. Ako je prouzrokovana šteta u iznosu koji prelazi četristo pedeset hiljada dinara, učinilac će se kazniti zatvorom od tri meseca do tri godine. Ako je prouzrokovana šteta u iznosu koji prelazi milion i petsto hiljada dinara, učinilac će se kazniti zatvorom od tri meseca do pet godina. Uređaji i sredstva kojima je učinjeno ovo krivično delo, ako su u svojini učinioca, oduzeće se.

Računarska sabotaža (čl. 299). Ko unese, uništi, izbriše, izmeni, ošteti, prikrije ili na drugi način učini neupotrebljivim računarski podatak ili program ili uništi ili ošteti računar ili drugi uređaj za elektronsku obradu i prenos podataka sa namerom da onemogući ili znatno omete postupak elektronske obrade i prenosa podataka koji su od značaja za državne organe, javne službe, ustanove, preduzeća ili druge subjekte, kazniće se zatvorom od šest meseci do pet godina.

Pravljenje i unošenje računarskih virusa (čl. 300). Ko napravi računarski virus u nameri njegovog unošenja u tuđ računar ili računarsku mrežu, kazniće se novčanom kaznom ili zatvorom do šest meseci. Ko unese računarski virus u tuđ računar ili računarsku mrežu i time prouzrokuje štetu, kazniće se novčanom kaznom ili zatvorom do dve godine. Uređaj i sredstva kojima je učinjeno ovo krivično delo oduzeće se.

Računarska prevara (čl. 301). Ko unese netačan podatak, propusti unošenje tačnog podatka ili na drugi način prikrije ili lažno prikaže podatak i time utiče na rezultat elektronske obrade i prenosa podataka u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist i time drugom prouzrokuje imovinsku štetu, kazniće se novčanom kaznom ili zatvorom do tri godine. Ako pribavljena imovinska korist prelazi iznos od četiristo pedeset hiljada dinara, učinilac će se kazniti zatvorom od jedne do osam godina. Ako pribavljena imovinska korist prelazi iznos od milion i petsto hiljada dinara, učinilac će se kazniti zatvorom od dve do deset godina. Ko ovo delo učini samo u nameri da drugog ošteti, kazniće se novčanom kaznom ili zatvorom do šest meseci.

Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka (čl. 302). Ko se, kršeći mere zaštite, neovlašćeno uključi u računar ili računarsku mrežu, ili neovlašćeno pristupi elektronskoj obradi podataka, kazniće se novčanom kaznom ili zatvorom do šest meseci. Ko upotrebi ovako dobijen podatak, kazniće se novčanom kaznom ili zatvorom do dve godine. Ako je došlo do zastoja ili ozbiljnog poremećaja funkcionisanja elektronske obrade i prenosa podataka ili mreže ili su nastupile druge teške posledice, učinilac će se kazniti zatvorom do tri godine.

Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži (čl. 303). Ko neovlašćeno sprečava ili ometa pristup javnoj računarskoj mreži, kazniće se novčanom kaznom ili zatvorom do jedne godine. Ako delo učini službeno lice u vršenju službe, kazniće se zatvorom do tri godine.

Neovlašćeno korišćenje računara ili računarske mreže (čl. 304). Ko neovlašćeno koristi računarske usluge ili računarsku mrežu u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist, kazniće se novčanom kaznom ili zatvorom do tri meseca. Gonjenje za ovo krivično delo preduzima se po privatnoj tužbi.

2) Krivična dela protiv autorskih i srodnih prava.

Povrede autorskih i srodnih prava nisu novina i njihova pojava se ne vezuje za pojavu računarskih medija i komunikacija. Ipak, razvoj tehnologije u poslednjih nekoliko decenija omogućio je stvaranja potpuno novih načina za njihovo izvršenje. Računarski programi, filmovi, muzika, ali i knjige, umetničke fotografije i slično, predmet su konstantne razmene između računara i računarskih mreža. Jako mali broj ovih razmena je legalan, odnosno predstavlja

savremeni oblik kupo-prodaje. Razvoj Interneta omogućio je da se različite ljudske tvorevine zaštićene autorskim pravima prenesu sa jednog kraja sveta na drugi (odnosno sa jednog računara na drugi) jako brzo, ponekad u intervalu od samo nekoliko minuta. Takođe, razvoj drugih tehnologija omogućio je prebacivanje ovih sadržaja na pogodne medije (CD i DVD diskovi, *flash* memorije, i sl.) i njihovo neograničeno kopiranje i distribuciju, koja uključuje i korišćenje Interneta za *download* materijala koji predstavljaju autorska dela, naravno uz prethodno plaćanje «članarine» od strane korisnika sajta koji *download*-uje. Svi oblici ove tzv. „*piraterije"* su veliki problem svih država bez diskriminacije, koja bi se mogla učiniti logičnom obzirom na razlike u njihovoj razvijenosti, zakonodavstvu i rigoroznosti državnih organa koji bi ovu pojavu trebali da spreče. Piraterija modernog doba je uistinu globalan fenomen, obzirom da praktično gotovo da nema tačke na planeti na kojoj računarska tehnologija i Internet nisu poznati. Pribavljena uz minimalne troškove, autorska dela se mogu prodavati po cenama desetak puta nižim od tržišne, a ipak donositi ogromnu zaradu. Zarade od ovakvih poslova, prema nekim procenama, mogu da premaše i zaradu od prodaje narkotika, što dovoljno govori o masovnosti ovih pojava.

Ono što je međutim, karakteristično za pojavu neovlašćenog distribuiranja autorskih dela jeste i druga dimenzija razvoja savremenih tehnologija, koja se ogleda u filozofiji da se svakom pojedincu trebaju pružiti podjednake šanse za upoznavanje i rad na računarima sa najnovijim programima i da velike kompanije koje praktično imaju monopolski položaj u pojedinim granama proizvodnje npr. računarskih programa, na svojim proizvodima ostvaruju (procentualno) daleko veću zaradu nego što to čine kompanije u drugim granama industrije. Na taj način bavljenje računarima, ili čak bavljenje određenim profesijama koje se danas ne mogu zamisliti bez upotrebe računara i određenih računarskih programa, postaje privilegija bogatih. Zbog toga, oni distribuciju takvih proizvoda, koje su prethodno „obradili", odnosno lišili tehničke zaštite postavljene zbog zaštite autorskih prava, ne rade iz lukrativnih pobuda. Takvi programi se mogu naći potpuno besplatno na internetu ili lokalnim računarskim mrežama.[195]

Druga karakteristika vredna pomena na ovom mestu tiče se razvoja različitih računarskih mreža koje ne koriste internet sajtove za skidanje nelegalnog sadržaja, već posebne računarske programe pomoću kojih se njihovi računari direktno „umrežuju" i pomoću kojih mogu direktno deliti sve računarske programe i druge legalne i nelegalne sadržaje, a da se pri tome praktično ne

[195] O autorskim pravima na internetu, videti drugi deo ove knjige.

može ući u trag njihovoj razmeni, odnosno sadržini podataka koju su dva računara razmenila. Ovaj postupak je zloupotreba inače jako podržavane i popularne ideje da se korisnici sličnih interesovanja mogu umrežavati radi razmene korisnih informacija i drugih sadržaja naučne, zabavne i druge sadržine.

Konvencija o visokotehnološkom kriminalu Saveta Evrope ne posvećuje mnogo prostora ovom problemu, pre svega zato što u oblasti zaštite autorskih i srodnih prava postoje odgovarajući međunarodni dokumenti, čiji je domašaj sada proširen i na izvršenje inkriminisanih dela korišćenjem računara i računarskih mreža.

Konačno, treba napomenuti da zakonodavstva najvećeg broja zemalja prepoznaju kao krivično delo proizvodnju, pribavljanje radi prodaje, prodaju i druge načine distribucije, ali ne i kupovinu i upotrebu ilegalnih računarskih programa i drugih autorskih dela od strane fizičkih lica. Količina koja razdvaja posedovanje radi lične upotrebe od posedovanja radi dalje distribucije nije međutim još uvek jasno određena. Većina zemalja koristi kombinovanu metodu vrednosti falsifikata i fizičkog broja kopija koje se nađu u posedu pravnog ili fizičkog lica.

3) Akti rasističke i ksenofobične prirode.

