Univerzitet Singidunum



Žaklina Spalević

PRAVNI ASPEKTI SAJBER PROSTORA

Beograd, 2020.

UNIVERZITET SINGIDUNUM

Žaklina Spalević

PRAVNI ASPEKTI SAJBER PROSTORA

Drugo izdanje

Beograd, 2020.

PRAVNI ASPEKTI SAJBER PROSTORA

Autor:
dr Žaklina Spalević

Recenzenti:
dr Miodrag Mićović
dr Dragana Kolarić
dr Milan Palević
dr Zoran Miladinović
dr Mladen Veinović

Izdavač:
UNIVERZITET SINGIDUNUM
Beograd, Danijelova 32
www.singidunum.ac.rs

Za izdavača:
dr Milovan Stanišić

Priprema za štampu:
Jelena Petrović

Dizajn korica:
Aleksandar Mihajlović

Godina izdanja:
2020.

Tiraž:
900

Štampa:
Caligraph, Beograd

ISBN: 978-86-7912-676-4

Copyright:
© 2020. Univerzitet Singidunum
Izdavač zadržava sva prava.
Reprodukcija pojedinih delova ili celine ove publikacije nije dozvoljena.

Sadržaj

1 Uvod 1
2 Pravo intelektualne svojine u Cyber prostoru 8
2.1 Principi intelektualne svojine i autorskog prava 9
2.2 Autorsko pravo i autorskom pravu srodna prava 11
2.3 Nosioci autorskih i srodnih prava 14
2.4 Kršenje autorskih prava u cyber prostoru 15
2.5 Javno vlasništvo intelektualne svojine 19
2.6 Licence otvorenog sadržaja i licence kreativne zajednice 21
2.7 ACTA (Anti - Counterfeiting Trade Agreement) multilateralni sporazum ... 25
2.8 Audio-vizuelna dela u cyber prostoru 28
2.9 Autorska prava i internet domeni 29
2.10 Krivična dela oštećenja i krađe intelektualne svojine u Zakonodavstvu Srbije 35
3 Elektronsko poslovanje u Cyber prostoru 38
3.1 Elektronski ugovori 42
3.2 Elektronske fakture 46
3.3 Zaštita elektronskih dokumenata, ugovora i faktura 48
3.4 Elektronska trgovina 60
3.5 Elektronsko bankarstvo 73
3.6 Mobilno bankarstvo 79
3.7 Kriptovalute 85
3.8 Otkrivanje prevara u elektronskom poslovanju uz pomoć digitalne forenzike 90
4 Servisi elektronske vlade u službi građana 98
4.1 Koncepti i primena elektronske demokratije 100
4.1.1 Elektronsko glasanje (e-glasanje) 102
4.1.2 Elektronska participacija (e-participacija) 110
4.2 Elektronska uprava (e-Uprava) 112
5 Elektronski servisi u službi vlade i građana 126
5.1 Elektronski nadzor osuđenika 127

5.2 Elektronsko praćenje poštanskih usluga 134
5.3 Elektronski servisi u turizmu 138
5.4 Sistemi nadgledanja saobraćaja....144
5.5 Servisi e-vlade u borbi protiv terorizma....150
6 Kriminalne aktivnosti bazirane na informaciono komunikacionim tehnologijama 154
6.1 Cyber kriminal kao globalna pretnja svetskom poretku....157
6.1.1 Cyber ratovanje i cyber oružje 160
6.1.2 Dark web 164
6.2 Ilegalne aktivnosti u cyber prostoru....167
6.3 Pravna regulativa na polju cyber ratovanja....177
6.4 Analiza kaznenog zakonodavstva za kompjuterski i cyber kriminal 183
6.4.1 Konvencija Saveta Evrope o cyber kriminalu....183
6.4.2 Kazneno pravno zakonodavstvo cyber kriminala u Nemačkoj 184
6.4.3 Kazneno pravno zakonodavstvo cyber kriminala u Austriji 185
6.4.4 Kazneno pravno zakonodavstvo cyber kriminala u Francuskoj 186
6.4.5 Kazneno pravno zakonodavstvo cyber kriminala u Republici Srbiji ...189
6.4.6 Kazneno pravno zakonodavstvo cyber kriminala u bivšim Jugoslovenskim republikama 192
7 Opasnost upotrebe cyber prostora od strane mladih....196
8 Zaključak 206
9 Literatura....210
10 Indeks pojmova....228

1
Uvod

Tokom istorijskog razvoja i napretka društva novi pronalasci kao i nove tehnologije vrlo često su na samom početku svoj postanka uzimane sa rezervom. Tačnije u svakome od nas postoji doza odbojnosti prema nečemu što je novo i čije usvajanje i primena u svakodnevnom životu i radu može dovesti do remećanja već uspostavljene rutine. Međutim nekon određenog vremena korišćenja i unapređenja svaka tehnološka inovacija pronalazi sebi primenu. Period razvoja i usvajanja računarstva od prvih personalnih računara pa do danas ima slični životni put kao i ostatak tehnogija. Tačnije jedna velika razlika između primene informaciono komunikacionih tehnologija i ostataka industrijskih pronalazaka je u brzini razvoja novih uređaja. Razvoj ICT (Information and Comunication Technologies) u poslednjih nekoliko decenija imao je strahoviti rast. Sami rast broja korisnika kretao se od domena primene od strane pojedinaca ili istraživačkih centara do domena primene od strane pojedinaca.

Na makroekonomskom nivou primena informaciono komunikacionih tehnologija utiče se na povećanje konkurentnosti i produktivnosti ekonomije, doprinosi se otvaranju novih radnih mesta, a na mikroekonomskom nivou utiče se na organizacionu strukturu tržišta preko smanjivanja troškova za početak rada privrednog društva, smanjuje se ekonomski uticaj udaljenosti kao i reduciraju se troškovi za pristup informacijama, podstiče se razvoj novih i usavršavanje postojećih proizvoda, kao i razvoj novih efikasnijih načina isporuke usluga i dobara. Ova činjenica nalaže i pravno regulisanje upotrebe informacione tehnologije, koja postaje imperativ vremena i kontrolisanog održivog socijalnog razvoja. Benefit korišćenja interneta je višestran, on direktno utiče na vezanost kompanija sa dobavljačima, potrošačima, konkurentima i partnerima kao i na način na koji se koristi za marketing promocije svojih brendova i proces proizvodnje svojih proizvoda. Na ovakav način razvila se oblast danas poznata kao elektronska trgovina. Elektronska trgovina kao takva stvara nova elektronska tržišta, gde se komunikacija i prodaja obavljaju putem internet servisa bez ličnog kontakta i sa mogućnošću obaljanja istih na velikoj udaljenosti. Na ovakav način sami proces trgovine postaje globalan, po mnogima možda ne savršen ali svakako veoma efikasan. Pored procesa trgovine organizovanog putem servisa baziranih na upotrebi informaciono komunikacionih uređaja i interneta veliko mesto u poslovanju pre svega kompanija jesu servisi koji spadaju u domen elektronskog poslovanja. Samo elektronsko poslovanje zasnovano je na upotrebi elektronskih ugovora i elektronskih faktura. Proširenjem elektronskog poslovanja na domen fizičkih lica došlo se do novih servisa koji su u upotrebi i od strane pravnih lica takođe. U ove servise mogu se pobrojati elektronsko i mobilno bankarstvo. Kako bi neometano funkcionisali elektronski servisi online plaćanja, elektronske trgovine i elektronskog bankarstva koncept elektronskog novca morao je biti razvijen. Elektronski novac kao virtualna valuta pristuna samo u računarskom sistemu u velikoj meri zamenio je papirni novac i rad sa istim. Proces elektronskog bankarstva, elektronske trgovine i upravljanja novcem obavlja se vrlo efikasno putem bilo kog računarskog uređaja i prisupa internetu. Sa sve većom upotrebom elektronskog novca razvila se ideja kreiranja kriptovaluta koje bi u potpunosti zamenile klasičan novac kao i finansijski sistem nama danas poznat. Sama ideja bazirana je na decentralizaciji novčanog sistema, što praktično znači da su ovako kreirane kriptovalute nezavisne od svetske banke, međunarodnog monetarnog fonda kao i od banaka uopšte. Kriptovalute kojima se

trenutno trguje a koje su detaljnije opisane u narednim poglavljima nastaju u procesu koji je poznat kao rudarenje (mining). Iako nisu preuzele vodeće mesto u trgovini sve je veći broj korisnika koji se bavi mining-om kriptovaluta kao i transakcijama koje obuhvataju prodaju i kupovinu istih na berzama koje se bave ovakvim vidom trgovine. Takođe određeni broj korisnika odlučuje se za kupovinu kriptovaluta u zamenu za klasičan novac putem web servisa ili bankomata instaliranih na određenim lokacijama.

Prednosti upotrebe informaciono komunikacionih tehnologija i interneta pored pravnih i fizičkih lica prepoznale su i državne uprave velikog broja zemalja. Prednosti koje upotreba ovakvih servisa nudi ogledaju se u olakšanoj komunikaciji između vladinih agencija, lokalne samouprave i građana svake od zemalja. Elektronski servisi su u najvećem broju slučajeva organizovani u okviru portala pod nazivom e-Uprava. Ovakav portal poseduje i Republika Srbija, i isti je u funkciji već određeni broj godina, naravno u različitim verzijama i sa različitim servisima koje nudi. U zavisnosti od implementiranih tehničkih rešenja i sugurnosnih mehanizama servisi su organizovani u više grupa. Grupe su najčešće organizovane u servise za poslovne korisnike, fizička lica i državnu upravu. U zavisnosti od toga kojoj grupi se pristupa razlikuje se broj elektronskih servisa u okviru grupe koji se mogu u potpunosti realizovati elektronskim putem. Ovo praktično znači da korisnik korišćenjem konkretnog servisa može celokupnu aktivnost započeti i završiti elektronskim putem. Određeni broj zemalja radio je i radi na uvođenju elektronskog glasanja kao jednog od vidova upotrebe elektronskih servisa. Elektronsko glasanje kao takvo nudi mogućnost da zemlje koje su implementirale ove servise imaju znatno olakšan pristup glasanju i demokratiji. Sama ozbiljnost problema elektronske demokratije i elektronskog glasanja kao ključni akcenat stavlja na bezbednost, transparentnost i tačnost ovakvih servisa. Dodatni servisi kreirani od strane državnih organa a dati u službi građana jesu i servisi elektronske participacije i elektronskih recepata.

Veliki broj elektronskih servisa kreiran je sa ciljem da stalno bude u upotrebi od strane državne administracije, državnih agencija, zaposlenih u lokalnoj samoupravi i svih građana kojima je pristup ovakvim servisima odobren. Domeni upotrebe ovakvih servisa kao i prava i privilegije korisnika razlikuju se u zavisnosti od toga da je korisnik lice zapošljeno u državnoj upravi, fizičko lice ili pravno lice. U ove servise mogu se ubrojati i servisi za elektronsko praćenje osuđenika koji su u programu osluženja kazne vanzavodskih prostorija. Takođe u ove servise spada i sistem za nadgledanje saobraćaja i obradu prikupljenih podataka u cilju lakšeg regulisanja saobraćaja i evidentiranja načinjenih prestupa. U transportnoj industriji koriste se elektronski servisi za praćenje poštanskih usluga pomoću kojih kako građani tako i transportna kompanija mogu pratiti kretanje pošiljke i pakete. Ovakav metod doprinosi brzini organizovanja dostave pisama i pošiljki, kao i većem zadovoljstvu građana pruženom uslugom. Zbog sve većeg broja problema uzrokovanih različitim kriminalnim i terorističkim aktivnostima vlade velikog broja zemalja uvode servise koji omogućavaju praćenje sumnjivih osoba i lociranje sumnjivih aktivnosti.

Klasični koncepti zakonskih regulativa i pravne prakse stavljeni pred veliki izazov brzim razvojem informaciono komunikacionih tehnologija, elektronskih servisa, cyber prostora, razmene podataka putem interneta kao i celokupnog digitalnog sveta. Samim

tim ni domen pravnih regulativa koje se primenjuju u oblasti intelektualne svojine i autorskih prava nije mogla biti izuzetak. Problem koji je javlja usled nedovoljnog poznavanja zakonskih i pod zakonskih akata i prava nosioca intelektualne svojine karakterističan je u domenu upotrebe sadržaja bez ovlašćenja i ustezanja. Praktično korisnici interneta u velikom broju smatraju da nesmetano mogu koristiti sve sadržaje koje pronađu na internetu. Ovakvim pristupom mnogi od njih krše autorsko pravo. Takođe postoji određeni broj korisnika koji smatra da u cyber prostoru nema zaštite sadržaja autorskim pravom. Funkcionalnost u pogledu neograničene dostupnosti različith sadržaja zaštićenih autorskim pravom dovela je do remećenja tradicionalnog koncepta autorskih prava. Na ovakav način sami razvoj informaciono komunikacionih tehnologija neposredno je uticao na povećanje broja oblika i načina orijentisanih ka ugrožavanju prava intelektualne svojine. Brza dostupnost književnih dela, naučnih radova, muzičkih i video sadržaja deluje izazovno po korisnike interneta koji ne vode previše računa o tome koji od sadržaja je zaštićen autorskim pravom. Autorskim pravom i pravom intelektulne svojine zaštićen je znatno veći broj dela nego što to veliki broj korisnika misli. Pored uobičajenih autorskih dela u ovu kategoriju spadaju i digitalna dela, razne vrste softvera kao i audio i vizuelna dela. U cyber prostoru najveći broj zloupotreba orijenatisan je u pravcu kršenja autorskih prava nad audio i video materijalom dostupnim na internetu. U prilog činjenici da su autorska prava audio i vizuelnih dela najugroženija svedoči i podatak o velikom broju web portala na kojima se najnovija dela iz audio ili video industrije mogu preuzeti bez ikakve nadoknade. Naravno da se za preuzimanje ili korišćenje dela zaštićenih autorskim pravom ne mora obavezno naplaćivati nadoknada ali se svakako mora tražiti saglasnost autora ili izdavačke kuće koja zadržava sva prava. Pomenuta kršenja autorskih prava u cyber prostoru organizovana su putem direktnog preuzimanja fajlova, putem preuzimanja uz pomoć torrent fajlova kao i u vidu streaming reprodukovanja audio i video materijala. Sama činjenica velikih problema narušavanja prava intelektualne svojine uz pristustvo kvalitetnih zakonskih regulativa kako nacionalnih tako i međunarosnih govorio o tome da je počinioce teško razotkriti. Teško otkrivanje počinioca posledica je anonimnosti u korišćenju deep weba ili pak slabog angažovanja nadležnih službi za visokotehnološki kriminal.

Cyber prostor iako kreiran na zdravim osnovama i dobrom razvojnom idejom godinama je zbog prednosti koje nudi kriminalnom miljeu takođe atraktivan. Neki ga koriste kako bi ometali rad drugih, neki u cilju pribavljanja ekonomske dobiti napadom na elektronske servise za rezervaciju, elektronsko plaćanje, elektronsko bankarstvo, pojedini za krađu ličnih podataka i prodaju istih na crnom tržištu dark web-a, dok ga određene grupe koriste za planiranjem, organizaciju i izvođenje terorističkih napada. Bilo kako bilo procenat krivičnih dela različitog profila izvedenih upotrebom cyber prostora jako je veliki pa sa tim u vezi i odgovor zakonodavnih tela na nacionalnom ili međunarodnom nivou mora biti odgovarajući. Prosto je nedopustivo pa portali poput onih za prodaju narkotika, prostituciju, korišćenje dece u pornografskoj industriji rade nesmetano duži niz godina.

Svaka od zemalja ulaže napore u rešavanje ovakvih problema ali oni ipak nekako opstaju. Sve pomenute aktivnosti mogu se klasifikovati kao cyber kriminal. Cyber kriminal kao takav može se okarakterisati kao protivzakonit oblik ponašanja, ili kao oblik ponašanja za koji se može očekivati da će biti kriminalizovan u nekom periodu vremena. Svaki od ovakvih oblika ponašanja moraju se izvršavati ili sa računarskim sistemima, ili unutar računarskih sistema i mreža ili pak mora biti usmeren protiv računarskih sistema i mreža. Ovako posmatrano može se definisati da je cyber kriminal oblik kriminalne aktivnosti koja se odvija u elektronskom ili cyber okruženju, dok se u ovom okruženju računarski uređaji i računarske mreže mogu pojaviti u različitim oblicima. Neki od mogućih oblika jesu da se računarski uređaji i računarske mreže mogu pojaviti kao sredstvo izvršenja, cilj napada, elektronski dokaz ili samo okruženje izvršenja krivičnog dela. Sa stanovišta zakonodavnih sistema različitih država cyber kriminal se definiše na različite načine. Način definisanja cyber kriminala zavisi od usvojene politike krivičnog gonjenja, kao i karakteristikama i stepenu razvoja konkretnog društva i konkretne zemlje. Kazneno pravno zakonodavstvo razlikuje se u različitim zemljama. Svaka od zemalja prilagodila je pravne okvire svom cyber prostoru i svojim građanima. U većini slučajeva propisi su donošeni ili po principu usklađivanja sa evropskim i svetskim konvencijama, prilagođavanejm već postojećih normi ili kreiranjem zakonskih regulativa i normi od početka uz prethodno definisanje pravnih okvira.

Kao i većina cyber prostora ni cyber prostor Republike Srbije nije ostao van uticaja pojedinaca ili grupa čija je delatnost bavljenje određenim oblikom cyber kriminala. Kada je upitanju zastupljenost bavljenja cyber kriminalom istraživanja pokazuju da je ovaj procenat u Republici Srbiji jako veliki, pa je samim tim Republika Srbija svrstana u visoko rizična i nesigurna cyber područja. Poseban akcenat stavljen je na porast broja aktera u cyber kriminalu. Nespremnost pravosuđa da se obračuna sa ovakvim vidom kriminala olakšali su prelazak pojedinaca koji se bave sitnim malverzacijama u cyber prostoru da pređu u sferu čistog kriminala. Upravo ova činjenica ohrabrila je mnoge pojedince da iz domena sitnih pokušaja pređu u osobe koje se ozbiljno bave cyber kriminalom. Ovakav trend malo je usporilo nekoliko prijava istražnim organima, na osnovu koji su pokrenute istražne radnje. Cilj istražnih radnji je da se službe zadužene za rešavanje problema iz domena cyber kriminala okrenu rešavanju ovakvih kriminalnih aktivnosti. Činjenica je da su na samom početku aktivnosti cyber kriminalaca pravosudnom sistemu često bile nejasne i apstraktne. Kao pioniri u ovoj borbi sa rešavanjem prvih tužbi u Republici Srbiji suočili su se sudovi u Beogradu, Pančevu i Nišu.

Generalno posmatrano uočljivo je da brzinu razvoja ICT i njihovu primenu u velikoj meri nije pratio razvoj ostatka društva. Pod ovim se pretežno misli na razvoj zakonskih regulativa koje bi pratile ovu oblast. Nekako se stiče utisak da su se ljudi iz domena zakonodavstva kasno probudili i shvatili u kom obimu je primena računarstva i Interneta prisutna kod stanovništva kao i kolike probleme pored velikih prednosti može doneti. Takođe stiče se utisak da zakonske regulative koje pokrivaju organizaciju i uređenje cyber prostora kao da kasne za novitetima pa se iste donose tek problemi nastanu.

Na osnovu iznetog zaključujemo da su informacione i komunikacione tehnologije i na njima zasnovano tržište elektronskih komunikacija jedan od najpropulzivnijih privrednih sektora. Regulatornim mehanizmima usmerava se razvitak tržišta elektronskih komunikacija kako bi se postigla raspoloživost usluga usklađena potrebama i mogućnostima građana, privrede i društva u celosti, te ulaganje u nove tehnologije kojima će se to kontinuirano ostvarivati. Evropska unija primenjuje i kontinuirano razvija zajednički regulatorni okvir za područje elektronskih komunikacija koji uključuje opšte i posebne mere podsticanja i zaštite tržišne konkurencije provajdera informacionih i komunikacionih usluga.

Naime, autonomna krivična odgovornost predstavlja najzahtevniji i najveći izazov za teoriju i praksu, jer podrazumeva stvaranje novih krivičnopravnih oblika odgovornosti koji se zasnivaju na ponašanju i delovanju pravnog lica. U smislu iznetog, jednim od boljih rešenja smatra se uvođenje uporedne odgovornosti pravnih i fizičkih lica. Cilj uporedne odgovornosti pravnih i fizičkih lica jeste uokviravanje odgovornosti za učinjena krivična dela, jer se sa razvojem komunikacionih i računarskih tehnologija ne može u mnogim privrednim subjektima odrediti kvantitativna pojedinačna odgovornost lica za učinjena krivična dela, posebno kada je reč o cyber kriminalu koji svakodnevno dobija nove pojavne oblike.

Pravna lica u Srbiji, sve do donošenja novog Zakona o odgovornosti pravnih lica za krivična dela,[1] odgovarala su za prekršaje i privredne prestupe. Međutim, postojala je velika praznina na polju krivične odgovornosti pravnih lica, odnosno pravno lice je bilo nemoguće procesuirati kroz krivični postupak, protivpravne radnje i postupke pravnih lica. Ovde mislimo, pre svega, na one radnje i postupke pravnih lica, te odgovornog lica u pravnom licu, koje sadrže elemente krivičnih dela.

Međutim, po prirodi stvari nemoguće je da pravno lice odgovara za sva krivična dela, naprotiv, postoji čitava lepeza krivičnih dela koja pravna lica objektivno nikada ne mogu učiniti. Smisao uvođenja krivične odgovornosti pravnih lica se sastoji u potrebi za kaznenom reakcijom na ona tzv. tipična krivična dela, koja pravna lica gotovo redovno čine, a za njih krivično ne odgovaraju.

Ovakvu pravnu situaciju, ili ti pravni vakuum, razrešio je doneti Zakon o odgovornosti pravnih lica za krivična dela. Ovaj zakonski akt na celovit način reguliše i pokriva, kako materijalni aspekt krivične odgovornosti pravnih lica, tako i procesni aspekt, propisivanjem pravila krivične procedure tokom vođenja krivičnog postupka protiv okrivljenih pravnih lica, kao i krivičnih sankcija koje im se mogu izreći.

[1] *Zakon o odgovornosti pravnih lica za krivična dela*, Službeni glasnik RS, br. 97/2008.

Narodna skupština Srbije je, znači, usvajanjem Zakona o odgovornosti pravnih lica za krivična dela prihvatila stanovišta izneta u našoj pravnoj teoriji o neophodnosti uvođenja odgovornosti pravnih lica za krivična dela u kazneno pravni sistem Srbije. Ujedno je prihvaćeno stanovište izneto u pravnoj teoriji da je uspostavljanje takve odgovornosti moguće i potrebno, pre svega, iz kriminalno-političkih razloga. I treće, ovakvo rešenje je neophodno radi usaglašavanja sa pravnim standardima sadržanim u mnogobrojnim relevantnim međunarodnim dokumentima, kao i radi ujednačavanja sa već postojećim krivičnim zakonodavstvima u državama članicama Evropske unije koje već regulišu pitanje odgovornosti pravnih lica za krivična dela, imajući pri tom u vidu i krivična dela kompjuterskog kriminaliteta.

Ova uporedna odgovornost je posebno značajna u regulisanju elektronske uprave zaštite životne sredine, koja kako u većini zemalja, tako i u Republici Srbiji nije regulisana, ali je nephodna ukoliko želimo da institcionalizujemo i pratimo u potpunosti ovaj proces.

2
Pravo intelektualne svojine u Cyber prostoru

Razvoj informaciono komunikacionih tehnologija i interneta u mnogim aspektima ljudskog života i rada doveo je do velikih promena. Slobodno se može reći da se trenutno više od 90% informacija nalazi u digitalnom formatu. Ovako kreiran cyber prostor trenutno je postao najveći resurs informacija na svetu. Pored javno dostupnih informacija, veliki procenat različitih informacija koje se mogu pronaći u okviru cyber prostora predstavlja informacije zaštićene autorskim pravom. Izuzetno prisutan problem prilikom korišćenja informacija dostupnih u cyber prostoru jeste i zaštita intelektualne svojine. Veliki broj korisnika svesno ili nesvesno zanemaruje činjenicu da su dela kojima pristupaju zaštićena autorskim pravom, i da se ne mogu slobodno koristiti. Ogromna dostupnost autorskih dela u digitalnom obliku kao što su naučni radovi, književna dela, audio i video materijali, različite vrste softvera u mnogome je otežala primenu koncepata autorskih prava. Upravo iz ovog razloga dobro poznati tradicionalni koncept autorskih prava morao se prilagoditi digitaliaciji sadržaja koje je potrebno zaštiti. Kako bi se zaštitila autorska dela u digitalnom obliku kreirani su novi koncepti kao što su: licence otvorenog sadržaja, open source softver, coy left licence, licenci kreativne zajednice (Creative Commons Licenses - CCL), idt.

U okviru ovog poglavlja obrađeni su osnovni principi intelektualne svojine i autorskog prava. Poseban akcenat stavljen je na primenu Zakonskih regulativa u cilju regulisanja intelektualne svojine i autorskog prava u okviru cyber prostora kao i na primere zloupotreba i kršenja autorskih prava od strane korisnika ICT i interneta.

2.1 Principi intelektualne svojine i autorskog prava

Intelektualna svojina može se posmatrati kao vlasništvo na dobrima nematerijalnog karaktera. Pod ove osobine dobra koja spadaju u intelektualnu svojinu moraju biti proizvod intelekta osobe kojoj dobro pripada. Veoma često pomenuta dobra su i proizvod kreativnosti i inovativnosti osobe kojoj dobro pripada. Posmarano iz ugla nastanka intelektualna svojina podstiče stvaralačku stranu čoveka, i posredno utiče na pomeranje granica nauke i tehnike. Ukoliko se sagledaju dobra koja nastaju kao proizvod intelektualnog stvaralaštva čoveka može se utvrditi da intelektualna svojija utiče i na povećanje i obogaćivanje sveta književnim i umetničkim delima. Iz ugla autor dela ili njegovog stvaraoca intelektualna svojina predstavlja specifična prava samog autora, pronalazača ili nosioca prava intelektualne svojine. Kao što je već navedeno jako je bitno istaći da intelektualna svojina ne predstavlja materijalno vlasništvo, već skup prava i ovlašćenja. Ovaj skupa prava i ovlašćenja nosiocu prava intelektualne svojine može biti priznat od strane institucija zaduženih za uspostavljanje pravnog poretka. Ovo praktično znači da su prava i ovlašćenja obezbeđena autoru i stvaraocu dobra. To je svojevrstan sistem zaštite nematerijalnih dobara koja su nastala kao produkt ljudske kreativnosti i inovativnosti. Pravni okviri intelektualne svojine bazirani su na sporazumima i ugovorima koji su nastali kao produkt rada radnih grupa na međunarodnom nivou, kao i na pravnim normama definisanim u nacionalnom zakonodavstvu svake od zemalja. Rezultat rada pomenutih grupa je sistem pravne

zaštite intelektualnog vlasništva svakog pojedinca ili grupe autora kojima se rezultat njihovog rada štiti. Prava intelektualne svojine datiraju još od Ustava Sjedinjenih Američkih Država. Definisana su u okviru člana 1 tako da daju Kongresu autoritet: ,,da podstiče unapređivanje nauke i korisnih veština, obezbeđujući piscima i pronalazačima isključivo pravo, na ograničeno vreme, na njihova dela i pronalaske". Zahvaljujući vrlo ranim naporima u ovoj oblasti kao i multilateralnim konvencijama koje pokrivaju ovu oblast, područje intelektualne svojine jedna je od retkih grana prava koja uživa visok stepen usaglašenosti u većini pravnih sistema. Intelektualna svojina se deli na dve kategorije:

- **Industrijska svojina**. U ovu kategoriju mogu se uvrstiti patenti kao najpoznatiji oblik industrijske svojine. Pored patenata u kategoriju industrijske svojine takođe spadaju žigovi kompanija, oznake geografskog porekla, dela nastala kao rezultat industrijskog dizajna, pa čak i šeme integrisanih kola,
- **Autorsko pravo i srodna prava.** U ovu kategoriju ubrajaju se dela književnosti, nauke i umetnosti. Ukoliko se posmatra broj aktera na razvoju samog dela koje se štiti autorskim pravom u ovu kategoriju najčešće se svrstavaju dela koja su rezultat intelektualnog i stvaralačkog napora pojednca.

Bez obzira o kojoj kategoriji intelektualne svojine se radi mogu se izdvojiti različiti principi zaštite. Prvi od principa zašite naziva se razotkrivanje suštine. Ovaj princip definiše da autor mora predstaviti srž konkretnog vlasništva svetu kako bi mu samo vlasništvo moglo biti priznato. Ovo praktićno znači da autor kreirano intelektualno delo sa jedne strane mora prikazati svetu, dok sa druge strane za isto delo mora dokazati da je zaista njegovo, i da niko pre njega nije svetu prikazao isto ili u velikoj meri slično delo. Drugi princip zaštite naziva se teritorijalni princip. Ovaj princip definiše da se intelektualna svojina može štititi ili na nacionalnom ili na regionalnom nivou. Ovo praktično znači da država ili regija u kojoj je autor podneo zahtev za zaštitu dela sprovodi proces zaštite prava intelektualne svojine. Za svaki predmet proglašen intelektualnom svojinom definiše se vremensko ograničenje trajanja zaštite što predstavlja treći princip zaštite. Primera radi u Republici Srbiji maksimalno vreme trajanja zaštite nekog dela u vidu patenta iznosi 20 godina. S druge strane maksimalno vreme zaštite žigova iznosi 10 godina uz mogućnost neograničenog obnavljanja zaštite. U praksi zaštita industrijskog vlasništva primera radi patentiranje nekog pronalaska ili proizvoda postiže se uobičajenim postupcima. Ovi postupci podrazumevaju priznavanje prava ili registrovanja konkretnog patenta. Sami proces priznavanja prava sprovode nadležna tela za određeno područje. Pomenuto područje u najvećem broju slučajeva je država na čijoj teritoriji je delo koje se zeli zaštiti nastalo. U manjem broju slučajeva može se raditi o zaštiti na području regije. Ukoliko se posmatra na ovakav način regija bi pokrivala šire područje pa bi na takav način i sama zaštita imala snažnije dejstvo. Primera radi Zavod za intelektualnu svojinu Republike Srbije zadužen je za sprovođenje postupka za dodeljivanje prava intelektualne.

Autorskim pravom se štite ljudske tvorevine, koje imaju duhovni sadržaj, koje su originalne i izražene u određenoj formi. Autorsko delo može biti originalna intelektualna tvorevina koja može pripadati književnom, naučnom ili umetničkom području. Da bi se delo svrstalo u autorsko mora imati individualni karakter. Ako se

posmatra domen intelektualnih tvorevina iz književnog područja ovde bi se mogli svrstati romani, pesme, pripovetke, i dramska dela. Pod tvorevinama iz domena naučnog područja mogu se posmatrati pronalasci, patenti, i u novije vreme računarski programi i baze podataka. Na kraju u tvorevine umetničkog područja mogu se svrstati filmovi, muzička dela, koreografska dela, dela likovne umetnosti, dela athitekture, primenjenih vrednosti, skice, fotografije, itd.

2.2 Autorsko pravo i autorskom pravu srodna prava

Prema Zakonu o autorskim i srodnim pravima Republike Srbije autorsko delo definisano je kao duhovna tvorevina originalnog karaktera. Ovako kreirana duhovna tvorevina mora biti izražena u određenoj formi. Ovo praktično znači da bez obzira umetničku, naučnu ili drugu vrednost samog dela, kao i njegovu namenu, veličinu, sadržinu i način ispoljavanja delo mora ispoštovati određenu formu. Sama forma dela odnosi se i na dopuštenost javnog saopštavanja njegove sadržine[2].

Svaki autor raspolaže moralnim, imovinskim i ostalim pravima definisanim Zakonom i to od samog trenutka nastanka autorskog dela. Pod moralnim pravima autoru se smatra pravo priznavanja autorstva nad njegovim delom, kao i pravo da njegovo ime bude jasno navedeno na svakom izdatom primerku dela. Takođe autor ima pravo da objavi svoje delo. Tačnije autor prema ovom zakonu može odrediti sami način na koji će se predmetno delo objaviti. Na osnovu svega navedenog proizilazi pravo autora na zaštitu integriteta dela, da se suprostavi bilo kakvom nezakonitom iskorišćavanju svog dela. Posebno je autoru dato pravo suprostavljanja iskorišćavanju dela u slučaju kada se iskorišćavanjem na bilo koji način vrši atak na čast i ugled autora. Pod imovinskim pravima spada pravo na umnožavanje dela. Pored prava na umnožavanje dela imovinskim pravom regulisano je i pravo sticanja ekonomske dobiti u vidu distribucije dela ili njegovog davanja u zakup. Ukoliko se radi o delu koje se može izvoditi, predstaviti ili reprodukovati, imovinskim pravom se definiše i pravo izvođenja, kao i pravo prenošenja, emitovanja, i javnog saopštavanja dela kao i svi drugi oblici činjenja dela javno dostupnim. Ukoliko se delo javno emituje imovinskim pravom se definiše i pravo na prilagođavanje, aranžiranje i drugu izmenu dela, kao i pravo javnog saopštavanja dela koje se emituje i pravo javnog saopštavanja dela sa nosača zvuka ili slike. Grupa ostalih prava obuhvata pravo na pristup primerku dela, pravo sleđenja, kao i pravo zabrane izlaganja originalnog primerka ukoliko se radi o delima likovne umetnosti. Što se tiče dela iz domena arhitekture u grupu ostalih prava može se ubrojati i preče pravo autora koje se odnosi na izmenu primerka arhitekturnog dela. Takođe u slučajevima korišćenja dela od strane drugih lica ostalim pravima se propisuje pravo autora na posebnu naknadu.

[2] Zakon o autorskim i srodnim pravima, Službeni glasnik RS, br. 104/2009, 99/2011, 119/2012 I 29/2016 – odluka US

Posmatrano sa pravne strane u praksi ovo znači da za sticanje i održavanje autorskopravne zaštite nije propisan upravni postupak pred određenim državnim organom. Takođe nije potrebno ispuniti bilo kakve formalnosti ili plaćanje taksi. U Sektoru za autorsko i srodna prava i međunarodnu saradnju vrši se deponovanje, odnosno registracija autorskih dela i predmeta srodnih prava. Sve ovo se radi sa jednim ciljem a to je lakše dokazivanje i razlikovanje registrovanih dela. Na ovakav način lako se mogu razlikovati registrovana dela od neregistrovanih, i lako se može utvrditi povreda autorskih prava.

Pored autorskog prava Zakonom je predviđeno i definisanje srodnih prava autorskom pravu. Ova prava najčešće se odnose na pravnu zaštitu autorskih dela koja obahvataju:

- pravo interpretatora;
- pravo proizvođača fonograma;
- pravo proizvođača videograma;
- pravo proizvođača emisije;
- pravo proizvođača baze podataka;
- pravo prvog izdavača slobodnog dela i
- pravo izdavača štampanih izdanja na posebnu naknadu.

Kao što se iz navedenog može videti u najvećeom broju slučajeva zaštita srodnim pravom odnosi se na audio i video zapise, dela nastala u radiodifuziji, kao i na domen zaštite organizacionih poslovnih i finansijskih ulaganja u iste.

Pravom interpretatora svakom interpretatoru za izvedenu interpretaciju zagarantovana su sva moralna i imovinska prava. U smislu ovog zakona interpretator je fizičko lice radno angažovano na interpretaciji određenog dela. Ovde spadaju muzičari, glumci, pantomimičari itd. Delo koje se interpretira ne mora obavezno da bude autorsko delo, što znači da interpretator bez bilo kakvih problema može izvoditi tuđa dela koja jesu ili nisu zaštićena autorkim pravom. Takođe lica koja pružaju tehničku podršku prilikom izvođenja dela ne mogu biti kategorisana kao interpretatori.

Kako se pod fonogramom podrazumeva snimanje zvuka ili niza zvukova na nekon nosaču zvuka, zakonom je definisano da proizvođač fonograma ima imovinska prava nad keiranim zapisom. Zakonom je definisano da proizvođač fonograma može biti fizičko ili pravno lice. U oba slučaja bitna činjenica je da je fonogram nastao u organizaciji ili sredstvima pomenutog fizičkog ili pravnog lica. Proizvođač fonograma u ovom smislu snosi odgovronost za prvo snimanje zvuka, odnosno niza zvukova.

Pravom filmskog producenta (proizvođača videograma) definisano je da je videogram snimak filmskog dela na nosaču slike i zvuka. Pored filmskog dela u videogram se može uvrstiti i niz pokretnih slika koje mogu ali ne moraju biti praćene zvukom, takođe snimljene na nosaču slike i zvuka. Producent polaže pravo na videogram i on može biti fizičko ili pravno lice. Praktično producent može biti bilo fizičko bilo pravno lice koje je inicijator snimanja filmskog dela. Takođe zadatak producenta je obezbeđivanje finansijskih sredstava kojima se pokrivaju svi troškovi predviđenog snimanja. S obzirom da producent rukovodi celokupnim procesom snimanja dela, sva odgovornost procesa snimanja je takođe na njemu. Pravom proizvođača videograma definisano je da se on

može suprostaviti iskorišćavanju svog videograma kako u originalnoj tako i u izmenjenoj formi. Ovo je posebno značajno ukoliko se samim iskorišćavanjem mogu ugroziti imovinski interesi proizvođača videograma.

Kada je reč o emisijama, svaki elektromagnetni ili drugi signal pretvoren u zvučni, vizuelni ili pak zvučno-vizuelni sadržaj kreiran kako bi bio dostupan široj javnosti može se okarakterisati kao emisija. Iz tog razloga definisana su prava proizvođača emisije, koja se mogu svrstati u kategoriju imovinskih prava. S tim u vezi svako fizičko lice ili kompanija pod čijim je rukovodstvom ili čijim je finansijama emisija proizvedena poseduje određena prava nad istom.

Pravom proizvođača baze podataka definisan je proizvođač baze podataka. Sam baza podataka u ovom smislu predstavlja skup pojedničnih podataka, autorskih dela ili drugih bilo kojih drugih materijala. Svi podaci u okviru baze podataka moraju biti uređeni primenom neke metodike za uređenje podataka. Sa masovnom upotrebom digitalnih podataka definisana je i baza podataka kao skup digitalno uređenih prethodno nestruktuiranih podatka ili materijala. Ovim podacima takođe se pristupa elektronski, dok se materijali koriste za njeno neometano funkcionisanje. U grupu materijala mogu se svrstati rečnici, indeksi, ili sistem za dobijanje ili prikazivanje informacija. U okviru intelektualne svojine može se reći da baze podatka zauzimaju posebno mesto i mogu se posmatrati kao potpuno nova oblast. Sa aspekta proizvođača baze podataka, proizvođač može biti fizičko lice ili kompanija. Da bi konkretno lice postalo nosioc prava proizvođača baze podataka potrebno je da je ono pre svega sačinilo bazu podataka. Pod kreiranjem baze podataka podrazumeva se pribavljanje, provera ili prezentacija njenog sadžaja. Ovim Zakonom jasno se definiše ko može postati ovlašćeni korisnik baze podataka, kao i prava i privilegije ovlašćenog korisnika. Kada su u pitanju elektronske baze podataka postupak utvđivanja prava proizvođača i ovlašćenih korisnika biva znatno otežan velikim brojem zlopotreba od strane neovlašćenih korisnika.

Pravo izdavača se posebno ustanovljava kao pravo prvog izdavača slobodnog dela, koje se stiče saopštavanjem dela koje dotad nije saopštavano a koje se saopštava nakon isteka imovinskih prava autora. Imovinska prava autora nad delom koje je zaštićeno autorskim pravo ističu nakon što protekne 70 godina od smrti autora. Lice koje zakonito izvrši ovakvo izdanje ima imovinska prava jednaka imovinskim pravima autora. Organizacije za kolektivno ostvarivanje autorskih i srodnih prava predstavljaju pravno telo pred kojim izdavači štampanih izdanja kao i autori štampanih dela mogu ostvariti svoja prava. Pravo prvog izdavača slobodnog dela je imovinsko pravo, što je zajednička karakteristika svih srodnih prava osim prava interpretatora. Nosilac prava nema nikakva moralnopravna ovlašćenja, jer on nije duhovni stvaralac dela. Imovinskopravna ovlašćenja nosioca prava prvog izdavača slobodnog dela analogna su imovinskopravnim ovlašćenjima autora. Vremenski period trajanja prava prvog izdavača slobodnog dela zakonom je određen na 25 godina počevši od dana izdavanja slobodnog dela, odnosno od dana njegovog prvog saopštavanja javnosti na drugi način[3].

[3] Dušan Popović, „Kritički osvrt na srodnopravnu zaštitu izdavača: zaštita privrednog ili kulturnog poduhvata“, Časopis za pravne i društvene nauke, Pravni fakultet Beograd ,Vol. 63, No. 1, 2015.

Izdavači štampanih izdanja imaju pravo na posebnu propisanu naknadu. Naknada je propisana i sprovodi se na istovetan način kao što je to slučaj sa autorima. Kada je reč i štampanim delima autori ovih dela mogu ostvariti svoja prava isključivo posredstvom organizacije za kolektivno ostvarivanje autorskih i srodnih prava. Autor i izdavač u unapred definisanoj razmeri dele sredstva prikupljena u vidu taksi koje plaćaju proizvođači, uvoznici i korisnici uređaja za fotokopiranje i pružanje usluga umnožavanja. Obično se za ove uluge licu kome je ona pružena naplaćuje naknada.

2.3 Nosioci autorskih i srodnih prava

Uopšteno govoreći stvaraoci dela koja su zaštićena autorskim pravom kao i njihovi nalsednici i pravni sledbenci nazivaju se nosiocima autorskog prava. Sva svoja prava definisana Zakonom nosioci mogu ostvariti na dva načina: individualno ili kolektivno. Individualno ostvarivanja prava praktično znači da je konkretna osoba stvorila orginalnu intelektualnu tvorevinu. U tom slučaju sami autor činom stvaranja dela ostvario je autorsko pravo, i nije u obavezi da ispunjava bilo kakve druge formalnosti kao što su regisracija ili depozit rada. Ukoliko je više autora radilo na stvaranju dela, pri čemu je delo kao takvo nedeljiva celina svakom od autora pripada zajedničko autorsko pravo nad stvorenim delom. Ovako kreirano delo naziva se koautorsko delo. Sa druge strane ukoliko je delo moguće podeliti na pojedinačne delove na kojima su autori aktivno radili, a nakon toga radi njihovog zajedničkog korišćenja spojili sve delove u zajednični rad u tom slučaju svaki pojedinačni učesnik ima autorsko pravo na svom autorskom delu.

Već pomenuta organizacija za kolektivno ostvarivanje autorskih prava nikada se ne osniva radi sticanja dobiti. Nosioci autorskog odnosno srodnih prava posredstvom organizacije za kolektivno ostvarivanje prava mogu da ostvaruju imovinska prava i prava na potraživanje naknade. Autori mogu da potražuju naknadu za ona svoja dobra koja su zaštićena autorskim pravom. Zakonom je definisano da ukoliko autor ostvaruje samo imovinska prava to praktično znači da će on ugovorom morati na isključiv način da ustupi sva svoja prava organizaciji. Nakon ustupanja prava organizacija u ime autora obavlja poslove zaključivanja ugovora sa korisnicima predmetnih dela o neisključivom ustupanju tih prava.[4] Kada se radi o ostvarivanju prava na naknadu organizacija u ime nosioca autorskih prava a na njegov zahtev vrši naplatu od korisnika dela. U ovakvim slučajevima organizacija zadržava pravo da vrši kontrolu iskorišćavanja predmeta pod zaštitom autorskim pravom. Shodno Zakonu u slučaju spora organizacija ima pravo i dužna je da pred sudom kao ovlašćeno lice štiti interese i prava nosioca autorskog prava.

Ovako definisani nosioci poseduju određena prava i privilegije koja se odnose na konkretno autorsko delo. Prava i privilegije omogučavaju nosiocu da zabraniti ili

[4] Autorsko i srodna prava, Privredna komora Srbije, dostupno na: http://www.kombeg.org.rs/aktivnosti/c_privprav/Detaljnije.aspx?veza=13054 datum pregleda 05.12.2017.

odobriti reprodukovanje u svim oblicima, uključujući štampanje i zvučne zapise. Takođe nosioc ovim pravima može odobriti javno izvođenje i saopštavanje dela. U slučaju zahteva za prevođenjem dela na druge strane jezike, kao i zahteva za eventualnom adaptacijom na nosiocu autorskog prava je da li će ili neće iste odobriti.

2.4 Kršenje autorskih prava u cyber prostoru

Popularizovanju upotrebe interneta i njegovom brzom širenju u mnogome je doprinelo otvaranje mreže za javni pristup, jednostavnost publikovanja sadržaja, lako pronalaženje istog kao i pristup velikoj količini informacija različitog sadržaja na jednom mestu. Velika količina informacija dovela je do teškog razlikovanja sadržaja koji je zaštićen autorskim pravima od onog koji nije. Ukoliko se uporedi sa štampanim delima kao i delima na nosiocima slike i zvuka kod kojih je jasno naznačeno ko je nosioc autorskog prava i da li je delo zaštićeno autorskim pravom, u slučaju cyber prostora korisnici nisu uvek u mogućnosti da ustanove legalne načine preuzimanja, izmene i kasnije reprodukcije određenog dela. Međutim korisnici ovakvih sadržaja uvek bi trebalo da imaju na umu da većina sadržaja podleže autorskim pravima.

Kršenje autorskih prava prilikom reprodukcije i/ili distribucije autorskim pravom zaštićenog digitalnog materijala u cyber prostoru nije novina i dešava se svakodnevno. Uopšteno govoreći mogu se istaći dva najznačajnija oblika i predmeta potencijalnih kršenja intelektualne svojine, a to su softver i multimedijalni sadržaji u digitalnom obliku. Softver i multimedijalni sadržaju kao takvi sa jedne strane najčešće podležu zaštiti autorskim pravo i nude se korisnicima interneta uz određenu nadoknadu. U ovu grupu sadržaja najčešće spadaju audio i video sadržaji, igrani i dokumentarni filmovi, komercijalni i softveri za kućnu i ličnu upotrebu, kao i multimedijalni tutorijali kreirani od strane pojedinca ili organizacije[5]. Ovako kreiranim digitalnim sadržajima kršenjem autorskih prava pristupa se putem različitih vidova mreža za razmenu fajlova, piratskih servera, web sajtova, kao i uz pomoć hakovanih računara. Razmena fajlova predstvalja proces upload-a datoteka na internet. Ovako datoteke postaju javno dostupne i mogu se preuzeti i reprodukovati. Celokupan proces obavlja se upotrebom legalnog softvera, dok se njegova upotreba koja dovodi do kršenja autorskih prava smatra nelegalnom. U cilju razmene i kopiranja fajlova bez poštovanja autorkih prava koriste se i servisi koji omogućavaju računarima direktno međusobno povezivanje bez posredovanja centralnog servera. Jedan od prvih servisa za razmenu muzičkih fajlova pojavio je 2000. godine. Ovaj servis nosio je naziv *Napster* i omogućio je milionima korisnika razmenu uglavnom autorskim pravima zaštićene muzičke fajlove. Posle niza sudskih sporova servis je ugašen. Gašenje ovog servisa nije obeshrabrilo korisnike ovakvih servisa u pokušajima kreiranja i upotrebe novih.

[5] Vidoje Spasic, Branko Stevanovic, „Dokazivanje digitalnih povreda prava intelektualne svojine – osvrt na anglosaksonski pravni sistem“, Zbornik radova Pravnog fakulteta u Nišu, Broj 69, pp. 203 – 226., 2015.

Novi servisi koji su i danas u upotrebi u svom radu primenjuju drugačiji protokol koji u velikoj meri onemogućava krivično gonjenje lica. Ovaj protokol nazvan je *BitTorrent*. Sama činjenica da lice koje učestvuje u razmeni fajlove ne može biti procesuirano dovela je do masovne upotrebe ovih servisa. Ovi servisi poslednjih godina nisu ograničeni samo na deljenje muzičkih fajlova. Putem ovi servisa korisnici mogu preuzeti gotovo sve digitalne sadržaje od muzike preko video sadržaja sve do različitih vrsta softvera. Princip rada torent servisa organizovan je tako da korisnik nelegalne kopije sadržaja zaštićenog autorskim pravom pomoću javno dostupnog i legalnog softvera kreira torent fajl i upload-uje ga na neki od prepoznatljivih web sajtova za skladištenje ovakvih fajlova. S tim u vezi potrebno je istaći da kreirani torrent fajl ni u kom slučaju nije nelegalan, jer on samo sadrži informacije o većem fajlu koji ne mora obavezno da predstavlja fajl koji je zaštićen autorkim pravom. Da torent fajl nije nelegalan dokazuje i presuda suda države Ajova iz 2014. godine, kojom je ovaj sud masovnu tužbu protiv BitTorrent korisnika odbio kao neosnovanu. U prilog odbijanju išla je činjenica da nije bilo moguće dokazati vezu između torrent fajla i internet pirata[6]. Proces preuzimanja digitalnog sadržaja sa mreže pomoću torrent fajla svakog od korisnika ovakvih servisa čini prestupnikom. Postupak preuzimanja digitalnog sadržaja zaštićenog ili ne auorskim pravom počinje tako što korisnik pomoću softvera pokreće preuzeti torent fajl. Korisnik ustvari preuzima mnogo malih delova na koje je digitalni fajl podeljen. U isto vreme i drugi korisnici od samog korisnika preuzimaju one delove fajla koje je on već preuzeo na svoj računar. Ovo praktično znači da sve delove fajla koje je već preuzeo korisnik deli sa drugim korisnicima, dok one koje još uvek nije preuzeo preuzima od drugih korisnika. Na kraju celokupnog procesa digitalni fajl preuzeo je toliko veliki broj korisnika da osoba koja je inicirala deljenje može da prestane sa istim. Ovako kreirana mreža je decentralizovana, pa se pretraga digitalnih fajlova svodi na pretragu torrent fajlova u kojima se nalazi spisak računara sa željenim datotekama. Neki od prepoznatljivih servisa koju su korišćeni i/ili koji se i danas koriste za deljenje torrent fajlova su The Pirate Bay, Kickass.to, Demonoid, MiniNova, Zamunda, itd. Veliki broj sudskih presuda protiv različitih servisa za deljenje torent fajlova svedoči o tome koliko je borba protiv ovakvog kršenja autorskih prava postojana. Jedan od primera je sudski spor koji se vodio pred sudom u Finskoj. Naime nakon upada policije na Bit Torent sajt pod nazivom Finreactor uhapšeno je jedanaest osoba. Za načinjenu štetu zbog distribucije autorskim pravom zaštićenog digitalnog materijala naloženo im je da plate pola miliona eura odštete i 200 000 eura na ime sudskih troškova. Ceo proces je nakon niza žalbi optuženoh stigao do Vrhovnog suda Finske koje je još jednom potvrdio prvostepenu presudu[7]. Šest administratora EliteTorrents.org sajta nakon preuzimanja kontrole nad sajtom od strane Federalnog istražnog biroa Sjedinjenih Američkih Država priznalo je krivicu za učešće u zaveri u kojoj su izvršena krivična dela kršenja

[6] Ernesto Van der Sar, „Judge Understands BitTorrent, Kills Mass Piracy Lawsuits“, dostupno na: https://torrentfreak.com/judge-understands-bittorrent-kills-mass-piracy-lawsuits-140130/, datum pregleda: 06.12.2017.

[7] Enigmax, „The Pirate Bay Trial: Understanding Finreactor“, Torrent Freak, dostupno na: https://torrentfreak.com/the-pirate-bay-trial-understanding-finreactor-090223/, datum pregleda: 05.12.2017.

autorskih prava i objavljivanja radova pre njihovog komercijalnog izdavanja. Njima su nakon suđenja izrečene kazne zatvora, kućnog pritvora kao i novčane kazne. Izrečene zatvorske kazne zasnovane su na krivičnom zakonu[8]. Hapšenje Artem Vaulina vlasnika KickAssTorents izvedeno je u koordinisanoj akciji IRS-a[9] i Homeland Security-a[10]. U postupku pribavljanja činjenica koje su dovele do hapšenja učestvovali su takođe Facebook i Apple putem čijih servisa je ustanovljena IP adresa računara sa koga je Artem pristupao. Ista IP adresa je korišćena za kupovinu na iTunesu kao i za pristupanje KickAssTorents facebook stranici. Takođe je bila povezana sa Bitcoin računom na koji su pokrovitelji uplaćivali donacije u cilju podrške KickAss torentu. Artem je optužen za kršenje autorskih prava i pranje novca. Na računu otvorenom u litvanskoj banci u cilju čuvanja novca prikupljenog od nelegalnih transkacije u toku perioda od sedam meseci istražitelji su evidentirali nešto više od 31 milion dolara. Procenjuje se da je sami torent servis tokom svog postojanja distribuirao različite digitalne sadržaje u vrednosti od preko milijardu dolara[11].

Direktno preuzimanje se web sajtova još jedan je od metoga deljenje digitalnih sadržaja. Ovakav metod kao i svi ostali nije nelegalan ukoliko sadržaj koji se deli nije zaštićen autorskim pravom. Primera radi ukoliko se radi o softverskim rešenjima otvorenog koda (open source), takvi softveri se mogu deliti putem bilo kog servisa bez ikakave bojazni od zloupotrebe autorskih prava. Čak šta više same softverske kompanije ili pojedinci koji su razvili konkretan softver su inicijatori deljenja kako bi što veći broj korisnika bio u mogućnosti da isproba samo rešenje i predloži promene u samom kodu. Preuzimanje digitalnog sadržaja koji podleže zaštiti autorskim pravom direktno sa web sajtova razvilo se zbog činjenice da preuzimanje pomoću torenta zavisi od većeg broja korisnika pa ponekad zna da bude sporije ili da se ne završi do kraja uspešno. Kod direktnog preuzimanja digitalni sadržaj se pakuje u određeni format (obično je to .rar ili .zip). Tako kreirani fajl se zatim deli na više jednakih delova, od kojih se svaki upload-uje na server određenog web sajta. Linkovi koji vode do pojedinačnih delova obično se publikuju na nekom od foruma ili drugih web sajtova kako bi bili lako dostupni korisnicima. Nakon preuzimanja pojedinačnih delova korisnik mora da pojedinačne delo spoji u jedna digitalni fajl nakon čega sledi nesmetano korišćenje. Neki od primera web sajtova za direktno preuzimanje su Mega.co.nz, FileShare.link, itd. U optužnici protiv vlasnika Megauploada Kim Dotcom-a kao i tri direktora uhapšenih na Novom Zelandu 2012 godine navodi se da su kršenjem autorskih prava oštetili nosioce autorskih prava različitih filmova, serija i drugih sadržaja za više od 500 miliona dolara. Oni su uhapšeni po optužnici zvaničnika

[8] Andre Yoskowitz, „Elite Torrents admin gets 18 months in jail“, News by afterdawn, dostupno na: http://www.afterdawn.com/news/article.cfm/2008/09/10/elitetorrents_admin_gets_18_months_in_jail, datum pristupa: 05.12.2017.

[9] https://www.irs.gov/

[10] https://www.dhs.gov/

[11] Greg Sandoval, „An interview with alleged KickassTorrents founder in his jail cell in Poland“, The Verge, dostupno na https://www.theverge.com/2017/5/23/15681160/kickasstorrents-founder-artem-vaulin-interview-bittorrent, datum pristupa: 06.12.2017.

SAD-a[12]. U optužnici se navodi da je Dotkom, koji je inače rodom iz Nemačke sa trenutnim mestom boravka u Hongkongu i Novom Zelandu zaradio u 2010. godini 42 miliona dolara. Zanimljivo je da pored dva mesta boravka Dotkom ima i dvojno državljanstvom Finske i Nemačke. Procena stručnjaka je da su na bazi pretplate za premium naloge ovaj servis a samim tim i njegovi vlasnici zaradili nešto više od 175 miliona dolara[13].

Jedan od trendova kršenja autorskih prava koji se pojavio sa razvojem veće brzine interneta jeste online gledanje sadržaja (streaming). Ovakav princip u upotrebi je kod gledanja digitalnog sadržaja u vidu različitih video zapisa, serija, filmova, emisija, itd. Takođe u ovu grupu sajtova spadaju i sajtovi koji omogućavaju praćenje sporskih ili drugih kanala za koje je potrebno platiti mesečnu pretplatu. Praktično sajtovi koji pružaju ovakve usluge obično su registrovani u zemljama u kojima zaštita autorskih prava nije preterano razvijena pa se kršenje intelektualne svojine toleriše. Oko kršenja autorskih prava gledanjem digitalnog sadržaja pomoću streaming-a podeljena su mišljenja sudrske prakse. U jednom rešenju je pokrajinski sud u Kelnu u odluci ustanovio, da vlasnik IP-adrese zaštićenog autorskog dela preko tzv. berze za razmenu fajlova (npr. BitTorent) neovlašćeno pristupio podacima zaštićenih autorskih dela. Zbog ovih prestupa sud je u rešenju konstatovao, da internet servis provajderi moraju otkriti identitet korisnika tj. posetioca web sajta, koji na ovaj način krše autorska prava. Specifičnost ovog slučaja ogleda se u tome da se nije radilo o konkretnom preuzimanju sadržaja već streaming-u. Advokatska kancelarija koja je i pokrenula spor protiv velikog broj korisnika (oko 60000) agrumentovala je svoj postupak time da prilikom pozivanja video stream-ova dolazi do keširanja sadržaja i da je na takav način moguće napraviti kopiju videa koji je zaštićen autorskim pravom[14]. Naime u ovim sporovima ostalo je sporno da li je advokatska kancelarija imala pravo da na bilo koji način vrši praćenje korisnika i snimanje IP adresa korisnika koji su posećivali konkretan poral. S tim u vezi sud u Hamburgu je konstatovao povredu prava privatnosti od strane agencije zbog finansijskih interesa. Ovakva sudska odluka predstavlja ne samo pobedu korisnika Redtube portala, već i svih onih, koji posećuju streaming web sajtove.

Da kršenje autorskih prava nije svojstveno samo pojednicima ili manjim kompanijama spremnim da zarad finansijske dobiti prekrše autorska prava drugih svedoče i primeri narušavanja prava intelektualne svojine od strane velikih kompanija. Jedan od takvih primera je i digitalna biblioteka kompanije Google. Ova biblioteka

---

[12] Rich McCormick, „Megaupload founder Kim Dotcom can be extradited to the US to face copyright charges“, The Verge, dostupno na: https://www.theverge.com/2015/12/22/10655646/megaupload-founder-kim-dotcom-can-be-extradited-to-the-us-to-face, datum pregleda: 05.12.2017.

[13] Sean Gallagher, „The Fast, Fabulous, Allegedly Fraudulent Life of Megaupload's Kim Dotcom“, Wired, dostupno na: https://www.wired.com/2012/01/kim-dotcom/, datum pregleda: 07.12.2017.

[14] Andrej Diligenski, „Ispitivanje IP-adresa i ugrožavanje privatnosti zbog kršenja autorskih prava gledanjem streaming-a-slučaj Redube“, Zaštita podataka o ličnosti, dostupno na: http://partners-serbia.org/privatnost/blog/ispitivanje-ip-adresa-i-ugrozavanje-privatnosti-zbog-krsenja-autorskih-prava-gledanjem-streaming-a-slucaj-redtube/, datum pregleda: 07.12.2017.

nudi veliki broj digitalizovanih knjiga svojim korisnicima. Neadekvatna realizacija izuzetno dobre ideje dovela je do sudskog spora između kompanije Google i autora čija su se dela bez odobrenja za digitalizaciju našla u biblioteci. Spor se završio presudom suda po kojoj je Google mora da plati troškove autorima[15].

2.5 Javno vlasništvo intelektualne svojine

Javno valsništvo intelektualne svojine (javni domen) predstavlja inovacije, znanje, kreacije nad kojima fizička ili pravna lica ne mogu ili ne žele da imaju i održavaju vlasničke interese. Dela i inovacije svrstana u ovu kategoriju predstavljaju svojevrsno nasleđe čovečanstva. Ovo praktično znači da se ovakva dela mogu koristtiti bez ikakave mogućnosti kršenja autorskih prava.

Zaštita intelektualne svojine a samim tim i autorskog prava je po svojoj prirodi privremena. Prema Bernskoj konvenciji iz 1886. godine javnom vlasništvu pripadaju dela kojima je prestala autorsko pravna zaštita. Ovo praktično znači da intelektualna dela i kreacije nakon prestanka prava intelektualne svojine prelaze u javno vlasništvo intelektualne svojine. To je opšti, završni i nepovratni status intelektualnih kreacija i komercijalnih simbola koji nisu zaštićeni odredjenim oblikom intelektualne svojine. Karakteristično za dela u javnom vlasništvu jeste da ne mogu biti prisvojena u privatne svrhe kao i to da su dostupna svakome za slobodno kopiranje i korišćenje[16]. Novo delo koje može nastati menjanjem, unapređenjem i/ili inkorporacijom dela iz javnog vlasništva ne mora obavezno predstvaljati javnu svojinu. Novonastalo delo može sadržati delove koji se mogu zaštititi autorskim pravom, tačnije može biti vlasništvo autora koji ga je kreirao. U tom slučaju ukoliko autor koji je kreirao novo delo na bazi dela iz javnog vlasništva nije jasno naglasio da delo stavlja u javno vlasništvo korisnici takvog dela se trebaju odnositi prema delu kao da nad njim ili nad nekim njegovim delom postoje zadržana autorska prava.

Autorska dela na različite načine mogu postati deo javnog vlasništva. Neki od načina prelaska dela iz domena zaštićenog autorskim pravima u domen javnog vlasništva su:

- **Izostanak pravne zaštite.** U ovu grupu mogu se ubrojiti različita dela, kako onda dela koja su nastala pre donošenja zakona o zaštiti intelektualne svojine, dela za koja je nemoguće utvrditi ko je autor, kao i dela na koja se ne može primeniti zakon o zaštiti intelektualne svojine.
- **Prestanak pravne zaštite istekom roka**. Sva dela koja podležu zaštiti autorskim pravom u zavisnosti od nivoa primenjene zaštite imaju definisan vremenski rok važenja zaštite. Nakon isteka tog roka dela prelaze u javno vlasništvo. Primera

[15] Overbeck Wayne, Belmas Genelle, „Major Principles of Media Law“, Stamford: Cengage Learning, pp. 281, 2011.
[16] Miodrag Marković, „Opšti uvod u pravo intelektualne svojine“, Seminar IS i privreda u srbiji, 2007.

vremenski rok važenja patenata je 20 godina[17]. Jedan od ciljeva patentnog sistema je da stavi nove tehnologije u javno vlasništvo, kroz svoje informativne funkcije. Na primer priznanje patenta zavisi od otkrivanja pronalaska, tj. odavanja tajnosti pronalaska. Objavljivanje pronalaska od strane zavoda za patente čini ga dostupnim javnosti i omogućuje drugima da shvate pronalazak, da budu njime inspirisani i da ga koriste za istraživanje ili eksperimente (zavisno od patentnog zakona koji se primenjuje) kao oslonca za dalji razvoj tehnologije. Takodje jednom kada patent istekne, javnosti ne samo da je je dopušteno već se i ohrabruje da koristi pronalazak koji pripada javnom domenu[16].

- **Odricanje od pravne zaštite.** Stavljanjem dela u javni domen autor se odriče prava koja je imao nad im delom. Ovakvo odricanje s obzirom da je dobrovoljno i neopozivo ne može se kasnije opozvati, pa samim tim autor ne može povratiti prava koja je imao nad konkretnim delom. Zakoni pojedinih zemalja regulišu ovu oblast po pitanju dela koja se mogu proglasiti javnim vlasništvom. Primera radi u SAD-u je Zakonom definisano da se sva dela kreirana od strane Vlade tretiraju kao javno vlasništvo.

U skladu sa Bernskom konvencijom određena dela se mogu podrazumevano klasifikovati u javno vlasništvo u. Član 2 stav 4 ove konvencije definiše da zvanični tekstovi zakonodavne, administrativne i pravne prirode, kao i zvanični prevodi ovakvih tekstova ne mogu se zaštiti autorskim pravom. Pored ovakvih dokumenata članom 2 stav 8 Bernske konvencije definisano je da u domen javnog vlasništa obavezno spadaju i dnevne vesti i informacije. Veliki broj zemalja prati konvenciju onako kako je definisana u cilju ograničavanja zaštite autorskim pravom, dok pojedine zemlje vrše i dopunu svojim nacionalnim zakonima. U zemljama poput Alžira, Kine, Francuske, Italije, Koreje pod javnim vlasništvom se smatraju u najmanju ruku zakoni i pod zakonski akti, kao i sudske odluke[18]. Pojedine države u nekim slučajevima vrše proširenje domena podrazumevanog javnog vlasništva na dela proizvedena ili subvencionisana od strane države ili drugih javnih ustanova. U grupu ovakvih država ubrajaju se Brazil, Malezija, SAD. Primera radi Nemačka odobrava i slobodu korišćenja i izmene takvih dokumenata. Sudska praksa ponekad isključuje dela koja imaju normativnu vrednosti, kao što su bankovne novčanice, zvanični ispiti za određene profesije, kao i misljenja data od strane nekog sudije. Da postoje i države koje ne primenjuju principe ove konvencije svedoče i primeri država koje priznaju Crown Copyright kao što su Velika Britanija i Australija. Zemlje koje praktikuju ovakvu zaštitu sklanjaju službena dela iz javnog domena i daju im zaštitu autorskim pravom, dok je nosilac zaštite država (u slučaju Australije) ili kraljica (u slučaju Velike Britanije)[19]. Ako posmatramo dnevne vesti kao jedan od oblika javnog vlasništva Kina,

[17] Dragan Prlja, Mario Reljanović, Zvonimir Ivanović, „Internet pravo“, Institut za uporedno pravo Beograd, 2012.

[18] As far as official translations of such acts are concerned, see J. GINSBURG & T. RICKETSON, The Berne Convention for the Protection of Literary and Artistic Works – 1886-1986, Oxford Press, 2006, § 8.108

[19] Severine Dusollier,“Scoping study on copyright and related rights and the public domain”, WIPO, 2010.

Kosta Rika, Italija, Korea bile bi neke od zemalja koje ovo pravilo eksplicitno pružaju. Sa druge strane postoje i zemlje u kojima se ovo pravilo primenjuje u skladu sa sudskom praksom zbog nedostatka originalnosti[20]. Postoje i primeri da države nacionalnim zakonima određene kategorije dela prebacuju iz autorskim pravom zaštićene kategorije u domen javnog vlasništva. Članom 11 Zakona o autorskim pravima (Copyright Act) Čile je definisao da dela koja su dobijena eksproprijacijom od strane države postaju javno vlasništvo. Ovakva praksa uvedena je početkom 70-tih godina kada je vlada socijalista na ovakav način održavala duh vremena kada su eksproprijacije za javni interes bile politička strategija. Članom 66 Zakona o autorskim pravima Kosta Rike kao i članom 45 istog zakona Brazila definisano je da dela zaštićena autorskim pravom postaju javno vlasništvo nakon smrti nosioca autorskog prava ukoliko nosilac prava nema zakonske naslednike.

Uvođenje javnog vlasništva veoma je značajno. Gotovo se može reći da je uvođenje javnog vlasništva podjednako značajno kao i postojanje autorskih prava. Razlozi za uvođenje javnog vlasništva različiti su i kreću se od domena obrazovnog karaktera preko demokratskog i ekonomskog pa sve do uspostavljanja slobodne konkurencije. Uloga javnog vlasništva ogleda se u stvaranju pozitivne atmosfere slobodnog stvaralaštva, kulturološke različitosti, inovativnosti pojedinaca i gupe, kao i razvoju nauke i kulture. Posebno je značajan uticaj javnog domena u kulturi i nauci. U ovim oblastima javni domen se ogleda u stvaranju kulturnih i naučnih dobara koja će biti dostupna svima. Na ovakav način uvođenjem javnog domena dela su zaštićena od privatizacije i prisvajanja. Još bitnija osobina javnog vlasništva jeste uspostavljanje balansa između svima dostupnih dela i isključivosti koju nosi intelektualna svojina[19].

2.6 Licence otvorenog sadržaja i licence kreativne zajednice

Velika količina informacija koja se razmenjuje putem internet servisa, kao i različitost publikovanog sadržaja stvorili su potrebu definisanja opštih licenci. Ovim licencama definisan je način i mera u kojoj se može koristiti odeđeno autorsko delo. Ovo praktično znači da će privilegije korišćenja autorskog dela zavisiti od vrste licence koja se primenjuje nad njim.

Pravilima definisanim u okviru ovih licenci autor samostalno donosi odluku da li će ili neće dozvoliti komercijalnu ili nekomercijalnu upotrebu svog dela. Nekomercijalno korišćenje autorskog dela u praksi ne mora obavezno značiti i neostvarivanje ekonomske dobiti za autora dela. Praktično autor u ovom slučaju ipak može ostvariti ekonomsku dobit ukoliko sa izdavačkom kućom sklopi ugovor. Na osnovu ovako definisanog ugovora autoru će sama izdavačka kuća isplatiti određenu ekonomsku nadoknadu. U procesu licenciranja licencama otvorenog sadržaja autori moraju poštovati proceduru licenciranja kako bi se za predmetno delo moglo smatrati da je

[20] See for instance, the US Supreme Court case, International News Service v. Associated Press, 248 U.S. 215, 234 (1918).

zaista i licencirano. Kako se za upotrebu dela licenciranog licencom otvorenog sadržaja ne zahteva finansijska nadoknada svaka ovakva licenca sadrži klauzulu na osnovu koje licenca ne daje nikakvu garanciju autoru dela. Zavisno od karakteristika privilegija koje nude licence otvorenog sadržaja mogu se podeliti na licence opšteg tipa ili licence specijalne namene. Takođe prema prirodi ove licence se mogu podeliti na licence sa malim ograničenjima i licence kojima su jasno definisana ograničenja korišćenja dela. Primera radi Licence kreativne zajednice su licence kojima se jasno definišu ograničenja u slobodi korišćenja autorskog dela[21].

U domen licenci specijalne namene kojima se definišu posebna prava i privilegije korišćenja spadaju licence za softverska rešenja. S tim u vezi može se reći da se kod distribucije softvera definišu različite licence u zavisnosti od privilegija dodeljenih korisniku. Što se tiče softvera otvorenog izvornog koda (engl. open source software) on predstavlja vrstu softverskih licenci kod kojih je programski kod dostupan svakome ko želi da ga unapredi ili razvije. U sklopu ovih licenci definišu se različite druge podele, ali suština besplatnog softvera ostaje ista. Podela u licencama otvorenog izvornog koda definisana je na:

- copyleft licence. Ove licence definisane su tako da ograničavaju slobodu korisnicima softvera i na taj način čuvaju otvorenost samog softvera.
- permissive licence. Ove licence imaju za cilj da korisniku softvera daju što veći stepen slobode.

Njihove glavne razlike su vezane za upotrebu izvornog koda u drugim projektima kao i upotrebi softvera proizašlog iz tih novih projekata. Primeri softvera otvorenog izvornog koda: Linux, OpenOffice, apache web server. Primeri ovako koncipiranih licenci koje su danas u upotrebi dati su u nastavku:

- GPL (General Public License). Ovaj tip licence daje korisniku veoma široka prava koja se ogladeaju u mogućnosti redistrubucije i obrnutog inženjeringa. Ovo praktično znači da korisnik može vršiti izmene na softveru. Iako se korisniku omogućava vršenje izmena nad izvornim kodom softvera on ipak mora ispuniti određene uslove propisane ovim tipom licenci. Jedan od osnovnih uslova je i obaveza objavljivanja svih izmena izvornog koda.
- LGPL (Lesser General Public License), licenca se uglavnom primenjuje na softverske biblioteke. Ovo praktično znači da korisnik može da distribuira i modifikuje softver tako da sve što je povezano sa bibliotekom potpada pod samu licencu i može se tako distribuirati, dok sama kreirana aplikacija koja koristi biblioteku ne može biti pod ovom licencom[22].

[21] Lawrence Liang, „Guide to Open Content Licenses", Piet Zwart Institute e for postgraduate studies and research Willem de Kooning Academy Hogeschool Rotterdam, 2005, dostupno na: http://www.theartgalleryofknoxville.com/ocl_v1.2.pdf, datum pregleda: 09.12.2017.

[22] Andrew M. Laurent, „Understanding Open Source and Free Software Licensing", O'Reilly Media, Inc, 2004. Dostupno na: https://www.safaribooksonline.com/library/view/understanding-open-source/0596005814/, datum pristupa: 09.12.2017.

- BSD (Berkeley Source Distribution). licenca garantuje krajnjem korisniku potpunu autonomnost nad softverom. Na ovakav način korisniku se mogućava da predmetni softver i njegov izvorni kod iskoristi kao deo softvera zatvorenog koda objavljenog pod vlasničkom licencom.

Jedan od možda najboljih primera primene licenci otvorenog sadržaja jeste GNU pokreti ili GNU zajednica. Ova zajedica predstavlja jednu od prvih praktičnih i uspešnih incijativa koje omogućavaju korisnicima softvera da slobodno koriste prednosti koje nudi korišćenje informaciono komunikacinih tehnologia. Sami pokret počeo je sa aktivnostima 1984. godine. Njegov cilj bio je stvaranje operativnog sistem otvorenog koda pod nazivom UNIX. Za GNU GPL licencu slobodno se može reći da predstavlja jednu od široko poznatih licenci kada je softverska industrija u pitanju. Samom licencom definisana je sloboda korišćenja softvera, njegovog kopiranja, izmene kao i distribucije svih verzija softvera nastalih na bazi osnovne verzije. Copy left princip i ovde je prisutan. Praktično distribucija slobodnog softvera mora da se vrši pod istovetnim uslovima pod kojima je prvobitno sami softver korisnik dobio. Na ovakav način GPL daje slobodu i korisniku i softveru.

Ograničenja u korišćenju dela definisana autorkim pravom pre pojave interneta u najvećem broju slučajeva odnosila su se na ograničavanje ili zabranu prikazivanja samog dela ili pak strogu zabranu preštampavanja i umnožavanja kako od strane pojedinca tako i od strane drugih izdavača. Ovako definisana ograničenja autorskog prava postala su limitirajući faktor za druge korisnike autorskih dela koja su nastala sa razvojem tehnologije. Praktično razmena, kopiranje ili čuvanje podataka i informacija ne mogu se obavljati na način propisan tehnologijama. Upravo iz tih razloga sama upotreba tehnoloških uređaja ili novih softverskih rešenja nad podacima i informacijama dostupnim na internetu svakodnevno dovodi do kršenja autorskih prava. Potrebno je naglasiti da pomenute licence kreativne zajednice nisu zamena za autorska prava. Praktično one su definisane kako bi bile dopuna autorskih prava i kako bi omogućile prilagođavanje potrebama i željama svakog pojedinačnog autora. Primenjene nad autorskim pravom ove licence ga čine znatno fleksibilnijim. U isto vreme one pružaju standardizovan način čuvanja autorskog dela uz dozvolu za korišćenje dela na unapred definisan način. Svaka od ličenci kreativne zajednice sa jedne strane štiti autore dela i pruža im mogućnost da zadrže autorska prava, dok sa druge strane korisnicima dela pruža mogućnost umnožavanja, distribucije i korišćenja zaštićenih dela. Ovo je posebno omogućeno ukoliko se dela koriste u nekomercijalne svrhe, mada i odobravanje korišćenja u komercijalne svrhe nije retkost. Skup licenci kreativne zajednice obuhvata šest licenci. Ove licence razlikuju se prema stepenu fleksibilnosti koji je ponuđen korisniku. Svaka od šest licenci omogućava korisniku kopiranje sadržaja[23]. Opis licenci kreativne zajednice dat je u sledećoj tabeli[24].

[23] Dragan Milić, „Creative commons licenses – licence kreativne zajednice – pojam i vrste“, dostupno na: http://www.milic.rs/blog/autorsko-pravo/164-creative-commons-licenses-licence-kreativne-zajednice-pojam-i-vrste, datum pregleda: 05.12.2017.

[24] Creative Commons, „O licencama“, dostupno na: https://creativecommons.org/licenses/?lang=hr, datum pregleda: 05.12.2017.

Tabela 1. Opis licenci kreativne zajednice

Oznaka	Naziv	Objašnjenje
CC BY	Imenovanje	Ova licenca dopušta drugima da distribuiraju, modifikuju, prilagođavaju i nadograđuju autorsko delo, čak i u komercijalne svrhe. Upotreba u komercijalne svrhe obavezuje navođenje imena autora onako kako je to odredio sami autor ili davaoc licence. Ovo je najslobodnija od svih licenci i preporučuje se u slučaju daljeg korišćenja licenciranih materijala.
CC BY-SA	Imenovanje – deljenje pod istim uslovima	Ovom licencom autor dozvoljava umnožavanje,redistribuciju, menjanje kao i javno saopštavanje dela čak i u komercijalne svrhe. Sve ovo mora biti urađeno uz navođenje imena autora na način odredjen od strane autora ili davaoca licence. Novonastalo delo bazirano na autorskom delu se takođe može licencirati ali pod istim uslovima kao i originalno.
CC BY-ND	Imenovanje- bez prerada	Ovom licencom autor dopušta redistribuiranje, komercijalno i nekomercijalno, dokle god se delo distribuira celovito i u neizmenjenom obliku, uz isticanje autora.
CC BY-NC	Imenovanje - nekomercijalno	Ovom licencom se dozvoljava remiksiranje, menjanje i nadogradnja originalnog dela u nekomercijalne svrhe. Nadogradnja samog dela moguća je iz navođenje imena autora onako kako je to odredio sami autor ili davaoc licence. Prerade moraju imati navedeno ime originalnog autora ali ne moraju se licencirati pod istim uslovima kao originalno delo.
CCBY-NC-SA	Imenovanje- deljenje- pod istim uslovima	Ovim tipom licence drugima je dopušteno da remiksiraju, menjaju i prerađuju autorsko delo u nekomercijalne svrhe, pod uslovom da navedu autora izvornog dela i licenciraju svoja dela nastala na bazi autorovog pod istim uslovima.
CC BY-NC-ND	Imenovanje- nekomecijalno- bez prerada	Ovo je najrestriktivnija od navedenih šest osnovnih licenci – dopušta drugima da preuzmu autorsko delo i da ga dele s drugima pod uslovom da navedu autora. Takođe preuzeto delo se ne sme menjati ili koristiti u komercijalne svrhe.

Pregledom opisanih licenci uočava se činjenica da svaka od šest licenci bez obzira na nivo privilegija koji nudi korisnicima autorskog dela zaštićenog licencom zahteva od njih imenovanje autora originalnog dela. Zanimljiva je činjenica da čak i slučajevima kada je na osnovu dela zaštićenog autorskim pravom kreirano novo delo, novo delo može i ne mora biti licencirano istom licencom ali autor originalnog dela mora biti naveden.

Upotreba licenci kreativne zajednica prvobitno je bila orijentisana ka fizičkim licima (autorima kreativnih dela), međutim sa sve većim problemima sa kojima se kreativna zajednica susreće po pitanju zaštite autorskih prava sve je veći broj korisnika ovih licenci iz reda pravnih lica i državnih organa. Sve ovo svedoči o značaju ovakvog kreiranja i korišćenja licenci.

2.7 ACTA (Anti - Counterfeiting Trade Agreement) multilateralni sporazum

Količina digitalnog sadržaja dostupnog u cyber prostoru omogućila je veliki broj zloupotreba dela zaštićenih pravom intelektualne svojine. Danas gotovo da ne postoji delo koje se u cyber prostoru ne može pronaći i kao takvo korisiti kako uz poštovanje autorskih prava tako i zloupotrebom istih. Koliko veliki problem za intelektualnu zajednicu predstavlja zloupotreba autorskih dela u cyber prostoru svedoče i međunarodni sporazumi kreirani u cilju osmišljavanja efikasnog sistema zaštite intelektualne svojine. Ovi sporazumi moraju biti prilagođeni vremenu u kome su digitalne tehnologije daleko zastupljenije od tradicionalnih papirnih formi publikovanja dela.

Jedan u nizu ovakvi sporazuma je i ACTA međunarodni sporazum čiji je cilj zaštita intelektualne svojine. Pregovori po pitanju sporazuma zaključeni su 1.oktobra 2011. godine potpisivanjem u Tokiju. Zemlje potpisnice koje su i vodile pregovore bile su Singapur, SAD, Maroko, Kanada, Japan, Novi Zeland, i Južna Korea. Nekoliko meseci nakon potpisivanja sporazumu se priključila i Evropska unija, tačnije 22 zemlje članice. Pored činjenice da su 22 zemlje članice Evropske Unije potpisale priključenje ovom sporazumu posle niza negodovanja parlament EU je 4.7.2012. je odbio ovaj sporazum. Od ukupnog broja poslanika Evropskog Parlamenta 478 polsanika je glasalo protiv sporazuma, 39 je bilo za ratifikovanje, dok je 165 poslanika ostalo uzdržano[25].

Rad na ovom sporazumu i njegovo kreiranja od samog početka bilo je obavijeno velom tajne. Samu tajnost ovog sporazuma povećava činjenica da u prve pregovore nisu bile uključene vodeće svetske institucije poput UN, STO ili SOIS. Prvi pregovori povodom ovog sporazuma započeti su 2006. godine između zvaničnika SAD-a i Japana. Kasnije su se pregovorima priključile najveće i najmoćnije države sveta poput

[25] BBC News, „Acta: Controversial anti-piracy agreement rejected by EU“, dostupno na: http://www.bbc.com/news/technology-18704192, datum pregleda: 10.12.2017.

članica EU. Zvanično su pregovori započeti 2007. godine. U isto vreme pojedine zemlje koje su bile uključene u neformalne pregovore napuštaju zvanične pregovore čime izražavaju protivljenje ideji celog sporazuma. Ono što je možda unelo i najveću sumnju u namere ovakvog sporazuma bila je to što su pojedine zemlje sadržinu sporazuma proglasile državnom tajnom. U prilog nepoverenju prema ovom sporazumu išlo je i to što su adminstracije Džordža Buša i Baraka Obame odbile da verzije ACTA sporazuma o kojima se pregovaralo učine dostupnim javnosti. Pored SAD-a Evropska unija takođe je proglasila pregovore državnom tajnom. Evropska unija pravdala je ovakav postupak objašnjenjem da bi javno objavljivanje tematike pregovora ugrozilo njenu pozuciju u ovom sporazumu kao i odnose se sa državama partnerima[26]. Kanada je primera radi obvjavila kao javno samo ime dokumenta, dok je sadržina ostala tajna. Novi Zeland kao jedna od učesnica pregovora iznosio je obećanja da će tajnost ovih pregovora biti na snazi kraći vremenski period, tačnije dok od zemalja partnera ne dobije dozvolu za objavljivanje podataka. Međutim sami pregovori ostali su državna tajna sve do njihovog završetka[27]. Takođe važna činjenica po pitanju skrivanja ovog sporazuma jeste i to da bi sadržina ovog sporazuma sigurno ostala tajna da Vikiliks 2008. Godine nije otkrio da postojanje pregovora i deo sadržine sporazuma.

Osnovne odredbe ACTA sporazuma izražene u prambuli legitimne bile su zaštita autorskih prava, prava intelektualne svojine kao i sprečavanje falsifikovanja intelektualnih dobara i piraterije. Krajnji efekat potpisanog sporazuma bili su pravni metodi suprotni odredbama definisanim u regionalnim i međunarodnim dokumentima o ljudskim pravima. Osnovna ljudska prava ugrožena ovim sporazumom bila su pravo na privatnost, pravo na slobodno izražavanje, dostupnost medikamentima kao i pravo na pravično suđenje. Rešenje ovog sporazuma protiv falsifikovanja usmereno je ka primoravanju internet kompanija i internet servis provajdera da prate aktivnosti svojih korisnika na mreži, kao i da cenzurišu sadržaje. Jednim članom ovog sporazuma data je mogućnost zemljama potpisnicama da preko nadležnih organa vrše praćenje korisnika na mreži. U grupu nadgledanih korisnika svrstavaju se korisnici cyber prostora za koje postoji sumnja da su prekršili i aktivno krše principe zaštite autorskim pravom. Takođe ovaj sporazumum uvodi i globalnu agenciju koja bi se bavila suzbijanjem piraterije putem elektronskih servisa. Kazne za ovakve prekršaje definisane su i kreću se u opsegu od novčanih kazni pa do kazni zatvora za ozbiljnije kršenje autorskih prava. Pored već pomenutih primera nedostataka ovog sporazma pojedini poznavaoci ove oblasti izdvajaju pet najtežih[28].