Razvoj računarskih sistema drastično je uticao na brzinu i količinu informacija koju svaki pojedinac može da razmenjuje sa ostatkom sveta koji poseduje odgovarajuću tehniku. Tako danas različite Internet prezentacije, čak i one lokalnog sadržaja, imaju od nekoliko stotina, pa do nekoliko stotina hiljada posetilaca na mesečnom nivou. Osim očiglednih dobrih strana ovakvog razvoja – upoznavanje različitih kultura, dostignuća, bolja informisanost iz različith izvora, i sl – internet nosi i opasnost od širenja ideja koje su označene kao društveno opasne i nepoželjne i koje se ne mogu tako lako diseminirati klasičnim načinima širenja propagande. Reč je između ostalog i o širenju rasne, verske, nacionalne i drugih oblika mržnje i netrpeljivosti, pre svega kroz postavljanje prezentacija na Internetu koje ili veličaju fašističke, nacističke i slične ideje, ili o određenim kategorijama ljudi govore sa očiglednim predrasudama, neretko i svesno ulazeći u neistine i uz isticanje ideja o fizičkoj eliminaciji takvih grupa, odnosno pojedinaca. Svaka država je potpisnica međunarodnim dokumenata o ljudskim pravima i zabrani diskriminacije, i dužna je da ovakve pokušaje spreči i adekvatno kazni. Ali kako sprečiti pojavu pokušaja širenja ideja mržnje preko interneta? Ovaj problem je tokom poslednjih godina postao veoma aktuelan, pre svega zato što je postavljanje osnovne Internet prezentacije usavršavanjem korisničkih programa

i omasovljavanjem Interneta postalo kako tehnički jednostavno, tako i finansijski prihvatljivo čak i za pojedince koji nemaju veće izvore prihoda (ili ih nemaju uopšte, kao što je slučaj npr. sa maloletnicima ili nezaposlenim licima, licima koja optužena za neko krivično delo i nalaze se u bekstvu i sl.).

Jedan od odgovora međunarodne zajednice je i potpisivanje Dodatnog protokola uz Konvenciju o visokotehnološkom kriminalu Saveta Evrope 2003. godine. Protokol poznaje četiri moguća oblika rasističkog ili ksenofobičnog ponašanja preko računara ili računarskih sistema: rasturanje rasističkog ili ksenofobičnog materijala preko računarskih sistema, rasno motivisana pretnja, rasno motivisana uvreda, kao i delo poricanja, značajnog umanjivanja, odobravanja ili pravdanja genocida ili dela protiv čovečnosti. Državama-potpisnicama ostavljena je sloboda da li će poslednja dva dela uvrstiti u nacionalno zakonodavstvo. Takođe, Protokol sadrži i odredbu prema kojoj potpisnice neće morati da bilo koje od ovih dela uvrste u zakonodavstvo ako su ona već na prikladan način predviđena njihovim važećim propisima. U svakom slučaju, reč je o pokušaju da se na nadnacionalnom nivou reguliše ovaj problem korišćenjem već postojeće veze između država koje su potpisnice osnovne Konvencije o visokotehnološkom kriminalu.

4) Dečija pornografija.

Ovde je reč o još jednom delu koje nije „originalno“ delo visokotehnološkog kriminala, ali je internet omogućio da se ono razvije do neslućenih dimenzija. Ujedno, ovo je jedno od dela – slično stavljanju sadržaja rasističke prirode na Internet prezentacije – za koje nije potrebno značajno znanje o rukovanju računarima, tako da ga može počiniti svako ko se nalazi povezan na neku računarsku mrežu. Najkraće rečeno, delo dečije pornografije se sastoji u tome da se nelegalni sadržaji na kojima su predstavljeni aktovi dece, ili deca u bilo kakvom seksualnom kontekstu, učine dostupnim drugim licima. Motiv za ovako nešto ne mora biti lukrativan – besplatni sadržaji su isto tako nelegalni kao i oni za koje se plaća. U ranim fazama razvoja interneta ovo delo se uglavnom izvršavalo tako što su se stavljali oglasi o prodaji kompakt diskova sa dečjom pornografijom. Ovakav pristup je omogućavao policiji da relativno efikasno deluje – policajac koji bi se predstavio kao zainteresovani potencijalni kupac stupio bi u lični kontakt sa osobom koja je prodavala ovakve sadržaje i prilikom pokušaja prodaje bi je

hapsio.[196]Danas, tako nešto se događa isključivo kao izuzetak, a pravilo je da se ovakvi sadržaji prenose putem umrežavanja korisnika. Na taj način se jako teško može uočiti izvršenje ovog dela – sadržina razmene između dva (ili više) računara je privatna komunikacija koja se ne može presresti bez razloga. Čak i kada postoje razlozi i osnov presretanja, danas se u svakom trenutku putem različitih korisničkih programa vrši umrežavanje računara koji prenose ogroman broj informacija, od kojih je većina potpuno legalna. Manji procenat nelegalnih, a posebno specifične sadržaje kao što je dečja pornografija, gotovo da je nemoguće otkriti.

Samo delo nije unifikovano kada je reč o inkriminacijama u različitim zakonodavstvima. Uglavnom postoje dve razlike u pristupu. Prvo, neke zemlje inkriminišu samo činjenje dostupnim (pod kojim se podrazumeva i prodaja) ovih sadržaja, dok druge smatraju kažnjivim i posedovanje.[197] Druga razlika je još drastičnija: dok većina zemalja iskorišćavanje dece za snimanje ovakvih sadržaja izdvaja kao posebno, izuzetno teško krivično delo, zakonodavstva manjeg broja zemalja korišćenje (mučenje) dece u te svrhe povezuju sa kasnijom distribucijom (i/ili posedovanjem) dečje pornografije – i oba postupka posmatraju kao lakša krivična dela. U drugom slučaju, pozitivna može biti samo činjenica da se korišćenje dece radi snimanja slika ili video zapisa pornografskog sadržaja posmatra u sticaju sa drugim krivičnim delima (silovanje, seksualni odnos sa licima mlađim od određenog uzrasta, protivpravno zadržavanje lica, otmica, i sl.) pa je moguće izreći kaznu (kumulativnu ili jedinstvenu, u zavisnosti od pravnog sistema) koja odgovara težini ovakvog postupanja. Ipak, čini se da visokotehnološkom kriminalu pripada samo distribucija i posedovanje ovih sadržaja, dok se njihova proizvodnja mora inkriminisati kao posebno krivično delo za koje su predviđene daleko strožije kazne.

Mora se takođe napomenuti da ova vrsta krivičnih dela nije na jedinstven način regulisana u različitim zakonodavstvima kada je reč o starosti osoba koje se nalaze u materijalima pornografske sadržine. Tu do izražaja dolaze i civilizacijske i kulturne razlike, pa granica varira

---

[196] Ovakva akcija policije je izvedena i u Srbiji 2006. godine. Branislav Grković, *Sajber kriminal – zlostavljači iz* anonimnosti, časopis Vreme, 08. februar 2007. godine.

[197] Iako se zabrana posedovanja ovakvog materijala ne može nikako dovesti u pitanje, nacionalna zakonodavstva po pravilu ne prave razliku u samoj količini materijala koja je nađena na nečijem računaru ili bilo kom drugom nosaču informacija. Nije neverovatna situacija da neko npr. prima svakodnevne (ili periodične) neželjene elektronske poruke (*e-mail*) koje sadrže reklamu neke Internet prezentacije sa ovakvim sadržajem i u okviru takve reklame nekoliko primeraka fotografija i video zapisa. Ukoliko se takva pošta automatski preko korisničkog programa za pregled *e-mail*-a sortira u poseban folder za neželjenu poštu, korisnik računara čak ne mora biti ni svestan postojanja ovakvog sadržaja. Da li je on kriminalac? Prema nekim zakonodavstvima, odgovor bi morao da bude pozitivan, što je nelogično i kontraproduktivno rešenje.

od 14 godina do 21 godine starosti. Takođe, iz istih razloga pojedine države još uvek nisu ni prihvatile inkriminaciju ovih postupaka.

Ono što ni Konvencija ni nacionalna zakonodavstva ne rešavaju efikasno jeste upravo pitanje kako inkriminisati upotrebu savremenih tehnologija od strane samih lica koja se ovim odredbama štite? Najčešće se može primeniti neka od odredbi koje se inače nalaze u okviru inkriminacija ostalih seksualnih delikata, kao i krivične (ne)odgovornosti maloletnih osoba. Čini se ipak da se mora pre svega precizno utvrditi donja granica kažnjivosti takvih postupaka, koja mora biti u skladu sa ostalim krivičnim delima iz ove oblasti. Potom se mora jasno odrediti društveni stav prema onim delima koja bi i prema tako utvrđenim granicama spadala u kažnjiva – čini se da u ovom slučaju klasične krivičnopravne sankcije ne dolaze u obzir, i da se pre svega mora mobilisati porodica i šire okruženje takvih lica da bi se ovakvi problemi rešili. Obrazovno-vaspitne ustanove do sada po pravilu nisu adekvatno reagovale, a često nisu reagovale uopšte, iako su imale saznanja o postojanju slučajeva dečije pornografije koja se ne samo distribuirala u školi, nego je tamo i proizvedena.[198]

5) Računarske prevare.

Sasvim sigurno najmaštovitija i najširа grupa krivičnih dela koja se mogu izvršiti korišćenjem računarskih mreža su različiti oblici prevara. Evropska konvencija o visokotehnološkom kriminalu poznaje samo dva oblika ovakvih dela: falsifikovanje i prevaru, oba u slučaju kada su povezani sa upotrebom računara. Na taj način, domašaj Konvencije je učinjen jako ograničenim i nacionalna zakonodavstva moraju otići korak dalje u regulisanju ove vrste visokotehnološkog kriminala. Treba najpre razlikovati one vrste prevara kod kojih je računar samo sredstvo komunikacije između kriminalca i žrtve od onih koje zahtevaju visokotehnološko znanje i tehnologiju da bi mogle biti realizovane.