1. ACTA trgovinski sporazum definisan na ovakav način ne pravi razliku između korisnika koji zaista krše autorska prava i onih protiv kojih je podneta neosnovana prijava. Ovo praktično znači da bi prema ovom sporazumu bilo dovoljno da nosioc

[26] Neowin Staff, „EU Council refuses to release secret ACTA documents“, FFII's Press Release, dostupno na: https://www.neowin.net/news/eu-council-refuses-to-release-secret-acta-documents, datum pregleda: 09.12.2017.

[27] Tech Liberty NZ, „Acta – The NZ Official Information Requests“, dostupno na: http://techliberty.org.nz/acta-the-nz-official-information-requests/, datum pregleda: 12.12.2017.

[28] Rakić Vodinelić Vesna, „Opasne pravne posledice ACTA“, Pescanik, dostupno na: http://pescanik.net/opasne-pravne-posledice-acta/, datum pristupa: 15.12.2017.

autorskih prava podnese prijavu da neko lice narušava autorska prava kako bi za isto provajder morao da dostavi sve podatke. Posmatrano iz ovog ugla ACTA je znatno restriktivnija od TRIPS-a, s obzirom da je prema TRIPS-u provajder u obavezi da dostavi podatke o korisniku i njegovim aktivnostima samo u slučaju kada je u istražnom postupku dokazano da je lice narušilo pravo intelektualne svojine.

2. ACTA sporazumom je pored građanskopravne zaštite, svim državama potpisnicama nametnuta obaveza krivičnopravne zaštite. Praktično članom 23 ovaj sporazum nameće kriminalizaciju povreda prava inteletualne svoije. Ovakva praksa u suprotnosti je sa deirektivom EU 2004/48. Kako je svako lice protiv koga je podneta prijava u isto vreme i krivo može se zaključiti da ACTA ne obezbeđuje pravični istražni postupak i pravično suđenje, kao ni zaštitu prava okrivljenog u istražnom pustupku. Takođe ovaj sporazum ne pravi razliku u stepenu kršenja autorskog prava, pa sa tim u vezi sporazum ne pravi razliku da li korisnik sadržaj preuzeo samo za sebe ili ga je iskoristio kako bi njime stekao dodatan profit.

3. Članom 12 ovog sporazuma nisu definisane procesne garancije za optuženog koje su uobičajene u procesnom pravu. Primera radi opruženom licu bi se oduzela sva dobra za koja se tvrdi da su nastala kao rezultat povrede prava intelektualne svojine. Ovakav postupak bio bi sproveden bez da se optuženom prethodno omogući da se izjasni po svim tačkama optužnice.

4. Članom 16 ovog sporazuma pojedinim državnim organima daju se znatno veća ovlašćenja nego što je to uobičajena praksa. Primera radi granični službenici dobijaju ovlašćenja koja smeju da imaju samo sudski organi. Ovo praktično znači da granični službenici usled sumnje da lice koje prelazi granicu u svom lap topu ili IPad-u poseduje falsifikovana intelektualna dobra (muziku, filmove, itd.) mogu narediti pregled uređaja i njegovo oduzimanje. Takođe službenicima se daje ovlašćenje da ovakva dobra okarakterišu kao dobra namenjena komercijalnoj upotrebi a ne ličnoj upotrebi kao što je to najčešće slučaj.

5. Ovim sporazumom predviđena je zaplena i uništavanje lekova sa generičkim imenom koja su najčešće u upotrebi u nerazvijenim zemljama. Zabrinjavajuća je činjenica da se u slučaju generičkih imena za lekove ne radi o falsifikovanim lekovima već o lekovima za čije je ime isteklo vreme zaštite ili se zbog odredbi nacionalnog prava stavljaju u promet pod generičkim imenom. Sumnja se da ovakvim odredbama štite interesi kompanija koje se bave biotehnologijom. S tim u vezi pomenute kompanije bi bile u mogućnosti da zaštite neki od patenata u oblasti biotehnologije u više zemalja. Praktično one bi u tom slučaju bile pod zaštitom ACTA sporazuma i znatno lakše bi mogle da ostvare svoja prava.

Sve ovo ukazuje da koncept ACTA trogovinkog sporazuma bez obzira na važnost zaštite autorskih prava stavlja akcenat na ograničavanje sloboda pojedinaca i omogućavanje stvaranja finansijske dobiti pojedinim kompanijama. Ograničenja po pitanju medikamenata i biotehnologije pored činjenice zanemarivanja humanosti navode i na razmišljanje o uticaju finansijskog lobija velikih kompanija na kreiranje ovog sporazuma.

2.8 Audio-vizuelna dela u cyber prostoru

Generalnu definiciju audio-vizuelnog dela je teško dati obzirom da danas nacionalni zakoni imaju zadatak da definišu audio-vizuelno delo. Prema Bernskoj konvenciji audio-vizuelna ili kinematografska dela svrstana su u opšti oblik zaštite autorskih prava. S obzirom na same karakteristike ovakvih dela autorska prava moraju obuhvatiti neke izuzetke. Što se tiče nosioca autorskog prava oni se određuju na osnovu pravnih odredbi zemlje u kojoj je delo nastalo. Prema zakonu o autorskim i srodnim pravima audio-vizuelna dela mogu se podeliti na kinematografska i televizijska dela. Ukoliko ovakvu podelu primenimo na audio-vizuelne zapise koji se mogu naći u digitalnom formatu kinematografska dela postaju filmska dela koja se dalje mogu uže podeliti na spektar dokumentarnih, igranih i animiranih filmova, kao i autorskih televizijskih emisija.

Ukoliko se struktura filma kao audio-vizuelnog dela posmatra malo detaljnije može se uočiti da se film kao takav može razdvojiti na veći broj dela od kojih svako može biti zaštićeno autorskim pravom. Na prvom mestu izdvaja se scenario koji predstavlja pisano autorsko delo, zatim muzička komponenta kao posebno autorsko delo audio karaktera. Na ovakav način čak se i slika može izdvojiti kao zaseban element. Da su ove karakteristike filma sagledane od strane nacionalnih zakona svedoči i Zakon o autorskim pravima Republike Srbije. Članom 11 ovog zakona definisano je da se pisac scenarija, režiser i direktor fotografije smatraju autorima filma. Ukoliko je muzika u filmu komponovana isključivo za potrebe filma onda se i kompozitor može smatrati koautorom filma. U slučaju animiranog ili crtanog filma glavni animator se takođe može smatrati koautorom ovog dela. Autorima pomenutih dela članom 33 propisano je isključivo pravo da zabrane ili odobre korišćenje ili javno saopštavanje svog dela uz pomoć uređaja za reprodukovanje istih[2].

Kada je u pitanju distribucija ili umnožavanje filmskog dela prema Zakonu, jedini je ovlašćen da odobri umnožavanje i distribuciju filmskog dela je filmski producet. Napredovanje informaciono komunikacionih tehnolofija doveo je do toga da se filmska dela masovno umnožavaju. Takođe se njihova nelegalna distribucija vriši putem interneta. Iako su nosači ovakvih dela zaštićeni, uvek se pronalazi način da se zaštita zaobiđe a delo kopira i dalje distribuira. Većina zemalja svojim zakonima definisala je prekršajne i krivične sankcije za svakog ko vrši neautorizovano uklanjanje zaštite sa nosača audio-vizuelnog dela, njegovo kopiranje i distribuciju.

Televizijski i radio programi kao drugi vid audio-vizuelnih dela različito se definišu prema Bernskoj konvenciji u odnosu na Zakon o autorskim i srodnim pravima. Bernska konvencija ih kao takve ne raspoznaje već ih katogoriše u dela izražena postupkom sličnim kinematografiji. S druge strane Zakon o autorskim i srodnim pravima ovakva dela eksplicitno spominje kao televizijska dela. Bitna činjenica je da i u jednom i u drugom slučaju televizijski i radio programi svrstavaju u kategoriju dobara zaštićenih autorkim pravom. Članom 29. Zakona o autorskim i srodnim pravima radijski i televizijski program se mogu posmatrati kao načini izražavanja

nekog drugog autorskog dela. U isto vreme data je mogućnost da se radijske emisije posmatraju i kao zasebna autorska dela. Da bi se radijske emisije posmatrale kao zasebna autorska dela one moraju ispunjavati određene kriterijume. Jedan od kriterijuma je i originalnost. Samim Zakonom predviđeno je i pravo proizvođača ovakve emisije. S tim u vezi data su i prava reemitovanja emisija, presnimavanja, umnožavanja, itd. Ovo je jedan od osnovnih načina korišćenja koji u isto vreme ostavlja mogućnost za potencijalne zloupotrebe odnosno neovlašćeno emitovanje ovakvih emisija u cyber prostoru[29]. Konstantna upotreba internet radio-stanica, njihova sve veća popularnost zbog mogućnosti emitovanja širom sveta bez ograničenja broja emitera brojem slobodnih frekvencija dovodi do činjenice da je u ovom domenu jako bitan i pojam proizvođača ovakvih emisija. O popularnosti online radio stanica svedoči i podatak da je 2012. godine broj slušaoca online radio stanica na mesečnom nivou u SAD iznosio 26 miliona, dok je broj slušaoca u 2016. godini iznosio 57 miliona[30]. Trenutna merenja za tekuću 2017. godinu pokazuju da je broj slušalaca na mesečnom nivou 65.85 miliona, dok je prosečno nedeljno vreme slušanja 14 sati i 39 minuta. Predviđanja su da će u 2018. godini 55.8% ukupne SAD populacije i 68.4% ukupnog broja SAD internet korisnika postati korisnici interent radio-stanica[31].

2.9 Autorska prava i internet domeni

Način dodeljivanja internet domena menjao se sa povećanjem broja korisnka i registrovanih domena. Karakteristično za nazive internet domena je i to da dva ista naziva ne mogu postojati, jer bi njihovo postojanje zbunjivalo kako korisnike prilikom pretrage interneta tako i DNS (Domain Name System) sistem koji je zadužen za njihovo preslikavanje u jedinstvene IP adrese. U praksi način dodeljivanja naziva internet domena stavio je u suprotnost autorska prava i prava korisnika koji je već dobio na korišćenje određeni internet domen. Određeni period vremena primenjivalo se pravilo dodeljivanja naziva internet domena prema vremenu podnošenja zahteva. To praktično znači da se između dva lica koja su podnela zahtev za istim nazivom internet domena, naziv internet domena dodeljuje licu koje je zahtev podnelo ranije. Problem koji se kasnije javio sa ovakvim načinom dodele naziva internet domena nastao je zbog sve veće upotrebe interneta od stane komapanija. Problem je u tome da li je moguće nazive internet domena dodeljivati ravnopravno ili je ipak potrebno uvesti ograničenja. Ova ograničenja bi trebala da dodele veće privilegije kompanijama i institucijama.

[29] Žaklina Spalević, Zoran Trajcevski, Zeljko Bjelajac, Milan Pocuca, Duško Dimitrijević, „Regulatory Framework Distribution of HDTV in the Western Balkan Countries“, TTEM - Technics Technologies Education Management, Vol. 8, No. 3, pp. 1173 - 1183, 2013.

[30] The statistics portal, „Number of digital radio listeners in the U.S. from 2012 to 2016“, dosupno na: https://www.statista.com/statistics/191657/us-weekly-internet-radio-listeners-since-2009/, datum pregleda: 12.12.2017.

[31] The statistics portal, „U.S. Online Radio - Statistics & Facts“, dostuono na: https://www.statista.com/topics/1348/online-radio/, datum pregleda: 12.12.2017.

Primera radi ukoliko bi korisnik interneta registrovao interent domen www.nokia.com, svaki od korisnika koji želi da pregleda novu ponudu telefona poznate kompanije nailazio bi kako na zvaničnu adresu kompanije tako i na adresu fizičkog lica pod istim imenom. U ovakvom slučaju postoji mogućnost da bi korisnik odustao od dalje pretrage misleći da je to zvaničan sajt kompanije. Ovakva situacija mogla bi dovesti do ekonomskih gubitaka kompaniji.

Poseban problem javlja se kada fizičko lice ili kompanija zakupe internet domen kako bi vršili promociju sebe ili određene delatnosti kojom se bave. U praksi se dešava da pojedinci ili kompanije zakupljuju domen koji je jako sličan sa nazivom domena za koji bi velika kompanija mogla biti zainteresovana. U najvećem broju slučajeva pojedinci ili kompanije koje su ranije zakupile domen mogu se posmatrati kao utsajderi nepoznati tržištu. Jedan od primera namernog zakupljivanja ovakvog domena jeste primer novinara američkog lista Wired. Ovaj novinar je 1994. godine u cilju istraživanja zakupio internet domen pod nazivom www.mcdonalds.com. U sporu između Mc Donald's firme i novinara koje je pokrenut tužbom Mc Donald's.-a novinar je pobedio. Na ovako originalan način novinar je svetskoj javnosti ukazao na mogućnost zauzivanja internet domena velikih kompanija. Cilj ovog novinara nije bilo sticanje imovinske dobiti već samo ukazivanje na postojanje problema. Nesporna je činjenica da je sudska praksa bila samo uvertira i najava donošenju budućih pravila, kojima se kasnije reguliše ovo pitanje. Tako na primer sudska praksa Sjedinjenih Američkih Država dala je značajan doprinos kasnijem donošenju Zakona o zaštiti potrošača od Cybersquatting. Na regulisanje pravne zaštite zaštićenih znakova od pojave Cybersquatting-a i na donošena konkretna pravila, značajan uticaj imala je i bogata sudska praksa Velike Britanije[32]. Jedan od prvih sporova između pojedinaca i velikih kompanija oko naziva internet domena vodila je kompanija Nissan. Ukratko, čovek sa prezimenom Nissan registrovao je internet domene pod nazivom www.nissan.com i www.nissan.net kako bi vršio prezentaciju svoje firme Nissan Computers. Ova firma bavila se prodajom računara. Tužba protiv ovog čoveka pokrenuta je od strane automobilskog giganta Nissan automobili, tražeći u itoj oduzimanje domena. Sama tužba pokrenuta je nakon niza neuspelih pregovora kako o ustupljivanju ovih domena tako i o njihovom otkupu. Tokom sudskog spora kompanija je Nissan u jednom trenutku tražila odštetu od 10 miliona dolara na račun štete prourokovanje korišćenjem domena sa njihovim imenom. Kompanija Nissan je ovaj spor izgubila i to u više navrata i na više instanci[33]. Pitanje koje se tokom svih ovih godina postavlja jeste da li registrovane firme na osnovi registracije ili žiga imaju preče pravo na određeni internet domen. Pored različitih rešenja može se doći do zaključka da nazivi internet domena ne spadaju u domen autorskih prava, pa se samim tim ni preče pravo zakupa ne može dobiti pozivanjem na autorsko ili pravo intelektualne svojine[34].

---

[32] Zak Muscovitch, „A Short History of Cybersquatting Law", Dostupno na: http://domain-name-lawyer.blogspot.com/2013/04/a-short-history-of-cybersquatting-law.html, datum pregleda: 12.12.2017.

[33] Uzi Nissan, „Nissan vs Nissan, Nissan Motor Sued Nissan Computer For Trademark Infringement, Trademark Dilution And Cyber-Squatting", digest.com, dostupno na: http://www.digest.com/Big_Story.php, datum pregleda: 13.12.2017.

[34] Graham J. Smith, „Interent Law and Regulation", London, 2002.

U cilju rešavanja problema naziva internet domena dodeljenih većem broju lica ili već opisanih problema u sporovima između privatnih lica i kompanija kao i između kompanija po pitanju prava nad nekim nazivom internet domena sudska praksa se razvijala zajedno sa nastalim problemima. Isto tako na zakonskim regulativama koje bi regulisale ovu oblast radilo se paralelno na nacionalnom nivou i na nivou međunarodnih institucija i radnih tela. Posebno je akcenat stavljen na pravne akte koji uređuju odnos naziva internet domena i imena žigova. Ovo je posebno važno u odsustvu međunarodnih pravnih normi koje bi se primenjivale na rešavanje sukoba koji nastaju povodom registracije imena Internet domena. Akcenat na međunarodne pravne norme stavljen je iz razloga jer nacinalni sudovi u slučaju ovakvih sporova primenjuju pravo intelektualne svojine, što dovodi do davanja prednosti nad internet domenom nosiocima prava intelektualne svojine u odnosu na obične korisnike. Isto tako kao logična implikacija zbog nedostataka konkretnih zakonskih rešenja nacionalnih zakonodavstva kojima su regulisani internet domen imena sa jedne strane i intenzivnije međunarodne trgovine roba i usluga sa druge strane, kao neminovna nameće se potreba donošenja pravnih akata kojima se ovo pitanje reguliše u širokim okvirima. Još jedan od razloga za donošenje pravnih alata koji bi se primenjivali na međunarodnom nivou jeste i činjenica da internet kao takav ne prepoznaje nacionalne granice. Tako, Evropska Komisija u 2002. godini je usvojila Regulativu (EZ) 733/2002 za implementaciju internet domena .eu[35], koji egzistira zajedno sa ostalim nacionalnim domenima zemalja članica Unije[36]. Usvajanje ove regulative imalo je za cilj ne samo implementaciju .eu domena, nego i osnivanja Registra i opšteg okvira politike za njegovu funkcionalnost.

Zatim sledi usvajanje Regulative (EZ) 874/2004 za utvrđivanje pravila u vezi sa implementacijom, funkcija .eu Top Level Domain-a i principa za registraciju . Ova pravila uključuju alternativno rešavanje sporova, koja se sprovodi od strane EURid Registry. U tom smislu je i usvajanje Regulative (EZ) 1654/2005[37], Regulative (EZ)1255/2007[38] i Regulative (EZ) 560/2009[39] za izmenu i dopunu Regulative (EZ) 874/2004. Imajući u vidu uspostavljanje novog alternativnog mehanizma rešavanja

[35] Commision Regulation (EC) No. 733/2002 of the European Parlament and of the Council of 22 April 2002 on the implementation of the .eu Top Level Domain (Official Journal of the European Communities L 113/1).

[36] Commision Regulation (EC) No. 733/2002, Član 1, stav 2

[37] Commision Regulation (EC) No 1654/2005 of 10 October 2005 amending Regulation (EC) No 874/2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration (Official Journal of the European Union L 266/35)

[38] Commision Regulation (EC) No 1255/2007 of 25 October 2007 amending Commission Regulation (EC) No 874/2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration (Official Journal of the European Union L 282/16)

[39] Commision Regulation (EC) No 560/2009 of 26 June 2009, amending Regulation (EC) No 874/2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration (Official Journal of the European Union L 166/03).

sporova u vezi internet domen imena, od važnosti je spomenuti donošenje i usvajanje Jedinstvene politike za rešavanje sporova o internet domen imena (Uniform Domain Name Dispute Resolution Policy, UDRP Policy) i Propisa za rešavanje sporova o internet domen imena (Rules for Uniform Domain Name Dispute Resolution Policy, UDRP Rules). Isto tako, od važnosti primene UDRP postupka su i dopunska pravila koja usvaja svaki od akreditovanih provajdera nadležan za sprovođenje administrativnog postupka za rešavanje sporova u vezi internet domen imena. Naime, opšta pravila UDRP postupka, kao i dopunska pravila, daju značajni doprinos u cilju harmonizacije na globalnom nivou koja su u vezi sa rešavanjem sporova o internet domen imenima[40].

U praksi, problem nastaje kad privredni subjekt ne može da koristi svoj žig ili naziv svoje firme kao internet adresu, jer je neko drugi već registrovao adresu takve sadržine, pa od vlasnika žiga ili naziva firme traži otkup internet domena. Ovo je dovoljan razlog da vlasnik žiga ili naziva firme zatraži pravnu zaštitu protiv vlasnika internet domena zbog povrede žiga, jer registracija tuđeg žiga kao internet adresa smatra se komercijalnom upotrebom žiga. Pravni problemi se mogu rešavati na dva načina:

- Vansudski, putem arbitražnog postupka ispred međunarodnih ovlašćenih provajdera za rešavanje sporova u saglasnosti pravila UDRP postupka.
- Putem sudskog spora pred nacionalnim sudovima primenom nacionalnog prava

Prednost vansudskog rešavanja sporova ogleda se i kroz činjenicu teritorijalne udaljenosti subjekata spora. Dakle, u pitanju je racionalniji postupak od sudskog postupka koji za stranke spora, pre svega štedi novac i vreme. Mogućnost alternativnog, odnosno vansudskog rešavanja sporova o internet domen imenima, uvodi se od strane Internet korporacije za dodeljivanje imena i brojeva (ICANN) u 1999. godini, donošenjem jedinstvene politike o rešavanju ove vrste sporova (UDRP Policy). Konkretnije, reč je o upravnom postupku za rešavanje sporova u vezi imena internet domena. Prednosti koji nudi mehanizam vansudskog rešavanja sporova u vezi imena internet domena i primena pravila UDRP postupka, je pribegavanje rešavanju sporova od strane van sudskih organa. To se potvrđuje i činjenicom da još odmah nakon osnivanja ICANN-a, NetworkSolutions Inc., do tada jedini odgovoran za registraciju generičkih najviših internet domen imena, uvedena je klauzula kojom se obavezuju svi aktuelni nosioci imena domena da prihvate izmenjene propise sa kojima se reguliše registracija imena domena[41]. Neizbežan ograničujući faktor primene vansudskog rešavanja sporova je i činjenica da prema pravilima UDRP postupka, nije predviđeno tražiti naknadu štete. Ovo podrazumeva da Administrativna komisija saglasno propisanim pravilima po kojima postupa i donosi svoje odluke, nema ovlašćenja da u korist oštećene strane u sporu, donese odluku o nadoknadi štete uključujući i advokatske troškove. Ovo svakako nisu jedini problemi u realizaciji sporova vansudskim postupkom.

---

[40] Ljubisa Stefanoski, „Upravn postupak registracije internet domen imena i pravna zaštita“, doktorska disertacija, Prani fakultet, Univerzitet u Nišu, 2015.

[41] Domain Name Law and Practice- An International Handbook, edited by Torsten Bettinger, Oxford University Press, 2005.

Uzimajući u obzir sva navedena ograničenja i negativne strane vansudskog rešavanja sporova, sasvim je očekivano da još uvek preovlađuje sudski način rešavanja sporova o internet domen imena. Sudski postupak rešavanja sporova, je daleko skuplji i sporiji, u odnosu na vansudsko rešavanje sporova o internet domen imenima. Međutim, i sudski postupak ima svoje prednosti. Najpre, radi se o širem dijapazonu primene sudskog postupka na niz otvorenih pitanja u vezi nastalih sporova povodom registracije internet domen imena, što nije slučaj kod vansudskog rešavanja sporova. Razlog je u tome što su ograničenja postupanja vansudskih organa isključivo samo na povrede žiga i nesavesno registrovanje internet domen imena. Naime, reč je o postupanju sudskih organa u tzv. mala fides sporovima, i u takozvanim bona fides sporovima, konkretnije i u sporovima koji nastaju između kompanija koja imaju isti naziv ili koriste isti žig u različitim sektorima i na različita tržišta, a na to imaju sasvim legitimno pravo [42]. Prednost sudskog postupka je u tome što se tužiocu omogućuje da dobije odštetu na osnovu prethodnog utvrđenja visine štete zbog zlonamerne registracije. Prednost je isto tako i mogućost javnog objavljivanja presude u javnim glasilima ili na internetu, a sankcija se logično sastoji u diskreditovanju osuđenog.

Bona fides dolazi iz latinskog jezika i označava: u dobroj veri, istinito, iskreno, bez namere da se obmane. Naime, radi se o moralnom pravilu koje po svom sadržaju odgovara nečelu savesnosti i poštenja kao pravni standardi čiji pojam nije određen, već se ostavlja sudu da ga konkretizuje u pojedinim slučajevima, držeći se njegovog opšteg značenja kao smernice. Osnova takozvanih bona fides sporova, proizlazi iz sudara prava intelektualne svojine i internet prava. Ključni razlozi pojave bona fides sporova su nespojivost dva fundementalna principa teritorijalnost i specijalnost žigovnog prava, sa globalnim karakterom internet domen imena i njihovom jedinstvenošću. Bona fides sporovi mogu se podeliti na dve kategorije:

- Sporovi između kompanija koje su aktivne u raznim sektorima i na raznim tržištima
- Sporovi koji obuhvataju različite pravne kategorije

Bona fides sporovi su kategorija sporova koja nastaju između kompanija koje imaju isti naziv ili koriste isti žig u različitim sektorima i na različitim tržištima. Primer iz prakse je spor Prince plc protiv Prince Sportswear Group Inc. Privredno društvo Prince Sportswear Group, nosialc žiga „Prince“, u 1997. godine, pokušalo je da registruje ime internet domena prince.com, ali je došlo do saznanja da je to ime domena već registrovano u 1995. godine, od strane engleskog privrednog društva Prince plc, koje se bavi nuđenjem kompjuterskih usluga. To je bio dovoljan razlog za podizanje sudskog spora. Sud, na osnovu utvrđenih činjenica da u konkretnom slučaju nema povrede prava na žig i razvodnjavanje žiga kako što je tvrdio, doneo odluku u korist privredog društva, nosiocu spornog imena internet domena[43].

U praksi postoje i slučajevi kada spor može nastati i između kompanija koja se bave istom ili sličnom delatnošću, a da pritom kompanije deluju na različitim geografskim područjima. Takav je slučaj SG 2 protiv Brokat informations systeme GmbH. Reč je o

[42] Diane Rowland, Eliyabeh MacDonald, „Information Technology Law“, 3rd ed. Cavendish Publishing Limited, London, 2005.
[43] Ibidem

sporu između francuske kompanije SG 2 koja u svojstvu nosioca registrovanog žiga "payline" iz 1996. godine, nudi usluge internet plaćanja, s jedne strane, i nemačke kompanije Brokat informations systeme GmbH, registrovana u Štutgartu, u svojstvu nosioca registriranog nemačkog žiga "payline" koji koristi sistem "Brokat-payline" kao poddomen „brokat.de/payline" u okviru svog domena brokat.de i pri tom nudi iste usluge kao i kompanija SG [44]. Francuska kompanija SG 2 zatražila je od francuskog suda izricanje zabrane kompaniji Brokat zbog navodnog kršenja prava korišćenjem njegovog registrovanog francuskog žiga "payline", za iste robe i usluge, na nemačkom sajtu. Apelacioni sud doneo je presudu u korist francuske kompanije SG 2 i pored toga što nemačka kompanija nikada nije nudila svoj sistem internet plaćanja u Francuskoj. Odluka suda zasnivala se na tome da je internet sajt kompanije Brokat bio dostupan širom svetu, a između ostalog i u Francuskoj i da je zbog toga naneta šteta na francuskoj teritoriji, pa je sud kompaniji Brokat naredio da se uzdrži od daljeg korišćenja žiga "payline"[45].

U praksi, postoje i sporovi između dva savesna subjekta koji žele da registruju istoimeni domen, na šta imaju sasvim legitimno pravo. U konkretnim slučajevima spora, sud mora da odluči čije je subjektivno pravo "jače"[46]. Naime, reč je o slučajevima kada strane tvrde da postupaju u dobroj veri, navodeći pri tom da za to imaju opravdani interes i prilažu argumente da imaju pravo na konkretni karakteristični znak. Uobičajeno, ovakve vrste sporova vode se povodom registracije internet domen imena koji sadrže trgovačka imena ili nazive firmi koje su već registrovana i uživaju pravnu zaštitu žiga, lična imena pojedinaca, nazivi žigova, imena gradova ili država i slično[47].

Kao primeri iz francuske sudske prakse Borner (Börner) i Sindler (Spindler) navode slučajeve u kojima je sud doneo odluku u korist Liliane Bettencourt (glavni akcionar Kompanije L'Oréal) i Aamelie Mauresemo (čuvena francuska teniserka) čija su lična imena bila predmet registracije internet domena. Naime, na osnovu člana L.711-4 Francuskog zakona o intelektualnoj svojini, sud je registrantima internet domena „lilianebettencourt.com" i „ameliemauresemo.com", naložio da se uzdrže od njihove upotrebe, obrazloženjem da postoji povreda ličnih prava nosioca ličnih imena [48].

---

[44] Zuzana Slovakova, „Protection of trademarks and the Internet with respect to the Czech law", Journal of International Commercial Law and Technology Vol.1, Issue 2, 2006, pp.72-79.

[45] Ulf Maunsbach, „Some Reflexions Concerning Jurisdiction in Cases on Cross-border Trademark Infringements Through the Internet", Stockholm Institute for Scandianvian Law 1957-2010, vol. 47, 2004, pp.494. Dostupno na: http://www.scandinavianlaw.se/pdf/47-23.pdf, datum pregleda: 12.12.2017.

[46] Goce Naumovski, Dušan Popović, „Information Technology Law", Iustinianus Primus Law Faculty, SS.Cyril and Methodius University of Skopje, Skopje, 2011, pp.1-50.

[47] Gerald Spindler, Fritjof Borner, „E-Commerce Law in Europe and the USA", Springer, Germany, 2007 pp.115

[48] Intellectual Property Code (Legislative Part), Law No 92-597 of 1 July 1992 as last amended by Law No 96- 1106 of 18 December 1996. Dostupno na: http://oami.europa.eu/ genhtm/mark/nl_fr_1_en.htm, datum pregleda: 15.12.2017.

Suprotna odluka suda, doneta je pred nemačkim sudovima gde se vodio spor između pojedinaca sa imenima Shell i Krupp i preduzeđa identičnih naziva [49]. Naime, nemački sudovi su doneli presudu protiv pojedinaca koji su registrovali svoja lična imena (prezimena) kao imena internet domena, pri tom zasnivajući svoju odluku na interesu privrednog društva, i činjenici da ona ima prednost u odnosu na važnost upotrebe spornih imena domena od strane pojedinaca.[50]

2.10 Krivična dela oštećenja i krađe intelektualne svojine u Zakonodavstvu Srbije

Definisanjem krivičnih dela vrši se upotpunjavanje zaštite prava intelektualne svojine u okviru pravnog sistema jedne zemlje. Procesuiranje dela usmerenih ka oštećenju ili krađi intelektualne svojine spada u domen rada Posebnog tužilaštva za borbu protiv visokotehnološkog kriminaliteta.

Ovo tužilaštvo obavlja poslove procesuiranja krivičnih dela određenih Krivičnim zakonikom a usmerena protiv bezbednosti računarskih podataka. Pored ovako definisanih krivičnih dela u delatnost tužilaštva spadaju i sva ona dela kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarske mreže kao i računarski sistemi. Primera radi u ovakva dela mogu se uvrstiti dela protiv intelektualne svojine, dela protiv imovine, privrede pa čak i saobraćaja. Takođe rad tužilaštva je zasnovan na procesuiranju dela u kojima se vrši povreda autorskog prava i to ukoliko se radi o pirateriji u komercijalne svrhe pri čemu broj umnoženih primeraka dela prelazi 2000, ili se pak istragom ustanovi da je autoru naneta materijalna šteta u iznosu preko milion dinara. Ukoliko su računari i računarske mreže korišćeni za potrebe izvršenja krivičnih dela protiv slobode i prava čoveka, kao i u cilju narušavanja polnih sloboda, javnog reda i mira kao i ustavnog uređenja i bezbednosti pomenuto tužilaštvo u obaveze je da procesuira i ovakva dela. Članom 199 ovog zakona definisno je krivično delo neovlašćenog iskorišćavanja autorskog dela. Može se slobodno reći da je narušavanje autorskog dela i drugog dobra srodnog prava kako opširno definisano[51]. Primera radi stavom 1 ovog člana propisan je prvi oblik koji čini lice koje neovlašćeno objavi, snimi, umnoži ili na drugi način javno saopšti u celini ili delimično bilo koje autorsko delo. Primenom ovog stava u istražnom postupku nije od značaja o kolikom se broju kopija radi. Bilo da se radi o jednoj ili više kopija maksimalna propisana kazna je kazna zatvora do tri godine. Ipak određene razlike mogu se napraviti u smislu da li je

[49] Imke Bubert, Matthias Buening, „Domain Name Issues - European Jurisdiction“, Electronic Commerce Legal Issues Platform, ESPIRIT Project 27028, 2013. Dostupno na: www. qlinks.net/lab991216/trademarks.doc, datum pregleda: 17.12.2017.
[50] Dušan Popović, „Imena internet domena i pravo intelektualne svojine“, Institut za uporedno pravo, Monografija Beograd 2005, str. 35-36.
[51] Krivični zakonik, "Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 i 94/2016.

delo učinjeno radi sticanja imovinske koristi ili ne. Pa tako ukoliko je delo učinjeno radi sticanja imovinske koristi lice koje je delo učinilo može se kazniti kaznom zatvora od šest meseci do pet godina. Bitna činjenica definisana ovom odredbom jeste da se ne pravi razlika da li je lice delo počinilo radi sticanja imovinske koristi za sebe ili za drugog. Prema stavu 4 člana 199 Krivičnog zakonika propisana je novčana kazna ili kazna zatvora do tri godine za lica koja prodaju, daju u zakup ili drže uređaje čija je namena uklanjanje, zaobilaženje ili osujećivanje tehnoloških mera namenjenih sprečavanju povreda autorskih i srodnih prava ili sama povreda autorskih prava. Takođe krivičnim zakonikom definisane su i sankcije protiv lica koja neovlašćeno uklanjaju ili menjaju elektronske informacije o nosiocu autorskih prava zapisane na digitalnom elektronskom delu. Takođe novčana kazna ili kazna zatvora do tri godine propisana je članom 200 krivičnog zakonika za lica koja uklone ili izmene informaciju o nosiocu autorskog ili srodnosg prava i takvo delo stave u promet, emituju ili javno saopšte. Članom 201 Krivičnog zakonika definisane su krivične sankcije protiv osoba koje deluju protiv pronalazačkog prava. Ovim članom definisana je končana kazna ili kazna zatvora do tri godine za lica koja nude ili stavljaju u promet proivod ili postupak koji je zaštićen petentom[52]. Kazna zatvora može se povećati do osam godina ukoliko je stavljanjem u promet dela zaštićenog patentom stečena imovinska korist veća od milion dinara[53]. Takođe ovim članom Krivičnog zakonika definisana je i kazna za svako lice koje objavili ili na bilo koji način učini javno dostupnim delo ili suštinu tuđeg prijavljenog pronalaska i to u vremenskom periodu pre nego što predmetno delo bude objavljeno na način predviđen zakonom. Propisana kazna za ovakvo delo može biti novčana ili kazna zatvora do dve godine[54]. Mere za neovlašćeno podnošenje prijave patenta ili bilo kakvo drugo falsifikovanje i navođenje pronalazača definisane su u stavu 4 člana 201 Krivičnog zakonika.

Kazna zatvora za ovakvo delo može iznositi od šest meseci do pet godina[55]. Poslednja u nizu kategorija zaštite intelektuale svojine definisa Krivičnim zakonikom usmerena je protiv lica koja neovlašćeno koriste tuđi dizajn (Član 202).

Procesuiranje lica okrivljenih za ugoržavanje autorskih i srodnih prava obuhvaćenih ovim zakonom deo je sudske prakse u Republici Srbiji duži niz godina. Primera radi u 2012. godini za krivična dela protiv intelektualne svojine prijavljeno je 219 lica. Od ovih 219 lica za krivično delo neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava iz člana. 199. KZ prijavljeno je 24 lica[56]. Tokom 2013. godine zbog krivičnog dela neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava iz člana 199. KZ podneta krivična prijava protiv 19 lica. Tokom 2014. i 2015. godine

[52] Ibidem, član 201, stav 1
[53] Ibidem, član 201, stav 2
[54] Ibidem, član 201, stav 3
[55] Ibidem, član 201, stav 4
[56] Republika Srbija Republičko javno tužilaštvo, „Rad javnih tužilaštava na suzbijanju kriminaliteta i zaštiti ustavnosti i zakonitosti u 2012. godini“, Dostupno na: http://www.rjt.gov.rs/ci/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%98%D0%B5-%D0%BE-%D1%80%D0%B0%D0%B4%D1%83, datum pregleda: 15.12.2017.

zbog krivičnog dela neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava iz člana 199. KZ protiv 12 odnosno 10 lica podnete su krivične prijave. U toku 2016. godine zbog istog krivičnog dela podnete su krivične prijave protiv 4 lica[57]. Manji broj podnetih krivičnih prijava može se sagledati sa različitih aspekta. Jedan od aspekata može biti da je broj ovakvih dela manji pa je samim tim i broj prijava manji, dok drugi aspekt može biti pokazatelj slabe angažovanosti državnih organa na rešavanju ovog problema. Jedan od primera iz sudske prakse je i presuda Okružnog suda u Beogradu K1.vtk.br.19/08 od 10.10.2008.god. Ovom presudom Ž.J. (36) i S.M.(35) su proglašeni krivim zbog internet piraterije. Tokom istražnog postupka njima se stavljalo na teret da su u periodu od 2005. do 2008. godine na teritoriji opštine Kraljevo putem bežične veze neovlaščeno prodavali raznovrsta autorska dela. Tokom 2005. godine čak su osnovali i firmu „EXCALIBUR COM D.O.O" putem koje su primali novčane uplate na ime usluga koje su nudili. Korisnicima je nakon izvršene i dostavljanja dokaza o uplati bilo omogućeno preuzimanje primeraka različitih autorskih dela. Ovom presudom okrivljeni su osuđeni na uslovnu kaznu zatvora u trajanju od šest meseci. Istom presudom rok za proveravanje iznosio je dve godine.

Drugi primer istog krivičnog dela predstavlja presuda Okružnog suda u Beogradu K1.vtk.br.44/08 od 28.11.2008.god. Ovom presudom a za isto krivično delo piraterije oglašen krivim M.S. (30) iz Beograda. M.S je takođe tokom perioda od tri godine (01.01.2005-03.09.2008) neovlašćeno umnožavao i radi sticanje imovinske koristi stavljao u promet autorska dela. Celokupan proces umožavanja i distribucije radio je na adresi svog prebivališta, dok se komunikacija sa klijentima obavljana putem elektronske pošte kreirane korišćenjem poštanskog servisa yahoo.com. U momentu hapšenja od M.S su oduzeta dva računara, 10.327 komada neovlašćeno umnoženih optičkih diskova sa neovlašćeno umnoženim autorskim delima. Najbrojnija dela bila su u vidu filmova, televizijskih serija, muzike, stripova i drugih multimedijalnih sadržaja[58].

U jednom od procesa okrivljeni je tvrdio da je kolekcionar, i da je zaplenjene filmove sakupljao duži niz godina. Takođe je tvrdio da je pojedine filmove prebacivao sa VHS na DVX radi njihovog lakšeg čuvanja, kao i da je lično pravio omote. Međutim iako je se branio time da filmovi nisu namenjeni sticanju imovinske koristi istraga je pokazala da je na hard disku računara pronađen veći broj spremljenih omota kao i elektronskih kataloga. Ključni momenat za podizanje optužnice bilo je pronalaženje oglasa u kojima se pored nuđenja usluge presnimavanja nuđena i rasprodaja DVX diskova sa istim naslovima koji su pronađeni kod okrivljenog. Za svaki od naslova bilo je navedeno da količina nije ograničena, bila je navedena cena i broj telefona okrivljenog putem koga mu se zaineresovani kupci mogu obratiti.

---

[57] Republika Srbija Republičko javno tužilaštvo, „Rad javnih tužilaštava na suzbijanju kriminaliteta i zaštiti ustavnosti i zakonitosti u 2016. godini", Dostupno na: http://www.rjt.gov.rs/ci/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%98%D0%B5-%D0%BE-%D1%80%D0%B0%D0%B4%D1%83, datum pregleda: 15.12.2017.

[58] Dragan Prlja, Mario Reljanović, Zvonimir Ivanović, opus citatum.

3
Elektronsko poslovanje u Cyber prostoru

Nastanak i razvoj informaciono komunikacionih tehnologija i interneta doneo je brojne prednosti fizičkim licima i kompanijama. Ovako usmeren tehnološki napredak je inicirao novu eru u oblasti poslovanja koja je nazvana elektronsko poslovanje. Pojam elektronsko ili dogitalno poslovanje obuhvata online komunikaciju, novčane transakcije, elektronsku trgovinu i sve ostale akcije koje prate proces poslovanja, a u isto vreme se baziraju na upotrebi informaciono komunikacionih tehnologija i interneta. Ovako organizovano poslovanje od velike je koristi u cilju eliminisanja problema koje donosi vremenska razlika kao i geografska udaljenost između kompanija saradnika. Posebno se prednosti ogledaju u servisima za poručivanje, plaćanje i isporuku robe i usluga. Jako je zanimljiva činjenica da se opseg poslovanja upotrebom elektronskih servisa širi na promet robe i usluga koji do uvođenja ovog servisa nije postojao. U samoj unutrašnjosti privrednog društva na prvom mestu su zaposleni. Od njihovih osobina kako subjektivnih tako i objektivnih zavisi koliko će konkretna tehnologija i princip elektronskog poslovanja biti usvojeni i primenjivani. Ukoliko se nalazi u adekvatnom okruženju zaposleno lice može da iskoristi svoje kreativne i radne sposobnosti kako bi doprinelo ubrzanju procesa inoviranja postojećih procedura. Cilj svakog privrednog društva prilikom nastupa na tržištu je zadovoljan klijent. Tačnije cilj treba da bude orijentisan ka tome da svaki potencijalni klijent postane kupac. Dva momenta nakon uvođenja servisa elektronskog poslovanja su ključna. Prvi momenat je zapravo i prva prodaja proizvoda, usluge ili informacije. Drugi težak momenat je svaka naredna prodaja, i ona zavisi samo od pažnje koja je posvećena svakom pojedinačnom kupcu koji je već kupio proizvod, kao i od pažnje usmerene ka svakom potencijalnom kupcu[59].