U prvu grupu nesumnjivo spada jedna od najpopularnijih prevara ikada izvedenih putem *e-mail*-a, tzv. „nigerijsko pismo“. Prevara je jako jednostavna i koristi lakovernost ljudi, kojima se šalje „poverljivo“ pismo od izvesnog gospodina iz Afrike (prva pisma su koristila Nigeriju kao zemlju porekla poruke, otuda i naziv ove prevare) koji se našao na udaru „revolucionarne pravde“

[198]Gotovo da se ne može naći država u Evropi (sasvim sigurno i šire) u kojoj ne postoje Internet prezentacije na kojima su dostupni ovakvi sadržaji, iako su po nekim krivičnim zakonodavstvima stavljeni van zakona. U Srbiji je poznat slučaj iz Kragujevca, kada su „akteri“ video zapisa snimljenih mobilnim telefonom čak došli na naslovne strane pojedinih dnevnih novina.

i koji mora smesta svoje ogromno bogatstvo da prebaci na sigurne račune u Evropi. Najčešće su u pitanju sume od nekoliko stotina miliona dolara, od kojih je dotični gospodin spreman da izdvoji određeni procenat (5-20%, ponekad i više), ali postoji problem – na određeni račun treba smesta uplatiti izvesnu sumu novca kao garantiju veće uplate (ili kao naknadu troškova banci, ili sl). Gospodin u nevolji nikako nije u mogućnosti da tu transakciju realizuje, ali je preko „poverljivih izvora" saznao da ste baš vi čovek od izuzetne diskrecije i poverenja i moli vas da mu pomognete uplatom na taj-i-taj račun.... Sume koje su na ovaj način uzimane lakovernim ljudima su se kretale od 100-1,500$, a prevaranti nisu bili izbirljivi – ovakve poruke su slali na hiljade adresa, ostvarujući tako ponekad i neslućenu zaradu. Ljudi koji su prevareni najčešće nisu želeli da se za njihovu lakovernost sazna i odricali su se tih suma novca ne prijavljući policiji šta se dogodilo. Čak i kada bi prijavili, često je od same uplate do saznanja da od „procenta" od milion dolara nema ni govora proteklo nekoliko meseci, što je više nego dovoljno da prevaranti zametnu svoje tragove.

E-mail prevare su tako rasprostranjene da bi se samo o njima mogla napisati posebna studija. Na ovaj način se reklamiraju proizvodi koje ljudi obično ne žele da kupuju u javnosti – lekovi, nedozvoljene supstance, seksualna pomagala, poslovna pratnja – lista je beskonačna. Takođe, moli se za pomoć bolesnoj deci, gladnima u Africi, žrtvama cunamija u Aziji.... Prema istraživanjima sprovedenim u 2006. godini, oko 90% sve elektronske pošte koja stigne prosečnom korisniku Interneta je tzv. „neželjena pošta" (eng. *spam*) u kojoj se praktično svakodnevno kriju različite poruke koje vas mogu odvesti u svet Internet prevara.[199]

Ipak, suština prevare korišćenjem savremenih tehnologija nije samo u novim mogućnostima masovne komunikacije sa nepoznatim ljudima i korišćenjem njihove dobrote, lakovernosti i ostalih ljudskih osobina koje su karakteristične i za „klasične" obmane. Još od sedamdesetih godina XX veka, kada je jedan student otkrio da se (tadašnji) računari mogu koristiti za obavljanje telefonskih poziva bez naplate,[200] razvio se čitav niz zloupotreba. Najčešće su zloupotrebe vezane za plaćanje ukradenim kreditnim karticama, kao i druge finansijske malverzacije koje su po pravilu posledica prethodnog počinjenog drugog krivičnog dela, npr.

---

[199] Krebs Brian, *Year of Computing Dangerously*, Washington Post, 22.12.2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/12/22/AR2006122200367.html, 01.07.2012.

[200] Ova pojava je nazvana „friking" (eng. *phreaking*, što je skraćeni oblik dve reči – *phone* i *freaking*). Iako se smatra „klasičnom" računarskom prevarom za čije su suzbijanje telefonske kompanije uložile značajna sredstva, friking je i danas veoma rasprostranjen u svim državama sveta.

neovlašćenog pristupa informacijama na tuđem računaru. Sa ovakvim načinom prevare blisko je povezano tzv. „preuzimanje identiteta“, odnosno „predstavljanje“ kriminalaca na računarskoj mreži kao neke druge osobe.[201]

Osim ovih prevara, postoje i prevare koje su vezane za *spoofing*, radnju za koju još uvek nema ekvivalentnog prevoda na srpskom jeziku, a koja se sastoji od slanja elektronskih poruka sa tuđe *e-mail* adrese (što se svodi na „preuzimanje identiteta“), ili sa *e-mail* adrese koja podseća na originalnu adresu. Svrha ovakvog postupka je da adresant poruku shvati ozbiljno, da ona ne završi u njegovoj neželjenoj pošti. Na taj način se on dovodi u zabludu o tome ko mu piše, i kriminalac lakše sa njim gradi odnos poverenja koji dovodi do konačnog izvođenja prevare.[202] U ovu vrstu krivičnih dela spada i pravljene lažnih, „jednokratnih“ internet prezentacija koje navodno predstavljaju poznae kompanije iz najrazličitijih oblasti privređivanja. Ovakve prezentacije se po izvršenoj prevari gase, a počinioci po pravilu koriste i internet adresu i vizuelni izgled na osnovu koga se ne može posumnjati da se radi o prevari.[203]

6) Ostala dela koja uključuju korišćenje računara i računarskih mreža.

---

[201]Klasičan primer vezan je za tzv. *e-banking*, obavljanje bankarskih transakcija putem računarskih mreža. Osoba koja poseduje određene podatke (korisničko ime, lozinku) nekog korisnika *e-banking*-a, može pristupiti njegovim bankovnim računima i prebacivati novac na druge račune.

[202] Npr. poznate su elektronske poruke koje kruže Internetom u ime Citizen banke. Ovde je očigledna analogija sa Citi bankom iz SAD-a, jednom od najvećih banaka na svetu. U ovakvim porukama se budućnim „korisnicima“ za otvaranje računa i druge transakcije koje bi obavili nude različite pogodnosti, uz neizbežno posredovanje neke treće banke (u kojoj počinioci dela imaju otvoren račun). Citizen banka ne postoji, a bankovni račun preko kojeg se navodne transakcije obavljaju (a koji se nalazi u nekoj trećoj banci) odmah po izvršenoj prevari počinioci prazne i gase.

[203]Najpoznatija prevara ove vrste je izrada prezentacija velikih firmi koje se bave proizvodnjom korisničkih programa (npr. Microsoft). Prevara se najčešće izvodi tako što se dolaskom korisnika računara na odgovarajuću Internet prezentaciju u njegov računar ubacuje određeni program koji ne detektuju konvencionalni programi zaštite, a koji se manifestuje u izbacivanju reklamnih poruka ili sličnih postupaka koji opterećuju kako računar, tako i njegovog korisnika. Naravno, ubrzo na *e-mail* korisnika dolazi „spasonosna“ poruka od Microsoft-a da se *download*-om novog korisničkog programa efikasno eliminišu sve takve maliciozne tvorevine na računaru. Korisnik odlazi na preporučenu Internet prezentaciju, koja neobično podseća na originalnu, kupuje preporučeni korisnički program – i prevara je izvršena. Slanjem ogromne količine ovakvih poruka na prethodno „zaražene“ računare, prevaranti mogu u roku od samo nekoliko dana zaraditi ogromne količine novca. Tada lažna Internet prezentacija „nestaje“, a kupljeni programi koji navodno rešavaju korisnike računara nevolje koju su im sami autori tih programa nametnuli, u zavisnosti od malicioznosti počinioca ovog dela, stanje čine još gorim, ili ga vraćaju u prvobitni izgled. Za prevarante kojima je ovakav vid obmane suviše komplikovan, postoje i znatno lakši načini – npr. postavljanjem „originalne“ prezentacije nekog popularnog fudbalskog kluba i *on-line* „prodajom“ sezonskih karata po znatno nižoj ceni od uobičajene, takođe se mogu zaraditi znatne sume novca u roku od nekoliko dana.

Ostala krivična dela koja se mogu izvršiti korišćenjem računara ili računarskih mreža uglavnom se svode na nekoliko potpuno različitih grupa delovanja:

Povreda prava na zaštitu privatnih podataka o ličnosti: Nije nepoznato da se provajderi internet i drugih usluga mogu protivpravno služiti informacijama kao što su *e-mail* adresa, podaci o sajtovima koje posećujete i sl. Ovi podaci se prodaju ili ustupaju različitim kompanijama, koje ih koriste da bi na poštansku ili *e-mail* adresu korisnika računara slali reklamni materijal, ili za formiranje profila ličnosti koji znatno pomaže pristupu u slučaju različitih prevara. Kada osoba sakuplja podatke do kojih može doći preko računarskih mreža da bi stupila u bilo kakav (pismeni, usmeni, direktni) kontakt sa drugom osobom, može se govoriti o tzv. „*cyber-uznemiravanju*".

Prikupljanje podataka koji su označeni kao tajni: Moderna špijunaža se obavlja gotovo isključivo savremenim tehnologijama. Sateliti koji prate kretanje i lociranje određenih ljudi ili objekata, baze podataka u koje se može neautorizovano ući, to su glavna «oružja» savremenih špijuna, koji na ovaj način dolaze kako do vojnih i državnih tajni, tako i do važnih industrijskih podataka i patenata.

Prodaja nelegalnih supstanci i drugih predmeta preko računarskih mreža: O ovim delima je već bilo reči kod Internet prevara; ono što ih od njih razlikuje jeste da se u ovom slučaju kupoprodaja zaista odvija, ali je njen predmet neka supstanca ili druga stvar koja se ne može naći u pravnom prometu, ili se može naći samo uz posebnu dozvolu države (koja naravno u ovom slučaju ne postoji). Lekovi, eksploziv, planovi i udžbenici za pravljenje hemijskih otrova, ali i kradena umetnička dela, automobili, druge dragocenosti – sve to može biti predmet jednog ovakvog nelegalnog posla. U većini slučajeva je notorna činjenica da je supstanca ili predmet koji je predmet kupoprodaje ilegalan ili ukraden, ali postoje i slučajevi kada kupac to ne može znati – tada je ovakva prodaja bliža opisanom delu prevare.

5.3 PROCESUIRANJE DELA VTK I ELEKTRONSKI DOKAZI

5.3.1 PROCESNE ODREDNICE SADRŽANE U KONVENCIJI O VISOKOTEHNOLOŠKOM KRIMINALU SAVETA EVROPE

Kada je reč o međunarodnim standardima procesuiranja dela VTK, osnovne smernice sadrži Konvencija o visokotehnološkom kriminalu Saveta Evrope, o kojoj je već bilo reči u tekstu o delima VTK. Osim materijalnopravnih, Konvencija sadrži i važne procesnopravne odredbe,

koje se bave procesnim ovlašćenjima državnih organa prilikom istraživanja krivičnih dela vezanih za nove tehnologije. Procesnom pravu posvećen je drugi deo drugog poglavlja Konvencije. Kroz tekst se uvode neki klasični instrumenti istraživanja krivičnih dela u novoj, virtuelnoj sredini, u skladu sa specifičnostima koje su karakteristične za elektronski prostor i elektronske dokaze. Ova pravila su od značaja ne samo za određivanje normativnog okvira za prikupljanje elektronskih dokaza i njihovo potonje korišćenje na sudu (ili pred drugim nadležnim organima) već i za uspostavljanje granice između odbrane prava na privatnost korisnika interneta i legitimnog prava (i dužnosti) država da te iste korisnike zaštite u elektronskom okruženju.

Prema Konvenciji[204], nadležni državni organi imaju ovlašćenja da pregledaju i zaplene svaki računar ili nosač podataka na kome se nalaze, ili sumnjaju da se mogu nalaziti inkriminišući materijali, kao i da od provajdera elektronskih komunikacija prikupljaju podatke koji se odnose pre svega na upotrebu Interneta i kreditnih kartica, preko kojih se može doći do podataka o potencijalnom počiniocu krivičnog dela visokotehnološkog kriminala.[205] Jedna od verovatno najdalekosežnijih odredbi tiče se tzv. „presretanja podataka“, odnosno vrste prisluškivanja elektronskih komunikacija (član 21. Konvencije). Do ove mere će doći onda kada je za dokazivanje o postojanju krivičnog dela potrebno imati dokaze sakupljene u realnom vremenu, odnosno u trenutku kada se komunikacija vrši.[206] Ova oblast intervencije državnih organa je i najosetljivija, jer se praktično povređuje pravo na privatnost i pravo na prepisku, a sama Konvencija ne sadrži odgovarajuća ograničenja i garantije da takva prava neće biti zloupotrebljena (osim generalnog ograničenja da se pri izvršenju svih mera moraju poštovati međunarodni standardi ljudskih prava postignuti kroz pomenute međunarodne dokumente). Član 21, koji reguliše presretanje podataka, navodi da će se ova mera preduzeti za „ozbiljna dela“, ali se iz same Konvencije ne može uvideti na koja se dela tačno mislilo, i koje bi karakteristike mogle neko delo odrediti kao ozbiljno. Ovako formulisan, član 21. zapravo ostavlja državama-potpisnicama da same odrede kada će se primenjivati ovakve mere. Kada se posmatraju istrage koje mogu dovesti do jednog ili više izvršilaca krivičnih dela, kao što su dela organizovanog kriminala, terorizam, zlostavljanje dece, ovakva procedura je opravdana i jedina moguća.

---

[204] Tekst o procesnim radnjama i međunarodnoj saradnji preuzet iz: Reljanović Mario, *Konvencija o visokotehnološkom kriminalu Saveta Evrope sa Dodatnim protokolom*, u: Lidija Komlen nIkolić *et alia*, Suzbijanje dela visokotehnološkog kriminala, Beograd, 2009, str. 42-53.

[205] Članovi 19. i 20. Konvencije.

[206] Nasuprot tome je mera zaplene postojećih dokaza koji su ranije snimljeni na računaru ili drugom medijumu za čuvanje i prenos podataka, koju Konvencija takođe predviđa.

Problem je što Konvencija ne poseduje mehanizme zaštite, kako se ona ne bi sprovodila za elektronske komunikacije preko računara i računarskih mreža osoba koje nisu počinioci, niti su pod istragom za vršenje dela visokotehnološkog kriminala, već se mogu naći na udaru vlasti jedne zemlje iz sasvim drugih pobuda, koje veoma često nisu ni pravno utemeljene. Ipak, ne treba previše kritikovati ovo rešenje, obzirom da se radi o međunarodnom instrumentu, koji treba da zaživi kroz legislativu i praksu svake pojedinačne zemlje.[207] Ova odredba, kao i sve ostale odredbe Konvencije koje se tiču procesnog prava, isključivo su usmerene na prikupljanje podataka (u smislu dokaza) u krivičnim istragama ili krivičnom postupku. Konvencija ne predviđe automatsko prikupljanje i snimanje podataka od strane provajdera, koje bi oni mogli po potrebi ustupiti policiji ili drugim nadležnim organima, već samo ciljano sakupljanje nakon što dobiju nalog za tako nešto od organa koji sprovodi istražni ili krivični postupak.

Član 22. Konvencije bavi se nadležnošću države-potpisnice kada dođe do činjenja nekog od krivičnih dela iz Konvencije. Država će imati nadležnost za procesuiranje ukoliko je krivično delo počinjeno na njenoj terotoriji, na brodu ili avionu koji nosi njenu zastavu, kao i ako je krivično delo počinio državljanin te države, pod uslovom da je ono u drugoj državi koja poznaje istu takvu inkriminaciju, ili van državnih teritorija (npr. na slobodnom moru). Može se reći da kombinacija teritorijalno-personalne jurisdikcije nije najsrećnije rešenje, iako je reč o klasičnom instrumentu kada je reč o međunarodnim ugovorima. Ipak, visokotehnološki kriminal izmiče klasičnim obrascima krivičnih dela, pa i krivične nadležnosti, tako da ovakva formulacija ostavlja niz otvorenih pitanja, o čemu će više reči biti kasnije. Situaciju dalje komplikuje stav 2. istog člana, koji omogućava državama da ne primenjuju pravila o nadležnosti u određenim slučajevima ili pod određenim okolnostima. Kao da su i tvorci Konvencije bili svesni slabašnog dometa ovog rešenja, stavovi 3. i 4. pokušavaju da stvari postave na malo čvršćim osnovama – ako država ne izvrši ekstradiciju svog državljanina, mora mu suditi za počinjena dela na teritoriji druge države-potpisnice; takođe, odredbe o nadležnosti države sadržane u Konvenciji neće derogirati odredbe domaćeg prava, prema kojem država može i na neki drugi način uspostaviti svoju krivičnu nadležnost.