U domenu elektronskog poslovanja mogu se izdvojiti tri grupe aktera: Vlada (eng. Goverment), Kompanije (eng. Business), Klijenti (eng. Consumer). U zavisnoti od toga koji od aktera stupaju u elektronsko poslovanje mogu se izvojiti različiti modeli elektronskog poslovanja:

- G2G (Goverment to Goverment): ovaj model podrazumeva korišćenje elektronskih servisa od strane zaposlenih u državnoj upravi i lokalnoj samoupravi. Cilj je olakšana komunikacija vlade i lokanih organa samouprave.
- G2B (Goverment to Business): ovaj model podrazumeva saradnju vlade i poslovnih subjekata. Cilj ovog modela je smanjenje vremena čekanja na izvršenje složenih transakcija, što vodi povećanju efikasnosti i većem broju zadovoljnih kompanija, sa samim tim i povećanju investicija.
- G2C (Goverment to Consumer): ovaj model obuhvata servise koji su dostupni 24h dnevno i koji obezbeđuju saradnju vlade i građana. Pokretanjem ovakvih servisa korisnik pristupa svim potrebnim informacijama, vrši plaćanja administrativnih taksi i podnošenje različitih formi zahteva.

[59] Bogdan Gavrilović, „Osnovni modeli elektronskog poslovanja“, Kompjuterska bibiloteka, dostupno na: http://vesti.kombib.rs/osnovni_modeli_elektronskog_poslovanja.html, datum pregleda: 22.12.2017.

- B2G (Business to Goverment): ovaj model je proizašao iz B2B modela poslovanja. On obuhvata ovlašćene vladine agencije čiji je zadatak uspostavljanje efikasnijih poslovnih procesa. Takođe zadatak ovih agencija je i stvaranje vizuelne nadležnosti i smanjivanje broja različitih sistema uvođenjem centralizovanih funkcija.
- B2B (Business to Business): ovaj model predstavlja automatsku razmenu informacija između različitih organizacija. Na taj način organizacijama je omogućeno da izgrade nov način poslovanja. Tehnologije koje pripadaju ovom modelu olakšavaju obavljanje transakcija za prodaju robe i usluga. U pomenutim transakcijama akteri su poslovni subjekti što omogućava integraciju lanca nabavke.
- B2C (Business to Consumer): ovaj model predstavlja prodaju robe ili usluga krajnjim potrošačima posredstvom Interneta. Razlika u odnosu na B2B model ogleda se u tome što je ovoga puta kupovina organizovana između firme kao prodavca i fizičkog lica kao kupca robe ili uluga. Ovaj vid poslovanja za firmu predstavlja dodatnu uštedu u troškovima kirije, broja zaposlenih i drugih vidova nameta.
- C2G (Consumer to Goverment): ovaj model obuhvata aplikacije koje obično uključuju plaćanje poreza, izdavanje sertifikata ili drugih dokumenata.
- C2B (Consumer to Business): predstavlja model u kom potrošač putem interneta publikuje zahtev sa definisanom potražnjom robe i usluga kao i unapred definisanim budžetom. Prodavci vrše pregled ovakvih zahteva i na svaki pojedinačni zahtev daju svoju ponudu. Prikupljene ponude do unapred definisanog roka potrošači pregledavaju i odlučuju se za ponudu koja je njima najpovoljnija.
- C2C (Consumer to Consumer): ovaj model predstavlja saradnju između poslovnih subjekata u cilju razmene resursa. Resurski mogu biti u obliku proizvoda, informacija ili usluga. Uobičajeno se ovaj model realizuje preko nekog od online posrednika.Primer upotrebe ovakvog modela mogu biti online aukcije.
- B2E (Business to Employee): ovaj model predstavlja način definisanja procedura unutar privrednog društva. Definisane procedure obuhvataju odnos privrednog društva i zaposlenog. Iz ugla implementiranih tehnologija najčešće u okviru privrednog društva postoji informacioni sistem baziran na intranet-u. Putem ovog sistema zaposleni dobija informacije o svim svojim pravima, radnim zadacima, kao i o definisanim procedurama na nivou privrednog društva.
- B2B2C (Business to Business to Consumer): je noviji model koji predstavlja kombinaciju korišćenja B2B modela sa podrškom za B2C model. Ovo je veoma čest model prilikom udruživanja više kompanja u cilju kreiranja kompletnog CRM-a (Customer Relationship Management). Benefit upotrebe ovakvog modela je pružanje kompletne usluge od strane udruženih kompanija.
- C2B2C (Consumer to Business to Consumer): ovaj model obuhvata realizaciju plaćanja između potrošača korišćenjem nekog privrednog društva kao posrednika. Pod privrednim društvom kao posrednikom smatra se online privredno društvo. Primera radi ovde se mogu svrstati FreeLance sajtovi na kojima klijenti mogu pronaći stručnjake iz određene oblasti koji bi za njih realizovali određene projekte. U ovakvim poslovnim transakciama brigu oko regularnosti saradnje i plaćanja vodi web portal preko koga se celokupna komunikacija obavlja.

Ekspanzija elektronskog poslovanja posmatrano iz ugla pravnih regulativa otvorila je niz novih pitanja. Ova pitanja se ogledaju u pronalaženju načina za zakonsko regulisanje zloupotreba i krivičnih dela u domenu elektronskog poslovanja. Neka od krivičnih dela iz domena elektronskog poslovanja i upotrebe elektronskih servisa su zloupotrebe digitalni podataka, internet sabotaže, kreiranje i distribudija virusni datoteka, napadi na računarske sisteme, kao i različiti oblici pravara prilikom online ili drugih vidova elektronskog plaćanja. Od posebnog značaja su pitanja nadležnosti sudova u slučaju spora ukoliko su strane koje spore iz različitih zemalja. Sve pravne regulative moraju se definisati kako u nivou svake od zemalja tako i na međunarodnom nivou.

Osnovni pravni propisi kojima se reguliše oblast elektronskog poslovanja su Zakon o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju[60], Zakon o elektronskom potpisu[61] i Zakon o elektronskoj trgovini[62]. Podzakonski propisi koji omogućuju elektronsko poslovanje su: Pravilnik o tehničkotehnološkim postupcima za formiranje kvalifikovanog elektronskog potpisa i kriterijume koje treba da ispune sredstva za formiranje kvalifikovanog elektronskog potpisa[63], Pravilnik o bližim uslovima za izdavanje kvalifikovanih elektronskih sertifikata[64], Pravilnik o Registru sertifikacionih tela za izdavanje kvalifikovanih elektronskih sertifikata u Republici Srbiji[65], Pravilnik o načinu podnošenja poreske prijave elektronskim putem[66], Odluka o elektronskom načinu obavljanja platnog prometa[67], Odluka o elektronskom potpisivanju dokumenata s podacima koje banke dostavljaju Narodnoj banci Srbije[68], Pravilnik o načinu postupanja sa elektronskim ponudama i načinu sprovođenja elektronske licitacije u postupcima javnih nabavki[69].

[60] Zakon o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju, Službeni glasnik RS, br. 94/2017.
[61] Zakon o elektronskom potpisu, Službeni glasnik RS, br. 135/2004.
[62] Zakon o elektronskoj trgovini, Službeni glasnik RS, br. 41/2009 i 95/2013
[63] Pravilnik o tehničkotehnološkim postupcima za formiranje kvalifikovanog elektronskog potpisa i kriterijume koje treba da ispune sredstva za formiranje kvalifikovanog elektronskog potpisa, Službeni glasnik RS, br. 26/2008, 13/2010.
[64] Pravilnik o bližim uslovima za izdavanje kvalifikovanih elektronskih sertifikata, Službeni glasnik RS, br. 26/2008.
[65] Pravilnik o Registru sertifikacionih tela za izdavanje kvalifikovanih elektronskih sertifikata u Republici Srbiji, Službeni glasnik RS, br. 26/2008.
[66] Pravilnik o načinu podnošenja poreske prijave elektronskim putem, Službeni glasnik RS, br. 8/12, 113/13.
[67] Odluka o elektronskom načinu obavljanja platnog prometa, Službeni glasnik RS, br. 57/2004.
[68] Odluka o elektronskom potpisivanju dokumenata s podacima koje banke dostavljaju Narodnoj banci Srbije, Službeni glasnik RS, br. 28/2009, 47/2009
[69] Pravilnik o načinu postupanja sa elektronskim ponudama i načinu sprovođenja elektronske licitacije u postupcima javnih nabavki, Službeni glasnik RS, br. 50/2009.

3.1 Elektronski ugovori

Sklapanje elektronskih ugovora s obzirom da se obavlja na daljinu bez ličnog kontakta strana potpisnica zahteva definisanje mehanizama verodostojnosti poruka i obavljenih komunikacija. Najveći broj odredbi koje se odnose na elektronske ugovore sadržan je u Zakonu o elektronskoj trgovini. Prema Zakonu o elektronskoj trgovini ugovor u elektronskoj formi definisan je kao „*ugovor koji pravna i fizička lica zaključuju, šalju, primaju, raskidaju, otkazuju, kome pristupaju i koji prikazuju elektronskim putem uz korišćenje elektronskih sredstava"*[70]. Pitanja punovažnosti, zaključenja, dokazne snage, vremena zaključenja elekronskih ugovora regulisana su u skladu sa međunarodnim standardima koji su najšire prihvaćeni.

Forma ugovora. – Zakon o elektronskoj trgovini sadrži pravilo prema kome se ugovoru ne može osporiti punovažnost niti dokazna snaga na osnovu činjenice da je on sklopljen u elektronskom obliku. Time je postavljeno pravilo iste pravne snage elektronske forme u odnosu na pismenu formu ugovora.[71] Ovo pravilo se primenjuje na većinu potrošačkih ugovora. O opravdanosti nekih slučajeva isključenja, kao što su ugovori za koje je zakonom određena upotreba svojeručnog potpisa, može se raspravljati, ako se ima u vidu širenje upotrebe elektronskog potpisa i njegovo izjednačavanje, po snazi, sa svojeručnim potpisom[72]. Načelo iste pravne snage elektronske forme omogućava da se i ugovori za koje se zahteva pismena forma sklope razmenom elektronskih poruka, osim u slučajevima kada se predmetni ugovori prema svojoj formi ne mogu sklopiti u elektronskoj formi. Ako se za nastanak ugovora traži potpis, taj uslov je ispunjen ako je elektronski dokument potpisan kvalifikovanim elektronskim potpisom. U takvom slučaju ugovor ima istu snagu, pa samim tim elektronski potpis može zameniti svojeručni potpis, odnosno svojeručni potpis i pečat[73].

Pravna priroda izjave volje. - Inicijativa za zaključenje ugovora elektronskim putem može biti upućena neodređenom broju lica, kada se kaže da ima javni (otvoren) karakter, ili određenom broju lica, kada se govori o njenom privatnom ili zatvorenom karakteru.[74] Ako se elektronskim sredstvima nude robe i usluge uz naznaku cene određenoj osobi, putem elektronske pošte, tj. pouzdane i verifikovane e-mail komunikacije, izjava volje ima prirodu ponude. Kada se robe i usluge nude putem Web

---

[70] Zakon o elektronskoj trgovini, Opus citatum

[71] Prema Model zakonu o elektronskoj trgovini UNCITRAL-a iz 1996. godine zahtev za poštovanjem pismene forme ispunjen je upotrebom elektronskog dokumenta ukoliko je njegova sadržina pristupačna (da je čitljiv) i upotrebljiva (da se dalje može koristiti, za šta je neophodno da se sačuva u obliku u kome je primljen) [16, str.606], [17, str. 620].

[72] Silvija Petrić, „Zakon o elektronskoj trgovini i zaštita potrošača", tekst u zborniku „Zaštita potrošača i ulagatelja u europskom i hrvatskom pravu" (ur. Tomljenović, V., Čulinović-Herc, E.), Pravni fakultet Sveučilišta u Rijeci, Rijeka, 2005, str. 123-153.

[73] Dubravka Stojanović, „Normativno uređenje oblasti elektronskog potpisa", Pravo i privreda, br. 5 - 8/05, str. 471-482.

[74] V. Vigneau, Commerce électronique et protection du consommateur, Paris, 2010, pp. 297.

stranice, pravna priroda izjave volje se određuje na osnovu vrste sajta (kada se radi o interaktivnom sajtu, koji daje mogućnost kupcu da direktno naruči robu, smatra se da izlaganje robe na sajtu predstavlja ponudu koja važi dok se ne iscrpe zalihe, a ako to nije slučaj, izjava ima prirodu poziva na ponudu), ili se to čini uz pomoć pravila sadržanih u Zakonu o obligacionim odnosima[75].

Dejstvo izjave volje učinjene elektronskim putem. - Izjava volje koja je učinjena elektronski smatra se da je upućena odsutnom licu. Prema opštim pravnim pravilima ugovornog prava takva izjava proizvodi dejstvo tek kada stigne drugoj strani, odnosno kad je druga strana primi. S tim u vezi Zakon o elektronskoj trgovini određuje da su ponuda i njeno prihvatanje, primljene isključivo onda kada im osoba kojoj su upućene može pristupiti. U pogledu određenja vremena dospeća, odnosno prijema izjave treba praviti razliku između situacije kada se poruka upućuje profesionalnim subjektima i one kada se ista čini neprofesionalcima, odnosno potrošačima. Kada se radi o profesionalcima, polazi se od pretpostavke da su oni dužni da dnevno kontrolišu prispeće elektronskih poruka, zbog čega se smatra da se dan odašiljanja poruke i njenog prijema poklapaju. Izuzetno, ako je poruka prispela van radnog vremena, uzima se da je primljena prvog narednog radnog dana. Od potrošača se ažurnost u pogledu prijema elektronskih poruka ne može očekivati, zbog čega trenutak prijema poruke treba vezati za trenutak pristupa Internetu, odnosno pristupa sopstvenom poštamskom sandučetu[76].

Ako elektronski ugovor posmatramo kao ugovor o prodaji robe ili usluga sačinjen između dve strane onda se on u načelu može zaključiti na tri načina: putem elektronske pošte, elektronskom razmenom podataka i putem Interneta[77].

Putem elektronske pošte potencijalni prodavac i kupac međusobno razmenjuju elektronske poruke, što je danas jedan od uobičajenih načina odložene komunikacije. Ta komunikacija je, po pravilu, neformalna. Takođe ovakva komunikacija može biti i formalna pa je samim tim podobna da dovede do zaključenja punovažnog ugovora o prodaji. Ovaj stav potvrđuje i sudska praksa jer sudovi, kada dođe do spora povodom nekog ugovora o prodaji zaključenog na osnovu razmene elektronskih poruka, takvu komunikaciju smatraju relevantnom pod uslovom da su međusobno razmenjene elektronske poruke dostupne u informacionom sistemu strane kojoj su upućene.

Drugi način elektronske komunikacije je razmena elektronskih podataka (EDI-Electronic Data Interchange). U najopštijem smislu reč je o razmeni informacija od računara do računara, po pravilu, bez učešća ljudi. Ovaj vid komunikacije u cilju pregovaranja i zaključenja ugovora je uobičajen između lica koja kontiunirano sarađuju povodom kupovine i prodaje određene robe koja se redovno nabavlja, neretko i na dnevnoj bazi. Potencijalni kupac, naime, ima pristup preko svog računara u računar

[75] Službeni list SFRJ", br. 29/78, 39/85, 57/89, Službeni list SRJ, br. 31/93; u daljem tekstu ZOO.

[76] Tin Matić, „Formularni ugovori u elektronskom obliku“, tekst u „Zbornik Pravnog fakulteta u Zagrebu“ (ur. M. Petrak), Pravni fakultet Sveučilišta u Zagrebu, Zagreb, br. 3/08, str. 779-803.

[77] Katarina Jovičić, „Pravna pitanja elektronskih ugovora, s osvrtom na ugovor o prodaji robe“, Međunarodni tematski zbornik radova – Internet i društvo, pp. 353-363, 2014.

prodavca i može direktno iz njegovog magacina, koji se vodi u elektronskoj formi, da poručuje robu. Od ključnog značaja je da su strane ugovornice već uspostavile praksu zaključenja ugovora pod standardnim uslovima i ako je to slučaj, onda su ugovori zaključeni na pomenuti način punovažni i pravno obavezujući.

Internet trgovina je treći, takođe veoma čest način putem koga se zaključuju elektronski ugovori o prodaji, ali je ona više u upotrebi kod potrošačkih prodaja, premda nije isključeno ni da se trgovačke prodaje tako ugovaraju. Ceo proces trgovanja se u ovom slučaju odvija putem Internet prodajnih sajtova, npr. Amazon.com, preko koga se 24 časa dnevno prodaje hiljade najrazličitijih proizvoda širom sveta. Tehnika ugovoranja je, najčešće takva da se odabrani proizvod iz ponude objavljene na sajtu stavlja u virtuelnu korpu za kupovinu, a svaki kupac ostavlja informaciju o kreditnoj kartici sa koje će se elektronskim putem skinuti potrebna sredstva na ime plaćanja cene. Tako kupljena roba dostavlja se poštom na željenu adresu.

Pored velike primene elektronskih ugovora Zakonom o elektronskoj trgovini Republike Srbije su definisane i pravne oblasti u kojima se elektronski ugovori ne mogu primeniti. To su ugovori koji se moraju zaključiti samo u klasičnoj pisanoj formi i odnose se na[78]:

- ugovore o poklonu, jemstvu i zalozi,
- ugovore o raspolaganju imovinom lica kojima je oduzeta poslovna sposobnost,
- izjave stranaka i dugih učesnika u postupku za raspravljanje zaostavštine,
- 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,
- pravne poslove kojima se vrši prenos prava svojine na nepokretnosti ili kojima se ustanovljavaju druga stvarna prava na nepokretnostima,
- ugovore o utvrđivanju imovinskih odnosa između bračnih drugova,
- druge pravne poslove ili radnje, za koje je posebnim zakonom određena upotreba svojeručnog potpisa u dokumentima na papiru ili overa svojeručnog potpisa.

Slična praksa primera radi prisutna je i u Nemačkoj gde je je 2001. godine donet Zakon o izmenama pravila o pravnoj formi i ostalih pravila građanskog prava u vezi sa novim poslovno-pravnim komunikacijama, kojim je isključena mogućnost zaključenja u elektronskoj formi sledećih pravnih poslova[79]:

- davanje izjave u vezi sa ugovorom o radu,
- izdavati uverenja iz radnog odnosa,
- zaključivati ugovor o osiguranju,
- davanje izjave o delu
- priznanje duga,
- zaključiti ugovor o potrošačkom kreditu.

[78] Zakon o elektronskoj trgovini, Opus citatum Član 10.
[79] Direktiva o elektronskoj trgovini, Directive, 2000/31/EC

Prema članu 6., stavu 2. hrvatskog Zakona o elektronskom potpisu, sledeći pravni propisi se ne mogu zaključiti u elektronskoj formi[80]:

- pravni poslovi kojima se vrši prenos vlasništva na nekretninama ili se uspostavljaju druga stvarna prava na nekretninama,
- poslovi iz oblasti zaostavštine,
- imovinski predbračni, odnosno bračni ugovori,
- opterećenje i otuđenje imovine za koje je potrebno odobrenje centra za socijalni rad,
- ugovori o predaji i raspolaganju imovinom za života,
- ugovori o doživotnom uzdržavanju i sporazume u vezi s nasljeđivanjem,
- darovni ugovori,
- drugi pravni poslovi za koje je posebnim zakonom propisano da se sastavljaju u obliku javnobilježničkog akta, odnosno isprave i
- drugi pravni poslovi ili radnje za koje je posebnim zakonom ili na temelju zakona donesenim propisom izričito određena upotreba svojeručnog potpisa u dokumentima na papiru ili overa svojeručnog potpisa.

Poređenjem pravnih propisa koji se ne mogu zaključiti u elektronskoj formi u Republici Srbiji sa istovetnim pravnim propisima u zemljama okruženja i zemljama članicama Evropske Unije može se zaključiti da između ovih pravnih propisa nema značajnih razlika, čak je veliki deo njih istovetan.

Posebna karakteristika elektronskih ugovora kao i tradicionalinih jeste mogućnost njihovog dokazivanja kako pred nacionalnim tako i pred međunarodnim sugovima. Zaključeni elektronski ugovori moraju obezbediti sve potrebne informacije u cilju dokazivanja u slučaju sudskog spora. Da bi to bilo moguće, a imajući u vidu specifičnu formu elektronskih ugovora neophodno je da ponudilac koji posluje elektronskim putem obezbedi da tekst ugovora bude dostupan kupcu tako da on može da ga skladišti, ponovo koristi i reprodukuje kako u elektronskoj, tako i u pismenoj formi. Problem dokazivanja naročito dolazi do izražaja po pitanju čuvanja elektronskih podataka pomoću kojih se dokazuje postojanje i sadržaj ovih ugovora. U francuskom pravu profesionalci (trgovci, privrednici) dužni su da čuvaju sve podatke u periodu od deset godina od momenta zaključenja, odnosno izvršenja ugovora sa trenutnim izvršenjem prestacija. Ove osobe dužne su omogućiti pristup ovim podacima na zahtev druge strane, ako vrednost ugovora prelazi iznos od 120 eura. Budući da se u francuskom pravu zahteva pisana forma za dokazivanje ugovora (dokazna forma) čija vrijednost prelazi 1500 eura, Zakonom o elektronskom potpisu ugovorima zaključenim u elektronskoj formi dana je ista dokazna snaga kao i onima zaključenim na tradicionalan način, u pisanoj formi[81]. U pravnom sistemu Republike Srbije dokazna snaga elektronskih ugovora dodatno je potvrđena Zakonom o elektronskom dokumentu[82]. Ovim zakonom definisane su procedure postupanja u slučajevima kada se radi sa

[80] Zakon o elektroničkom potpisu, Republika Hrvatska.

[81] Genc Trnavci, „Zaključenje, punovažnost i dokazivanje elektronskih ugovora: komparativna analiza“, Zbornik Pravnog fakulteta Sveučilište u Rijeci, vol. 30, no. 1, pp. 449-472, 2009.

[82] Zakon o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju, Opus citatum, član 2.

elektronskim dokumentima, odnosno dokumentima koji su napisani u elektronskom formatu. Takođe procedure se uređuju i za dokumente koji su potpisani elektronskim potpisom. Kada se govori o međunarodnim elektronskim ugovorima pitanje koje se postavlja jeste određivanja suda koji je nadležan za rešavanje spora nastalog iz takvog ugovora, kao i pitanje izbora prava na osnovu čijih pravila spor treba raspraviti. U uporednom pravu, po pravilu, nema posebnih rešenja za elektronske ugovore već se, u interesu pravne sigurnosti, i na njih primenjuju postojeće norme međunarodnog privatnog prava[83]. Najbolje moguće rešenje u cilju olakšavanja vođenja sudskih sporova kada su upitanju elektronski ugovori sklopljeni na međunarodnom nivou jeste da ugovorne strane u samom ugovoru predvide rešenja za što je moguće veći broj potencijlno spornih pitanja. U suprotnom obe strane rizikuju da potencijalni spor vode na način, po pravilima i pred organizacijom koji nisu imale u vidu kada su sklapale ugovor.

3.2 Elektronske fakture

Elektronske fakture predstavljaju sve račune koji se izdaju i primaju elektronskim putem. Ovakav način izdavanja faktura donosi mnoge prednosti od kojih su brzina izdavanja i komunikacija jedne od najosnovnijih. Pored ove dve osobine ušteda novca i smanjenje grešaka u radu su još neke od pogodnosti upotrebe elektronskih faktura. Upotreba elektronskih faktura u Republici Srbiji pa čak i u mnogim zemljama okruženja još uvek je u razvoju o čemu svedoči ne tako veliki broj kompanija koje koriste pogodnosti ovog modela. Prema istraživanjima Evropske Unije, u procesu izdavanja i slanja elektronskih faktura mogu se ostvariti uštede i do 75 %. Pomenute uštede dobijaju se na osnovu smanjenja troškova štampanja faktura, njihovog slanja putem pošte ili kurirskih službi kao i na osnovu smanjenja troškova obrade istih. Christian Vindinge Rasmussen iz Norveške agencije za elektronsku javnu upravu Difi izneo je procenu da će se u narednih 6 godina uvođenjem elektronskih faktura ostvariti ušteda od neverovatnih 240 milijardi Evra na nivou EU. Skandinavske zemlje su lideri na svetskom nivou u ovom domenu[84]. Ukoliko se posmatra primena elektronskih faktura mogu se izdvojiti dva osnovna modela:

- Direktni model. Prema ovom modelu razmena elektronskih faktura obavlja se bez posrednika. Kod ovog modela mogu se razlikovati dva tipa. Prvi tip modela je model sa dobavljačem. Kod ovog tipa dobavljač šalje elektronske fakture svojim kupcima putem raznih kanala (web, e-mail, sms), ili kreira portal preko koga kupci mogu pogledati i preuzeti fakture u različitim elektronskim formatima (pdf, xml,...). Drugi tip model primenljiv je u situacijama kada primalac faktura svojim klijentima obezbedi informaciono komunikacioni sistem za prijem faktura. Fakture su najčešće

[83] Direktiva o elektronskoj trgovini, Opus citatum, član 1

[84] Elektronske fakture u Srbiji, Privredna komora Srbije, dostupno na: http://www.kombeg.org.rs/aktivnosti/udr_informatike/Detaljnije.aspx?veza=8819, datum pregleda: 20.12.2017.

definisane u unapred određenom formatu. Sami sistem koristi se za kompletnu obradu pristiglih faktura. Primenom ovakvog sistema primalac u velikoj meri smanjuje potencijalne grešeke prilikom obrade kao i vreme potrebno za samu obradu pristiglih faktura.

- Indirektni model. Suprotno direktnom modelu kod indirektnog modela komunikacija i prenos faktura između primaoca i izdavaoca fakture obavlja se putem posrednika. Primalac i izdavaoc faktura koriste sistem za razmenu elektronskih faktura koji obezbeđuje sigurnu razmenu, slanje i isporuku kao i mehanizam za utvrđivanje autentičnosti. Naravno i u ovom slučaju autentifikacija je zasnovana na kvalifikovanom elektronskom potpisu.

Istraživanja su pokazala da je upotreba elektronskih faktura najzastupljenija u Brazilu, Čileu i Meksiku. Velika zastupljenost elektronskih faktura posledica je angažovanja vlada ovih zemalja na planu usvajanja zakonskih okvira kojima se reguliše upotreba elektronskih faktura pretežno između pravnih lica. Sami proces prelaska sa upotrebe papirnih na upotrebu elektronskih faktura u Brazilu i Čileu završio se zaključno sa završetkom 2015. godine. Očekuje se da će grupi zemalja u kojima se primenjiju isključivo elektronse fakture vrlo brzo priključiti i zemlje poput Argentine, Perua, Gvatemale, Urugvaja i Ekvadora. Koliko je uvođenje elektronskih faktura značajno iz ugla ekonomije i finansijskog napretka pokazuje i činjenica da je ekonomija Meksika značajno napredovala uvođenjem automatizovanog načina poslovanja. Takođe usled lakšeg evidentiranja poreskih obaveznika i uspešnije naplate poreza stopa priliva sredstava u državnu kasu Meksika se povećala. Primer ekonomskog napretka Meksika svakako bi trebalo da prate ostale zemlje latinske Amerike. Takođe ovako dobru implementaciju elektronskog poslovanja i elektronskih faktura trebalo bi da prate i primene i evropske zemlje. Naravno da proces uvođenja elektronskih faktura i sistema elektornskog poslovanja nije ni malo lak i iza uspešne implementacije pre svega treba da stoje veliki napori vlade svake od zemalja. Na primeru Južne Amerije može se videti koliko je uvođenje ovakvih procesa zahtevno. Na samom početku odabrane su kompanije koje bi tokom devet meseci testirale sistem elektronskih faktura. Tokom tih devet meseci zakonodavni sistem je radio na kreiranju adekvatnih zakonodavnih regulativa koje bi pratile primenu elektronskih faktura. Nakon korekcije tehničkih nedostataka kao i usvajanja zakonskih i pod zakonskih regulativa određen je period tranzicije od maksimalno pet godina kako bi svi privredni subjekti prešli na upotrebu elektronskih faktura. Na prostorima Evropske unije takođe se radi na uvođenju i upotrebi elektronskih faktura, a o tome svedoči i podatak da su ove fakture najzastupljenije u B2G sektoru kao i da se procenjuje rast njihove upotrebe počevši od 2018. godine[85].

Da se u Republici Srbiji aktivno radi na uvođenju okvira za upotrebu elektronskih faktura i prelasku na upotrebu istih svedoči i potpisano objašnjenje između ministra finansija Dušana Vujovića i ministar trgovine, turizma i telekomunikacija Rasima Ljajića. Ovim obaveštenjem definisan je način izdavanja i knjiženja elektronskih

[85] Knjigovodstvene usluge, „Elektronske fakture“, dostupno na: https://www.knjigovodstveneusluge.rs/vesti/tag/elektronske%20fakture, datum pregleda: 22.12.2017.

faktura bez upotrebe pečata i potpisa. Takođe objašnjenjem je izjednačena upotreba papirnih i elektronskih faktura kada su upitanju pravna lica. Ključno pojašnjenje odnosilo se na to da je elektronska faktura je validna u elektronskom obliku, bez potpisa i pečata, ne mora da se štampa i ne mora da se šalje poštom[86,87]. Potencijlani problem koji se javlja sa fakturama kreiranim bez potpisa i pečata kao i bez bilo kakvog drugog vida zaštite jeste utvrđivanje činjenice o prijemu fakture od strane kupca robe ili dobara. Problem može nastati ukoliko firma potražilac sredstava pokrene postupak utuženja ili prinudne naplate putem sudskih izvršitelja bez infomracije da li je elektronska faktura zaista i stigla na adekvatnu adresu, kao i da li je adresa još uvek u upotrebi. S tim u vezi mora se definisati mehanizam koji će obezbediti povratnu informaciju o prijemu elektronske fakture. Potvrdu o prijemu elektronske fakture može izdati sami primalac fakture ili se potvrda može razmeniti preko ovlašćenog informacionog posrednika.

Još jedan od pokazatelja upotrebe elektronskih faktura u Republici Srbiji je i prisustvo kompanije Halcom i njena saradnja sa bankarskim sistemima. Naime Piraeus banka u saradnji sa Halcom je svojim klijentima obezbedila mogućnost razmene elektronskih faktura preko postojećeg rešenja za elektronsko bankarstvo. Halcom-ov standard nudi mogućnosti spajanja sistema sa već postojećim sistemom u okviru kompanije koja uvodi ovaj standard u svoje poslovanje. Halcom-ov sistem kreiran je tako da klijentima ponudi spajanje i razmenu podataka između velikog broja izdavaoca i primaoca, kao i podršku za celokupan proces likvidacije i plaćanja. Plaćanje e-fakture vrši se pomoću elektronskog bankarstva ili mobilnog plaćanje PlatiMo[88].

3.3 Zaštita elektronskih dokumenata, ugovora i faktura

Digitalni potpis

Digitalni potpis (Digital Signature) je skup podataka u elektronskom obliku. Ovaj elektronski skup podataka sa ciljem pružanja identifikacije potpisnika dokumenta obično je prodružen elektronskim porukama ili dokumentima. Ovo praktično znači da ovako definisan elektronski potpis obezbeđuje dokaz da sadržaj poruke nije izmenjen prilikom slanja od pošiljaoca do primaoca, kao i da je pošiljaoc zaista pravi. Osnovu

[86] N1, „Vlada: Elektronska faktura validna bez pečata i potpisa“, dostupno na: http://rs.n1info.com/a349053/Vesti/Vesti/Vlada-Srbije-Elektronska-faktura-validna-bez-pecata-i-potpisa-stampanje-nije-obavezno.html, datum predlega: 22.12.2017.

[87] Cekos in, „Objašnjenje u vezi sa izdavanjem i knjiženjem računa (faktura) u papirnom i elektronskom obliku bez upotrebe pečata i potpisa“, dostupno na: http://www.cekos.rs/obja%C5%A1njenje-u-vezi-sa-izdavanjem-i-knji%C5%BEenjem-ra%C4%8Duna-faktura-u-papirnom-i-elektronskom-obliku-bez, datum pregleda: 22.12.2017.

[88] Miodrag Ranisavljević, „Halcom e-fakture“, poslovni softver, dostupno na: https://www.poslovnisoftver.net/halcom-e-fakture/, datum pregleda: 22.12.2017.

digitalnog potpisa čini sadržaj same poruke. Pošiljalac nad svojom porukom primenjuje kriptografske algoritme pomoću kojih transformiše poruku u zapis fiksne dužine. Primera radi zapis poruke može biti 512 ili 1024 bita. Ovaj zapis zapravo predstavlja sami sadržaj poruke. Posmatrano iz ugla sigurnosti svaka promena u sadržaju poruke inicira proces izmene digitalnog potpisa kojim je poruka zaštićena. Proces komunikacije između pošiljaoca i primaoca se odvija tako što pošiljalac nakon što kreira dokument kreira i digitalni potpis na osnovu kreiranog dokumenta ili poruke. Digitalni potpis se kreira tako što ga pošiljalac enkriptuje svojim tajnim ključem. Nakon prijema poruke primalac vrši dekripciju poruke i to primenom javnog ključa. Kada dobije sadržaj poruke on na osnovu njega kreira digitalni potpis kako bi ga uporedio sa primljenim potpisom. U slučaju kada su potpisi identični primaoc može biti siguran da je poruka autentična i da je ona zaista poslata od pošiljaoca čijim je potpisom potpisana. Sigurnost u autentičnost poruke primaoc dobija na osnovu činjenice da je javnim ključem pošiljaoca uspešno dešifrovao potpis kao i na osnovu činjenice da je poruka stigla nepromenjena jer je utvrdio da su potpisi identiči. U praksi često dolazi do zabune pa se digitalni potpis poistovećuje sa digitalnom slikom ručnog potpisa što on svakako nije. Digitalni potpis je zamena za rukom ispisani potpis. Generalno se može zaključiti da digitalni potpis omogućava identifikaciju učesnika u komunikaciji kao i integritet podataka.

Upotreba elektronskog potpisa u Republici Srbiji regulisana je Zakonom o elektronskom potpisu[89]. Ovaj Zakon donet je još 2004. godine i od tada se u Republici Srbiji kreće sa razvoje i upotrebom servisa koji omogućavaju elektronsko potpisivanje dokumenata. Ovim zakonom uređuje se upotreba elektronskog potpisa u pravnim poslovima, poslovanju i ostalim pravnim situacijama. Takođe uređuju se i prava i obaveze koje su u vezi sa elektronskim sertifikatima.

Odredbe ovog zakona se primenjuju u slučajevima kada se radi o saradnji između organa državne uprave, saradnji između organa i stranaka kao i prilikom dostavljanja odluka u bilo kojoj vrsti sudskog spora koji se vodi pred državnim organima. Tačnije u slučaju vođenja postupaka elektronski potpis se može koristiti ukoliko je zakonom za konkretan postupak definisana upotreba elektronskog potpisa.

Odredbama ovog zakona definišu se dve vrste potpisa, a to su elektronski potpis i kvalifikovani elektronski potpis. Elektronski potpis je već duže vreme u upotrebi i mogu ga kreirati sami korisnici putem različitih eoftverskih alata. On bukvalno predstavlja oznaku autorstva nad elektronskim dokumentom koji je njime potpisan. Problem koji se javlja sa ovakvim potpisom je slaba ili gotovo nikakva zaštita, pa se on veoma lako može falsifikovati, kopirati, a samim ti i zloupotrebiti. Kvalifikovani elektronski potpis kao drugi oblik elektronskog potpisa predstavlja verziju koja je nastala poštovanjem različitih procedura i sigurnosnih mehanizama i protokola. Praktično opis procedura nastanka i upotrebe digitalnog potpisa dat u prethodnim sekcijama odgovara kvalifikovanom elektronskom potpisu. S tim u vezi kvalifikovani elektronski potpis se naziva i digitalni potpis. Praktično razlika između elektronskog i kvalifikovanog elektronskog potpisa ogleda se samo u stepenu implementirane zaštite,

[89] Zakon o elektronskom potpisu, Opus citatum.

odnosno u informaciji koju potpis u sebi sadrži. Autentičnost elektronskog i kvalifikovanog elektronskog potpisa utvrđuje se dekripcijom informacije koju oni sadrže. Zakonom o elektronskom potpisu definisamo je da kvalifikovani elektronski potpis mora da zadovolji sledeće uslove[90]:

- isključivo mora biti povezan sa potpisnikom,
- nedvosmisleno identifikuje potpisnika,
- nastaje korišćenjem sredstava kojima potpisnik može samostalno da upravlja i koja su isključivo pod nadzorom potpisnika,
- direktno je povezan sa podacima na koje se odnosi, i to na način koji nedvosmisleno omogućava uvid u bilo koju izmenu izvornih podataka,
- formiran je sredstvima za formiranje kvalifikovanog elektronskog potpisa,
- proverava se na osnovu kvalifikovanog elektronskog sertifikata potpisnika.

Ukoliko se uporedi sa svojeručnim potpisom i pečatom u papirnom obliku, elektronski potpis u odnosu na podatke u elektronskom obliku ima isto pravno dejstvo[91]. Elektronski sertifikat služi kao veza između elektronskog potpisa i samog identiteta potpisnika.

Digitalni (Elektronski) sertifikat

Elektronski (digitalni) sertifikat (Digital Certificate) je elektronski dokument koji izdaje sertifikaciono telo (CA-Certification Authority). Elektronski sertifikat može da se shvati kao digitalna lična karta. Poređenje sa digitalnom ličnom kartom moguće je jer ovaj sertifikat sadrži podatke kako o korisniku sertifikata tako i o sertifikacionom telu koje je izdavaoc sertifikata. Ovim sertifikatom ostvaruje se veza između podataka potrebnih za autentifikaciju elektronskog potpisa i samo identiteta potpisnika. Kako bi se autentifikacija uspešno obavila digitalni sertifikat sadrži javni kriptografski ključ korisnika kome je dat na korišćenje. Javni kriptografski ključ odgovara tajnom kriptografskom ključu koji je takođe u upotrebi prilikom enkripcije podataka. Zadatak sertifikacionog tela je da obezbedi mehanizam utvrđivanja tačnosti podataka u sertifikatu, tačnije da obezbedi garanciju da javni ključ u predmetnom sertifikatu zaista pripada korisniku čiji su podaci navedeni u tom sertifikatu. Na ovakav način korisnici na osnovu izgrađenog poveranja u sertifikaciono telo mogu biti sigurni da konkretan javni ključ zaista pripada korisniku koji je podatke enkriptovao odgovarajućim tajnim ključem. Samom distribucijom elektronskih sertifikata koji su javni dostupni vrši se i distribucija javnih ključeva koje sertifikat sadrži. Na ovakav način omogućena je pouzdana distribucija javnih ključeva. Svaki elektronski sertifikat potpisan je tajnim ključem sertifikacionog tela što onemogućava bilo kakvo falsifikovanje istog. Za verifikovanje validnosti digitalnog sertifikata koristi se javni ključ tj. sertifikat sertifikacionog tela.

[90] Ibidem, član 7
[91] Ibidem, član 10

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.

Sertifikaciono telo zaduženo za izdavanje elektronskih sertifikata može biti bilo koje pravno lice. Svako pravno lice koje želi da obavlja poslove izdavanja sertifikata mora se registrovati za obavljanje ove delatnosti. Za vođenje registra svih sertifikacionih tela zaduženo je ministarstvo. Prilikom registracije sertifikaciona tela dužna su da ispune niz tehničkih i personalnih zahteva. Ovi zahtevi dati su u sklopu Zakona o elektronskom potpisu. Takođe sertifikate može izdavati i organ državne uprave. Republika Srbija ima šest registrovanih sertifikacionih tela za izdavanje kvalifikovanih elektronskih sertifikata. Ova tela su pobrojana u nastavku[92]:

- Javno preduzeće „POŠTA SRBIJE" – Sertifikaciono telo Pošte
- PRIVREDNA KOMORA SRBIJE – PKS CA (Sertifikaciono telo Privredne komore Srbije)
- ELECTRONIC BANKING BUREAU – EBB CA
- MUP RS – Sertifikaciono telo MUP RS
- HALCOM BG CA
- „E – Smart Systems" d.o.o. – ESS CA
- Sertifikaciono telo Ministarstva odbrane i Vojske Srbije

Postupak izdavanja kvalifikovanih elektronskih sertifikata je sličan kod svih registrovanih sertifikacionih tela. Ukoliko za primer uzmemo Sertifikaciono telo MUP-a Republike Srbiije postupak je sledeći[93]. Korisnik podnosi zahtev nadležnoj policijskoj stanici, prema prebivalištu odnosno boravištu. Za podnošenje zahteva potrebna je lična karta sa čipom kao i lozinka/PIN za ličnu kartu, koja se dobija u koverti prilikom preuzimanja lične karte. Nakon podnošenja zahteva korisnik potpisuje ugovor o izdavanju kvalifikovanog elektronskog sertifikata i isti se može koristiti. Celokupna usluga je potpuno besplatna. Da bi elektronski sertifikati a samim ti i elektronski potpis mogao da se koristi korisnik mora da poseduje čitač smart kartica

[92] Ministarstvo trgovine, turizma i telekomunikacija, „Elektronski potpis", dostupno na: http://epotpis.mtt.gov.rs/elektronski-potpis/, datum pregleda: 05.01.2018.
[93] Ministarstvo unutrašnjih poslova, „Sertifikaciono telo MUP-a Republike Srbije", dostupno na: http://ca.mup.gov.rs/, datum pregleda: 05.01.2018.

kao i instaliran lanac sertifikata na svom računaru. Svi potrebni sertifikati se mogu preuzeti potpuno besplatno sa sajta Ministarstva Unutrašnjih poslova. Takođe moraju imati instaliran odgovarajući Middleware za ličnu kartu. Verzija Middleware-a koju je potrebno da korisnici instaliraju razlikuje se u zavisnosti od lične karte koju korinik poseduje. Jedna verzija Middleware-a se koristi za lične karte izdati pre 18.08.2014. godine, dok se druga verzija koristi za lične karte izdate posle 18.08.2014. godine. Obe verzije se mogu preuzeti potpuno besplatno kao što je to slučaj sa sertifikatiima. Problem koji se javlja sa upotrebom elektronskih sertifikata jeste podrška za rad na određenim operativnim sistemima. Celokupna softverska podrška Sertifikacionog tela MUP-a Republike Srbije radi isključivo na Windows operativnom sistemu. Korisnici čiji računari rade na drugom operativnom sistemu nisu u mogućnosti da koriste elektronske sertifikate izdate od strane ovog kvalifikovanog sertifikacionog tela. U ovakvim slučajevima korisnici se moraju za dodelu sertifikata obratiti nekom drugom kvalifikovanom sertifikacionom telu, kao šte je recimo Pošta Srbije. Sertifikati ovog tela rade gotovo na svim platformama (Windows, OS X, Linux). Međutim ovakva uluga kod Pošte Srbije nije besplatna pa korisinici moraju izdvojiti određeni svotu novca za upotrebu sertifikata. Svota novca zavisi od zahtevane usluge i definisana je zvaničnim cenovnikom[94]. Sertifikati se izdaju na period od jedne do pet godina, pa i cena zavisi od perioda korišćenja. Primera radi cena sa porezom kvalifikovanog elektronskog sertifikata na smart kartici zajedno sa čitačem na period korišćenja od jedne godine iznosi 3325 din, dok ukoliko se radi o periodu korišćenja od pet godina cena sa porezom iznosi 4545 din. Postupak izdavanja je maltene isti kao u slučaju MUP-a, stim što se ovde zahtev podnosi u najbližoj ekspozituri Pošte.

Vremenski žig

Kako bi se obezbedila pouzdana informacija o vremenu stizanja elektronskog dokumenta (ugovora, fakture, ...) kreiran je vremenski žig. Vremenski žig zaprevo predstavlja zvanično vreme koje je pridodato elektronskom dokumentu ili pak grupi elektronskih dokumenata. Vremenskim žigom potvrđuje se sadržaj elektronskog dokumenta u vremenskom trenutku u kome mu je vremenski žig pridružen. Takođe vremenskim žigom može se potvrditi sadržaj svakog dokumenta u grupi. Neki od osnovnih razloga korišćenja vremenskog žiga su[95]:

- Onemogućavanje krivotvorenja podataka u elektronskom dokumentu pridruživanjem tačnog vremena unosa vremenskog žiga. Praktično vremenski žig se unosi nekoliko trenutaka kasnije u odnosu na elektronski potpis, iz čega proističe da je nemoguće da trenutak elektronskog potpisivanja bude posle unosa vremenskog žiga.

[94] Sertifikaciono telo Pošte, „Cenovik“, dostupno na: http://www.ca.posta.rs/cenovnik.htm, datum pregleda: 05.01.2018.

[95] Dragan Spasić, „Vremenski žigovi sertifikacionog tela pošte“, Zbornik radova XXVIII Simpozijuma novim tehnologijama u poštanskim ulugama i telekomunikacionom saobraćaju – PosTel 2010, Beograd, 2010, str. 175-184.

- Nakon isteka roka važnosti elektronskog sertifikata kojim je elektronski potpis kreiran vremenski žig idalje omogućava uspešnu verifikaciju elektronskog potpisa.
- Vremenskim žigom je omogućena uspešna verifikacija elektronskog potpisa i posle opoziva elektronskog sertifikata kojim je elektronski potpis kreiran.

U praksi se mogu razlikovati različite šeme vremenskog žiga u zavisnosti od tehnologije izrade, primenjenih kriptografska rešenja, i zahtevanog stepena sigurnosti. Neke od šema su: Public key infrastructure (PKI), Linking-based schemes, Distributed schemes, Transient key scheme, MAC.

Public key infrastructure (PKI). Kod ove šeme token vremenskog žiga je zaštićen korišćenjem digitalnog potpisa baziranog na infrastrukturi javnog ključa. PKI povezuje javne ključeve sa odgovarajućim korisnicima (pojedinci ili organizacije). U zavisnosti od nivoa sigurnosti koju je potrebno obezbediti povezivanje se može izvršiti automatskim procesom ili nadzorom čoveka. Praktično PKI predstavlja seriju procesa i standarda koji se koriste kako bi obezbedili da elektronski transfer informacija protekne bezbedno. Ovo je industrijski standard koji se koristi u elektronskom poslovanju, Internet bankarstvu, poverljivim email-ovima kao i za obezbeđenje drugih mrežnih aktivnosti. Iz ugla kriptografije ovo je tehnika koja omogućava entitetima da sigurno komuniciraju putem nebezbednih javnih mreža, kao i da verifikuju identitet svakog od entiteta u komunikaciji putem digitalnog potpisa. U skopu ove infrastrukture može se izdvojiti nekoliko ključnih komponenti. Sertifikaciono telo kao prva komponenta predstavlja nezavisno telo za distribuciju digitalnih sertifikata. U principu ovo telo obezbeđuje pošiljaocu javni ključ pomoću koga pošiljaoc vrši enkripciju podataka pre slanja. U isto vreme sertifikaciono telo primaocu poruke obezbeđuje tajni ključ pomoću koga će primljene podatke dekriptovati. Praktično sertifikaciono telo poseduje sopstveni sertifikat, javni i privatni ključ. Ovaj sertifikat se koristi u procesu verifikacije digitalnog potpisa koji sertfikaciono telo koristi. Pored obezbeđivanja sertifikata koji se koristi u procesu komunikacije između pošiljaoca i primaoca sertifikaciono telo mora da bude u mogućnosti da odbaci izgubljeni ili kompromitovani sertifikat a da pritom datu informaciju učini dostupnom[96]. Drugu komponentu u ovoj infrastrukturi predstavlja digitalni sertifikat koji se koristi u cilju potvrđivanja identiteta vlasnika javnog ključa. Javni ključ je deo samog sertifikata. Dodatno sertifikat potvrđuje da vlasnik javnog ključa sadržanog u sertifikatu poseduje odgovarajući privatni ključ. Svakom od sertifikata dodeljen je period vremena tokom kog je aktivan. U sličaju narušavanja validnosti sertifikat može postati neaktivan pre isteka ovog perioda. Ova funkcija služi kao način za rešavanje nestandardnih situacija, na primer, ako je privatni ključ kompromitovan pa se samim tim više ne može verovati sertifikatu. Javni i privatni ključevi kao treća komponenta ove infrastrukture su specijalno kreirani parovi brojeva koji ogućavaju digitalno potpisivanje sadržaja. Privatni ključ vrši identifikaciju vlasnika i mora se čuvati od ostalih. Suprotno njemu javni ključ kao što mu samo ime kaže se distribuira javno i njegov zadatak je da verifikuje podatke koji su potpisani odgovarajućim privatnim ključem.

[96] Net security training. „What is a Public Key Infrastructure“, Dostupno na: https://web.archive.org/web/20161009124244/http://www.net-security-training.co.uk/what-is-a-public-key-infrastructure datum pregleda: 29.12.2017.

Linking-based schemes[97]**.** Vremenski žig kreiran pomoću ove šeme sastoji se od međusobno povezanih tokena u cilju obezbeđenja većeg stepena sigurnosti. Ovo praktično znači da su podaci koji se odnose na prethodne tokene uključneni u trenutni token. Ove šeme se kreiraju u cilju detekcije lažnih vremenskih žigova koji su nastali pod dejstom malicioznog izdavaoca vremenskih žigova. Izdavaoc vremenskih žigova (TSA - Time-Stamping Authority) se može implementirati tako da sadrži bazu podataka sa dve sekvence podataka *A* vrednosti i *S* vrednosti. Na osnovu podnetog zahteva za vremenski žig u vremenu *T(i)*, TSA izračunava info objekat vremenskog žiga koji uključuje vrednost trenutnog vremena, hash vrednost dokumenta, serijski broj i naziv TSA. *A(i)* se izračunava primenom hash funkcije nad info objektom vremenskog žiga, *S(i)* se izračunava takođe primenom hash funkcije samo ovoga puta nad ulazima *A(i), S(i-1)*, i po mogućnosti nad što većim brojem *S(j)* vrednosti*, j<i-1*. Nakon ovog procesa TSA generiše token vremenskog žiga inkapsuliranjem kreiranog info objekata vremenskog žiga i vrednosti korišćene za izračunavanje *S(i)* u obrađeni objekat sa podacima. Ovako kreirani token vremenskog žiga se vraća podnosiocu zahteva putem kanala koji obezbeđuje integritet podataka i originalnu autentifikaciju. Token se periodično (svakog dana ili nedelje) objavljuje putem javnih medija, primera radi dnevnih novina. Sam proces objavljivanja obavlja se na autentičan način, tako da korisnici uvek mogu bez problema naći token.

Pored korišćenja hash funkcije u postupku kreiranja tokena mogu se koristiti binarna stabla ili skip liste. Po pitanju binarnih stabala najčešće se koriste Merkle-lova stabla. Korišćenjem ovih stabala smanjuje se količina podataka koju je potrebno skladištiti. Kod ovako kreirnanih binarnih stabala uvodi se notacija runde. Praktično tokom jedne runde obrade TSA na osnovu pristiglih zahteva konstruiše binarno stablo oblučivanja korišćenjem SHA-1 ili MD5 hash funkcija. Heširani dokumenti predstavljaju listove stabla. Kako bi stablo bilo balansirano broj čvorova mora da bude stepena 2. Balansirano stablo nije efikasno kada broj dokumenata nije blizu stepenu dvojke. Skip liste kao treći metod kreiranja tokena za vremenski žig od nedavno je u upotrebi kao zamena za balansirano stablo. Algoritmi dodavanja i brisanja u skip listu su jednostavniji i brži od istih algoritama kod balansiranog stabla.

Upotreba bilo kod od pomenutih metoda prilikom kreiranja vremenskog žiga zavisi kako od složenosti samog procesa kreiranja tokena tako i od procesa verifikacije na drugoj strani. Kod kreiranja lančanih šema vremenskog žiga pomoću hash funkcija protokol verifikacije se sastoji od nekoliko faza. Najpre se vrši preračunavanje niza hash vrednosti počevši od prethodno objavljene vrednosti. Zatim se vrši provera da li vrednost *A(i)* koja se nalazi u tokenu vremenskog žiga poklapa sa info objektom vremenkog žiga. Nakon utrvđenog poklapanja pokušava se rekonstrukcija *S(i)* na osnovu vrednosti *A(i)* i *S(i-1)* (kao i na osnovu većeg broja vrednosti S). Vrednost *S(i)* mora odgovarati onoj u TSA bazipodataka. Nakon poređenja datih i izračunatih vrednosti, preračunavanje prelazi na narednu objavljenju vrednost. Verifikacija je uspešna ukoliko je naredna objavljena vrednost tačna. Prema ovom modelu verifikacija

[97] Alexis Bonnecaze, Pierre Liardet, Alban Gabillon, and Kaouther Blibech, „Improving Time Stamping Schemes: A Distributed Point of View“, Satoshi Nakamoto Institute, 2002

je zavisna od dva objavljivanja tokena. U slučaju kreiranja tokena vremenskog žiga pomoću balansiranog binarnog stabla proces verifikacije je manje složen nego što je to bio slučaj kod lančanja hash vrednosti. Ovde se verifikacija sastoji iz dve faze. U prvoj fazi proverava se da li je hash funkcija dokumenta jednaka vrednosti H_i koja je inkludovana u vremenski žig. U drugoj fazi proverava se konzistentnost između vrednosti TS_r koja se nalazi u TSA bazi podataka i iste vrednosti generisane iz tokena vremenskog žiga. Vrednost TS_r se inicijalno u procesu kreiranja tokena memoriše u TSA bazi podataka, a kreira se sa svakom rundom tokena koji se publikuju.

Distributed schemes. U slučaju distribuiranih šema veći broj servera za kreiranje vremenskog žiga učestvuje u procesu kreiranja novog žiga. Na ovakav način otklonjeni su problemi nedostupnosti servera i gubitka. Distribuirane šeme su kreirane od strane većeg broja servera kojima se može upravljati nezavisno. Ovakve šeme su daleko postojanije posmatrano iz ugla otkaza servera i mrežnih napada, nego što je to slučaj sa šemama koje se kreiraju upotrebom samo jednog servera. Problem koji se javlja u procesu kreiranja ovakvih šema jeste broj zahteva za kreiranjem vremenskog žiga koji se mogu obraditi. Prilikom realizacije sistema za kreiranje distribuirane šeme sistem mora obraditi sledeće probleme: kako selektovati aktivne servere, koliko servera treba biti selektovano, da li serveri trebaju biti sinhronizovani, kako minimizovati broj interakcija između servera, kako konstruisati vremenski žig iz primljenih fragmenata tokena i kako minimizovati veličinu vremenskog žiga. Problem veličine vremnskog žiga mora biti realizavan tako da ni u kom slučaju veličina vremenskog žiga ne zavisi od broja aktivnih servera. Ovo praktično znači da ukoliko veći broj servera učestvuje u kreiranju vremenskog žiga, broj fragmenata će biti veći a samim tim i veličina jednog fragmenta će biti manja.

Transient key scheme. Generalno posmatrano ova šema je slična šemi baziranoj na infrastrukturi javnog ključa. Razlika je u tome što se u slučaju ove šeme parovi ključeva generišu i dodeljuju u kratkim vremenskim intervalima umesto dodeljivanja pojedincima i organizacijama. Pored ove razlike kod transient key šeme blokovi kriptografskih podataka su međusobno povezani tokom vremena. Podaci enkriptovani privatnim ključem povezanim sa određenim vremenskim trenutkom mogu biti bez ikakve provere povezani sa tim vremenskim intervalom. Ovo praktično znači da je par ključeva aktivan samo nekoliko minuta nakon čega se privatni ključ trajno uništava. Ova karakterisitka predstavlja glavnu razliku u odnosu na PKI šemu iz prostog razloga jer transient key šeme ne zavise od dugoročne sigurnosti privatnih ključeva. Kada vremenski interval u transient key sistemu istekne, novi par javnog i privatnog ključa se generiše. U ovom procesu privatni ključ koji je korišćen u prošlom vremenskom intervalu se koristi za digitalnu sertifikaciju novog javnog ključa. Tek nakon ovog procesa se privatni ključ iz prošlog vremenskog intervala uništava. Kako se u ovoj šemi parovi ključeva vezuju za tačan interval vremena i kako je njihovo trajanje ograničeno na fiksan kvant vremena izvor vremena mora biti standardizovan i poznat svim pošiljaocima i primaocima. Kako lokalno sistemsko vreme može biti promenjeno od strane korisnika ono se nikada ne koristi kao izvor vremena prilikom kreiranja ključeva. Umesto toga podaci se u skladu sa ANSI ASC X9.95 standardom digitalno potpisuju vremenom dobijenim od UTC (*Universal Time Coordinate*) čija se tačnost

meri u milisekundama. Kao dodatna sigurnosna mera svi zahtevi za potpisivanjem primljeni tokom istog vremenskog kvanta se čuvaju u log fajlu koji se nadovezuje na javni ključ na početku novog intervala. Ovakav mehanizam onemogućava dodavanje novih potpisanih događaja u intervalni lanac nakon kreiranja novog vremenskog intervala. Kako bi se obezbedila bolja zaštita od potencijalnog narušavanja sigurnosti koju donosi ulančavanje, može se iskoristiti cross validacija pomoću treće strane u vidu nezavisnih servera. Mreža međusobno povezanih cross-certifying servera u distribuiranom okruženju kreira lanac poverenja koji je jak kao najjača veza. Cross-certifying proces zahteva da se vremenski žig kreiran u intervalnom lancu servera od poveranja poklapa sa vremenskim žigom cross-certifying servera. Ovo praktično znači da je razlika u poklapanju vremena manja od sume preciznosti dva vremenska žiga plus vreme koje je potrebno za izvršenje cross sertifikacije. Cross sertifikacija se opciono može konfigurisati tako što serveri za cross sertifikaciju autentifikuju jedni druge korišćenjem dodatnih metoda kao što su klasični PKI sertifikati. Na ovakav način cross sertifikacija daje nezavistan dokaz o postojanju događaja u vremenskom lancu kao i o postojanju njegovog javnog ključa i sve to u tačnom vremenskom trenutku[98].

MAC (Message Authentication Code). Ukoliko se posmatra iz ugla kriptografije MAC predstavlja mali deo informacije koji se koristi u procesu potvrđivanja autentičnosti poruke. Drugim rečima koristi se kako bi se potvrdilo da poruka potiče od pravog pošiljaoca (njegova autentičnost) i da nije izmenjena tokom prenosa (njegov integritet). MAC algoritam prihvata tajni ključ i poruku proizvoljne dužine koja mora biti ista na ulazu i izlazu iz MAC algoritma. MAC vrednost štiti kako integritet podataka u poruci tako i njegovu autentičnost omogućavajući verifikatorima (koji poseduju tajni ključ) da otkriju bilo kakvu promenu sadržaja poruke. MAC se razlikuje od digitalnog potpisa s obzirom da su obe MAC vrednosti kreirane i verifikovane korišćenjem istog tajnog ključa. Ovo podrazumeva se pošiljaoc i primaoc poruke moraju dogovoriti o korišćenju istog ključa pre pokretanja komunikacije, kao što je to slučaj kod primene simetrične enkripcije. MAC algoritam može biti konstruisan od drugih kriptografskih primitiva, kao što su kriptografske hash funkcije (na primer HMAC), ili block cipher algoritmi OMAC (One-key MAC), CBC-MAC (Cipher Block Chaining Message Authentication Code), i PMAC (Parallelizable MAC). Bilo kako bilo neki od najbržih MAC algoritama kao što su UMAC (baziran na kriprografskim hash funkcijama) i VMAC (block cipher algoritam) su konstruisani na osnovu univerzalnog hesiranja (universal hashing). Univerzalno heširanje odnosi se na random selektovanje hash funkcije iz familije hash funkcija sa određenom matematičkom pripadnošću. Ovo garantuje mali broj očekivanih kolizija čak i ako su podaci odabrani od strane napadača.

Pomenute šeme za kreiranje i upotrebu vremenog žiga moraju biti standardizovane. Postoji veći broj standarda koji pokrivaju oblast kreiranja vremenskog žiga. Tri najosnovnija standarda su RFC 3161, ANSI X9.95 i ISO/IEC 18014. RFC 3161 standard je kreiran od strane Task Force internet inženjera. Ovo je najkorišćeniji

[98] Proof space, „System Technical Overview“, dostupno na: http://fios.com/proofmarksystemtech.pdf, datum pregleda: 02.01.2018.

standard kod kreiranja vremenskog žiga. Ovaj standard sadrži detaljan opis komunikacije između podnosioca zahteva za kreiranjem vremenskog žiga i TSA izdavaoca, kao i razloge za uvođenje sigurnosnih mera prilikom rada sa vremenskim žigom. Mnogi TSA nude vremenski žig koji je u skladu sa ovim standardom. Pored svih pomenutih pogodnosti ovaj standard je još i jedini besplatni od sva tri pomenuta, što može biti još jedan od razloga njegove veliki upotrebe. ANSI X9.95 standard opisuje pravila, obaveze i zahteve koriniska vremenskog žiga, izdavaoca vremenskog žiga, podnosioca zahteva za izdavanjem vremenskog žiga, kao i učesnika u kreiranju vremenskog žiga na kojima se oslanja bilo koji od procesa. Standard takođe specificira objekte podataka, dijagram toka, obradu grešaka i izuzetaka, kao i formate poruka. Takođe pored pomenutog standard definiše metode za kreiranje digitalnog potpisa, MAC-a šeme, povezanih tokena (linked token) šeme i transient key šeme. Pored toga, standard nudi sveobuhvatan skup ciljeva kontrole vremenskog žiga kako bi se potvrdio pouzdani sistem vremenskog žiga koji bi koristio profesionalni stručnjak za reviziju. Kako ovaj standard nije besplatan njegova cena u trenutku pisanja ovog rada iznosila je 100 dolara[99]. ISO/IEC 18014 standard je kreiran od strane međunarodne organizacije za standardizaciju. Sami standard se sastoji od tri dela. Prvi daje uopštene definicije servisa za kreiranje vremenskog žiga. Drugi specificira mehanizme pomoću kojih se kreiraju nezavisni tokeni. I treći deo se bavi mehanizmima koji kreiraju povezane tokene[100]. Cena ovog standarda je 88 švajcarskih franaka. Različite šeme za kreiranje vremenskog žiga bazirane su na jednom ili više određenih standarda. Činjenica da određena šema ispunjava veći broj standarda govori o tome da konkretna šema ispunjava veći broj zahteva, ali ne mora jednobrazno obezbeđivati veću sigurnost i postojanost vremenskog žiga. Primera radi PKI zadovoljava sva tri pomenuta standarda, dok MAC šema ili transient key šema zadovoljavaju samo ANSI X9.95 standard a opet su se u praksi pokazale kao sigurnije.

Pored primene različitih zaštitenih mehanizama prilikom kreiranja vremenskog žiga moraju postojati i pravni okviri kojima se reguliše ova oblast. Zakonom o elektronskom dokumentu, elektronskoj identifikaciji, i uslugama od poverenja u elektronskom poslovanju Republike Srbije definisano je da se o pružanju kvalifikovane usluge od poverenja zaključuje ugovor između pružaoca i korisnika kvalifikovane usluge od poverenja, a na zahtev korisnika[101]. Svaki zahtev podnesen kako bi se kreirao vremenski žig mora sadržati određene podatke kako iz elektronskog dokumenta tako i iz elektronskog potpisa. Sadržaj strukture podataka vremenskog žiga je u skladu sa standardom RFC 3161 „Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)" i obavezno uključuje[102]:

---

[99] American National Standards Institute, „ANSI X9.95-2016 - Trusted Time Stamp Management and Security“, dostupno na: https://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+X9.95-2016, datum pregleda: 02.01.2018.

[100] International Organization for Standardization, dostupno na: https://www.iso.org/home.html, datum pregleda: 05.01.2018.

[101] Zakon o elektronskom dokumentu, elektronskoj identifikaciji, i uslugama od poverenja u elektronskom poslovanju, Opus citatum, član 30.

[102] Pravilnik o izdavanju vremenskog žiga, Sližbeni glasnik RS, br. 112/2009

- identifikator izdavaoca vremenskog žiga,
- serijski broj vremenskog žiga,
- objekat za formiranje vremenskog žiga, koga čini kriptografski otisak iz zahteva za formiranje vremenskog žiga,
- identifikator algoritma kojim je formiran kriptografski otisak
- datum i vreme formiranja vremenskog žiga
- elektronski potpis strukture podataka vremenskog žiga
- elektronski sertifikat putem koga se može verifikovati elektronski potpis, kao i kompletan lanac sertifikata sertifikacionog tela koje je izdalo elektronski sertifikat izdavaocu vremenskog žiga
- identifikator algoritma koji je korišćen pri formiranju elektronskog potpisa
- oznaku Politike izdavanja vremenskog žiga

Vreme koje je zapisano u vremenskom žigu prilikom kreiranja vremenskog žiga odgovara tačnom trenutku formiranja tog žiga. Tolerancija vremena zapisanog u vremenskom žigu u odnosu na UTC vremensku skalu ne sme biti veća od jedne sekunde.

Izdavalac vremenskog žiga mora biti upisan u Registar izdavalaca vremenskog žiga. Postupak registracije počinje podnošenjem zahteva od strane potencijalnog izdavaoca. Izdavalac vremenskog žiga prilikom podnošenja zahteva za upis u Registar izdavalaca vremenskog žiga podnosi akt o opštim uslovima za pružanje usluge izdavanja vremenskog žiga. Ovim aktom korisnicima su definisane sve potrebne informacije na osnovu kojih mogu odlučiti da li će prihvatiti ovu uslugu i ukoliko je prihvate u kom obimu će je korisiti. Prilikom izdavanja vremenskog žiga jedan od međunarodnih standarda kojim se treaba rukovoditi jeste i ETSI TS 102 023 "Policy requirements for time-stamping authorities"[103]. Na osnovu podnetog zahteva za upis u Registar izdavalaca ministarstvo nadležno za informaciono društvo proverava ispunjenost uslova za registraciju izdavaoca vremenskog žiga. Sama provera obuhvata obuhvata[104]:

- proveru Politike izdavanja vremenskog žiga i Internih pravila rada izdavaoca vremenskog žiga, kao i njihove usklađenosti sa Zakonom i ovim pravilnikom,
- proveru operativnog rada izdavaoca vremenskog žiga,
- proveru ispunjenosti tehničkih i bezbednosnih uslova za komponente koje koristi izdavalac vremenskog žiga za izdavanje vremenskog žiga.

Što se tiče sistema za formiranje vremenskog žiga definisani su uslovi koje on mora da ispuni. Uslovi su definisani tako da svako izdavanje vremenskog žiga zadovolji zakonske regulative, međunarodne standarde i stručna pravila. Pomenuti standradi i pravila definisani Pravilnikom o izdavanju vremenskog žiga u Republici Srbiji su:

- ETSI TS 101 861 "Time stamping profile";
- RFC 3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

[103] Pravilnik o izdavanju vremenskog žiga, Opus citatum, član 4.
[104] Ibidem, član 15.

Izdavalac vremenskog žiga takođe mora da obezbedi da asimetrični ključevi na osnovu kojih se kreira vremenski žig budu generisani i čuvani u strogo kontrolisanim i bezbednim uslovima. Svaki asimetrični par kriptografskih ključeva mora biti pridružen sistemu za formiranje vremenskog žiga. Ukoliko dođe do generisanja novog para asimetričnih ključeva mora se generisati i novi elektronski sertifikat. Generisanjem novog elektronskog sertifikata ne prestaje važenje starog elektronskog sertifikata. Period validnosti elektronskog sertifikata sistema za formiranje vremenskog žiga je najmanje pet godina, a period korišćenja asimetričnog privatnog ključa je najviše tri meseca[105]. Ukoliko se uporedi period validnosti elektronskog sertifikata i period korišćenja asimetričnog privatnog ključa u Republici Srbiji sa drugim izdavaocima vremenskog žiga može se uvideti da je u Sloveniji period validnosti sertifikata isti dok je period korišćenja asimetričnog ključa veći i iznosi 3 godine. Ovo važi ukoliko je Ministarstvo za javnu upravu Slovenije izdavaoc vremenskog žiga. S druge strane ukoliko je Pošta Slovenije izdavaoc vremenskog žiga period validnosti sertifikata je takođe 5 godina, dok je period validnosti ključa kraći i iznosi jednu godinu.

Sami postupak zaštite dokumenta vremenskim žigom započinje korisnik nakon svih unetih izmena. Praktično korisnik najpre izvrši elektronsko potpisivanje dokumenta korišćenjem odgovarajuće aplikacije, koja prema Timestamp serveru pošalje zahtev za vremenskim žigom. Nakon toga Timestamp server generiše vremenski žig koji pošalje ka korisničkoj aplikaciji, koja vremenski žig pridruži elektronskom potpisu dokumenta. Svaki od Timestamp servera mora da poseduje određene karatkeristike kako bi odgovorio zahtevima za kreiranjem vremenskog žiga.

Izdavaoci vremenskog žiga upisani u Registar izdavaoca vremenskog žiga u Republici Srbiji su:

- Direkcija za elektronsku upravu i
- Javno preduzeće „Pošta Srbije“-Sertifikaciono telo pošte.

Direkcija za elektronsku upravu izgradila je infrastrukturu potrebnu za izdavanje vremenskih žigova za potrebe državnih organa, organa lokalne samouprave i javnih službi Republike Srbije. Ovo praktično znači da fizička lica kao i pravna lica putem direkcije za elektronsku upravu nemaju mogućnost korišćenja vremenskog žiga. Ovo telo izdaje vremenski žig u skladu sa preporukama u RFC 3161 „Internet X.509 Public Key Infrastructure Time-Stamp Protocol – TSP“). Da bi određeni državni organ, organ lokalne samouprave ili javne službe koristio uslugu RS-GOV TSA potrebno je da podnese zahtev na Portalu eUprava, i potpiše ga kvalifikovanim sertifikatom. Od korisnika se zahteva korišćenje kriptografskog otiska podataka po SHA-256 algoritmu. Celokupna usluga izdavanja vremenskog žiga je besplatna za državne organe, organe lokalne samouprave i javne službe.

Sa druge strane sertifikaciono telo Pošte je izgradilo sistem za izdavanje vremenskih žigova primenom rešenja kompanije Thales e-Security[106] i postalo je izdavalac vremenskih žigova (TSA) u Republici Srbiji. Usluga izdavanja vremenskog

[105] Ibidem, članovi 18 i 19.
[106] Thales Security, dostupno na: https://www.thalesesecurity.com/, datum pristupa: 09.01.2018.

žiga javnog preduzeća „Pošta Srbije“, se naplaćuje prema usvojenom cenovnuku i to prema dva moguća tarifna modela: Prepaid i Postpaid model. Svi prepaid paketi imaju vremensko ograničenje od jedne godine od dana aktivacije paketa. Broj žigova u prepaid paketu se kreće od 200 do 10000, dok se cena paketa kreće od 1600 do 40000 dinara respektivno. U postpaid paketu broj granice su od 0 do preko 500000, a cena je definisana prema potrošnji. U cenu za pravno lice uračunato je otvaranje jednog administratorskog naloga koji ima mogućnost da kreira korisničke naloge za zaposlene iz svog pravnog lica ili jednog korisničkog naloga. Otvaranje dodatnih administratorskih ili korisničkih naloga od strane zaposlenih iz Sertifikacionog tela Pošte, naplaćuje se po ceni od 100,00 dinara po jednom nalogu. Što se tiče fizičkih lica ona su očekivano ograničena na jedan korisnički nalog. Takođe ovo sertifikaciono telo nudi kupovinu TSA elektronskog sertifikata za vremenski žig u iznosu od 6000 din za period korišćenja od pet godina.

3.4 Elektronska trgovina

Kada se govori o elektronskim poslovnim transakcijama one se mogu izvršavati između pravnih lica ili između pravnog lica i pojedinca. Koncepcija elektronskih transakcija u oba slučaja donosi poboljšanje statusa kupca i prodavca. Prodavci robe i usluga daleko lakše kreiraju strategiju svog poslovanja koja se bazira na potrebi informaciono komunikacinoh servisa. Ovako koncipirana strategija neminovno će dovesti do smanjenja troškova, povećanja preglednosti na tržištu kao i povećanja konkurentnosti. Posmatrano iz ugla potrošača njima se pruža mogućnost da biraju kvalitetniju robu s hodno njihovim potrebama.

Sve ovo se posebno odrazilo na dinamični rast elektronske trgovine, koji se u najvećoj meri može objasniti bitnim smanjenjem troškova poslovanja, ali i pojednostavljenjem samog procesa ugovaranja. E-trgovina se razlikuje od tradicionalne trgovine samo na osnovu sredstava rada. Princip trgovine je ostao isti. Praktično e-trgovina predstavlja poslovnu komunikaciju i prenos dobara i usluga putem računarskih mreža, kao i prenos kapitala korišćenjem digitalnih komunikacija. Slično tradicionaloj trgovini i ovde se mogu izdvojiti određeni elementi elektronske trgovine:

- Predmet prodaje. U principu putem elektronske trgovine moguće je prodati dve stvari predmet i uslugu. Prema predmetu prodaje eTrgovina se ne razlikuje mnogo od tradicionalne. Jedina razlika je u načinu isporuke.
- Mesto prodaje. Kod elektronske trgovine mesto prodaje je web portal ili takozvani webshop. Webshop je jednako vidljiv i dostupan svima, vreme webshopa je neograničeno a i reakcije ka kupcima su brzi i istovetne. Praktično u okviru ovog elementa elektronske trgovine može se razlikovati više modela[107]. Prvi u nizu je **on-line prodavnica** koju formiraju trgovačke kuće u cilju lakseg i bržeg dolaska do

[107] Vujović, S., Elektronsko poslovanje i elektronska inteligencija, Beogradska poslovna škola, Beograd, 2005

klijentele. Za ovaj vid prodavnice potrebno je implementiranje i hostovanje web portala na čijim stranicama korisnici mogu naći katalog proizvoda sa potrebnim informacijama. Proces poručivanja se obavlja putem telefona ili elektronske pošte. Isporuka poručene robe se obavlja putem kurirskih službi na već ustaljen način. **Virtuelna prodavnica** je vrsta prodavnice koje su u suprotnosti sa tradicionalnim prodavnicama i postoju samo u cyber prostoru. Sastoje se od računara i softverskih programa stavljenih u funkciju web portala. **Mešovita realno / virtuelna prodavnica** je jedan od najčešćih modela elektronske trgovine. Praktično ovakvo mesto prodaje je organizovano u vidu fizički postojanih prodavnica koje pored tradicionalnog načina kupovine nude i mogućnost kupovine na daljinu putem elektronskih servisa u sklopu interneta. **Klupska trgovina** je model koji se zasniva na osnivanju potrošačkih klubova. Ovako osnovani klubovi predstavljaju svojevrsnu marketinšku aktivnost. Ovakvo prodajno mesto se bazira na razmeni informacija u okviru diskusione grupe na Internetu. Jedan od primera je i svetska knjižara Amazon. **Dispečerska prodavnica** je model u kome postoji jedna glavna prodavnica na čiju adresu stižu sve porudžbenice. Nakon pristizanja ona ih sortira i prosleđuje saradničkim prodavnicama koje se nalaze u zajedničkom sistemu sa dispečerskom prodavnicom. **Model elektronskog distributivnog centra** pradstavlja distribuciju nematerijalnih proizvoda. U grupu nematerijalih proizvoda koji se distribuiraju putem ovakvog centra mogu se uvrstiti računarski programi, muzika, elektronske novine, knjige, filmovi,... **Aukcijska kuća** organizovana je na principu sličnom klasičnoj berzi, sa razlikom u tome što se ovde trgovanje realizuje pomoću informaciono komunikacionuh tehnologija i Interneta.

- Marketing. Kao i kod tradicionalnog vida trgovine i kod elektronske trgovine je potrebno da korisnici u što većem broju saznaju za adresu web sajta na kome se nudi prodaja proizvoda ili uluga i da isti posete. Razlika je u tome sto ovde korisnici i potencijalni kupci ne odlaze fizički do predmetne prodavnice već posećuju konkretnu internet adresu.
- Prijem narudžbina. U sklopu elektronske trgovine elektronska prodavnica obezbeđuje automatizovan prijem porudžbina. Ovo praktično znači da se celokupan prijem porudžbina obavalja preko web portala što smanjuje troškove angažovanja radne snage. Korisnik portala praktično nakon razgledanja i odabira proizvoda koji želi da kupi odabira dodeljivanje proizvoda u virtualnu potrošačku korpu. Nad proizvodima u virtualnoj korpi korisnik ima apsolutnu kontrolu što praktično znači da tokom boravka na portalu može menjati njen sadržaj sve do momenta dok ne odabere konačnu kupovinu. Korisnik, sve ovo može činiti iz svog doma, i za celokupan proces izbora proizvoda može uzeti onoliko vremena koliko mu je potrebno bez požurivanja ili čekanja u redu.
- Način plaćanja. U elektronskoj trgovini u zavisnosti od mesta prodaje mogu se razlikovati različiti načini plaćanja. Jedan od najbržih i za korisnika najlakši način plaćanja je plaćanje putem kreditne kartice. U isto vreme ovakav način plaćanja mora biti ispraćen sigurnosnim mehanizmima, s obzirom da samo plaćanje zahteva unos broja kreditne kartice i njegovo slanje putem Interneta. Iz ovog razloga se veoma često plaćanje u elektronskoj trgovini prepušta nekoj od banaka koje pružaju usluge elektronskog transfera novca. U upotrebi je još jedan način plaćanja koji

kompbinuje elekronsku trgovinu i dostavljanje proizvoda putem različitih kurirskih službi. Ovo praktično znači da korisnik nakon poručivanja proizvoda isti dobija na kućnu adresu pri čemu plaćanje za isti vrši kuriru nakon dostave proizvoda.

- Isporuka. Transport proizvoda od prodavca do kupca u najvećem broju slučajeva organizovan je posredstvom kompanija koje su specijalizovane za posao transporta. U manjem broju slučajeva isporuku vrši i firma koja je obavila prodaju.
- Reklamacija / vraćanje proizvoda. Kao i tradicionalnoj trgovini i u domenu elektronske trgovine potrebno je obezbediti mehanizam reklamacije proizvoda ukoliko kupac nije zadovoljan proizvodom koji je kupio. U zavisnosti od proizvoda ili usluge koja je prodata može se obezbediti povraćaj novca u određenom opsegu od potpunog do delimičnog povraćaja. Delimičan povraćaj novca često je prisutan kod prodaje usluga.
- Garancija. Kao i u slučaju tradicionalne trgovine i kod elektronske trgovine teret garancije snosi proizvođač proizvoda. Uloga podavca je samo posrednička. U slučaju kada uređaj u garantnom roku pokaže neispravnost pokrivenu garancijom proizvođač je dužan da za konkretan proizvod obezbedi adekvatno servisiranje ili zamenu novim proizvodom.
- Tehnička podrška. U ovom delu elektronsko poslovanje donosi mogućnost značajne uštede kroz automatizaciju tehničke podrške. Postoji nekoliko nivoa kroz koje se pomoć korisnicima može obezbediti bez potrebe za telefonskim operaterima kao što je to bio slučaj kod tradicionalne trgovine robom i uslugama. Neki od nivoa su help dokumentacija, često postavljanja pitanja, kao i poluinteraktivni sistemi za pomoć. Kod poluinteraktivnih sistema web portal vodi korisnika kroz odeljke na web portalu počevši od opštih pa sve do onih specifičnih. Takođe je veoma često obezbeđena i podrška u vidu elektronske pošte. Kod ovakve podrške najčešće se definiše određeni rok u kome prodavac ili proizvođač moraju odgovoriti na postavljeno pitanje. Ovakav način tehničke podrške omogućava postavljanje velikog broja pitanja u vezi sa proizvodom kao i dobijanje odgovora na ista u bilo koje doba dana.

Elektronska trgovina predstavlja jedan od najsavremenijih načina vršenja poslovnih aktivnosti. Zastupljena je u svim sferama društvenog života, kako u privrednom sektoru tako i u fizičkom i državnom sektoru. Posebno je bitna činjenica da razvoj elektronske trgovine otvara nove mogućnosti za zapošljavanje. Zapošljavanje je posebno izraženo u malim i srednjim privrednim društvima. Na ovakav način se stimuliše ekonomski rast i ulaganje u inovacije, a doprinosi se i jačanju konkurentnosti industrije. Kako bi se sam proces trgovine u kome najmanje mora biti dva učesnika protekao na uređen način i kako bi se eventualni problemi otklonili morao je biti definisan set zakona koji regulišu ovu oblast. Na oblast elektronske trgovine primenjuju se odredbe sledećih zakona:

- Zakon o elektronskoj trgovini
- Zakon o elektronskom potpisu
- Zakon o elektronskom dokumentu
- Zakon o zaštiti potrošača
- Zakon o poštanskim uslugama
- Zakon o obligacionim odnosima
- Krivični zakonik

Međusobni odnos pomenutih zakona kao i njihova pozicija u sklopu elektronske trgovine dat je na slici 1. Sa konkretne slike se može uočiti zavisnost između pojedinih zakona i konkretnih faza kroz koje prolazi jedna instanca e-trgovine.

Kako bi se izjednačila elektronska trgovina sa tradicionalnom trgovinom jedan od zakona koji je donet je i Zakon o elektronskoj trgovini[108]. Cilj zakona jeste obezbeđivanje pravne sigurnosti za sve učesnike u elektronskoj trgovini, s obzirom da ova oblast dugo vremena nije bila definisana. Pravna sigurnost obezbeđuje se propisivanjem obaveza i odgovornosi svih učesnika u komercijalnim elektronskim aktivnostima. Takođe još jedna od prednosti donošenja Zakona o elektronskoj trgovini je i pravno regulisanje online trgovine, kao i plaćanje platnim karticama u okviru ovih servisa.



Slika 1. Grafički prikaz primene zakano u okviru elektronske trgovine

Svako pravno lice koje želi da uvede proces elektronske prodaje putem servisa elekronske trgovine prethodno se mora registrovati. U postupku elektronske trgovine možemo razlikovati pružaoca usluga i korisnika usluga. Pružaoc usluga dužan je da korisniku usluga obezbedi sve podatke i obaveštenja koji su od značaja i koji se

[108] Zakon o elektronskoj trgovini, Službeni glasnik RS, Opus citatum

primenjuju prilikom samog zaključenja ugovora. Svi podaci moraju biti obezbeđeni pre zaključenja ugovora. Takođe dužan je da obezbedi podatke o ugovornim odredbama, opštim uslovima poslovanja, kao i kodeksima ponašanja u skladu sa kojima se pružaoc usluga postupa. Sve informacije moraju biti dostupne u elektronskom obliku i moraju tako da ih korisnik usluga može veoma lako pregledati. Nadzor nad primenom ovog zakona vrše dva ministarstva. Tržišni inspektori vrše inspekcijski nadzor ispred ministarstva trgovine i usluga, dok inspektorat za poštanske usluge i inspektorat za poslove telekomunikacija i informatike vrše inspekcijski nadzor ispred ministarstva za telekomunikacije i informaciono društvo. Radi vršenja nadzora, pružaoci usluga dužni su da ovlašćenim licima omoguće pristup računarskoj opremi i uređajima. Takođe pružaoci usluga su u obavezi da bez odlaganja pokažu ili dostave potrebne podatke i dokumentaciju u vezi sa predmetom nadzora[109].

Zakon o elektronskoj trgovini koncipiran je tako da omogući sledeća poboljšanja:

- brže pronalaženje najpovoljnijih uslova kupovine određenog proizvoda ili usluge, bez obzira na destinaciju na kojoj se ona nalazi.
- pristupačnije poslovne transakcije u domenu marketinga, dizajna i proizvodnje
- bolja zaštita potrošača i provajdera

Kako u elektronskoj komunikaciji nema kontakta između učesnika došlo je do problema definisanja adekvatnog načina zaključenja ugovora u poslovnom svetu. Ovaj način morao je biti definisan zakonskim odredbama. U ovom smislu najpre se svaki kupac mora izjasiti o tome da prihvata ponudu koju je dobio u elektronskom obliku. Sama pravna sigurnost obezbeđena je činjenicom da je ovakav ugovor nemoguće osporiti samo zato što je sklopljen u elektronskom obliku. Takođe nad elektronskim ugovorima mogu se primeniti sva obligaciona prava. Niži nivo pravne sigurnosti omogućava lakše i brže pronalaženje ponuđača za konkretan proivd, kao i pristupačnije obavljanje poslovne transakcije.