Treći deo Konvencije se bavi međunarodnom saradnjom država na suzbijanju visokotehnološkog kriminala, i to pre svega na način koji bi trebao da prevaziđe praktične

[207] Što se u komentaru ovog rešenja izričito i navodi. *Convention on Cybercrime – Explanatory Report*, *loc.cit*, str. 44.

prepreke pri sprovođenju nacionalnog zakonodavstva za krivična dela koja po pravilu prelaze državne granice, a često i podrazumevaju učešće pojedinaca iz nekoliko zemalja širom sveta.[208]

Glavne odredbe ovog dela posvećene su saradnji država na organizovanoj ili spontanoj razmeni podataka koji se tiču eventualnog izvršenja nekog od krivičnih dela vezanih za upotrebu elektronskih komunikacija, kao i mogućnosti ekstradicije počinilaca takvih dela iz jedne države-potpisnice u drugu. Svaka država-potpisnica mora poveriti određenom telu posao saradnje sa drugim državama u oblasti visokotehnološkog kriminala, a u slučaju hitnosti, saradnja može biti uspostavljena i direktno između pravosudnih organa dve države, kao i preko Interpola i drugih relevantnih kanala saradnje, dakle bez dugih procedura koje bi išle preko centralnih vlasti država a koje su predviđene kao pravilo pri saradnji u ovoj oblasti. Prema članu 31. Konvencije, svaka država-potpisnica može tražiti od druge da sprovede određene istražne radnje na svojoj teritoriji, ako je to neophodno za vršenje istrage u vezi sa nekim od dela predviđenih Konvencijom. Ukupno gledano, Konvencija predviđa različite vidove saradnje država, prilagođene tehnologiji vršenja istraga i procesuiranja ove vrste krivičnih dela. Takođe, državama je ostavljeno dosta prostora da u praksi, ili dodatnim bilateralnim sporazumima, dalje preciziraju one vrste saradnje za koje imaju poseban interes.

Kada je o ekstradiciji reč, treba posvetiti pažnju izuzecima – kada država neće biti u obavezi da izruči neko lice. To je pre svega slučaj kada je u pitanju nedostatak dvostruke inkriminacije, ali Konvencija predviđa i dopunski uslov – delo mora biti označeno kao ozbiljno u samom zakonu, odnosno za njegovo izvršenje mora biti zaprećena minimalna kazna od jedne godine zatvora, ako drugačije predviđeno nekim drugim međunarodnim ugovorom između država u pitanju koji se može primeniti na datu situaciju. Takođe, između država koje nemaju međusobne bilateralne ili multilateralne ugovore o ekstradiciji, Konvencija će služiti kao osnov za ekstradiciju.

5.3.2 ELEKTRONSKI DOKAZI[209]

Elektronski dokazi počeli su da se pojavljuju u sudskim i drugim postupcima uporedo sa povećanjem značaja elektronskih tehnologija, naročito računara, u svakodnevnoj komunikaciji i poslovanju, kao i sa naglim razvoj visokotehnološkog kriminala. Npr. donošenjem Zakona o

[208]Članovi 23-35. Konvencije.
[209] Videti: Prlja Dragan, Reljanović Mario, *Pravna informatika, op.cit*, str. 65-70.

elektronskom potpisu[210] u Srbiji je otvorena mogućnost da se komunikacija vrši putem tzv. elektronskog dokumenta, koji se definiše kao „dokument u elektronskom obliku koji se koristi u pravnim poslovima i drugim pravnim radnjama, kao i u upravnom, sudskom i drugom postupku pred državnim organom“. Obzirom da ovakvi dokumenti imaju snagu javne isprave, logično je očekivati da će se pojavljivati u većoj meri u različitim postupcima pred državnim organima. I više od toga, Zakonom o elektronskoj trgovini[211] stvorene su pretpostavke pružanja usluga zaključenjem ugovora u elektronskoj formi. Danas gotovo sva nacionalna zakonodavstva poznaju pojam elektronskog ili digitalnog dokaza, i imaju određena pravila koja regulišu načine na koje se elektronski podaci, odnosno dokumenti, mogu upotrebiti kao dokazna sredstva.

Zakonom o elektronskom dokumentu[212], elektronski dokument se definiše kao skup podataka sastavljen od slova, brojeva, simbola, grafičkih, zvučnih i video zapisa sadržanih u podnesku, pismenu, rešenju, ispravi ili bilo kom drugom aktu koji sačine pravna i fizička lica ili organi vlasti radi korišćenja u pravnom prometu ili u upravnom, sudskom ili drugom postupku pred organima vlasti, ako je elektronski izrađen, digitalizovan, poslat, primljen, sačuvan ili arhiviran na elektronskom, magnetnom, optičkom ili drugom mediju. Članom 4. istog Zakona propisano je da se elektronskom dokumentu ne može se osporiti punovažnost ili *dokazna snaga* samo zato što je u elektronskom obliku. Zakonik o krivičnom postupku takođe predviđa mogućnost prikupljanja elektronskih dokaza[213]. I domaća i strana doktrina je zauzela stav prema kojem elektronski dokazi imaju snagu jednaku bilo kojoj drugoj vrsti dokaznih sredstava.[214]

---

[210] Službeni glasnik RS, 135/2004.
[211] Službeni glasnik RS, 41/09.
[212] Službeni glasnik RS, 51/09.
[213] Član 22. ZKP.
[214] Videti npr. Banović Božidar, *Elektronski dokazi*, Revija za kriminologiju i krivično pravo, br. 3/2006, str. 223-231. Prlja i Savović navode i niz stranih autora koji imaju isti stav povodom prihvatljivosti elektronskih dokaza na sudu: Rice Paul R, *Electronic Evidence: Law and Practice*, ABA Section of Litigation 2005; Siemer Deanne C, Rothschild Frank D., Bocchino Anthony J., and BeskindDonald H., *Effective Use of Courtroom Technology: A Lawyer's Guide to Pretrial and Trial* (2002); *Developments in the Law: Electronic Discovery*, 38 Loyola L.A. L. Rev. 1745 (2005); Anderson, G. Ross Jr., *Computer Animation: Admissibility and Uses*, South Carolina Trial Lawyer Bulletin 9 (Fall 1995); J. Shane Givens, *Comment, The Admissibility of Electronic Evidence at Trial: Courtroom Admissibility Standards*, 34 Cumb. L. Rev. 95 (2003-2004); Andrew M Grossman, *No, Don't IM Me— Instant Messaging, Authentication, and the Best Evidence Rule*, 13 Geo. Mason L. Rev. 1309 (2006); Gregory P. Joseph, *A Simplified Approach to Computer-Generated Evidence and Animations*, 156 F.R.D. 327, 335-37 (1994); Listrom Linda L, Harlan Eric R, Ferguson Elizabeth H, Redis Robert M., *The Next Frontier: Admissibility of Electronic Evidence,* ABA, Summer 2007.. Navedeno prema: Prlja Dragan,.Savović Miodrag, *E-mail kao dokazno sredstvo u uporednom pravu*, Strani pravni život 2/2009, str. 82.

Elektronski dokaz je svaki elektronski zapis koji je nastao na računaru ili sličnom uređaju, od strane čoveka ili je automatski generisan, a koji može služiti u dokaznom postupku pred sudom ili drugim državnim organima. Kraće rečeno, to je *informacija koja ima dokaznu snagu a koja je pohranjena ili preneta u elektronskoj formi.*[215] Ovako široko određen pojam elektronskog dokaza je logična posledica njihove moguće raznovrsnosti, ali u svakom slučaju ne utiče na ukupnu percepciju istih, kao ni na njihovo razlikovanje od nekih drugih vrsta dokaza. Elektronski dokazi su specifični po tome što sudu ili drugom organu pred kojim se vodi postupak, mogu biti predstavljeni i u ne-elektronskoj formi. Npr, e-mail komunikacija se može predstaviti u „originalnoj" formi, putem računara ili nosača/čitača elektronskih podataka, ali se takođe može izvesti i u papirnoj formi – odštampana elektronska pošta.

Elektronski dokazi su prihvaćeni od srpskih sudova ravnopravno sa ostalim vrstama dokaza[216], i nema nikakve zakonske ili praktične prepreke da u svim postupcima pred državnim organima oni zauzmu istu poziciju.

Cilj sakupljanja dokaza u sudskom ili drugom postupku jeste pravično odlučivanje o predmetu postupka, odnosno „utvrđivanje svih činjenica i okolnosti koje mogu biti od uticaja na rešavanje konkretne stvari"[217]. Elektronski dokazi se u tom smislu ne razlikuju prema svojoj svrsi, pa samim tim ni prema načinu izvođenja i upotrebe u različitim postupcima. Pravila koja važe za ostale, „obične" dokaze, primenjivaće se shodno i na elektronske dokaze. Elektronski dokazi se ipak razlikuju od klasičnih dokaznih sredstava po nekoliko karakteristika koje su posledica njihove prirode. Najpre, oni nastaju u prostoru elektronskih komunikacija i elektronskih podataka: svaki elektronski podatak je niz jedinica i nula, koje kreiraju smislene podatke koje korisnik koristi; potom, ovaj prostor nije precizno definisan, niti teorijski ni u praksi – može se lako dogoditi da pojedini dokazi budu tako dobro skriveni da se ni pored najboljih alata i znanja ne mogu otkriti; delo VTK dakle realno može proći nekažnjeno, ali čak i neopaženo – žrtva ili žrtve nekog dela visokotehnološkog kriminala uopšte ne moraju biti svesne da se to delo dogodilo.

---

[215]Scientific Working Group on Digital Evidence (SWGDE),*Digital Evidence: Standards and Principles*,Forensic Science Communications, Vol. 2, 2/2000, str. 1.

[216]Videti npr. slučajeve K 1930/05 pred Okružnim sudom u Beogradu i K 1782/07 pred Drugim opštinskim sudom u Beogradu.

[217]Prlja Dragan, Savović Miodrag,*E-mail kao dokazno sredstvo u uporednom pravu*, Strani pravni život 2/2009, str. 71.

Zbog toga se elektronski podaci po pravilu prikupljaju od strane specijalizovanih organa ili jedinica policije, koje poseduju posebne softverske i hardverske alate za njihovo pretraživanje i prikupljanje. Prilikom izvođenja ovih istražnih radnji, moguće je primeniti jednu od dve raspoložive tehnike: kopiranje ili kloniranje elektronskih podataka.

Kopiranje podataka predstavlja repliciranje nekog elektronskog fajla sa jednog računara na drugi, odnosno sa jednog nosača podataka na drugi. Kopiranje podataka je operacija sa kojom se svaki korisnik računara svakodnevno susreće, kroz uobičajene *copy&paste* komande. Kopiranje podataka ne mora uvek da bude garantija da je njihova pretraga sprovedena detaljno i kvalitetno, odnosno da su svi elektronski fajlovi prebačeni na pravilan način; još manje može biti garantija da neće doći do korupcije dokaza, odnosno njihove izmene prilikom kopiranja. Ovo se pre svega odnosi na tehničke izmene sadržaja samog dokumenta, koji nakon toga može postati na neki način „drugačiji“, odnosno različit od originala, a u mnogim slučajevima i potpuno neupotrebljiv. Ovo se pre svega dešava zato što osim elektronskih fajlova koje vidimo, postoje i „nevidljivi“ fajlovi. Oni mogu uticati na pokretanje, odnosno nepokretanje ili potpuni gubitak sadržine nekog kopiranog fajla. Npr. ukoliko postoji programski fajl .exe ekstenzije na računaru koji se pregleda, on se ne mora nužno pokrenuti nakon kopiranja na drugi računar, jer su na izvornom računaru ostali drugi fajlovi koji su imali svrhu da „pomognu“ pravilno pokretanje glavnog fajla. Ovi drugi, pomoćni podaci, mogu biti smešteni u fajlovima operativnog sistema računara, mogu biti nevidljivi po svojoj prirodi, ili još češće, namerno sakriveni od strane autora, odnosno korisnika programa. Takođe, svaka aplikacija koja je napravljena kao baza podataka ima korisnički interfejs koji je vidljiv, dok se sve informacije „povlače“ iz fajlova koji mogu biti smešteni u bilo kom delu memorije računara ili drugog uređaja. Mehaničkim kopiranjem bi se u ovom slučaju prebacila samo „ljuštura“, dok bi korisni (suštinski) podaci ostali samo na izvornom računaru, ili drugom nosaču elektronskih podataka. Iz ovih razloga se pribegava *kloniranju podataka*, koje je znatno delikatnije i zahtevnije, kako tehnički tako i vremenski. Kloniranju podataka mogu pristupiti samo specijalno obučena lica koja poseduju posebne alate za njegovo izvođenje. Klonirati neki sadržaj znači napraviti njegovu potpunu repliku, zajedno sa svim elementima koji se pri kopiranju ne bi videli, odnosno ne bi preneli na kopiju. Njime se dakle postiže potpuna istovetnost originala i „klona“.

Tokom vremena, a naročito u poslednjoj deceniji, razvila se dobra praksa prikupljanja elektronskih podataka, na osnovu uporednih iskustava i iskustvu specijalizovanih pravosudnih i

policijskih organa Srbije koji se bave procesuiranjem i suzbijanjem visokotehnološkog kriminala. Da bi se razumeo ceo proces prikupljanja elektronskih informacija i stvaranja elektronskih dokaza, on se mora raščlaniti na pojedine faze. Da li će u konkretnom slučaju zaista doći do svih navedenih aktivnosti, zavisi od prirode dokaza za kojima se traga, njihovog obima, kao i okolnosti koje su specifične za taj slučaj. Celokupan proces se dakle može podeliti na sledeće faze: 1) priprema istražnog postupka u delu prikupljanja elektronskih podataka; 2) pristupanje računaru ili drugom uređaju u toku istražnog postupka; 3) kopiranje određenih elektronskih podataka i/ili privremeno oduzimanje računara ili drugog uređaja; 4) kopiranje ili kloniranje (ukoliko nije izvršeno u prethodnoj fazi) elektronskih podataka sa privremeno oduzetog računara ili drugog uređaja; 5) analiza prikupljenih elektronskih podataka; 6) zahtevi za dostavljanje sekundarnih elektronskih podataka i njihova analiza; 7) oformljavanje elektronskih dokaza na osnovu prikupljenih elektronskih podataka; 8) izlaganje elektronskih dokaza u postupku i/ili veštačenje.

Priprema istražnog postupka svodi se na analizu dostupnih podataka o predmetu, odnosno predmetima koji su kao potencijalni dokazi cilj vršenja istražnih radnji. Pretpostavka je da istražni organ ne može unapred znati na koje će se računare i ostale uređaje naići prilikom sprovođenja istražnih ovlašćenja; međutim, mora se unapred napraviti okvirni plan – na osnovu okolnosti slučaja – koja bi dokumenta, komunikacija i sl. elektronski podaci mogli biti od značaja za sam postupak.

Pre pristupanja prikupljanju podataka i njihovoj analizi, trebalo bi *identifikovati računare i druge uređaje* koji se mogu okarakterisati kao relevantni za pretraživanje elektronskih podataka. Ovo je sasvim logičan sled događaja; pri tome, istražni organ ne mora nužno biti ograničen planom koji je prethodno napravio, već ga modifikuje na licu mesta na osnovu novih saznanja do kojih eventualno može doći. Potom se donosi odluka da li će se pristupiti zapleni računara i drugih uređaja. Kada se tačno zna koji se podaci traže i kada je evidentno da se oni mogu kopirati i kao takvi koristiti u daljem postupku, pristupiće se njihovom kopiranju a računari ili drugi uređaji će se oduzeti samo ukoliko bi dalje zadržavanje takvih elektronskih podataka za stranku značilo mogućnost produžavanja protivpravnog delovanja. Odluka da li će pristupiti zapleni ili ne je dakle usko povezana sa odlukom *da li će se pristupiti kopiranju ili kloniranju*.

Bez obzira da li je u pitanju kopiranje ili kloniranje, prilikom rada na računaru ili drugom uređaju mora se postupati sa krajnjim oprezom. Ukoliko se donese odluka da se podaci kloniraju,

to bi trebalo uraditi nakon što se računar ili drugi uređaj privremeno oduzme; pretraživanje podataka na mestu uviđaja nije preporučljivo – trebalo bi proceniti koji računari i drugi uređaji mogu biti privremeno oduzeti i potom pretraženi u forenzičkoj laboratoriji; najbolje rešenje jeste da se svaki uređaj na licu mesta blokira posebnim alatima. Razlozi za ovakav stepen opreza leže u činjenici da se lice čiji se podaci pregledaju može odlučiti da na neki od prethodno pripremljenih ili *ad hoc* smišljenih načina, neke od elektronskih podataka uništi. Ovo se može izvršiti na jako veliki broj načina, napomenućemo samo neke od najčešćih: prilikom uključivanja računara u struju, ili njegovog priključenja na mrežu, aktivira se softver za brisanje podataka; prilikom gašenja računara, pokreće se softver za brisanje podataka (otuda bi se računar ili drugi uređaj morao gasiti direktnim izvlačenjem strujnog kabla, uz prethodnu proveru da li postoji neki pomoćni izvor napajanja)[218]; prilikom unosa odgovarajuće lozinke (šifre) da bi se otvorio zaštićeni fajl, aktivira se njegovo uništenje; uništenje podataka se vrši preko Interneta, lokalne ili druge mreže na koju je računar povezan, dok rukovalac računarom toga ne mora ni biti svestan. Svaki od navedenih, kao i neki drugi načini uništenja elektronskih podataka, mogu se dogoditi i aktiviranjem softvera za uništenje nakon određenog vremena; na taj način se može dogoditi da sadržaj podataka na računaru ili drugom uređaju ne bude isti na mestu uviđaja i na mestu njihovog kloniranja, pretraživanja ili analiziranja, ukoliko je došlo do privremenog oduzimanja stvari – ovaj problem se rešava tzv. blokatorima, posebnim alatima IT forenzike.

Pretraživanje i analiza prikupljenih elektronskih podataka su aktivnosti koje su direktno povezane sa izborom načina sprovođenja postupka prikupljanja elektronskih podataka. Ukoliko se prikupljanje podataka vrši na mestu uviđaja, na istom mestu će se izvršiti i njihovo pretraživanje i analiza. Ovo se događa samo kada se ciljano traga samo za specifičnim podacima. Ako to nije slučaj i pretraživanje se vrši na kopiji/klonu u IT laboratoriji sa ciljem da se ispitaju svi sumnjivi podaci, lica koja vrše pretragu imaju znatno obimniji posao ali i više vremena i olakšavajuću okolnost da rade na podacima koji predstavljaju repliku originala. Analiza nekog podatka se svodi na iznalaženje odgovora na sledeća pitanja: da li je podatak od značaja za postupak; da li je u pitanju privatni podatak, tajni podatak ili drugi podatak za čiju analizu i upotrebu postoje zakonska ograničenja; da li je potrebno pronaći i sekundarne podatke kako bi se

[218]Videti npr. detaljnije uputstvo za pripadnike policije: *Criminal Enforcement Command, Computer Crimes Unit*, Maryland State Police, Internet adresa: http://ccu.mdsp.org/home.htm, 01.08.2010.

elektronski podatak oformio kao elektronski dokaz[219], kao i gde se oni nalaze; koja metoda oformljenja i izlaganja budućeg elektronskog dokaza u kasnijem postupku najviše odgovara prirodi elektronskog podatka u pitanju.