Uticaj donošenja Zakona o elektronskom potpisu i zakona o elektronskom dokumentu na regulasanje oblasti elektronske trgovine ogleda se u regulisanju odnosa dveju ugovornih strana. Ovaj set zakona omogućava sklapanje već pomenutih e-ugovora kao i njihovo elektronsko potpisivanje. Ugovori se sklapaju kako bi regulisali prodaju robe ili usluga. Ovako zaključeni ugovori svojim odredbama regulišu prava i obaveze svake od stranaka u ugovoru kao način rešavanja eleventualnog spora. Ugovorom može biti definisano koji sud je nadležan za rešavanje nastalog spora. Kako strane potpisnice mogu biti iz različitih zemalja čak i sa različitih kontitenata potrebno je ugovorom definisati u kojoj od zemalja bi se eventualni spor mogao voditi.

U cilju zaštite položaja potrošača Zakonom o zaštiti potrošača[110] uređuju se prava i obaveze potrošača kao i instrumenti i načini zaštite prava potrošača. Primenom ovog zakona cilj je da se potrošači adekvatnije informišu o svim pravima koje imaju u postupku kupovine proizvoda. Takođe odredbama zakona definasana su i prava i obaveze udruženja i saveza potrošača koja su osnovana sa ciljem povećanja zaštite

[109] Ibidem, član 12 i član 22.
[110] Zakon o zaštiti potrošača, Službeni glasnik RS, br. 62/2014, 6/2016-dr. zakon

potrošača. Povećanje zaštite potrošaća ogleda se kako u njihovom informisanju tako i u vansudskom i sudskom rešavanju nastalih potrošačkih sporova, kao i u rešavanju drugih pitanja koja mogu doprineti adekvatnijoj zaštiti potrošača. Zaštita potrošača definisana odredbama ovog zakona u Republici Srbiji sprovodi se od septembra 2014. godine. Odredbe ovog zakona premenjene na e-trgovinu odnose se na zaštitu potrošača u ostvarivanju prava iz elektronskih ugovora sklopljenih na način definisan zakonom o elektonskom dokumentu. Prema ovom zakonu svaka od strana potpisnica ugovora ima pravo na jednostuki raskid ugovora. Ovako kreiran Zakon o zaštiti potrošača usaglašen je sa zakonodavstvom EU i prati dve direktive:

- Direktivu 97/7/EZ prodaja na daljinu[111]
- Direktivu 2000/31/EZ o elektronskoj trgovini[112]

Prema odredbama samog zakona dužnost trgovca je da pre zaključenja ugovora o prodaji robe ili pružanju usluga, potrošača na obavesti o[113]:

- Osnovnim obeležjima robe,
- poslovnom imenu, matičnom broju, adresi sedišta i broju telefona,
- prodajnoj ceni ili načinu na koji će se prodajna cena obračunati ako se zbog prirode robe ili usluge prodajna cena ne može utvrditi unapred, kao i o svim dodatnim poštanskim troškovima i troškovima transporta i isporuke i mogućnosti da se ti troškovi mogu staviti potrošaču na teret,
- načinu plaćanja, načinu i roku isporuke, načinu izvršenja drugih ugovornih obaveza,
- postojanju zakonske odgovornosti zbog nesaobraznosti robe ili usluge ugovoru,
- načinu izjavljivanja reklamacije trgovcu, a naročito o mestu prijema i načinu postupanja trgovca po njima, kao i uslovima koji se odnose na ostvarivanje prava potrošača po osnovu saobraznosti,
- prilikom ponude i prodaje tehničke robe o dostupnosti rezervnih delova, priključnih aparata i sličnih delova, tehničkog servisa, odnosno održavanja i opravke za vreme i posle prestanka perioda u kojem odgovara za nesaobraznost ugovoru, odnosno posle prestanka proizvodnje i uvoza robe,
- uslovima za raskidanje ugovora, ako je zaključen na neodređeno vreme ili ako se produžava automatski.

Ako trgovac i potrošač zaključe ugovor, svi pomenuti podaci o kojima je prodavac trebao da obavesti kupca postaju sastavni deo ugovora. Sav teret dokazivanja da je obaveza obaveštenja potrošača izvršena na adekvatan način snosi trgovac. Ukoliko trgovac ne postupi u skladu sa obavezom obaveštavanja potrošač ima pravo da traži poništenje ugovora. Poništenje ugovora može se tražiti bez obzira da li je trgovac prilikom neadekvatnog obaveštavanja imao nameru da potrošača navedene na

[111] Directive 97/7/EZ, dostupno na: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31997L0007 datum pristupa: 15.01.2018.
[112] Direktiva 2000/31/EZ, dostupno na: http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:32000L0031, datum pristupa: 15.01.2018.
[113] Ibidem, član 13.

prihvatanje uslova ugovora i njegovo zaključenje. Kupac ima pravo na poništenje ugovora tokom godinu dana od njegovog zaključenja. Izdavanje računa od strane trgovca za kupljenu robu je obavezno. Takođe izdavanje i slanje računa potrošaču, kao i slanje opomena usled naplate dospelih potraživanja mora biti besplatno. Prodavac je dužan da isporuči robu koja odgovara robi definisanoj u ugovoru. Zakonom je definisano da je roba saobrazna ugovoru[114]:

- ako odgovara opisu koji je dao prodavac i ako ima svojstva robe koju je prodavac pokazao potrošaču kao uzorak ili model,
- ako ima svojstva potrebna za naročitu upotrebu za koju je potrošač nabavlja, a koja je bila poznata prodavcu ili mu je morala biti poznata u vreme zaključenja ugovora,
- ako ima svojstva potrebna za redovnu upotrebu robe iste vrste,
- ako po kvalitetu i funkcionisanju odgovara onome što je uobičajeno kod robe iste vrste i što potrošač može osnovano da očekuje s obzirom na prirodu robe i javna obećanja o posebnim svojstvima robe data od strane prodavca, proizvođača ili njihovih predstavnika, naročito ako je obećanje učinjeno putem oglasa ili na ambalaži robe.

Pored svih navedenih obaveza prodavca, još jedna od obaveza je i izdavanje garancije za robu koja podleže izdavanju garancije[115]. Garancjom davalac iste potvrđuje da je prodata roba ili usluga u skladu sa ugovorom dogovorenom. Sama garancija može se dati u papirnom ili elektronskom obliku i sadrži sve podatke o robi navedene na jasan i razumljiv način. Garancija ne isključuje niti utiče na prava potrošača u vezi sa saobraznošću robe ugovoru. Obaveze potrošača u slučaju odustanka od ugovora takođe su uređene ovim zakonom[116]. Potrošač ima pravo da nakon zaključenja elektronskog ili ugovora na daljinu od istog odustane u roku od 14 dana. Pri ovakvom odustajanju potrošač ne mora da navede ni jedan razlog zbog koga odustaje od ugovora. Takođe u ovom slučaju potrošač ne snosi nikakve dodatne troškove osim troškova povraćaja. Na ovakav način potrošač snosi samo troškove poštarine prilikom vraćanja robe i odgovoran je samo za oštećenja koja su nastala kao posledica neadekvatnog rukovanja robom. Ukoliko potrošač pokrene pitanje odustajanja od ugovora nakon 14 dana od dana kupovine, dužan je da snosi troškove u iznosu koji je srazmeran pruženim uslugama do momenta obaveštavanja trgovca o pokretanju postupka za raskig ugovora. Iznos koji je potrebno platiti obračunava se na osnovu prodajne cene. Takođe ovim zakonom precizno su regulisane situacije u kojima potrošač nema prava na odustanak od ugovora[117]. Primera radi ukoliko se radi o pružanju usluge potrošač nema pravo da odustane od ugovora u slučaju kada je usluga u potpunosti pružena i u slučaju da postoji saglasnost potrošača da je upoznat sa odredbom ugovora po kojoj gubi pravo na odustanak od ugovora kada je isti izvršen u celosti.

[114] Ibidem, član 50.
[115] Ibidem, član 54.
[116] Ibidem, član 35.
[117] Ibidem, član 37.

Kako veliki broj potrošača nije dovoljno informisan o svojim pravima prilikom e-trovine potrebno je da svaka od zemlja preuzme ulogu edukatora i na najadekvatniji način obavesti građanstvo o pravima i obavezama koje su definisane zakonom. U Republici Srbiji postoji Odeljenje za zaštitu potrošača pri Ministarstvu Trgovine, koje je izdalo brošure o e-trgovini i e-kupovini zasnovane na Zakonu o zaštiti potrošača koje bi trebalo da se koriste kao adekvatan način za informisanje o procesu obavljanja sigurne kupovine. Ove brosušure lako su dostupne u elektronskom obliku i nude dovoljno informacija za svakog početnika u svetu e-trgovine.

Distribucija robe kako u tradicionalnoj trgovini, a posebno u trgovini putem elektronskih servisa obavlja se kao što je već i ranije bilo reči posredstvom poštanskih kompanija. Način adekvatnog obaljanja usluga, ponašanja zaposlenih, odnosa prema klijentima kao i prava i obaveza kako klijenta tako i kompanije u Republici Srbiji definisan je Zakonom o poštanskim usluga[118]. Ovim zakonom definisano je koji predmeti i roba se smeju i na koji način slati u vidu pošiljki kao i šta ne sme biti sadržina pošiljke. Takođe je definisano kako se vrši uručenje pošiljke i u kojim slučajevima primalac ima pravo da vrati predmetnu pošiljku[119]. Poštanska pošiljka za koju se utvrdi da ne može da se uruči ni primaocu, ni pošiljaocu smatra se neisporučivom pošiljkom. Svaka kompanija koja koja se bavi isporukom pošiljki od pošiljaoca do primaoca mora voditi računa da sadržaj pošiljke dostavi bez ikakvih oštećenja. Uslovi reklamacije i nadoknade štete pored definisanih okvira u okviru pomenutog zakona definišu se i posebnim pravilnikom svake od kompanija. Kompanije u posebnim uslovima imaju pravo provere sadržaja pošiljke u trenutku njenog preuzimanja, a pre početka transporta u prisustvu pošiljaoca. Ukoliko sadržaj paketa ne odgovara navedenom pošiljaoca snosi odgovornost. U praksi ovakvi slučajevi su retkost, što može uzrokovati probleme kako pošiljaocu i primaoca tako i poštanskoj kompaniji. Primera radi pošiljalac radi izbegavanja plaćanja skuplje nadoknade za prenos pošiljke može da ne navede da je u paketu lomljiv predmet. Neadekvanom zaštitom doći će do oštećenja istog za šta primalac može oktiviti kompniju. U ni jednom slučaju ovakvi sporovi ne idu na ugled samoj kompaniji iako odgovornost nije njena. Ukoliko je došlo do gubitka ili oštećenja sadržaja pošiljke poštanski operator dužan je da pošiljocu nadoknadi štetu. Takođe do nadoknade štete od strane poštanskog operatora može doći i ukoliko se rok za dostavu pošiljke bitno prekorači. Nadoknada troškova za prekoračenje roka za dostavu odnosi se na dostavu pošiljki u unutrašnjem saobraćaju[120].

Poslednji u nizu pomenutih zakona koji se primenjuju na regulisanje e-trgovine kako u samom procesu trgovine tako i nakon završene trgovine jeste Krivični zakonik[121]. Odredbe krivičnog zakonika stupaju na snagu kada tokom procesa e-trgovine dođe do različitih problema u ovoj oblasti. Primera radi ukoliko prodavac putem servisa e-trgovine neovlašćeno vrši distribuciju oružja i municije, narkotika, pornografskog materijala itd. Takođe ukoliko se ovakvim vidom prodaje stiče

[118] Zakon o poštanskim uslugama, Službeni glasnik RS, br. 18/2005, 30/2010 i 62/2014.
[119] Ibidem, član 34 i član 35.
[120] Ibidem, član 46.
[121] Krivični zakonik, Opus citatum.

neovlašćena dobit ili neovlašćeno prikupljanje i zloupotreba ličnih podataka korisnika, podataka o brojevima kreditnih kartica kao i njihova prodaja na crnom tržištu svaki od pojedinaca može biti krivično procesuiran shodno odredbama ovog zakona. Primena ovog zakona uvodi se kao krajnja mera, što znači da dela za koja je izrečena nisu ni u kom slučaju za potcenjivanje. Odredbe ovog zakona vezane za trgovinu uopšte a samim tim i za e-trgovinu podeljene su na: nedozvoljenu trgovinu, trgovinu uticajem, trgovinu ljudima i trgovinu maloletnim licima radi usvojenja. Za svaku od kategorija definisana je adekvatna kaznena mera. Primera radi novčanom kaznom ili kaznom zatvora od dve godine kazniće se svako lice koje stavi u promet robu ili druge vrednosne predmete za koje nema ovlašćenje za trgovinu. Takođe istom kaznenom merom kazniće se lice koje se neovlašćeno bavi posredovanjem u trgovini ili zastupanjem drugih organizacija prilikom prometa robe ili usluga[122].

Barijere implementacije e-trgovine kod zemalja u razvoju

Primena elektronske trgovine u svakodnevnom životu i radu ljudi uslovljena je mnogim faktorima pa se samim tim stepen njene primene razlikuje od regiona do regiona. Posmatrajući zemlje u razvoju mogu se izdvojiti određene barijere primene različitih servisa elektronske trgovine:

- Infrastrukturne barijere
- Socio-kulturne barijere
- Socio-ekonomske barijere
- Zakonodavne (pravne) barijere

Naravno ne može se zaobići činjenica da pored navedenih barijera određene zemlje u razvoju imaju različite upravne sisteme, rasnu podeljenost kao i to da su pod uticajem sankcija što im dodatno otežava sami razvoj e-trgovine. Aspekt posmatranja razvoja e-trgovine iz ugla zemalja u razvoju posebno je značajan jer se u grupu ovih zemalja prema zvaničnoj listi međunarodnog instituta za statistiku (International Statistical Institute) za 2017. godinu ubrajaju Republika Srbija i zemlje okruženja[123].

Posmatrajući infrastrukturne barijere može se uočiti da u ovu grupu spada opremljenost stanovništva računarskom opremom, pristup internetu, limitiran protok, loša telekomunikaciona infrastruktura pa čak i adekvatna snabdevenost električnom energijom. Većina zemalja u razvoju nije spremna za aktivno uvođenje e-trgovine zbog nedostataka u mrežnoj infrastrukturi koja je preko potrebna kako bi se učesnici u trgovini međusobno povezali. Primera radi telekominikaciona infrastruktura nije na istom nivou razvoja u svim zemljama, što dovodi do toga da je Internet u većini ovih zemalja veoma spor i skup. Takođe visoka cena računarske opreme posmatra se kao još jedna od barijera većoj upotrebi računara. Bez računara sa koga bi korisnik pristupio

[122] Ibidem, član 236.

[123] International Statistical Institute, „Developing countries“, Available: https://www.isi-web.org/index.php/resources/developing-countries.

Internetu nema ni samog pristupa pa ni učestvovanje u elektronskoj trgovni nije moguće. Veća dostupnost računara kao i pristup kvalitetnoj Internet konekciji po pristupačnim cenama uticaće na povećanje broja korisnika informaciono komunikacionih servisa a samom tim i korisnika e-trgovine[124]. Na ovakav način e-trgovina će se razvijati prema specifičnim potrebama korisnika. Međutim čak i sa pristupom potrebnoj opremi potrebno je određeno vreme kako bi stanonvništvo steklo poverenje u integritet online transakcija i na taj način korisnici postali aktivniji u korišćenju ovih servisa.

Pored infrastrukturnih barijera kao što je već navedeno postoje i socio-kulturne barijere. U ove barijere spada nivo poverenja u institucije, tradicionalna kupovina kao vid socijalnog okupljanja, nemogućnost žive interakcije između kupca i prodavca kao i jezik. Po pitanju poverenja u institucije koje se bave e-trgovinom izdvaja se način poručivanja, plaćanje i na kraju možda i najvažniji faktor a to je da li ce poručena roba zaista i stići. Nivo poverenja u servise poručivanja, plaćanja distribucije proizvoda u mnogome zavisi od zakonodavnog sistema zemlje u razvoju. Kada je pravni i zakonodavni sistem slabo razvijen nesigurnost korisnika bila ona opravdana ili ne dovodi do narušavanja poslovnih transakcija. Većina korisnika zemalja u razvoju nerado nastavlja sa korišćenjem servisa za e-trgovinu ukoliko je potrebno da u okviru istog unese osetljive finansijske informacije. Skeptičnost po pitanju upotrebe kreditnih kartica i davanja ličnih podataka kompanijama koje se bave e-trgovinom i posluju na Web-u veoma je izražena kod stanovništva zemalja u razvoju. Navedena skeptičnost veoma je uočljiva i kod stanovništva Republike Srbije koje možda baš iz tih razloga idalje posluje pretežno na tradicionalni način. Takođe uočljiva je veća upotreba onis servisa e-trgovine koji nude mogućnost plaćanja po prijemu robe što kupcima daje određeni nivo sigurnosti. Za veliki broj stanovnika zemalja u razvoju lični kontakt sa prodavcem ili kupcem, razmena mišljenja i mogućnost pregleda robe pre kupovine je neprocenljiv. U tom smislu tradicionalna kupovina nosi jednu vrstu socijalizacije i upoznavanja. Prodavci ovakav način trgovine vide kao mogućnost pružanja veće količine informacija samom kupcu kao i građenje marketinskih sposobnosti u cilju adekvatnijeg pristupa svakom pojedincu i većih prodajnih mogućnosti. Kao što je već navedeno jezik može biti limitirajući faktor u razvoju e-trgovine. Sama zamisao ovakvog vida trgovine zasniva se na tome da učesnici u ovom procesu mogu biti sa udaljenih geografskih područja. Ovo praktično znači da će informacije o proizvodima ili uslugama biti na različitim jezicima. Stanovništvo zemalja u okruženju veoma često u visokom procentu vlada samo maternjim jezikom dok pristup Internetu i komunikacija sa prodavcima zahteva određeni nivo edukacije i poznavanje više od jednog jezika. Engleski kao takav je jedan široko korišćenih jezika u zapadnim zemljama odakle i kreće razvoj novih tehnologija. Engleski kao takav je dominantan jezik u informacionim tehnologijama, e-trgovini, i glavni je jezik korišćen na Web-u.

Socio-ekonomske barijere povezane su sa ekonomskim uslovima, edukacionim sistemom, sistemima za transfer novca i distribucionim sistemima za fizički transfer

[124] Japhet Lawrence, Usman Tar, „Barriers to ecommerce in developing countries“, Information, Society and Justice, Vol. 3, No. 1, pp. 23-25, 2010.

dobara. Nedostatak informaciono komunikacionih veština stanovništva zemalja u razvoju nastao kao posledica lošeg edukacionog sistema predstavlja barijeru bržem prihvatanju pogodnosti koje e-trgovina nudi. Koliko je ovo ozbiljan problem svegoči i činjenica da određeni broj zemalja u razvoju u kurikulumu obrazovnog procesa nema predmete povezane sa računarstvom i osposobljavanjem kadrova za korišćenje računara. Kako bi uspešno koristili i prihodovali putem ponuđenih servisa ljudi se najpre moraju edukovati. Iz ugla sistema za plaćanje e-trgovina zahteva uspostavljanje pouzdanih i sigurnih online infrastruktura u cilju sprečavanja prevara i ostalih ilegalnih aktivnosti. Efikasnost sistema za plaćanje kao i sugurnost korišćenja istog u mnogome mogu ubrzati ili usporiti razvoj e-trgovine. Korisnici kreditnih kartica zemanja u razvoju u slučaju problema nastalih upotrebom elektronskog plaćanja snose celokupne gubitke, što je još jedan od razloga zašto se korisnici ne odlučuju trgovinu gde im sigurnost nije zagarantovana. Pored individualnih transakcija, celokupna efikasnost i realizacija benefita koje donosi e-trgovina zavise od brzine autorizacije, brzine plaćanja i kreiranja naloga. Poslednja u nizu socio-ekonomskih barijera jeste logistika. Jako je bitno da celokupna organizacija distribucije bude lako dostupna i da ispunjava očekivanja potrošača. Dostava danas za sutra ili u toku jednog istog dana neke su od najbržih mogućnosti dostave kupljene robe. Sam proces dostave trebalo bi da bude organizovan od strane prodavca. Republika Srbija se može pohvaliti da raspolaže kompanijama za dostavu robe na kućnu adresu. Sve kompanije su u privatnom vlasništvu, dok je samo jedna u državnom vlasništvu. Međutim proces dostave robe u drugim zemljama u razvoju idalje predstavlja veliki probelem. Ovaj problem se manifestuje kako u vremenu potrebnom za dostavu paketa tako i dostavnim lokacijama. Primera radi vreme dostave paketa kurirskih službi zemlje za isto rastojanje je duže nego što je to slučaj u razvijenim zemljama. Isto tako nije redak slučaj da za neke oblasti ili određena mesta kurirske službe ne vrše dostavu, nego kupac mora otići do centrale i preuzeti svoju robu.

Većina zemalja u razvoju nema usvojene zakonske regulative koje bi regulisale upotrebu informaciono komunikacionih tehnologija i Interneta. Ne postoji mogućnost napredovanja u korišćenju Interneta i svih pogodnosti u vidu servisa koje on nudu ukoliko ovakve regulative nisu donesene i ukoliko se ne sprovodi njihova primena[125]. Nedostatak regulativa, zakonskih i pod zakonskih akata kao i pravila nastalih iz ovih zakona sa ciljem širenja upotrebe e-trgovine jedna je od glavnih prepreka usvajanju e-trgovine. Inicijative svake Vlade treba da budu usmerene ka približavanju značaja upotrebe e-trgovine i ostalih ICT servisa građanstvu. Ovakve inicijative obično su zasnovane na promocijama upotrebe ICT servisa, edukaciji, kao i na uspostavljanju adekvatnog okvira za e-trgovinu. Obavezivanje i učešće Vlade u pružanju Internet usluga i smanjenju dažbina dovestiće do smanjenja troškova koji će zauzvrat učiniti opremu pristupačnijom i podstaći povezivanje građanstva na Internet.

[125] Slobodan Obradović, Žaklina Spalević, Mirjana Knežević, Dejan Tešić, Vesna Marković, Aleksandar Žorić, „Causes Delays in the Development of Card Business“, TTEM - Technics Technologies Education Management, Vol. 7, No. 4, pp. 1796 - 1808, Dec, 2012

Zloupotrebe elektronske trgovine

Elektronska trgovina kako to obično biva sa svime što ima zdravu osnovu koja može unaprediti i olakšati svakodnevni život i rad ljudi stalno je na udaru zlonamernih korisnika. O učestalim zloupotrebama svedoče razni primeri kako u svetu tako i u Republici Srbiji i zemljama okruženja. Metode zloupotrebe e-trgovine su najrazličitije od kreiranja lažnih web portala sličnih pravim, preko prikupljanja podataka o korisnicima, krađe brojeva kreditnih kartica, pa sve do slanja robe neodgovarajućeg kvaliteta ili naplaćivanja iste bez slanja.

Jedan od primera prevare izvršene putem servisa za e-trgovinu jeste i presuda osnovnog suda u Sremskoj Mitrovici kojom je korisnik Limundo servisa osuđen jer je prisvojio više od 30.000 dinara prodajom knjiga koje nikada nisu stigle do svojih krajnjih kupaca. Pored toga on je osuđen i za nepoštovanje predviđenog roka za uplatu novčane kazne od 30.000 dinara, tako da je ukupna kazna iznosila šest meseci zatvora uslovno. Pored navedene novčane kazne sud je licu naložio da izvrši uplatu u iznosu od 40.000 dinara u humanitarne svrhe. Proces je pokrenut tako što je Limundo na osnovu informacija o načinjenonj prevari isplatio korisnicima odštetu u vrednosti za koju su bili prevareni, dok je proces podnošenja krivične prijave preuzeo na sebe[126].

Jedan od primera prevara sa internet kupovinom je i primer osobe iz Ivanjice koja je nakon kupovine posteljine putem pošte dobila potpuno drugačiju posteljinu od poručene. Još gore je ono što je usledilo, a to je da se sa kupljene posteljine skidala boja. Osoba se nakon prespavane noći probudila sa licem ofarbanim u crveno. Ono što je veoma česta praksa a što se desilo i u ovom slučaju jeste da prodavac nakon toga više nije odgovarao na poruke. Sličan slučaj desio se sa mladićem koji je kupio patike putem inteneta i to preko zvanične web stranice prodavca. U pakovanju koje je dobio jedna patika je bila crna broj 39, dok je druga bila bela broj 38. Kako se radilo o poznatom proizvođaču zamena je izvršena ali uz plaćanje poštarine oba puta od strane kupca[127].

Pored sve učestalijih prevara u kojima kupac umesto poručenog prozvoda dobija neodgovarajući ili oštećeni proizvod mnogo su ozbiljnije prevare koje za cilj imaju krađu ličnih podataka i podataka o bankovnim računima. Ovakve prevare za razliku od prevara sa neodgovarajućim proizvodima kao posledicu imaju znatno veće ekonomsko oštećenje korisnika. Jedan od ozbiljnih napada u dva navrata izveden je nad korisnicima kompanije Target. Prvi napad je izveden je nad POS terminalima, i u ovom napadu 40 miliona kreditnih i debitnih kartica je ugroženo od strane neautorizovane strane. Ovaj napad na ime troškova izdavanja novih kartica koštao je

[126] Marko Mudrinić, „Od prevare na Limundu do zatvorske kazne“, Netokracija, dostupno na: http://www.netokracija.rs/limundo-prevara-zatvor-124958, datum pregleda: 12.01.2018.

[127] B. Bojović, „Srpkinja doživela dramu. Poručila sam posteljinu preko interneta. Probudila sam se ofarbanog lica, ceo dan sam iskašljavala boju“, dostupno na: https://www.blic.rs/vesti/ekonomija/srpkinja-dozivela-dramu-porucila-sam-posteljinu-preko-interneta-probudila-sam-se/yn5dp77. datum pregleda: 22.01.2018.

banke ukupno 153 miliona dolara neočekivanih troškova. Nekoliko nedelja kasnije desio se drugi napad usmeren protiv korisnika web portala. Ovaj napad ugrozio je imena, adrese, email adrese i brojeve telefona dodatnih 70 miliona korisnika. U sumi lični podaci ili podaci o kreditnim i debitnim karticama ili oba za 110 miliona korisnika bili su ukradeni. Kako bi se zaštitila od sličnih napada u budućim godinama i kako bi povratila poverenje kupaca ova kompanija je uvela besplatno skeniranje i nadleganje kreditnih kartica[128].

Sličan napad sa istim malwerom izveden je nad sistemom kompanije Neiman Marcus. U ovom napadu neautorizovan pristup i prisvajanje podataka izvršen je nad 1,1 milionom kreditnih i debitnih kartica. Od ukupnog broja ukradenih kartica do momenta uočavanja prevare 2400 kartica je zloupotrebljeno. Ovakvi napadi sve su učestaliji o čemu svedoči i ponuda sve većeg proja projekata u kojima se traže hakeri koji bi kreirali malwere za napad na kreditne kartice[129]. Građani posebnu pažnju treba da obrate na probleme umnožavanja internet stranica, gde je moguće obavljati internet transakcije i gde korisnici ostavljaju lične podatke. Jedna od preventivnih mera jeste otvaranje posebnog računa, na koji će se uplaćivati male sume novca, koje su dovoljne za plaćanje pojedinačnih stvari, tako da u slučaju ako se desi prevara putem internet kupovine, kupac neće biti oštećen za celi iznos svog glavnog računa.

Da zloupotrebe servisa e-trgovine nisu odlika samo pojedinaca kao i da velikoj meri ekonomski sistem država može biti na udaru ovakivih prevara svedoči i tužba Francuskog ministarstva upućena protiv poslovanja Amazona[130]. Francusko ministarstvo finansija saopštilo je da je pokrenulo sudski postupak protiv Amazon zbog zloupotrebe svog dominantnog položaja na tržištu, treće strane platforme prodavaca maloprodajnih kompanija. Ministarstvo je naglasilo da postoji "značajna neravnoteža" u poslovnim odnosima između Amazona i prodavaca koji prodaju proizvode na svojoj platformi, i zatražilo novčanu kaznu od Amazon od oko 10 miliona evra. Slučaj je baziran na dvogodišnjoj istrazi platformi proizvođača treće strane uključujući i Amazon. Ustanovljeno je da postoji značajan debalans u klauzulama kojima Amazon pod pritiskom tera kompanije koje prodaju na svom tržištu. Ovaj prekršaj predstavlja grupo kršenje poslovnog prava. Istražitelji su pronaši nekoliko klauzula u ugovorima sa prodavcima na platformi Amazona na francuskom tržištu za koje se smatra da su nezakonite. Ova platforma ima oko 3.6 miliona posetioca dnevno. Amazon je iskoristio svoj dominantan položaj na tržištu u cilju modifikacije ugovora u datom trenutku, tražeći kraće rokove isporuke ili blokirajući isporuke za vreme čekanja na dodatne korporativne informacije od proizvođača. Pored ovoga na prostoru Italije vršeno je istraživanje pod sumnjom da je Amazon izvršio utaju poreza od prodaje knjiga. Slučaj se završio plaćanjem kazne od 100 miliona eura. Najnovija inicijativa Luksemburga po

[128] Janna Leyde, „The Guide to E-Commerce Fraud“, 2Checkout.com, 2014.

[129] Elizabeth Harris, Nicole Perlroth, Nathaniel Propper, „Neiman Marcus Data Breach Worse Than First Said“, The New York Times, Available: https://www.nytimes.com/2014/01/24/business/neiman-marcus-breach-affected-1-1-million-cards.html?_r=0, date: 22.01.2018.

[130] Daily Sabah Tech, „France sues e-commerce giant Amazon for abusing marketplace rules“, Available on: https://www.dailysabah.com/technology/2017/12/18/france-sues-e-commerce-giant-amazon-for-abusing-marketplace-rules, date: 22.01.2018.

pitanju utaje poreza može koštati Amazon dodatnih 250 miliona eura. Da slučaj Amazona nije izvojeni slučaj utaje poreza govori i podatak da je procenjeno da godišnje samo Evropska Unija izgubi oko 5 biliona eura na osnovu prevara sa utajom poreza u okviru prodaje na daljinu i elektronske trgovine[131].

3.5 Elektronsko bankarstvo

Pojam elektronskog bankarstva predstavlja upotrebu novih tehnoloških rešenja, kako bi se omogućilo da korisnici nezavisno od mesta i vremena obavljaju novčane transakcije korišćenjem računarskih mreža. Na ovakav način je značajno olakšan transfer novčanih sredstava. Elektronsko bankarstvo može se realizovati na dva osnovna načina. Prvi način jeste mogućnost da banka koja poseduje fizičke filijale i nudi tradicionalne bankarske usluge otvori web portal na kome će svojim korisnicima ponuditi i usluge elektronskog bankarstva. Na ovakav način korisnicima se nude dodatne povoljnosti bez bilo kakve naknade. Cilj ovakvog vida poslovanja jeste da se usluge banke približe korisnicima kao i da se korisnici i osoblje banke poštede velikih gužvi i čekanja na šalterima banaka. Nasuprot ovakvoj organizaciji banaka koje nude kako tradicionalne usluge svojim klijentim tako i usluge elektronskog bankarstva, postoji i drugi način organizacije. Drugi način podrazumeva pružanje bankarskih usluga samo putem elektronskih uređaja i računarskih mreža[132]. Ovo znači da banke nemaju fizičke filijale, već se sve usluge pružaju virtualno. Ovakav vid poslovanja nudi korisnicima znatno jeftinije usluge, uz naplatu manjih provizija za obavljene usluge. Problem koji se ovde može javiti jeste kako obezbediti kvalitetnu uslugu klijentima bez fizičkog prisustva. Probleme ovakvog tipa virtualne banke reševaju tako što stupaju u saradnju sa bankama koje zaista fizički postoje. Na ovaj način svojim korisnicima nude mogućnost da u filijalama i na bankomatima banaka saradnica fizički preuzmu svoj novac. Glavni preduslov primene elektronskog bankarstva jeste računarski sistem. Ovo pre svega uključuje pristup Internetu, web servere, menadžment upravljanja bazama podataka, kao i web aplikacije koje generišu dinamičke HTML web strane. Svaki od delova koji čine jedan ovakav sistem mora ispuniti određene kriterijume kako u pogledu performansi, tako i u pogledu zadovoljena sigurnosnih standarda. Sigurnost podataka i privatnost korisnika sistema mora biti na prvom mestu. Na sigurnosnim mehanizmima radi se svakoga dana i posvećuje mu se sve veća pažnja.

U uslovima vrlo jake konkurencije pod čijim se uticajem gubi razlika između usluga koje nude banke, brokerske firme, osiguravajuća društva i investicione banake ovakve organizacije zlažu velike napore kako bi zadržale postojeće i primamile nove

[131] European Council, „VAT on electronic commerce: New rules adopted“, Available on: http://www.consilium.europa.eu/en/press/press-releases/2017/12/05/vat-on-electronic-commerce-new-rules-adopted/, date: 20.01.2018.

[132] J. Wenninger, “ The Emerging Role of Banks in E-Commerce”, Federal Reserve Bank of New York Current Issues in Economics and Finance, vol. 6, no. 3, 2000, 1–6

korisnike. U culju sagledavanja primene elektronskog bankarstva, potrebno je naglasiti da elektronsko bankarstvo ne mora uvek jednobrazno da znači Internet bankarstvo. Primene elektronskog bankarstva mogu se videti od upotrebe bankomata, kućnog bankarstva, web tv bankarstva, mobilnog bankarstva, SMS bankarstva, pa sve do Internet bankarstva. Osnovna razlika među navedenim primerima jeste u načinu realizacije usluga, broju učesnika u komunikaciji, kao i u tome da li banka direktno komunicira sa klijentom ili ne. Primera radi kućno bankarstvo predstavlja svaki vid komunikacije ostvarene između banke i klijenta, pri čemu se klijent u trenutku komunikacije nalazi u svom domu. Komunikacija se obavlja putem telekomunikacionih servisa. Kako bi se obezbedila mogućnost iskorišćenja govorne tehnologije i kovertovanje numeričkih podataka u glasovni signal potrebno je telefonske uređaje povezati sa dodatnim hardverskim dodatkom. Zadatak ovog hardverskog dodatka je upravo pomenuta konverzija numeričkih podataka.

Kod Web Tv bankarstva vrši se povezivanje televizije i interneta u jednu celinu. Ovakav vid bankarstva namenjen je ljudima koji nemaju pristup računaru, a u isto vreme imaju potrebu da koriste internet servise. U ovom slučaju vrši se povezivanje tv uređaja sa telefonskom infrastrukturom [133]. Na taj način se tv prijemnik pomoću daljinskog koristi za pokretanje i upravljanje internet servisima. Na tv prijemnik mogu se povezati kao dodatni uređaji tastatura i štampač. Ovakav oblik elektronskog bankarstva omogućava obavljanje kupovine od kuće, plaćanje računa, kao i vršenje bankarskih transakcija. Kako bi se obezbedila sigurnost ovakvog vida elektronskog bankarstva pored tv prijemnika još jedan od osnovnih uređaja jeste i čitač smart katrica.

Internet bankarstvo predstavlja plasiranje informacija iz domena bankarskih usluga kao i realizaciju novčanih transakcija upotrebom Interneta i informaciono komunikacionih usluga. Samim tim koncepcija internet bankarstva zasnovana je na upotrebi računarskih mreža, interneta i servisa koje nudi World Wide Web. Putem ovih servisa korisniku se nudi pristup svim uslugama putem web pretraživača. Iz svih navedenih razloga kao i zbog promene u konkurentskoh strukturi online bankarsvo je postalo proizvod za masovnu upotrebu. Uvođenjem internet bankarstva banke svojim klijentima nude mogućnost obavljanja većine poslova bez odlaska u banku. Takođe pristup servisima internet bankarstva nije uslovljen dodatnim harverskim resursima što znači da korinik može da pristupi internet bankarstvu sa bilo kog računara. Svi podaci o logovanju korisnika, njegovim zahtevima i transakcijama koje je obavio čuva sama banka tako da o tome korisnik ne mora da vodi računa. Tačnije korisnik ne vodi računa o tome da li će zapisi o transakcijama ili drugi tragovi istih ostati na računaru sa koga je pristupano. Na ovakav način obezbeđena je veća sigurnost klijentskih podataka s obzirom da banka vodi računa o svim podacima.

U internet bankarstvu sve transakcije se obavljaju on-line. Ovo praktično znači da je najvažniji tehnički uslov internet bankarstva sigurna internet konekcija. U zavisnosti od implemenitranog servisa klijentima je omogućen pristup na više načina:

[133] O. Šušak, „Elektronsko bankarstvo i elektronski novac", Univerzitet Singidunum, Beograd, 2010, pp. 31-100.

- putem korisničkog imena i lozinke,
- broja računa i id-a,
- putem broja računa i smart kartice.

Može se reći da pristup putem smart kartice pruža najviši nivo zaštite. Međutim i pored većeg nivoa zaštite ovakav način pristupa nije previše popularan. Možda najkorišćeniji način pristupa online servisima internet bankarstva jeste pristup putem korisničkog imena i lozinke. Ovakvim načinom pristupa korisnik nije uslovljen kupovinom dodatnog hardvera u vidu čitača smart kartice i korišćenjem istog na svakom računaru sa kog želi da ostvari pristup.

Kao i u tradicionalnom načinu pružanja bankarskih usluga i kod Internet bankarstva moraju da postoje sredstva kojima će se vršiti plaćanje. Jedan od vidova ovakvog načina plaćanja jeste elektronski novac. Elektronski novac predstavlja informaciju o monetarnoj vrednosti. Ova informacija se prenosi kroz računrske mreže koristeći kanale plaćanja različite od onih koje tradicionalno bankarstvo poznaje. Elektronski čekovi su drugi način plaćanja u elektronskom i Internet bankarstvu. Kod ovog načina plaćanja korisnik putem računara formira ček koji će kasnije koristiti u plaćanjima. Kako bi se osigurao ovakav ček korisnik ga mora digitalno potpisati, dodati digitalni sertifikat banke i spakovati u digitalnu kovertu. Treći način plaćanja koji se javlja u Internet bankarstvu jesu kreditne kartice. Kod kreditnih kartica podaci sa kartica se razmenjuju putem Interneta. Ovi podaci se razmenjuju bez šifriranja što uzrokuje da tajnost podataka i identitet pravog vlasnika u nekom trenutku mogu biti ugroženi. Upravo iz ovih razloga drugi vid plaćanja pomoću kartica jesu šifrirane kartice. Kod ovog načina plaćanja poruka u kojoj se šalju podaci o kreditnoj kartici se pre slanja enkriptuje. Druga strana prlikom primanja enkriptovane poruke proverava identitet vlasnika kreditne kartice. Provera ispravnosti podataka o kartici i digitalnom potpisu vrši banka koja ispravnost podataka potvrđuje potvrdom ispravnosti koju šalje.

Kako internet bankarstvo nudi mogućnost da korisnik pristupa svom nalogu i vrši transakcije sa bilo kog mesta potrebno je obezbediti visok nivo sigurnosti. Sigurnost ovakvih sistema trebalo bi da se zasniva na pravilno kreiranoj autentifikaciji korisnika na samom početku korišćenja sistema. U ovakvim slučajevima preporuka autora jeste da se koriste autentifikacioni tokeni. Autentifikacioni tokeni su prenosivi uređaji koji ne zahtevaju instalaciju i korišćenje dodatnog softvera i hardvera. Na ovakav način ostvarena je mobilnost ovakvih uređaja kao i njihovo korišćenje u različitim vidovima komunikacije. Sigurnost elektronskih bankarskih sistema trebala bi da bude obezbeđena na više nivoa.

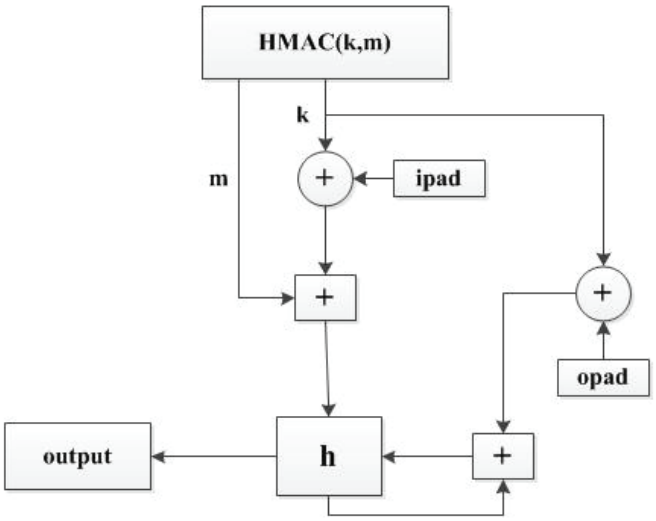
Kao jedan od nivoa u nastavku su prikazani sigurnosni mehanizmi na nivou TCP/IP protokol steka, tačnije Secure Sockets Layer (SSL) protokol. Generalno ovaj protokol je dizajniran za potrebe industrije i ima unapred zadatu namenu[134]. Ovaj protokol je dizajniran tako da zapravo predstavlja dva nivoa protokola. Osnovna uloga SSL protokola je da obezbedi sigurnosne servise protokolima višeg nivoa koji se nalaze

[134] McNub, C., „Network Security Assessemen“, O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472, 2nd edition, 2007, pp. 102-196

iznad njega. U TCP/IP strukturi protokol steka SSL protokol se nalazi između protokola višeg nivo i TCP protokola[135]. Handshake je protokol koji se nalazi u sklopu SSL protokola i može se slobodno reći da je ovo najkompleksnji deo SSL protokola. Handshake je našao primenu u domenu računarske komunikacije koji je uvek najranjiviji, a to je komunikacija izmedju servera i klijenta. Ovaj deo SSL protokola obezbeđuje svu potrebnu enkripciju kao putem MAC algoritama. Pored toga obezbeđuje kriptografske ključeve koji su porebni kako bi se zaštitili podaci koji se šalju putem SSL zapisa. Upravo u ovom delu je potrebno obratiti veliku pažnju i odabrati što bolji kriptografski algoritam u sklopu MAC algoritma. Poređenja radi u nastavku je data komparacija nekih od algoritama koji se mogu koristiti za ovu namenu. Zapravo kriptografski algoritmi se koriste u domenu funkcije za ekripciju u okviru MAC algoritma koji se primenjuje nad kompresovanim podacima. Heš ključ kod za autentifikaciju poruke ili takozvani HMAC predstavlja jedan od načina kodovanja koji se mogu koristiti za proces u kome se ustanovljava da li je dobijena poruka autentična. On se dobija korišćenjem kriptogrfskih heš funkcija u kombinaciji sa tajnim ključem. Ovime se može istovremeno potvrditi integritet podataka i autentičnost poruke. U tu svrhu može se koristiti bilo koja kriptografska heš funkcija kao što je na primer Tirger Hash, MD5 ili SHA-1. Ove haš funkcije se koriste u proračunu HMAC-a. Kriptografska snaga HMAC-a zavisi od kriptografske snage heš funkcije koje čine njegovu osnovu, od veličine ključa kao i od dužine heš izlaza u bitovima. Na slici 2. dat je šematski prikaz HMAC-a. Simbolom *h* na slici označena je korišćena kriptografska funkcija. Simbol *k* je tajni ključ dopunjen nulama do veličine bloka heš funkcije. Simbolom *m* označena je poruka koja se autentifikuje, + označava konkatenaciju, dok $\oplus$ označava XOR operaciju. *Opad* i *ipad* predstavljaju spoljašnje i unutrašnje dopunjavanje, tačnije predstavljaju dve heksadecimalne konstante dužine jednog bloka.