Za razliku od „običnih" dokaza, elektronski dokazi prolaze dvostruku proveru u postupku – jedna je provera njihove oformljenosti, a druga je ocena njihove dokazne snage. Oformiti elektronski dokaz od postojećih elektronskih podataka znači povezati sve činjenice koje se tiču nastanka elektronskih podataka, njihove validnosti i povezanosti (relevantnosti) za konkretan slučaj. Elektronski dokaz se npr. može oformiti tako što će se uz sadržinu mejla – elektronske komunikacije – pridodati i svi sekundarni dokazi (uz potvrdu njihove autentičnosti) koji potvrđuju kome mejl nalog pripada i nedvosmisleno dokazuju da je mejl poslat sa odgovarajućeg računara i određeno vreme. Dalje, uz ove činjenice moraju se pridodati i zapisnici i potvrde da je računar u pitanju privremeno oduzet, kloniran, da je izvršena forenzička analiza kloniranih podataka i da je potvrđeno da je to računar koji je nosio istu IP adresu sa koje je mejl poslat u vreme kada je poslat. Na taj način je oformljen elektronski dokaz koji povezuje tri tačke – računar – sadržinu komunikacije – tehničke detalje komunikacije i na taj način opredeljuje osobu koja je komunikaciju izvršila. U zavisnosti od okolnosti, oformljavanje elektronskih dokaza može biti i znatno jednostavnije.

Konačni cilj cele operacije sakupljanja i analize elektronskih podataka i stvaranja elektronskih dokaza, jeste njihovo prezentovanje u dokaznom postupku. Ono se može ostvariti na više načina, ali je osnovna razlika u tome da li se vrši njihovo veštačenje ili samo ocena na osnovu pregleda istih, kao i da li su oni pogodni da se prezentuju u papirnoj formi (odštampani) ili u originalnoj – elektronskoj formi na računaru ili drugom uređaju.

---

[219]Sekundarni elektronski podaci su zapravo elektronski podaci nastali kao proizvod obavljene elektronske komunikacije: to su IP adrese, vremena obavljanja Internet komunikacija, lokacija računara sa kojeg je komunikacija obavljena, itd. Neki od njih se mogu nalaziti na samom računaru; neki će biti dostupni kod provajdera odgovarajuće usluge; velika je verovatnoća da se neki mogu nalaziti i u inostranstvu. Oni su potrebni kako bi se kompletirala slika koju potencijalno pruža neki elektronski podatak. Npr, elektronska pošta koja je poslata sa neke opšte mejl adrese, sačinjene tako da se ne može vezati za određenu osobu ili preduzeće, može poslužiti kao elektronski dokaz samo ukoliko se preko drugih podataka poveže sa strankom ili odgovarajućom osobom; u našem primeru, ako je komunikacija bila sa adrese *ime.prezime@1234.com*, a pod pretpostavkom da je sadržina tog mejla nađena na nosaču elektronskih informacijama koji može ali ne mora pripadati direktoru preduzeća, pomoću sekundarnih podataka može se npr. dokazati da IP adresa pošiljaoca, vreme i fizička lokacija računara sa kojeg je mejl poslat zaista pripada tom direktoru. Ponekad se ovakva vrsta dokaza ne mora tražiti od samog provajdera, već se može naći i kod administratora lokalne mreže u preduzeću.

6. ZAKLJUČAK

Stvaranje nove digitalne zajednice neprekidnim povećavanjem brojem korisnika interenta neumitno je uslovilo enermni rast digitalnih informacija u svim oblicima. Ova pojava uzdrmala je tradicionalne koncepte u gotovo svim oblastima života i rada i nametnula je potrebu traženja novih rešenja. Neke od tih oblasti svakako su i oblasti intelektualne svojine, autorskih prava, zaštite podataka i privatnosti, elektronskog poslovanja i visokotehnološkog kriminala.

Neograničena dostupnost književnih dela, naučnih radova, muzičkih radova, video radova, i drugih autorskih dela u digitalnom obliku uzdrmala je iz temelja tradicionalni koncept autorskih prava. Potreba zaštite autorskih prava i želja izdavača da što efikasnije zaštite digitalna autorska dela u potpunosti je u suprotnosti sa željom velikog broj članova digitalne zajednice da slobodno razmenjuju znanje i kreativne resurse koji čine opšte kulturno i intelektualno nasleđa čovečanstva. Niz pokušaja traženja pravog rešenja ponudio je kao jedno od mogućih rešenja stvaranje licenci otvorenog sadržaja koje nude autorima mogućnost odlučivanja u kojoj meri će svoja dela učiniti dostupnim ostatku digitalne zajednice. Na ovaj način ogromna riznica znanja dostpunog u digitalnom obliku postaje i dalje svakoga dana sve veća, ali su jasno povučene granice u koju se svrhu određeno autorsko delo može koristiti, a u koju ne. Ovako se otklanjaju dileme oko pravnih posledica koje mogu nastupiti korišćenjem nekog autorskog dela. Najbolji primer ove vrste licenci su "Licence kreativne zajednice" koje danas prihvata ogroman broj autora i institucija u najvećem broju zemalja sveta. Ove licence su pravi primer dobrih rešenja u oblasti ostvarivanja sloboda i prava u digitalnoj zajednici. Digitalna zajednica danas je zajednica kreativnih ljudi, zajednica stvaralaca jednog jedinstvenog resursa ljudskog znanja. Ovaj jedinstveni resurs svakoga dana je sve bogatiji i dostupan je svima pod jednakim uslovima kao moćna osnova za dalju kreativnost i stvaralaštvo.

U sajber prosturu danas se nalazi ogromna količina podataka o građanima koje stvaraju sami građani, razne državne i nedržavne institucije. Raspolaganje tim podacima, odnosno njihova svakodnevna zloupotreba mora biti predmet pravnog regulisanja. Izučavanje zaštite podataka na internetu može obuhvatiti i zakonska rešenja koja se tiču postojanja određenih organa koja se staraju o primeni propisa o zaštiti podataka. Podaci o kojima je ovde reč mogu biti kako podaci o

ličnosti, tako i podaci koji se odnose na funkcionisanje pravnih lica ili državnih organa i institucija, a zaštita podrazumeva dvostruku aktivnost: sa jedne strane, ne smeju se učiniti javnim podaci koji nisu kao takvi određeni propisima; sa druge strane, to je problem obezbeđivanja integriteta računara i računarskih sistema u kojima se nalaze podaci koji su postavljeni na internet u nekom restriktivnom obliku (za strogo određeni broj korisnika koji imaju interes da u njih imaju uvid i sa njima dalje raspolažu). Pored regulisanjem zaštite privatnosti i podataka neophodno je posebnu pažnju dati području bezbednosti računarskih sistema i računarskih mreža, odnosno bezbednosti svih korisnika računara koji pristupaju sajber prostoru.

Danas se moderno poslovanje i ne može zamisliti bez poslovanja u sajber prostoru. Najveći rast upravo beleži broj elektronskih transakcija u sajber prostoru, a granica poslovanja se proširuju na robe i usluge koje do pojave ovog tip poslovanja nisu ni postojale. Ekspanzija elektronskog poslovanja otvorila je niz novih pitanja koja je trebalo pravno regulisati. Sklapanje elektronskih ugovora zahtevalo je precizno definisanje utvrđivanja verodostojnosti elektronskih poruka i autentičnosti elektronskih komunikacija, a takođe je zahtevalo i definisanje procesnih pravila pri sklapanju elektronskih ugovora. Mnogobrojne zloupotrebe elektronskih podataka, lažno predstavljanje na internetu, elektronske prevare, elektronske sabotaže, unošenje virusa u računarske sisteme,neovlašćeno menjanje elektronskih podataka, linkovanje bez predhodne dozvole, i mnoge druge nedozvoljene radnje prilikom elektronske trgovine zahtevale su da bude pravno regulisane. Neisporučivanje naručenih dobara preko mreže, nedovoljan kvalitet isporučene robe, i mnogi drugi načini nanošenja štete potrošačima pri elektronskom poslovanju zahtevali su da pravne norme na najbolji mogući način zaštite sve veći broj potrošača koji robe nabavljaju putem virtuelnih prodavnica, a plaćanja vrše elektronskim putem. Posebno značajna pitanja su zaštite patenata, poslovnih tajni, pitanja plaćanja poreza i pitanja nadležnosti prilikom vođenja sporova, a naravno i ona su pravno regulisana u okviru nacionalnih zakonodavstava, kao i na međunarodnom nivou.