Dve kriptografske heš funkcije koje se mogu primeniti u bloku koji je označen sa *h* jesu MD5 i SHA1. MD5 obrađuje poruke koje imaju promenljivu dužinu i kreira izlaz fiksne dužine od 128 bitova. Ovaj algoritam radi sa 128-bitnim vektorom stanja, podeljenim na četiri 32-bitne reči. Ove reči su inicijalizovane sa određenim fiksnim konstantama. Glavni algoritam radi pojedinačno sa svakom 512-bitnom blok porukom. U algoritmu svaki blok menja stanje. Obrada bloka poruke sastoji se od četiri slične runde. Svaka runda se sastoji od šesnaest međusobno sličnih operacija zasnovanih na nelinearnoj funkciji, modularnom sabiranju i levoj rotaciji. Postoje četiri moguće nelinearne funkcije i u svakom krugu se koristi različita funkcija. SHA-1 algoritam u odnosu na MD5 kreira izlaz iz poruke koji je veličine 160 bitova, sa maksimalnom dužinom poruke od 2^{64}-1 bitova. Izlaz se bazira na principima koji se primenjuju i u projektovanju kod MD5. Ipak, iako na izgled nema velikih razlika između ova dva algoritma one ipak postoje.

[135] M. Veinović, A. Jevremović, „Računarske mreže", Fakultet za informatiku i računarsvo, Univerzitet Singidunum, Beograd, 2011



Slika 2. Blok šema HMAC algoritma

Pored veličine izlaza broj rundi u SHA-1 je veći nego kod MD5 i iznosi 80, nasuprot broju rundi kod MD5 koji iznosi 64. Svaka od rundi ima jedan bit rotacije više, što dovodi do toga da se mešanje kao operacija razlikuje[136]. Izračunavanje bita rotacije je kod SHA-1 isto u svim rundama, dok se kod MD5 razlikuje od runde do runde i za svaku rundu se iznova računa. Ovaj dodatni bit čini da SHA-1 bude znatno otporniji na kolizione napade. Kolizija se u ovom algoritmu pojavljuje samo teoretski, nikada praktično nije dostignuta, što je njegova velika prednost. Funkcije kombinovanja bitova i zaokruživanja kod ova dva algoritma se takođe razlikuju. Ako se pogleda broj elementarnih operacija za svaki ulazni bajt (što se manje ili više slika na veličinu koda ili brzinu, posebno na GPU), može se primetiti da je SHA-1 oko 30% zahtevniji algoritam od MD5, dok je novija verzija ovog algoritma pod nazivom SHA-356 približno duplo zahtevniji od SHA-1.

RSA algoritam obezbeđuje enkripciju javnim ključem kako bi se osigurala poverljivost poruka. Tačnije, ovaj sistem koristi jedinstveni par javnog i privatnog ključa kako bi kreirao digitalni potpis. Glavni problemi u domenu transakcije poruka uključuju ne samo privatnost podataka koji se prenose, već i autentičnost i pošaljioca i primaoca. Primalac može iskoristiti originalni hash algoritam za kreiranje i upoređivanje novog sažetka poruke koji se dobija dekripcijom dobivene poruke sa originalnim sažetkom poruke. Ako su jednaki, poruka sigurno nije izmenjena prilikom transporta. Iako enkripcija javnim ključem i digitalni potpis osiguravaju poverljivost i autentičnost poruke, postoji potencijalna opasnost da informacije koje pošaljiaoc daje nisu tačne. Na primer, pošaljioc može da enkriptuje broj bankovne kartice koji pripada nekom drugom, koristeći svoj privatni ključ. Da bi se osigurala validna autentifikacija,

[136] V. Vučković, P. Rajković, „Zaštita informacija“, Elektronski fakultet Niš, 2010.

postoji potreba za procesom sertifikacije. Treća strana, kojoj veruju i pošiljaoc i primalac izdaje par ključeva korisnicima koji obezbede dovoljno podataka za utvrđivanje identiteta. Jedna pretpostavka se bazira na poverenju primaoca da ključevi CA, koji se koriste u procesu sertifikacije, nisu kompromitovani. Pod pretpostavkom da SET utiče na stepen korišćenja RSA enkripcije za kućno bankarstvo i online servise za plaćanje, postavlja se pitanje da li SET treba da bude usvojen i za sve bankarske transakcije koje se ne vezuju za kreditne kartice. SET može da omogući plaćanja bez kartica, jer nije specifičan za transakcije sa njima, već podržava generičke transakcije, autentifikaciju, sertifikaciju, enkripciju i slično. Primena različitih enkripcionih sistema, različitih načina sigurne komunikacije i utvrđivanja identiteta sigurno će se razlikovati kod davaoca usluga i klijenata. Svi sigurnosti mehanizmi i mehanizmi enkripcije podataka se moraju idalje razvijati i usavršavati.

Sistemi elektronske trgovine, elektronskog poslovanja, elektronskog bankarstva pa samim tim i Internet bankarstva moraju biti regulisani zakonskim odredbama kako bi izvršavali svoje delantnosti. U zavisnosti od regiona do regiona elektronsko bankarstvo je u većoj ili manjoj meri pokriveno odgovarajućim zakonskim regulativama. U zavisnosti od toga da li se radi o poslovnim ili privatnim korisnicima, odnosu banke prema klijentima ili odnosu klijenta prema banci, zakonske regulative se razlikuju od zemlje do zemlje[137]. Takođe, organizacija obavljanja medjunarodnog elektronskog bankarstva može biti veoma usporena pravnim barijerama.

Prema zakonu o platnim uslugama, elektronski novac kao što je već navedeno ranije označava elektronski snimljenu novčanu vrednost. Ova vrednost predstavlja novčano potraživanje koje je izdato nakon prijema novčanih sredstava kojima se izvršavaju transakcije. Imalac elektronskog novca može biti kako fizičko tako i pravno lice kome je ovakav novac izdat. Takođe imalac elektronskog novca može biti lice bilo fizičko ili pravno koje je podnelo zahtev izdavaocu novca radi izdavanja istog, ili lice koje ima neki vid novčanog potraživanja[138]. U skladu sa stavom 1 člana 111 Zakona o platnim uslugama elektronski novac može prihvatiti svako fizičko ili pravno lice koje ima zaključen ugovor sa izdavaocem elektronskog novca ili nekim od pružaoca platnih usluga. Takođe obezbeđena je mogućnost da izdavaoc elektronskog novca prihvati elektronski novac izdat od strane nekog drugog izdavaoca. Na ovakav način obezbeđena je saradnja između različitih izdavaoca elektronskog novca.

Tajnost i zaštita elektronskog novca propisana je članom 74 i 75 Zakona o platnim ulugama[139]. Pomenutim članom 74. definisana je tajnost podataka o platnim uslugama. Prema ovom članu tajnim se smatraju svi podaci korisnika platnih usluga kako oni o njegovoj ličnosti tako i o obavljenim transakcijama i promenama na računu do kojih je

---

[137] Žaklina Spalević, Mirjana Knežević, Željko Bjelajac, Foreign Investments in Banking Systems of Serbia and Western Balkan Countries, TTEM - Technics Technologies Education Management, Vol. 7, No. 2, pp. 747 - 757, Jun, 2012.

[138] Zakon o platnim uslugama, Službeni glasnik RS, br.139/2014, dostupno na: http://www.nbs.rs/export/sites/default/internet/latinica/20/zakoni/pp_platnim_uslugama_novo.pdf, datum pristupa 15.01.2018.

[139] Ibidem

pruzalac usluga došao tokom vremena pružanja usluga. Pristup podacima koji su predmet tajne može se obaviti isključivo pod uslovima definicanim u ovom članu zakona, nakon čega se obaveza čuvanja poslovne tajne nastavlja kao da pristupa nije ni bilo. Prema članu 75. ovog zakona pružaoci platnih usluga, učesnici u platnom sistemu i agent za poravnanje dužni su da postupaju u skladu s propisima kojima se uređuje zaštita podataka o ličnosti. Pružaocima usluga daje se mogućnost prikupljanja podataka isključivo radi sprečavanja ili otkrivanja zloupotreba ili prevarnih radnji koje su neposrednoj vezi sa platnim ulugama koje pružaoc usluga nudi.

Veoma često korisnici elektronskog bankarstva i elektrosnke trgovine nisu dovoljno upućeni o svojim pravima i obavezama prema davaocu usluga. S jedne strane to je greška samih korisnika jer ne posvete dovoljno pažnje ugovoru koji potpisuju kao i obaveštenjima koja dobijaju prilikom prvog pokretanja neke elektronske usluge[140]. Federalna komisija za trgovinu u SAD-u objavila je pravni bilten koji definiše i jasno stavlja do znanja korisnicima koja su njihova prava kada koriste elektronske metode plaćanja. U ovom biltenu elektronskog bankarstva korisnici mogu da dobiju informacije o tipovima ličnih informacija koje banka može da objavi. Takođe, isti dobijaju upustva na koji način da postupe kada dođe do greške u obeloganjivanju informacija, kao i tome koje su prave institucije kojima se treba obratiti u slučaju ovakvih propusta. Prema važećim zakonima u SAD-u korisnik od strane banke i finansiskih institucija mora dobiti informacije o pravima i obavezama, obavezama koje korisnik ima kada koristi elektronske bankarske servise, periodične izveštaje i listing plaćanja.

Ako se uporede informacije koje su dostupne korisnicima u SAD-u i korisnicima elektronskog bankarsva u Republici Srbiji dolazi se do zaključka da nema velikih razlika. Razlike se mogu javiiti u domenu institucija zaduženih za realizovanje nastalih problema i propusta.

3.6 Mobilno bankarstvo

Mobilno bankarstvo oslanja se na korišćenje mobilnih uređaja za pružanje usluga klijentima. Sve usluge mobilnog bankarstva mogu se svrstati u tri osnovne grupe. Prva grupa predstavlja servise uz pomoć kojih klijenti mogu da koriste usluge koje su vezane za korisnikov račun u banci. To znači da klijenti mogu da obavljaju transfere novca, izdaju trajne naloge za plaćanje računa, prenos novca na pod račune, prijavljivanje polise osiguranja i slično. Druga grupa predstavlja usluge koje se odnose na trgovinu hartijama od vrednosti, akcijama, itd. Jednom rečju ovde se mogu svrstati brokerske usluge. Treću grupu usluga predstavljaju informativne poruke o stanju na računi, datumu i vremenu poslednjih transkacija, kao i o lokacijama bankomata i

[140] Miloš Ilić, Žaklina Spalević, Mladen Veinović, „Elektronsko Bankarstvo – Primena i Sigurnost“. Sinergija University International Scientific Conference 2015, Bijeljina, str. 113-117, DOI: 10.7251/ZRSNG1501113I

ekspoziturama banke. Osnovna karakteristika mobilnih uređaja koji su u upotrebi jeste da su prenosivi i raspoloživi u bilo koje vreme na bilo kom mestu[141]. Mobilni servisi su dodali element mobilnosti konvencionalnim elektronskim bankarskim servisima koji se mogu realizovati preko fiksnih mreža. Na ovakav način u učesnike u mobilnim transkacijama mogu se ubrojati mobilni operateri, banke, različite finansijske institucije, kao i trgovci i potrošači[142].

Postojeći servisi mobilnog bankarstva koje banke nude svojim klijentima koriste različite komunikacione kanale i različite tehnologije. Govorna pošta pomoću IVR (Interactive Voice Response) omogućava interakciju klijenta i banke pozivanjem IVR broja[143]. Na ovakav način korisnik može dobiti pregled stanja, prometa i transakcija na svojim računima, ali i saznati više o uslovima poslovanja i ponudi banke. Takođe može dobiti i savet za rešavanje nekog tehničkog problema vezanog za korišćenje usluga mobilnog bankarstva. SMS, kao vrlo popularan mobilni servis, koristi se za obaveštavanje korisnika o stanju na računu, prilivima i odlivima sa računa. Poslednjih godina uvedena je i usluga prenosa novca slanjem SMS poruke, pri čemu je potrebno da su oba računa otvorena kod iste banke ili da su korisnici istih platnih kartica[144]. Bežični pristup ili WAP (Wireless Access Protocol) limitira korisnika da za korišćenje mobilnih bankarskih servisa mora da bude u domenu mrežne pokrivenosti. WAP je klijent – server aplikacioni standard za mobilne uređaje i website severe. Mobilni WAP terminali koriste mikro pretraživače na kojima se nalaze potrebne aplikacije za sve mobilne transakcije. Da bi se osigurala kompatibilnost nad različitim strukturama bežične mreže, WAP obezbeđuje različite protokole tako da aplikacije mogu da rade nezavisno. Danas se ovaj protokol koristi za većinu sajtova za mobilne uređaje koji su poznati pod nazivom WAP sajtovi[145]. WAP mobilno internet bankarstvo nudi korisnicima slično iskustvo i pogodnosti kao i osnovno internet bankarstvo. Sistem sigurnosti i nadgledanja upotrebe ovakvih aplikacija je sličan kao kod internet bankarstva. Samostalne klijentske mobilne aplikacije (Standalone Mobile Application Clients) su aplikacije koje omogućavaju izvršenje složenih bankarskih transakcija, sa najvećim stepen zaštite klijentskih podataka. Veoma lako se mogu prilagoditi u zavisnosti od složenosti korisničkog interfejsa obezbeđenog mobiilnim uređajem.

[141] Board of Governors of the Federal Reserve System, „Consumers and Mobile Financial Services“, Washington, DC 20551, 2014.
[142] Ilić Miloš, Spalević Žaklina., Spalević Petar, Veinović Mladen, „Mobilno bankartsvo-primena i sigurnost”, Zbornik radova 22. naučne i biznis konferencije – YUINFO, Kopaonik, pp. 252-255, 2016.
[143] Sanader D. „Mobilno bankarstvo: Novi trend u savremenom bankarskom sektoru“, Bankarstvo, vol 5, str. 86-109, 2014.
[144] Petrova K. „Mobile banking: backgroung, services and adoption“, In Delener, N. & Chao, C.-N. (eds), "Beyond Boundaries“. Proceedings of the 2002 GBATA International Conference, pp. 928-939, 2002.
[145] Paro, D. “Wireless application protocol (WAP): What is it all about....How does it work“, SANS Institute 2001

Ovakve aplikacije omogućavaju implementaciju sigurnog i pouzdanog komunikacionog kanala[146]. Rad aplikacija zahteva da mobilni uređaj podržava neki od razvojnih okruženja kao što je recimo J2ME, koji je industrijski standard za primenu mobilnih aplikacija, i zahteva da mobilni uređaj podržava Javu kao razvojni alat[147]. Problem koji se javlja jesu različite platforme na kojima rade različiti uređaji. J2ME grupiše API-e za mobilne uređaje koji imaju sličnu funkcionalnost u takozvane profile. S druge strane brzi razvoj mobilnih uređaja različitih funkcionalnosti dovodi do postojanja velikog broja profila, što znatno povećava troškove razvoja.

Pomenute tehnologije koje su u upotrebi kod realizacije mobilnog bankarstva moraju obezbediti adekvatnu sigurnost klijentskih podataka i transakcija. Kako različiti servisi koriste različite kanale komunikacije između klijentske aplikacije i banke različiti načini zaštite moraju biti obezbeđeni. Prvu grupu predstavljaju mehanizmi koji obezbeđuju sigurnost komunikacije ostvarene putem SIM kartice i GSM mreže. GSM mreže imaju sigurnosni mehanizam koji sprečava kloniranje SIM kartice i ilegalno korišćenje uređaja. Ovakva zaštita je obezbeđena je paralelnom autentifikacijom i enkripcijom podataka koji se prenose putem mreže. Autentifikacija SIM kartice se pokreće kada mobilna stanica pokušava da se konektuje na mrežu ili kada je terminal uključen. Autentifikacija SIM kartice zavisi od tajnog ključa koji je razmenjen između SIM kartice i AUC (Authentication Centers). Ovaj ključ je ugrađen na SIM karticu tokom proizvodnje od strane proizvođača, ali je takođe repliciran i u AUC. U cilju autentifikacije AUC generiše random broj koji se šalje pretpatniku. Tajni ključ sa SIM kartice i kreirani random broj se koriste za generisanje broja koji nosi naziv SRES (Signed RESponse) uz pomoć A3/A8 algoritma. Ako se SIM SRES poklapa sa AUC SRES onda je autentifikacija uspela. Problem sa A3 i A8 algoritmima je taj što oni zapravo nisu enkripcioni algoritmi već koriste COMP128 algoritam za enkripciju. Komunikacioni mehanizam koji se koristi kao zamena za ovaj algoritam i koji be trebalo da reši ove probleme je GPRS. Problemi ovog tipa moraju biti otklonjeni kako bi se ovaj mehanizam masovno koristio za mobilno bankarstvo. Ukoliko se radi o servisima koji se zasnivaju na upotrebi sesije kao što je slučaj slanja SMS-a sa korisničkim menijem i komunikaciji između klijenta i operatera putem odabira opcije iz menija može se obezbediti dodatan tajni ključ. U ovom slučaju AUC i SIM izračunavaju tajni ključ pomoću istih polaznih vrednosti primenom A5 algoritma. Ovako generisani ključ će se koristiti kod enkripcije i dekripcije komunikacione sesije. Grupa A5 algoritama enkripcije se koristi da spreči slučajne upade tako što enkriptuje komunikaciju između klijentskog uređaja i bazne stanice. Nad A5/1 algoritmom koji se koristi u zapadnim zemljama i koji važi za algoritam koji obezbeđuje jaku enkripciju sproveden je obrnuti inženjering i došlo je do njegovog probijanja. Razbijanjem enkripcije koju obezbeđuje A5/2 došlo se do A5/0 algoritma koji uopšte ne vrši enkripciju podataka. Svi ovi nedostaci dovode do zaključka da je zlonamerno

[146] Otair M., Tarawneh H. "Mobile Banking Based on Stand-alone Mobile Aplcation Clients", Journal of Information & System Management, vol. 1, num. 2, pp. 47-59, 2011

[147] Banerjee K., Rana M., Mahfuz M., Khan A. "Mobile Banking and Payment System Using Bluetooth Media", International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol: 11 No: 05, pp. 1-8, 2011.

presretanje ili upad u komunikaciju između uređaja i bazne stanice uvek moguće. Kako se ovi algoritmi koriste i u GPRS tehnologiji koja se nalazi kao envelop oko GSM-a, njihovo probijanje pokazuje da je i ovakav pristup nesiguran za mobilno bankarstvo.

Drugu grupu sigurnosnih mehanizama predstavljaju mehanizmi koji se nalaze iza aplikacija koje koriste WAP servise i Internet za uspostavljanje komunikacije između klijentske aplikacije i banke. WAP model ima sličnu strukturu kao mrežni OSI model. Kako je realizovan kao OSI model enkripcija i autentifikacija je obezbeđena preko WTLS (Wireless Transport Layer Security) nivoa, dok je sigunost bazirana na SSL (Secure Sockets Layer) protokolu. Generalno ovaj protokol je dizajniran za potrebe industrije i ima unapred zadatu namenu[148]. Ovaj protokol je dizajniran tako da zapravo predstavlja dva nivoa protokola. Kao što je ranije navedeno osnovna uloga SSL protokola je da obezbedi sigurnosne servise protokolima višeg nivoa koji se nalaze iznad njega. U TCP/IP strukturi protokol steka SSL protokol se nalazi između protokola višeg nivo i TCP protokola [149]. U realizaciji MAC algortima za potrebe mobilnog bankarstva koriste se već pomenute kriptografske tehnike sa ciljem kreiranja heš koda u okviru HMAC algoritma. Drugi problem može predstavljati korišćenje dvofaktorske autentifikacije/autorizacije na pogrešan način. Nije redak slučaj da mobilne aplikacije koriste kao dodatnu proveru korisnika ili naloga za plaćanje SMS poruku, a kao glavnu PIN ili lozinku. Ukoliko je napadač uspeo da stekne kontrolu nad prvim faktorom (sazna PIN / lozinku) mobilne aplikacije, SMS koji će mu stići na ukradeni mobilni uređaj vlasnika potpuno gubi bezbedonosnu funkciju. Ovakve forme napada se mogu sprečiti vezivanjem aplikacije za neko svojstvo mobilnog uređaja, mada se taj sistem pokazao nepraktičnim za korisnika.Noviji koncept zaštite koji se pojavio jeste korišćenje biometrije kao dodatne kontrole pristupa mobilnoj aplikaciji. Savremeni mobilni uređaji sadrže biometrijske senzore koje je veoma teško prevariti. Naravno, potrebno je vreme da bi se takve tehnike afirmisale kao sigurne i dostupne prosečnom korisniku i navele autore aplikacija iz sfere mobilnog bankarstva da im veruju.

Uslovi poslovanja banaka, kao i prava i obaveze klijenata i davaoca usluga moraju biti regulisani zakonom, kako bi se svi učesnici zaštitili. U Srbiji, najvažniji elementi koje mora da poseduje sistem elektronskog bankarstva propisani su Odlukom o minimalnim standardima upravljanja informacionim sistemom finansijske institucije. Ovom odlukom obuhvaćeni su informacioni sistemi u bankama, osiguravajućim kućama, davaocima finansijskog lizinga i društvima za upravljanje dobrovoljnim penzionim fondovima. U delu pod nazivom Elektronsko bankarstvo predviđeno je da je banka dužna da u poslovima elektronskog bankarstva primeni sigurne i efikasne metode autentifikacije. Proces autentifikacije mora se zasnivati na najmanje dva elementa potvrđivanja identiteta. Takođe banka mora da obezbedi odgovarajući mehanizam utvrđivanja svog identiteta na osnovu koga će korisnici biti u mogućnosti da utvrde autentičnost banke. U cilju obezbeđenja neporecivosti dokaznih radnji u vezi sa elektronskim bankarstvom banka mora da obezbedi postojanje sistemskih zapisa u

[148] McNub C. Network Security Assessement, Opus citatum.
[149] Veinović M., Jevremović A. „Računarske mreže“, Opus citatum.

kojima bi se čuvali podaci o svim aktivnostima korisnika[150]. Da bi se pristupilo korišćenju usluge mobilnog bankarstva, neophodno je da korisnik usluge potpiše Ugovor o korišćenju usluge mobilno bankarstvo za fizička lica. Radi sigurnosti obavljanja transakcija, banka korisniku usluge dodeljuje jednokratni kod za aktivaciju softverskog tokena koji je otvaranjem usluge instaliran na korisnikov mobilni uređaj. Korisnik usluge je dužan da koristi sigurnosni uređaj (mobilni uređaj) na način propisan uputstvima banke. Korisnik usluge je dužan da čuva sve lozinke koje koristi u radu sa uslugom koja mu se dodjeljuje nakon otvaranja usluge. Eventualnu štetu nastalu nepridržavanjem ovih odredbi snosi korisnik usluge. Tajnost i zaštita elektronskog novca i u slučaju mobilnog bankarstva propisana je članom 74 i 75 Zakona o platnim ulugama kao što je to bio slučaj i kod elektronkog bankarstva. Veoma često korisnici mobilnog bankarstva i mobilne trgovine nisu dovoljno upućeni o svojim pravima i obavezama prema davaocu usluga. Ova uobičajena greška samih korisnika je posledica neposvećivanja dovoljno pažnje sadržaju ugovora koji potpisuju, kao i obaveštenjima koja dobijaju prilikom prvog pokretanja neke elektronske usluge. Banka zadržava pravo izmene opštih uslova poslovanja. Ukoliko pak banka izmeni uslove poslovanja, izmenjeni uslovi poslovanja moraju biti javno dostupni korisniku i on mora biti obavešten o nastalim izmenama. Zakonski i podzakonski akti jasno definišu prava i obaveze kako banaka, tako i njihovih korsnika kako kod nas tako i u svetu. Ukoliko dođe do neželjenog propusta, problem koji se može javiti jeste zataškavanje istih od strane banki radi čuvanja sopstvenog ugleda. Takođe, problem koji se javlja jesu institucije koje bi trebale nastale propuste i štetu nanetu korisnicima istražiti i pronaći odgovorne.

Jedna od najpoznatijih prevara za koju je korišćeno elektronsko ili mobilno bankarstvo jeste unovčavanje najmanje 32 Vestern Union čeka. Svaki od čekova bio je na iznos između 195 i 500 dolara, prema zvaničnom izveštaju policije. Prema navodima policije prestupnik bi nakon kupovine u prodavnici deponovao uplatnicu na štedni račun Bank of America putem mobilnog depozita[151]. Kasnije bi se vratio i unovčio ček. Korišćena tehnologija u ovom slučaju poznata je kao mobilno daljinsko preuzimanje depozita (mRDC) koja omogućava korsnicima da bankarski ček deponuju, putem slike čeka poslate sa mobilnog telefona. Rizik za finansijske institucije koje omogućavaju mRDC je da kupac zadržava proveru papira, a potencijalno može da ga deponuje ponovo u drugim institucijama.

U prevari koja se odigrala u Indiji, prevaranti su podigli veću svotu novca sa bankovnog računa lekara i prebacili novac na razne račune. Policija je registrovala slučaj i istragom je utvrđeno da je iznos povučen 30. i 31. Marta 2012. godine sa računa lekara u banci Axis i prebačen na raznim računima banaka van Kerala[152]. Prevaranti su uspeli da kreiraju duplikat SIM kartice dr Shabeer Khan R Rovthara, a zatim blokirali njegov broj, a duplikat kartice je korišćen kako bi se počinila prevara.

---

[150] Odluka o minimalnim standardima upravljanja informacionim sistemom finansijske institucije, Službeni glasnik RS, br. 23/2013 i 113/2013

[151] Krebs B. „Double Cashing With Mobile Banking“, KrebsonSecurity, 2012

[152] NDTV, „Bank Froud Case“,Available on: http://www. ndtv. com /topic/bank-fraud-case, date:20.01.2018.

Jedan od napada na sigurnosne mehanizme koji koriste SMS kao kanal za slanje sigurnosnih kodova registrovan je od strane proizvođača antivirusa kompanije Kaspersky. Stručnjaci u ovoj antivirusnoj kompaniji pronašli su slobodnoj distribuciji na servisu Google Play određen broj malicioznih aplikacija namenjenih Android platformi. Ove aplikacije radile su tako što bi iz komunikacije između banke i klijenta koja se odvija putem SMS poruka izvlačile mTAN (Mobile Transaction Authentication) brojeve. Naime pomenuti brojevi su u upotrebi prilikom transkacija kako bi se sprečile transakcije sa kompromitovanih bankovnih računa. Praktično prilikom transkacije a pre obavljanja iste banka u vidu SMS šalje korisniku mTAN broj koji on unosi u predefinisano polje za unos ovog broja u okviru web portala banke[153]. Tek nakon unosa ovog broja korisniku je omogućeno da izvrši željenu transakciju. Da bi savladali ovu prepreku, kriminalci su razvili zlonamerne mobilne aplikacije koje automatski sakrivaju SMS poruke koje su povezane sa brojevima napadnutih banaka i krišom šalju takve poruke na servere koji su pod njihovom kontrolom. Kako bi ubedili žrtve da preumu njihove aplikacije koristili su taktike slanja lažnih email-ova ili prikazivanje lažnih obaveštenja prilikom pristupa sajtu banke sa zaraženih računara. Ova obaveštenja su savetovala instaliranje ovih aplikacija u cilju zaštite korisnika. Aplikacije slične ovima kreirane sa ciljem krađe SMS poruka u prethodnom periodu nakčešće su bile povezane sa bankarskim Trojancima Zeus-in-the-Mobile (ZitMo) i SpyEye-in-the-Mobile (SpitMo). Ovo je prvi slučaj da je mobilna komponenta specijalno razvijena za malver Carberp. Kako su ove aplikacije plasirane u najvećem broju slučajeva na teritoriji Rusije i primenjene nad korisnicima ruskih banki istraga je skoncentriana na ovim prostorima. Sama istraga je rezultirala hapšenjem odgovornih lica za tri najveća napada ovim malverom. Međutim ovaj malver još uvek se može kupiti na tržištu i njegova cena u zavisnosti od funkcionalnosti iznosi od 5000 do 40000 dolara. Navedeni primeri pokazuju da se korisnici mobilnih aplikacija nikada ne mogu potpuno zaštititi i da uvek postoji potencijalna opasnost od zloupotrebe ovih aplikacija. S tim u vezi potrebno je aktivno angažovanje stručnjaka na razvoju novih mehanizama zaštite kao i stručnjaka iz domena visokotehnološkog kriminala na otrkivanju počinioca i njihovom procesuiranju. Takođe sami korisnici se moraju edukovati o eventulanim mogućim problemima, načinu njihovog raspoznavanja i mehanizmima zaštite.

[153] Ilić Miloš, Spalević Žaklina., Spalević Petar, Veinović Mladen, „Mobilno bankartsvo-primena i sigurnost", opus citatum.

3.7 Kriptovalute

Tradicionalni način plaćanja korišćenjem novca kao sredstva razmene omogućava jednostavnu trgovinu vekovima unazad. Papirni novac uveden je kao sredstvo plaćanja sa ciljem zamene prvobitnih sredstava u obliku dragocenih metala. Novac kao sistem plaćanja služi i za praćenje poslovanja kao i očuvanje ekonomske vrednosti. U vremenu kada je uveden, papirni novac kao takav predstavljao je samo garanciju da će plaćanje biti obavljeno i da će vrednosne valute (zlato, srebro, dragoceni metali) nakon obavljenog posle biti prenete prodavcu. Ovakva garancija upravo je uvedena zbog težine prenosa metala i plaćanja u metalu. U ovakvim trgovinama poverenje je bazirano na posredniku koji je u isto vreme bio i izdavalac papirne garancije na iznos vrednosne valute. Ovo praktično znači da svaka od zemalja za novac koji poseduje i koji je u opticaju mora da ima pokriće u dragocenim metalima. Kroz istoriju pokriće se baziralo na zlatu kao dragoceom metalu. Međutim u novije vreme tokom dvadesetog veka upupavanjem novca u državnu ekonomiju, radom banaka u sektoru kreditiranja i pojavom elektronskog novca koji je bukvalno zapis vrednosti na računaru sve je manji broj zemalja koje poseduju pokriće za novac koji koriste. Sve ovo dovelo je do danas svima poznate svetske ekonomske krize.

Poslednja inovacija na polju valuta jesu digitalne valute koje bi mogle da omoguće da se trgovina, obračun i čuvanje vrednosti obavljaju najjeftinije i najefikasnije do sada, bez posredsva banaka, međunarodnih fondova kao i bez naplate taksi pri svakoj od transakcija. Kriptovalute su enkriptovane digitalne valute koje se prenose između ravnopravnih članova u mreži i koje su potvrđene u okviru javne evidencije (public ledgers) u procesu koji se naziva rudarenje (minig). Njihova upotreba bazirana je na poverenju bez posredovanja državnih organa, banaka, agencija, bukvalno bez ikoga između dve stranke u trgovini. Osnovni koncepti načina rada kriptovaluta su[154]:

- Public ledgers. Sve potvrđene transakcije od samog nastanka svake od kriptovaluta se čuvaju u okviru public leadgers-a. Identiteti vlasnika novčića su enkriptovani, dok sistem koristi druge kriptografske tehnike u cilju očuvanja legitimnosti vođenja evidencije. Ovakvom evidencijom osigurano je da digitalni novčanici mogu izračunati tačan balans potrošnje. Takođe, nove transakcije se mogu proveriti kako bi se osiguralo da svaka transakcija koristi samo novčiće koji su trenutno u vlasništvu potrošača. Ovo praktično znači da se na ovakav način osigurava da potrošač ne može trgovati više puta istim novcem.
- Transactions. Prenos sredstava između dva digitalna novčanika naziva se transakcija. Svaka transakcija se upisuje u public leadger-s i čeka na potvrdu. Kada se transakcija obavi digitalni novčanici koriste enkriptovan elektronski potpis kako bi obezbedili matematički dokaz da transakcija potiče od vlasnika novčanika. Sami proces potvrđivanja traje određeni period vremena za koje se vrši mining. Obično je to oko deset minuta za jedan novčić. Nakon toga mining potvrđuje transakciju i dodaje je u public leadger.

[154] CryptoCurrencyFacts, „How Does Cryptocurrency work“, Available at: https://cryptocurrencyfacts.com/how-does-cryptocurrency-work-2/, date: 25.01.2018.

- Mining (rudarenje). Najprostije rečeno mining je proces u kome se transakcija verifikuje i dodaje u public leadger. Kako bi dodao transakciju u leadger korisnik mora da reši izrazito kompleksan računski problem, nešto nalik matematičkoj slagalici. Sama tehnologija mining-a je otvorenog koda kako bi svako bio u mogućnosti da potvrdi transakciju. Prvi rudar koji reši slagalicu dodaje blok transakcija u leadger. Način na koji transakcije, blokovi i javni lanac leadger-a rade zajedno obezbeđuje da ni jedan pojedinac ne može lako da doda ili izmeni blok u lancu. Jednom kada je blok dodat sve korelacione transakcije postaju trajne i dodaju malu naknadu za obavljenu transakciju u novčanik minera, zajedno sa novokreiranim novčićima. Sami proces mining-a je ono što novčićima daje vrednost i poznat je pod nazivom *proof of work system*.

Tehnologija iza kriptovaluta, njihova anatomija, sami proces kreiranja i zaštite čini ih drugačijim od svih drugih valuta koje se mogu naći u opicaju. Prvi od faktora koji ih izdvajaju jeste *Adaptive Scaling*. Ovakv vid skaliranja znači da su kriptovalute kreirane tako da osiguraju istovetan nivo rada bez obzira na broj učesnika u mreži. Na primeru Bitcoina kao jedne od kriptovaluta u ekspanziji može se videti šta skaliranje praktično znači. Algoritam Bitcoina koji se koristi za rudarenje se prilagođava na osnovu toga koliko brzo rudari dobijaju nove novčiće. Cilj algoritma je da bude dovoljno složen kako se novi novčići ne bi lako dobijali ali da u istu ruku ne bude previše složen što bi uzrokovalo dugo vreme rudarenja i utrošak energije. Iz tog razloga algoritam prilagođava 2016 blokova kako bi se lakše ili kompleksnije rudarili u zavisnosti od toga koliko je vremena bilo potrebno da se izrudare prethodnih 2016 blokova. Teoretski ova modifikacija se obavlja na svake dve nedelje. Praktično ukoliko je mreži bilo potrebno 13 dana da izrudari 2016 blokova to znači da je algoritam suviše lak za rudarenje pa će složenost rasti. U suprotnom ukoliko je mreži potrebno 15 dana za rudarenje 2016 blokova to znači da je alogoritam suviše težak za rudarenje pa će složenost opadati. *AKA (Authentication and Key Agreement)* enkripcija se koristi u procesu kontrole kreiranja novčića i verifikaciji transakcija kod većine kriptovaluta, a samim tim i kod Bitcoina. Jedan od faktora koji kriptovalutama daju željenu jačinu i popularnost kod korisnika jeste i decentralizacija. Ovo praktično znači da za razliku od ostalih konvencionalnih valuta koje su u opticaju kriptovalute nisu pod kontrolom vlade ni jedne države tako da ne mogu biti regulisane od neke treće strane, kao što su državni organi, centralne banke ili međunarodni monetarni fondovi. Kreiranje kriptovaluta i transakcije u kojima se one koriste su otvorenog tipa, kontrolisane od strane softvera otvorenog koda i oslanjaju se na peer-to-peer mreže. Ne postoji ni jedan jedini entitet koji može u bilo kom domenu kreiranja i primene uticati na kriptovalute. Za razliku od tradicionalnih valuta koje su iz domena papirnog novaca sa razvojem tehnologije prešle u elektronski novac, kriptovalute se mogu naći samo u digitalnom obliku. Svaka transakcija predstavlja digitalni prenos novčića od jednog vlasnika do drugog bez postojanja fizičkih objekata. Kao što je već navedeno kriptovalute su open source. Ovo praktično znači da developeri mogu razviti API bez ikakvog plaćanja, kao i to da se svako može priključiti mreži bez ikakave nadoknade.

Ukoliko se pogledaju kriprovalute koje se mogu naći na tržištu poredak deset najvažnijih izgleda ovako:

- Bitcoin, vrednost tržišta oko 192 milijarde dolara, u opticaju oko 17 miliona novčića,
- Ethereum, vrednost tržišta oko 117 milijardi dolara, u opticaju oko 98 miliona novčića,
- Ripple, vrednost tržišta oko 52 milijarde dolara, u opticaju oko 39 milijardi novčića,
- Bitcoin Cash, vrednost tržišta oko 29 milijardi dolara, u opticaju oko 17 miliona novčića,
- Cardano, vrednost tržišta oko 17 milijardi dolara, u opticaju oko 26 milijardi novčića,
- Stellar, vrednost tržišta oko 11 milijardi dolara, u opticaju oko 18 milijardi novčića,
- NEO, vrednost tržišta oko 10.2 milijarde dolara, u opticaju oko 65 miliona novčića,
- Litecoin, vrednost tržišta oko 10 milijardi dolara, u opticaju oko 55 miliona novčića,
- EOS, vrednost tržišta oko 10 milijardi dolara, u opticaju oko 636 miliona novčića,
- NEM, vrednost tržišta oko devet milijardi dolara, u opticaju oko devet milijardi novčića.

Što se tiče Bitcoina otprilike u čitavom sistemu, 6 bitcoina se izrudari svakog sata. U opticaju je trenutno 17 miliona Bitcoina a maksimalni potencijal je 21 milion. Bitcoin se takođe može kupiti na većem broju berzi ili pak u direktno trgovini sa njegovim vlasnicima. Pretpostavlja se da je primarni cilj osnivača Bitcoina ideja da ova kriptovaluta postane sredstvo razmene i merilo vrednosti kako u realnoj zako i u virtuelnoj privredi. Uz sve oscilacije vrednosti i problem koje valuta proživljava, ovo je jedna od najvažnijih inovacija u monetarnoj sferi koja bi mogla iz temelja da promeni ekonomski sistem u kojem će ljudi živeti za par decenija. Nijedna država ne može uticati na odnos Bitcoina i drugih valuta prilikom konvertovanja iz jedne u drugu valutu. Celokupno konvertovanje i vrednost kriptovaluta je prepušteno zakonima slobodne trgovine. Za razliku od modernih valuta, u slučaju bitcoina pa i svih ostalih kriptovaluta ne postoji organnizacija koja bi imala monopol u ponudi valute. Takođe ne postoji ni ograničenje korišćenja isključivo jednog platežnog sredstva (legal tender law)[155].

Koliko je Bitcoin postao popularan svedoči i činjenica da sve više ljudi ulaže u ovu valutu. Njihova motivacija je kupovina Bitcoina i njegova kasnija prodaja po većoj ceni, a ne njegovo korišćenje za potrebe transakcija. Sa svime onime što nosi, Bitcoin je stalno na meti vlasti pojedinih nacionalnih država koje su promenama regulacije ili pretnjama uspele da na kratko uzdrmaju poverenje u digitalnu valutu. Ovo se može smatrati i logičnim ponašanjem s obzirom da uticajem na promet novca, bankarskim

[155] Pavle Mihajlović, „Bitcoin – Vesnik monetarne revolucije“, Dostupno na: https://startit.rs/bitcoin-vesnik-monetarne-revolucije/?utm_source=google&utm_medium=cpc&utm_content=bitcoin&utm_campaign=blog, datum pregleda: 24.01.2018.

kamatama, davanjem kredita, kao i uticajem na međunarodnom deviznom tržištu vlasti svake od zemalja u svojim rukama drže ekonomski status građana, a pritom u vidu taksi i poreza ostvaruju veliku dobit. Jedan od velikih udaraca na kriptovalute bilo je i gašenje berze za razmenu kriptovaluta pod nazivom MtGox.com. Takođe direktorka ove berze je pronađena mrtva u svom stanu u Singapuru. Sama smrt je klasifikovana kao neprirodna što može ukazivati na nesreću ili samoubistvo ali ne i na ubistvo. Takođe pored samih berzi na kojima se može vršiti razmena kriptovaluta i trgovanje njima sve je veći broj bankomata na kojima korisnici mogu kupiti recimo bitcoin-e ili bilo koju drugu kriptovalutu u zamenu za papirni novac ili plaćanje karticom. U najvećem broju slučajeva menjačnice su organizovane online i sami proces kupovine se obavlja putem kreditne kartice. Da ni Republika Srbija nije izuzetak kada su koristnici Bitcoina u pitanju svedoči podatak da je u vreme kada je ovo istraživanje vršeno Republika Srbija posedovala četiri automata za kupovinu kriptovaluta, tri u Beogradu i jedan u Novom Sadu[156].