Stotine milona ljudi koji svakodnevno koriste sajber prostor za poslovnu ili ličnu upotrebu često nemaju dovoljno pažnje, vremena ili volje da se valjano zaštite i upoznaju sa mogućim neprilikama koje ih mogu zadesiti ako lakoverno ili nedovoljno ozbiljno ulaze u različite vrste transakcija ili komunikacija. Činjenica je da se mnoga klasična krivična dela mogu počiniti na internetu, kao i da se pribavljanjem informacija o korisnicima može pripremiti ili omogućiti izvršenje gotovo svih krivičnih dela protiv života i fizičkog integriteta, imovine, autorskih prava,

kao i mnoga druga. Pored njih, postoje i krivična dela čiji su pojava i razvoj vezani isključivo za razvoj elektronskih komunikacija i interneta. Reč je o širokoj paleti ponašanja koja mogu biti i bezazlena, ali mogu voditi i najtežim krivičnim delima. Sva ova nedozvoljen ponašanja obuhvaćena su definisanjem novih krivičnih dela koja prati niz procesnih i forenzičkih specifičnosti. nacionalna zakonodavstva su morala da budu inovirana kako bi se nove situacije pravno regulisale. Naravno do sada postignuti nivo pravne regulative krivičnih dela visokotehnološkog kriminala sigurno nije konačan, već nas u narednom periodu očekuju dalja prilagođavanja u skladu sa razvojem situacije u sajber prostoru.

Sve rečeno u ovoj knjizi svakako može da predstavlja doprinos istraživanju pravnih problema u okviru sajber prostora, a trebalo bi svakako i da predstavlja podsticaj novim istraživanjima u ovoj oblasti.

7. LITERATURA

Aplin Tanya, *Copyright Law in the Digital Society: The Chalenges of Multimedia*, 2005.

Bainbridge David, *Introduction to Computer Law*, Longman, 2000.

Banović Božidar, *Elektronski dokazi*, Revija za kriminologiju i krivično pravo, br. 3/2006.

Bjelić Predrag, *Elektronsko trgovanje – elektronsko poslovanje u međunarodnoj trgovini*, Beograd, Institut za međunarodnu trgovinu i privredu, 2000.

Čok Vida, Lilić Stevan, Vranjanac Dušan, *Zaštita ličnih podataka u kompjuterizovanim informacionim sistemima - Komparativno-pravna analiza,* naučno-istraživački projekt, Institut za uporedio pravo, Beograd, 1987.

David Bainbridge, *Introduction to Computer Law*, Pearson Education Limited, London, 2000.

Dimitrijević Predrag, *Pravo informacione tehnologije*, SVEN, Niš, 2010.

Dimitrijević, Predrag, *Pravo informacione tehnologije - osnovi kompjuterskog prava*, SVEN, Niš, 2009.

Drakulić Mirjana i Drakulić Ratimir, *Pravna regulacija e-poslovanja*, Internet adresa: http://www.e-trgovina.co.yu/pravo/regulacija1.html, 17.08.2009.

Drakulić Mirjana, *Osnovi kompjuterskog prava*, DOPIS, Beograd, 1996.

Drozdova Ekatarina A, *Civil Liberties and Security in Cyberspace*, u: Abraham D.Sofaer, Seymour E.Goodman (ed.), *The Transnational Dimension of Cyber Crime and Terrorism*, Hoover Press, 2001.

Dworkin Gerald, *Judical Control of Copyright on Public Policy Grounds,* in: Inellectual Property and Information Law, Kluwer, 1998.

Efroni Zohar, Access – right : the future of copyright law, Oxford University Press, 2011.

Gerke, M i dr., *Priručnik za istragu krivičnih dela u oblasti VTK, Savet Evrope, 2008.*

Jehoram Tobias Cohen, *Copyright in Non-Orginal Wrutings Past - Present - Future ?*, in: Inellectual Property and Information Law, Kluwer, 1998.

Jelić Ivan, *Zajednica u savremenom informatičkom društvu*, 2006, Internet adresa: http://www.bos.rs/cepit/idrustvo2/tema14/zajednica.pdf.

Kabel Jan, *Inellectual Property and Information Law,* Kluwer, 1998.

Komlen-Nikolić Lidija et alia, *Suzbijanje visokotehnološkog kriminala*, Beograd, 2010.

Koumantas Georges, *Reflections on the Concept of Intellectual Property*, in: Inellectual Property and Information Law, Kluwer, 1998.

Krebs Brian, *Year of Computing Dangerously*, Washington Post, 22.12.2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/12/22/ AR2006122200367.html.

Lawrence Liang, *Guide to Open Content Licenses*, 2004, Internet adresa: http://media.opencultures. net/open_content_guide/ocl_v1.2.pdf.

Listrom Linda L, Harlan Eric R, Ferguson Elizabeth H, Redis Robert M., *The Next Frontier: Admissibility of Electronic Evidence,* ABA, Summer 2007.

Litman Jessica, *Digital copyright: protecting intellectual property on the Internet*, Prometheus Books, 2001.

Maisl Herbert, Etat de la Legislation Française et Tendences de la Jurisprudence Relatives à la Protection des donnees Personnalles, Revue Internationale de Droit Comparé, No. 3, 1987.

Mandić Damir, Planojević Nina, Tijanić Mihajlo, *Legal protection of copyright works that apper in web based application,* In: Selected topics in applied computing / Applied computing conference *2010 (ACC'10). - Timisoara : Politehnica University, 2010. Internet adresa:* http://www.wseas.us/e-library/conferences/ 2010/TimisoaraP/ACC/ACC-21.pdf.

National Research Council (US), *The digital dilemma: intellectual property in the information age*, National Academic, 2000.

Overbeck Wayne, Genelle Belmas, *Major principles of media law*, Stamford: Cengage Learning, 2011.

Prlja Dragan, Ivanović Zvonimir, Reljanović Mario, *Krivična dela visokotehnološkog kriminala*, Institut za uporedno pravo, Beograd, 2011.

Prlja Dragan, Reljanović Mario, *Pravna informatika*, Beograd, Službeni glasnik, 2010.

Prlja Dragan, Reljanović Mario, *Visokotehnološki kriminal – uporedna iskustva*, Strani pravni život 3/2009.

Prlja Dragan, Savović Miodrag, *E-mail kao dokazno sredstvo u uporednom pravu*, Strani pravni život 2/2009, str. 71.

Rakić Vodinelić Vesna, *Opasne pravne posledice ACTA*, Internet adresa: http://pescanik.net/ 2012/02/opasne-pravne-posledice-acta/.

Reljanović Mario, *Konvencija o visokotehnološkom kriminalu Saveta Evrope sa Dodatnim protokolom*, u: Lidija Komlen nIkolić *et alia*, Suzbijanje dela visokotehnološkog kriminala, Beograd, 2009.

Reljanović Mario, *Odnos prava na privatnost i pojedinih aspekata visokotehnološkog kriminala*, u: Komlen-Nikolić Lidija et alia, *Suzbijanje visokotehnološkog kriminala*, Beograd, 2010.

Reljanović Mario, *Visokotehnološki kriminal – pojam, regulativa, iskustva*, Strani pravni život 3/2007

Rice Paul R, *Electronic Evidence: Law and Practice*, ABA Section of Litigation 2005.

Rimmer Matthew, *Digital copyright and the consumer revolution: hands off ma iPod*, Edward Elgar, 2007.

Schafer Arthur, *Privacy - A Philosophical Overview*, *Aspects of Privacy Law*, Edited by Dale Gibson, Toronto, 1980.

Sidhartha Roy, *Cyber Crimes*, http://www.articlesbase.com/cyber-law-articles/cyber-crimes-539363.html.

Spasić Vidoje, *Autorska dela u digitalnom okruženju*, Pravni fakultet Niš, 2011.

Stamotoudi Irini, *Copyright Enforcement and the Internet*, Kluwer, 2010.

Stokes Simon, *Digital Copyright : Law and Practice*, 2005.

Vaidhyanathan Siva, *Copyrights and copywrongs: the rise of intellectual property and how it threatens*, NYU Press, 2003.

Van Duyn J. A., *The Human Factor in Computer Crime*, Los Angeles, 1985.

Warren Samuel, Brandais Louis, *The Right to be Left Alone*, Harvard Law Review, 1890.

CIP

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

004.738.5:34

ПРЉА, Драган, 1959-
Internet pravo / Dragan Prlja, Mario Reljanović, Zvonimir Ivanović. - Beograd : Institut za uporedno pravo, 2012 (Beograd : Kum). - 159 str. ; 21 cm

Tiraž 300. - Napomene i bibliografske reference uz tekst. - Bibliografija: str. 156-158.

ISBN 978-86-80059-83-9
1. Рељановић, Марио, 1977- [аутор] 2. Ивановић, Звонимир, 1976- [аутор]
а) Право - Интернет
COBISS.SR-ID 193944844