Najvažniji pokazatelj koji se može pratiti nije trenutna cena neke digitalne valute već ukupna vrednost svih transakcija koje se obave digitalnim valutama. Tokom više od 9 godina koliko postoji, Bitcoin se pokazao kao pouzdan vrednosni sistem. Opstao je i pored brojnih bezuspešnih pokušaja kompromitacije njegovog programskog kod-a. Samo je tokom 2017.godine njegova vrednost porasla više od 10 puta. Obzirom na njegovu ograničenu količinu i sve veću kompleksnost rudarenja novih, Bitcoin dobija status elektronskog zlata. Kao takav stvara novi vrednosni sistem budućnosti. Pitanje koje se postavlja jeste da li će prednosti koje donosi upotreba virtualnih novčića dugoročno dovesti do istiskivanja konvencionalnih valuta, prvo sa interneta, a potom verovatno i iz ostatka ekonomije. Poznavaoci ekonomije, nastanka i korišćenja valuta navode da je izuzetna sličnost ulaska na tržište i svakodnevnog korišćenja između kriptovaluta i papirnog novca. Takođe veliki broj istraživača je zagovornik ideje da će kriptovalute trajno zameniti tradicionalni novac.

Kao i sa tradicionalnim novcem, internet trgovinom, elektronskim plaćanjem i sa razmenom kriptovaluta javljaju se mogući problemi i zloupotrebe. Da nije sve savršeno u virtuelnom svetu kriptovaluta pokazuje i primer hakera u Južnoj Koreji, nakon čije pljačke je Bitcoin menjačnica Youbit bankrotirala[157]. Ova menjačnica dva puta bila je na udaru hakera, nakon čega je morala da proglasi bankrot. Prvog puta lopovi su ukrali preko 35 miliona dolara u kriptovalutama, dok se tačan iznos poslednje pljačke ne zna. Zna se samo da su drugog puta izgubili 17% sredstava, što je bilo previše da bi se oporavili. Posledica ovoga je da će korisnicima biti smanjena sredstva na 75% vrednosti. Za ovu pljačku optužena je Severna Koreja tačnije grupa hakera sa tog prostora za koju se smatra da radi pod zaštitom vlasti ove zemlje. Iako je reč o manjoj menjačnici, ovo je samo još jedan znak kako je ceo virtuelni posao sa kriptovalutama veoma ranjiv. Ono što otežava istragu je upravo jedan od najvećih faktora razvoja kriptovaluta a to je decentralizacija i činjenica da ne postoje državni niti globalni

[156] Ecd, „Automati za kupovinu Bitcoina“, Dostupno na: https://ecd.rs/pages/automat, datum pregleda: 26.01.2018.
[157] Aleksandar Mirković, „Bitcoin menjačnica bankrotirala posle hakerske pljačke“, PC Press.

organi zaduženi za regulisanje kriptovaluta. Ne postoji centralna banka, niti regulatorno telo, kao ni mogućnost vođenja bilo kakvog sudskog spora za rešavanje ovakvih problema.

Drugi primer prevare sa kriptovalutama dolazi iz USA. Američka federalna komisija za kontrolu trgovine podnela je prekršajnu prijavu protiv dvojice navodnih prevaranata sa kriptovalutama. U prijavi se zahteva da se ovi trgovci finasijski kazne pored toga što bi bili prinuđeni da isplate žrtve koje su prevarili. Navodna prevara je počela u aprilu prošle godine, malo pre neverovatnog rasta vrednosti kriptovaluta. Po optužbama Federalne komisije, ova situacija je otvorila priliku za prevarante. Oni su optužili trgovce da su uzeli novac kako bi trgovali kriptovalutama i pobegli sa njim. Jedan od optuženih je Patrick K. McDonnell koji stoji iza kompanije poznate po imenima CabbageTech i Coin Drop Markets koje su trgovale sa bitcoinom i litecoinom. On je optužen da je ubeđivao klijente da mu daju novac i kriptovalute kako bi trgovao sa njima. Umesto da im donese profit, McDonnell je jednostavno uzeo bitcoine i nestao. McDonnell je obećavao klijentima 300% povraćaj investicija u roku od samo jedne nedelje. Drugi osumnjičeni je Dillon Michael koji je sa svojom kompanijom The Entrepreneurs Headquarters Limited ubeđivao ljude da investiraju u njegov fond, a ustvari ih je varao čuvenom piramidalnom šemom. On je skupio više od milion dolara u bitcoin-ma od preko 600 ljudi[158]. Ukoliko se ovakve prevare uporede sa sličnim prevarama koje su se kroz istoriju dešavale može se zaključiti da ove prevare nisu nikakav novitet. Vlasnici velikog broja banaka koje su radile sa papirnim novcem nudeći velike kametne stope klijentima koji bi kod njih oročili novac na štednju pobegli su sa istim, ostavivši tako bez celokupne štednje ogroman broj građana. Građani Republike Srbije još uvek pamte prevare ovakvog vida sa kojima su bili suočeni[159]. Možda je to još jedan od razloga zašto građani još uvek nisu u potpunosti prihvatili elektronsko bankarstvo i sve prednosti koje elektronski novac nosi.

Prema pisanju Reuters-a a prema otkriću kompanije *Trustwave* cyber kriminalci su u jednoj od prevara 2014. godine ukrali 85 digitalnih novčanika u kojima su pored Bitcona bile smeštene i druge kriptovalute. Prevara je izvedena tako što su hakeri inficirali stotine hiljada računara virusom nazvanim „Pony“, čiji je zadatak bio prikupljanje kriptovaluta[160]. Podatak koji nije poznat istraživačima jeste kolika je vrednost kriptovaluta bila u novčanicima. O ozbiljnosti napada govori i činjenica da su ljudi iz Bitcoin fondacije koja propagira usvajanje virtualnih valuta i njihovu upotrebu u svakodnevnom životu i radu savetovali svim korisnicima digitalnih novčanika da bitcoin-e prebace na offline lokaciju i tako ih sačuvaju od napada. Iako su serveri koji su kontrolisali mašine zaražene ovim virusom ugašeni od strane kompanije *Trustwave,* zaposleni ove kompanije naglasili su da očekuju više novih napada na korinsnike

[158] Aleksandar Mirković, „Kriptovalute i varanje – novi unosni posao prevaranata“, PC Press.
[159] Društvo za borbu protiv prevara, „Ponzijeva šema (kako su Dafina i Jezda ojadili narod)“, dustupno na: http://www.prevara.info/index.php?option=com_content&task=view&id=31, datum pregleda: 26.01.2018.
[160] Jim Finkle, „Pony botnet steals bitcoins, digital currencies: Trustwave“, Reuters, Available on: https://www.reuters.com/article/us-bitcoin-security/pony-botnet-steals-bitcoins-digital-currencies-trustwave-idUSBREA1N1JO20140224, date: 26.01.2018.

kriptovaluta. Kreiranjem mreže računara inficiranih malwerom ostvaruje se mogućnost njihovog kontrolisanja sa udaljenih servera. Ovo praktično dovodi do novog vida prevare u kome se zaraženi računari koriste za potrebe rudarenja kriptovaluta koje cyber kriminalci kasnije prisvajaju kao svoje. Pored prisvajanja izrudarenih kriprtovaluta, dodatan vid štete nanete vlasnicima računara jeste i utrošak energije s obzirom da je rudarenje kriptovaluta energetski jako zahtevan posao.

Napad koji se desio 26. januara 2018 godine nad kriptovalutom NEM zastupljenom na prostoru Japana još jedan je u nizu napada na digitalne valute[161]. NEM je pandan Bitkoin, Eterijum i Lajtkoin kriptovaluti i trenutno je jedan od 10 najvrednijih novčića, koji se koristi uglavnom za finansijske transakcije i online plaćanja. Operatori kompanije Coincheck Inc objavili su da je u ovom napadu vrednost ukraden kriptovalute procenjena na oko 46.3 biliona jena, što predstavlja oko 400 miliona dolara. Operatori su postali svesni ozbiljnosti napada osam sati nakon samog napada. Zbog pretrpljenih gubitaka suspendovali su povlačenje svih kriptovaluta osim bitcoina. Smatra se da je ovo najveći napad u istoriji kriptovaluta. U zvaničnoj izjavi kompanija je objavila da će pokušati da refundira svojim korisnicima 260.000 NEM novčića po ceni od 88.549 jena po novčiću. Pored velikog finansijskog udara na kompaniju iz ugla povraćaja sredstava pojedini izvori navode da će ova kompanija biti kažnjena u skladu sa setom finansijskih zakona.

Bilo kako bilo euforija oko kriptovaluta uprkos brojnim napadima se ne smanjuje. Naprotiv svakog dana sve je veći broj korisnika koji istražuju ovu oblast kako bi pronašli najodrživiju kriptovalutu. Stabilnost kriptovaluta uslovиće broj korisnika koji će nastaviti sa njihovim korišćenjem. U zavisnosti od nivoa zastupljenosti, broja korisnika kao i obima transakcija izvršenih kriptovalutama usvajanje kriptovaluta kao sredstva plaćanja može zauzeti globalne razmene. U sistemu u kome su građani razočarani papirnim novcem kao i odnosom države i banaka prema njima ovako koncipirana decentralizovana valuta može izgraditi sebi put do svakodnevne ekonomske upotrebe.

3.8 Otkrivanje prevara u elektronskom poslovanju uz pomoć digitalne forenzike

Informacione tehnologije zajedno sa širenjem Interneta donele su pored velikog broja prednosti i nove oblike društveno neprihvatljivog ponašanja. Ovakvo ponašanje potrebno je sankcionisati na odgovarajući način. Pojava sajber kriminala izazvala je potrebu za anagažovanjem specijalno tehnički obučenih stručnjaka, za suzbijanje i prevenciju takvih kriminalnih radnji. Digitalna forenzička istraga u računovodstvu se odvija nakon što je došlo do incidenta i ona u širokom spektru pomaže obradu

[161] Julia Banim, „Cryptocurrency Trading Stopped After World's Largest Crypto Theft", Unilad, Available on: https://www.unilad.co.uk/news/cryptocurrency-trading-stopped-after-worlds-largest-crypto-theft/, date: 27.01.2018.

krivičnih predmeta pred sudom[162]. Najčešće se radi o industrijskoj špijunaži, finansijskim istragama u vezi sa ekonomskim pitanjima (pranje novca, prevare sa kreditnim karticama, prevare osiguranja) i korporativnoj politici (e-mail zloupotrebe, nedolično ponašanje i zapošljavanje)[163].

Većina vrhunskih digitalnih forenzičkih alata i tehnika nastala je u zadnjih dvadeset godina. Preovladavanje digitalnih medija i informacija u skoro svakom aspektu delovanja privrednog subjekta, uzrokuje povećanu potrebu za digitalnim forenzičkim stručnjacima. Digitalna forenzika obuhvata nalaženje, čuvanje, identifikaciju, izvlačenje, analizu, dokumentaciju i pripremu slučaja povezanog sa digitalnim podacima i događajima[164].

Informacione tehnologije i digitalno okruženje utiču na prevare i sajber kriminal zbog: povećane upotrebe informacionih tehnologija u poslovanju, povećane upotrebe podataka od strane revizora finansijskih izveštaja, povećanog korišćenja informacionih tehnologija od strane počinilaca prevara i sajber kriminalaca[165]. Interpol ističe da sve više kriminalaca koristi brzinu, praktičnost i anonimnost na internetu da izvrše širok spektar kriminalnih aktivnosti koje ne poznaju granice, bilo fizičke ili virtuelne, izazivaju velike štete i predstavljaju realne pretnje žrtvama širom sveta.[166]

Po procenama firme za bezbednost - *McAfee Labs* (izveštaj iz 2014. godine) sajber kriminal košta globalnu ekonomiju 445 milijardi dolara godišnje [167]. U globalnom privrednom okruženju *online* kriminalne aktivnosti su se intenzirivarale od 2010. godine. Prema istraživanju *Juniper Research* procenjuju se da će do 2019. godine troškovi sajber kriminala iznositi 2,1 triliona američkih dolara.[168] Zbog toga su u skoro svim zemljama pokrenute aktivnosti protiv sajber kriminala.

---

[162]UK Legislation, Criminal Damage Act 1971. Available on: http://www.legislation.gov.uk/ukpga/1971/48/contents, date 25.03.2017.

[163] Žaklina Spalević, Kosana Vićentijević, „Forenzičko računovodstvo i revizija u digitalnom okruženju“, Kultura polisa, vol. XIV, No. 33, pp. 203-216, 2017.

[164] Zabihollah Rezaee, Richard Riley, „Prijevara u finansijskim izvještajima, sprečavanje i otkrivanje“, drugo izdanje, Mate d.o.o. Zagreb, str. 301, 2014.

[165] West Virginia University, *Education and Training in Fraud and Forensic Accounting: A Guide for Educational Institutions, Stakeholder Organizations, Faculty, and Students*, NIJ Special Report, West Virginia University - Forensic Science Initiative, 2012, pp. 15.

[166]Cybercrime, Interpol, Available on: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime%20; date: 12.01.2018.

[167] McAfee, Inc., „*Net Losses: Estimating the Global Cost of Cybercrime“*, Santa Clara, USA, 2014, pp. 3. Available at: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf, date: 25.05.2017.

[168]Juniper Research, *Cybercrime Will Cost Businesses Over $2 Trillion by 2019, Finds Juniper Research*, PR Newswire; Available on: *www.prnewswire.com/news-releases/cybercrime-will-cost-businesses-over-2-trillion-by-2019-finds-juniper-research-503449791.html*, date: 19.3.2017.

Stručnjaci u zajednici tehnološke sigurnosti procenjuju da gubici zbog internet kriminala iznose do 100 milijardi dolara godišnje, nadmašujući vrednost krijumčarenja narkotika i opojnih sredstava na svetskom nivou[169].

Napredak tehnoloških dostignuća povećava opasnost za globalnu ekonomiju i sigurnost. *G*20 zemlje imaju velike gubitke od sajber kriminala. Četiri najveće privrede (SAD, Kina, Japan i Nemačka) imaju gubitak od 200 milijardi dolara godišnje. Zemlje sa niskim dohotkom imaju manje gubitke, ali se i to menja, jer će te zemlje povećati upotrebu interneta, a sajber kriminalci koriste mobilne platforme.[170]

Kako bi se što veći broj napada na vreme učio, a nosioci napada pravilno sankcionisali bilo je potrebno razviti celu jednu oblast forenzike koja je našla primenu baš u ovom domenu. Svaka osoba koja bi se bavila ovim vidom forenzike mora da poseduje određeno obrazovanje i da ispunjava uslove za bavljenje ovim poslom. U zavisnosti od regiona ili zemlje razlikuju se potrebene veština u ovoj oblasti. Primera radi u u SAD postoji nekoliko forenzičkih sertifikata koje istražitelji moraju imati da bi mogli da svedoče na sudu. Jedan od sertifikata je *Global Information Assurance Certification* (*GIAC*)[171]. Forenzičar koji poseduje taj sertifikat postaje sertifikovani *GIAC* forenzički analitičar - *Certified Forensic Analyst* - GCFA.

Tom's IT Pro kompanija za 2018. godinu favorizuje sledećih pet sertifikata iz oblasti digitalne forenzike: ACE: AccessData Certified Examiner, CFCE: Certified Forensic Computer Examiner, CHFI: Computer Hacking Forensic Investigator, EnCe: EnCase Certified Examiner, GCFA And GCFE Certifications.[172]

Prikupljanje elektronskih informacija je prvi korak tokom istrage digitalnih dokaza. Uspešna istraga digitalne forenzike zahteva angažovanje stručnjaka koji ima tehničke osnove kompjuterskih tehnologija i koji je upoznat sa relevantnim pravilima pravnog subjekta i istragom. Većina alata za analizu *e-podataka* može vratiti, isfiltrirati, izvući, sortirati i analizirati podatke iz računovodstvenih baza. Ovi alati takođe mogu identifikovati praznine, duplikate, informacije koje nedostaju i statističke anomalije[173]. Danas sa razvijenim softverima i tehnološkim sposobnostima za obradu velike količine podataka, 100% populacije u okviru datoteka se može analizirati i testirati. Jedna od prednosti IT alata u forenzičkom računovodstvu je da se podaci mogu preuzimati kod klijenta iz glavne knjige, mogu se preuzeti i novčani tokovi, mrežni disk, korisničke datoteke, razne vrste web evidencija, bilo gde da se nalaze elektronski podaci.

---

[169]Alison Diaz, *Meet A-Z: The Computer Hacker behind a Cybercrime Wave*, USA TODAY; Available on: http://usatoday30.usatoday.com/tech/news/computersecurity/2008-08-04-hacker-cybercrime-zeus-identity-theft_N.htm, date: 19.3.2017.

[170] Intel Security, *Net Losses: Estimating the Global Cost of Cybercrime*, USA, 2014, pp. 5.

[171] Giac Certifications, Available on: http://www.giac.org/, date: 29.01.2018.

[172]Ed Tittel, Kim Lindros, „Best Digital Forensics Certifications 2018", Available on: http://www.tomsitpro.com/articles/computer-forensics-certifications,2-650.html, date: 29.01. 2018.

[173] Zabihollah Rezaee, Richard Riley, Opus citatum, str. 303.

Prilike za usklađivanje tehnologija za analizu podataka za potrebe otkrivanja prevare i istraživanja su odavno prepoznate. U studiji koju su zajedno izdali Institut internih revizora (*The Institute of Internal Auditors - IIA*[174]), Američki institut sertifikovanih javnih računovođa (*The American Institute of Certified Public Accountants - AICPA*) i Asocijacija sertifikovanih istražitelja prevara (*Association of Certified Fraud Examiners - ACFE*[175]) „*Managing the Business Risk of Fraud: A Practical Guide*"[176], autori identifikuju kako analiza podataka, kontinuirana revizija i monitoring tehnike, kao i drugi srodni alati i tehnologije, mogu da se koriste za otkrivanje prevarnih aktivnosti. Studija opisuje analizu podataka, korišćenje tehnologija u identifikovanju anomalija, trendove i indikatore rizika u raznim transakcijama, kao i identifikovanje odnosa među ljudima u organizaciji i dešavanja.

Digitalna forenzička istraga ima za cilj da ispita dokaze u cilju otkrivanja prevarnih radnji, kada se to i kako desilo, ko je bio uključen i koliko novca je izgubljeno[177]. Metodologija digitalne forenzičke revizije daje smernice u cilju što lakšeg pronalažanja transakcija koje treba podvrgnuti testiranju, upućuje na načine lociranja skrivenih znakova prevare, identifikaciju *crvenih zastavica* koje dovode do nezakonitih transakcija, i navodi procedure planiranja ove revizije[178]. Ako dođe do prekida *lanca dokaza*, sud takve dokaze ne prihvata. Održavanje *lanca digitalnih dokaza* i metoda zaštite integriteta digitalnih dokaza se sprovode u cilju održanja životnog ciklusa digitalnog dokaza, da bi bio validan pred sudom ili u izveštaju za menadžment. Prema Yeager-u termin *lanac očuvanja* ili *lanac čuvanja* se odnosi na potpunu reviziju i kontrolu originalnog dokaznog materijala koji bi potencijalno mogao biti upotrebljen u legalne svrhe[179].

Doprinos pružanju kompleksnih računovodstvenih forenzičkih usluga daju nacionalni i međunarodni zakoni i propisi o privatnosti. Takvi propisi zahtevaju da forenzički računovođa pažljivo proceni potrebu da se dobiju poverljivi lični podaci. Ako je potrebno, forenzički računovođa će možda morati da sprovede mere bezbednosti da ublaži rizik od povrede podataka i prikupi samo podatke koji se mogu smatrati relevantnim za angažovanje. Ako dobije poverljive podatke forenzički računovođa će morati da sprovede odgovarajuće strategije za smanjenje opasnosti od neovlašćene korišćenja takvih informacija.[180]

---

[174]The Institute of Internal Auditors North America, Available on: https://na.theiia.org/Pages/IIAHome.aspx; date: 20.01.2018.

[175] Association of Certified Fraud Examiners, Availeble on: http://www.acfe.com; date: 20.01.2018.

[176]The Institute of Internal Auditors: Available on: http://www.theiia.org/media/files/fraud-white-paper/fraud%20paper.pdf; date: 25.01.2018.

[177]Tracy L. Coenen, „Expert Fraud Investigation: A Step-by-Step Guide", John Wiley & Sons, Inc., Hoboken, New Jersey, 2009, pp. 19.

[178] Leonard W. Vona, "Fraud Data Analytics Methodology: The Fraud Scenario Approach to Uncovering Fraud in Core Business Systems", John Wiley & Sons, Inc., Hoboken, New Jersey, 2016, pp. 10.

[179] R. Yeager, *„Criminal computer forensics management",* Proceedings of the 3rd annual conference on Information security curriculum development - InfoSecCD'06, 2006, pp. 168.

[180]AICPA, Available on: aicpa.org/InterestAreas/InformationTechnology/Resources/ Privacy/GenerallyAcceptedPrivacyPrinciples/Pages/Generally%20Accepted%2Privacy%20Principles.aspx, date: 19.3.2017.

Federalni istražni biro *Internet Crime Complaint Center* (IC3) u SAD, od 2003. godine prima žalbe u vezi sa online prevarama, uključujući prevare u oblasti prava intelektualne svojine, kompjuter napade (*hacking*), ekonomsku špijunažu, međunarodno pranje novca, krađu identiteta i druge oblike internet zločina.

Sajber kriminalci redovno napadaju privredne subjekte širom EU. Nemačka je najveća žrtva ove vrste kriminala u finansijskom sektoru, kao i u energetskom i farmaceutskom sektoru[181].

Na osnovu informacija od Internet provajdera u Velikoj Britaniji privredni subjekti su pogođeni 230000 puta sajber napadima u 2016. godini.[182] Državna revizija u Velikoj Britaniji procenjuje troškove sajber kriminala u Velikoj Britaniji između 18 i 27 milijardi funti godišnje[183].

Na osnovu izjave Američke agencije za nacionalnu bezbednost (US National Security Agency-NSA) globalni trškovi kompjuterskog kriminala procenjuju se na više od 385 milijardi dolara[184].

Najveća globalna pretnja kako naglašavaju *Ernst and Young* za opstanak privednih subjekata je visoko tehnološki kriminal. Funkcija informacione bezbednosti zadovoljava potrebe samo 17% privrednih subjekata, 93% privrednih subjekata održava ili povećava bezbednost. Privredni subjekti moraju biti okrenuti ka budućnosti i pripremiti se za nove tehnologije i zaštitu od prevarnih radnji putem istih.[185]

Statistički podaci u ovom istraživanju obuhvatili su u Hrvatskoj 47 vodećih privrednih subjekata iz oblasti finansijskih usluga, osiguranja, inženjeringa, građevinarstva, tehnologije i proizvodnje. U Hrvatskoj 25% anketiranih privrednih subjekata je bilo žrtva sajber kriminala (globalni nivo 32%). Uprkos navedenoj činjenici 22% ispitanih privrednih subjekata smatra da će imati sajber napade u naredne dve godine. Manje od polovine ispitanika (45% privrednih subjekata) u Hrvatskoj ima pripremljen plan odgovora na incidente sajber pretnji, a svaki peti

---

[181] Ponemon Institute, „2015 Cost of Cybercrime Study: Global“, Sponsored by Hewlett Packard Enterprise Independently conducted by Ponemon Institute LLC Publication Date: October 2015, 2015, pp.10

[182]Anmar Frangoul, „UK businesses were hit 230,000 times each by cyber-attacks in 2016, says internet service provider“, Available on: http://www.cnbc.com/2017/01/11/uk-businesses-were-hit-230000-times-each-by-cyber-attacks-in-2016-says-internet-service-provider.html, date: 25.05.2017.

[183] Baud, Emmanuel G, et al. „Europe Proposes New Laws and Regulations on Cybersecurity“, Jones Day. 1 Jan 2014. Web. 10 Jun 2014. Available on http://www.jonesday.com/europe-proposes-new-laws-and-regulations-on-cybersecurity-01-02-2014., date: 25.05.2017.

[184]McAfee, Inc., „Net Losses: Estimating the Global Cost of Cybercrime“, Opus citatum.

[185]Ernst & Young, „Cyber-crime is greatest global threat to organizations' survival today“, Available on: http://www.ey.com/lu/en/newsroom/news-releases/news_20131105_cyber-crime-is-greatest-global-threat-to-organizations-survival-today, date: 26.3.2017.

privredni subjekt (njih 21%) nema ni najmanju meru takvog plana. Interesovanje privrednih subjekata u Hrvatskoj koji bi angažovali forenzičkog istražitelja kada se ustanovi prevara je samo 9% od ispitanika u PwC-om istraživanju.[186]

Rezultati istraživanja PwC-a iz 2016. godine sajber kriminala u Rusiji[187] su sledeći: samo 26% privrednih subjekata ima plan za odgovor na sajber incidente, 43% privrednih subjekata direktno brine o sajber bezbednosti, 25% kompanija smatra da će biti pogođeno sajber kriminalom u naredne dve godine. Ovi rezultati su zasnovani na odgovorima preko 120 privrednih subjekata iz Rusije. Kao najčešće vrste prevare navedene su pronevera imovine (72%), prevare prilikom nabavki (33%), mito i korupcija (30%) i sajber kriminal (23%).

Prema podacima iz 2016. godine mala pravna lica su postala velika meta za sajber napade, što se može videti iz istraživanja koje je sproveo Symantec's[188]. Mala i srednja privredna društva zajedno sa ograncima inostranih kompanija koja posluju na teritoriji Republike Srbije potencijalna su meta cyber napada, iz prostog razloga jer nivo implementiranih protokola za unapređenje cyber bezbednosti njihovih sistema nije na odgovarajućem stepenu. S tim u vezi privredno okruženje naše zemlje iskazuje svojevrsnu potrebu za kreiranjem dokumenta koji bi ponudio rešenje situacija sa kojima se susreću privredni procesi, a u vezi sa pomenutim cyber napadima i zaštitom od istih.[189] Prema istraživanju *Vault Top* R*anked* najboljih 10 firmi koje se preporučuju za forenzičku reviziju u 2017. godini su[190]:

- PwC (Price water house Coopers),
- Ernst & Young (EY),
- Deloitte,
- KPMG,
- Grant Thornton,
- BDO USA,
- RSM US,
- Crowe Horwath,
- Baker Tilly Virchow Krause,
- Moss Adams

[186]Per Sunbye, Martina Butkovic, Ivana Rapic, "Globalno istraživanje gospodarskog kriminala iz 2016. – Hrvatska Naoružani i spremni za bitku (Vaši protivnici jesu!)", Available on: http://www.pwc.hr/hr/forenzicke-usluge/Globalno-istrazivanje-gospodarskog-kriminala-iz-2016-za-Hrvatsku.pdf, strana 4; date: 26.3.2017.

[187] PwC (PricewaterhouseCoopers): Russian Economic Crime Survey 2016*,* PwC Russia.

[188]Symantec, Innovation, Sophistication, Organization – Producing Ominous Results Available on: https://www.symantec.com/security-center/threat-report, date: 26.3.2017.

[189] Đekić, M. D. Sajber procedure za poslovno okruženje u Srbiji, Tehnika, 71(3), 2016, str. 471-474.

[190]Vault, 2018 Best Accounting Firms for Forensic Accounting: Available on: http://www.vault.com/company-rankings/accounting/best-firms-in-each-practice-area?sRankID=418; date: 26.3.2017.

Iako rastu potrebe za zaštitom i prevencijom cyber prevara, privredni subjekti ne angažuju dovoljno digitalne forenzičare. Mogući razlozi za neangažovanje svrstavaju se u to da su usluge zahtevne i prevazilaze finansijske mogućnosti klijenta da ih isfinansira, nedovoljna je informisanost i saznanje o uslugama koje su dostupne. Sem toga sve više privrednih subjekata u svojoj organizacionoj strukturi ima fraud odeljenje, pa je i to mogući razlog manjeg eksternog angažovanja digitalnog forenzičara računovođa. Ne treba zanemariti ni činjenicu da u uslovima pretprljene štete po osnovu prevara koje nisu materijalno značajne pravna lica su spremnija da prećute tu informaciju kako ne bi narušila svoju reputaciju.

Pored otkrivanja sajber prevara, izračunavanja iznosa prevarne radnje, izveštavanja o istažnom postupku, digitalne forenzičke računovođe imaju savetodavnu ulogu preventivnog karaktera da se suzbiju nezakoniti postupci i prevare, da se sačuva reputacija kompanije. S tim u vezi digitalna forenzika u cyber prostoru može se okarakterisati kao interdisciplinarna, jer objedinjuje znanja iz oblasti računovodstva, forenzičkog računovodstva, internih kontrola, poreskog i krivičnog prava, informacionih tehnologija.

Jako bitan element forenzičkog računovodstva za primenu u cyber prostoru jeste razvoj ove oblasti u domenu regulisanja kriptovaluta. Kriptovalute kao što je već navedeno nemaju regulaciono telo pa samim tim zadatak forenzičkog računovođe je višestruko teži. Softver koji bi se korisitio u ovu namenu mora da omogući lakše rešavanje prevara i kriminalnih delatnosti povezanih sa narušavanjem poretka kriptovaluta. Ovakav sistem mora da bude u mogućnosti da ispuni dve jako bitne karakteristike. Jedna se odnosi na zaštitu korisnika i otkrivanje počinioca, dok je druga orijentisana ka modelima forenzičkog računovodstva koji neće narušiti princip decentralizacije kriptovaluta.

4
Servisi elektronske vlade u službi građana

Razvoj informaciono komunikacionih tehnologija kao i njihova upotreba za vreme prošlog i veka u kome živimo postao je neraskidivi element svakodnevnog života i rada ljudi. U domenu primene ovih tehnologija razvili su i razvijaju se mnogobrojni elektronski servisi čiji je cilj da olakšaju i uproste mnoge aspekte ljudskog života i rada. Pored već pomenutih elektronskih servisa aktivno se radi na razvoju ili unapređenju već razvijenih elektronskih servisa za komunikaciju građanja ili privrednih subjekata sa državnim institucijama. Ovako razvijeni koncept u kome se na bazi elektronskih servisa građanima i pravnim licima nudi mogućnost online komunikacije sa državnim organima naziva se elektronska vlada. Elektronska vlada (e-vlada) koncipirana je na više nivoa u zavisnosti od toga ko su učesnici u interakciji. S tim u vezi mogu se izdvojiti sledeće grupe interakcije:

- između vlade i građanstva (G2C, government-to-citizens),
- vlade i poslovnih subjekata (G2B, government-to-business), i
- vladinih odeljenja međusobno (G2G, government-to-government).

Ovako koncipirano društvo zasnovano na upotrebi informaciono komunikacionih tehnologija podeljeno je na određene delove radi lakše koordinacije i funkcionisanja elektronskih servisa. Skup svih servisa naziva se elektronska uprava (e-uprava). Sama elektronska uprava dalje se može podeliti na:

- Elektronsku demokratiju (E-Democracy), koja može predstavljati proces glasanja na izborima spoveden korišćenjem informaciono komunikacionih tehnologija i interneta bez fizičkog odlaska na biračko mesto.
- Elektronsku administraciju (E-Administration), koja po definiciji zapravo predstavlja elektronsku upravu u užem smislu jer se radi u opštem smislu radi o administrativnim postupcima, i načinu njihovog olakšavanja a samim tim i ubrzavanja.
- Elektronsko pravo (E-Justice), koje predstavlja vođenje sudskog procesa putem elektronskih komunikacionih servisa. Umesto da se tužba napiše, štampa i odnese u sud ona se direktno šalje putem elektronske pošte ili putem sudskog portala. Sudski portal je specijalni interfejs suda na internetu kojim se vrši komunikacija. Putem ovog portala vrši se evidencija i obaveštavanje advokata putem elektronske komunikacije o nekom konkretno slučaju. Komunikacija se pretežno vrši elektronskim putem.

Kako je pre svega dostupnost servisa elektronske vlade i elektronske uprave uslovljena stepenom razvoja infomaciono komunikacionih tehnologija, primena ovih servisa nije podjednaka svuda u svetu. Barijere koje se javljaju po pitanju primene servisa e-vlade, a samim tim i e-uprave gotovo su istovetne sa barijerama razvoja e-trgovine. I kod jednih i kod drugih najveći problemi upotrebe ovakvih servisa javljaju se kod zemalja u razvoju.

4.1 Koncepti i primena elektronske demokratije

Elektronska demokratija predstavlja najveći uspeh vekovnog zalaganja i borbe za kvalitetniji društveni poredak i ustoličenje principa demokratije kao osnove slobodnog društva. Elektronska demokratija se može definisati kao korišćenje informaciono komunikacionih tehnologija i strategija od strane aktera demokratskog procesa (vlada, izabranih zvaničnika, medija, političkih organizacija, građana, birača) u političkim i upravljačkim procesima na nivou lokalnih zajednica, država ili na međunarodnom planu. Sama pojava elektronske demokratije u obliku teledemokratije vezuje se za razvoj kablovske televizije sedamdeetih godina, 20. veka. Ovaj model elektronske demokratije podrazumevao je pojedince koji direktno vladaju iz svojih fotelja putem upotrebe telekomunikacionih medija[191].

Informaciono komunikacione tehnologije se u proces kreiranja i upotrebe elektronske demokratije i njenih servisa koriste u cilju ojačanja demokratije, unapređenja institucija zaduženih za primenu demokratskih principa, kao i u cilju utemeljenja demokratskih procesa. Upotrebom ICT kao vida podrške elektronskoj demokratiji vrši se uključivanje građana u demokratske procese, njihovo angažovanje u procesu donošenja odluka i izboru predstavnika u okviru demokratskih institucija. Prema nekim defincijama e-demokratija se posmatra kao model demokratije u kome se javni servisi i internet koriste u cilju pružanja informacija građanima o dešavanjima i aktuelnostima kako u zemlji kao celini tako i u državnim institucijama. Na ovakav način građani će razmotriti dobijene informacije i doneti zaključak o mogućim izmenama. Na ovakav način oni su uključuju u aktivan proces definisanja načina vladavine i rada državnih organa u zemlji.

O kompleksnosti elektronske demokratije svedoči i podatak da se ona može podeliti na nekoliko vrsta:

- Likvidna elektronska demokratija. Karakteristično za likvidnu demokratiju je to da građanin svojim glasom bira predstavnika koji će na osnovu ukazanog poverenja učestvovati u demokratskim procesima. Iz tog razloga može se reći da je ovo oblik neposredne demokratije sa izabranim predstavnikom. Međutim pored toga građanin ima pravo da putem elektronskih servisa glasa o svakom pojedinačnom zakonu.
- Viki-demokratija. Viki demokratija je proces pisanja i donošenja zakona i podzakonskih akata koji se vodi preko viki sistema. Ovakvi sistemi bi trebalo da budu zasnovani na diskusijama sličnim onima koje se vode na Vikipediji.
- Kolaborativna e-demokratija. U ovoj vrsti e-demokratije vrši se kombinovanje pojedinačnih karakteristika koje imaju neposredna, predstavnička i elektronska demokratija. Ovakav vid demokratije bazira se na zajedničkom radu državnog sektora i nevladinog serktora, a sve sa ciljem pisanja i donošenja kvalitetnih zakona

[191]Damnjanović, I., „Elektronska demokratija (E-Democracy) kao mogućnost demokratizacije", Srpska politička misao, Broj 1, str. 85-98., 2009.

i strategija razvoja[192]. Ovakav udruženi rad se izvodi putem elektronskih servisa vladnih portala i čak putem društvenih mreža. Nezaobilazna je činjenica da članovi državnog sektora izabrani na izborima snose najveći teret izrade zakona, dok građani zadržavaju svoje glasačko pravo koje mogu iskoristiti pri glasanju o svakom pitanju koje je od interesa za njih. Pravo koje građani imaju a koje se odnosi na glasanje o svakom konkretnom pitanju, zakonu ili podzakonskom aktu potiče iz neposrednog modela demokratije.

Poređenjem opisanih modela iz ugla složenosti savremenog društva koje je protkano upotrebom različitih informaciono komunikacionih tehnologija može se uočiti da se u grupu jednodimenzionalnih modela mogu svrstati modeli predstavničke i neposredne demokratije. Predstavnički model upravljanja se često u literaturi kritikuje i stavlja mu se na teret da je kreiran za političku elitu. Poznato je da je politička elita često udaljena od običnog čoveka pa samim tim sistem koji je njoj okrenut često može biti odbačen od naroda. Ovakav defekt neposredna demokratija bi mogla da nadoknadi kvantitetom učešća građanina u procesu odlučivanja[193]. Pitanje koje se često postavlja jeste koliko vremena i znanja poseduju građani za aktivno učestvovanje u donošenju odluka? Vreme koje građani trebaju da odvoje za potrebe diskusije, kao i način realizovanja ovakvog pristupa dovode do toga da je potrebno kreirati novi hibridni model koji bi na efikasniji način u donošenje odluka uključio i zastupnike i pojedince iz reda građanstva.

Primenom mobilne tehnologije u domenu e-demokratije izdvojio se pojam mobilne demokratije (m-demokratija). Praktično gledano e-demokratija i m-demokratija mogu se posmatrati kao ista oblast, s tim što m-demokratija ima za cilj da iste demokratske ideje ali sa podrškom u mobilnim tehnologijama i uređajima. Ona se može posmatrati kao dodatni deo e-demokratije, čijom primenom se pokriva prostor na kome e-demokratija nija dostupna. Bitno je naglasiti da se ova dva pojma ni u kom slučaju ne trebaju posmatrati odvojeno.

M-demokratija se nahčešće bazirana na upotrebi mobilnih telefona. Mobilni telefon, kao personifikacija mobilnih tehnologija i uređaja, treba posmatrati kao svojevrsni demokratski i politički alat. Sa njim se uspostavljaju društvene mreže među ljudima, bilo licem u lice (ili glasom), bilo preko softvera za društveno umrežavanje ili najčešće njihovom kombinacijom. Umrežavanje ljudi preko mobilnih telefona ubrzava stvaranje formalnih i neformalnih grupa, koje nose velik potencijalni socijalni kapital. Sa političke tačke gledišta ovakve grupe su odlične za informisanje, mobilizaciju i organizaciju aktivista. Mobilni uređaji, koje uvijek uz sebe nose ljudi, dozvoljavaju stalnu dostupnost na bilo kojoj lokaciji i u bilo koje vreme, te se tako uspostavlja decentralizovana, ad-hoc i asinhrona komunikacija. Sumnja u demokratizaciju putem m-demokratije javlja se zbog potencijalne trivijalalizacije e-glasanja preko mobilnih uređaja.

---

[192]Sanford, C., Rose, J., „Characterizing eParticipation“, International Journal of Information Management, Vol. 27, No. 6, pp. 406-421., 2007.

[193]Pilipović, D., „Odnos e-demokratije i e-glasanja“, 7. Naučni skup Mreža 2015., Univerzitet Singidunum, Poslovni Fakultet Valjevo, str. 280-287, 2015.

Društveni proces donošenja odluka u e-demokratiji se sastoji od dve osnovne stavke:

- e-glasanja, koje je vezano za izborni proces,
- e-participacije koja govori o učestvovanju u demokratskom odlučivanju.

E-demokratija zamišljena je tako da svim članovima elektronske zajednice pruži adekvatan pristup svim političkim i opštedruštvenim procesima. E-demokratija preko simbioze demokratskih procesa i ICT aktivno u demokratski proces uključuje građane, političke organizacije, vladine agencije, i druge vladine i nevladine organizacije.

4.1.1 Elektronsko glasanje (e-glasanje)

Tradicionalna načela demokratije kao i načela elektronske demokratije zasnovana su na glasanju kao jednom od osnovnih principa izražavanja volje građana. Izbori i samo glasanje predstavljaju fundamentalnu osnovu brojnih demokratskih društava. Čak šta više, to je najkritičnija funkcija u društvenom poretku zasnovanom na demokratiji. Ukoliko se posmatra sami naziv *elektronsko glasanje* može se zaključiti da je upitanju neka forma glasanja i/ili obrade glasačkih listića koje se izvršava upotrebom elektronskih uređaja. U najširem mogućem obimu u grupu elektronskog glasanja spadala bi svaka forma glasanja u kojoj se koristi minimalno jedan elektronski uređaj ili elektronski postupak. Ukoliko se celokupan proces elektronskog glasanja posmatra kao zatvoreni sistem, ulaz u ovaj sistem predstavljao bi pojedinac, dok bi izlaz sistema predstavljao celo društvo. S druge strane najuže posmatrano elektronsko glasanje predstavlja demokratski proces izražavanja volje građana, obrađivanja i prikazivanja rezultata izbornog procesa u kome se koriste informaciono komunikacioni uređaji ili sistemi u većem ili manjem obimu[194].

Kod elektronskog glasanja u zavisnosti od stepena zaštite prilikom glasanja kao i u zavisnosti od samog načina realizacije elektronskog glasanja mogu se izdvojiti tri vrste elektronskog glasanja:

- Slabo kontrolisano e-glasanje. Omogućava glasaču najveću autonomiju s obzirom na činjenicu da glasač sam bira mesto koje mu odgovara za sami čin glasanja. Problem koji se ovde javlja jeste kontrola samog glasanja s obzirom na nepostojanja fizičkog prisustva izbornog osoblja ili organizatora. Nepostojanje kontrole veoma lako može dovesti sami proces glasanja u potencijalnu zloupotrebu i neregularnost. Ovako koncipirano e-glasanje zasniva se na upotrebi računarskih mreža i interneta u cilju distribucije glasačkog listića do centralnog mesta na kome se vrši prebrojavanje i generisanje rezultata.
- Polukontrolisano e-glasanje. Drugi naziv za polukontrolisano glasanje koji je u zvaničnoj upotrebi je i kiosk glasanje. Ovaj tip glasanja predstavlja prelazni tip

[194]Pilipović D., „Razvoj, trenutno stanje i perspektive e-glasanja“. U Zborniku Infoteh 2014. Jahorina: Elektrotehnički fakultet Istočno Sarajevo., 2014.

e-glasanja u kome organizatori delimično kontrolišu postavljene uslove. Sama glasačka mesta nalaze se u različitim objektima kao i kod tradicionalnog načina glasanja. Prisustvo organizatora ili izbornog osoblja nije obavezno na mestima za glasanje, s tim da oni ipak mogu biti prisutni ili s vremena na vreme mogu obići glasačko mesto u cilju provere regularnosti izbornog porcesa. Ovaj tip glasanja u određenoj meri je sličan sa tradicionalnim glasanjem, s tim što potpune kontrole ipak nema.

- Kontrolisano e-glasanje. Kontrolisano e-glasanje organizovano je tako da su na samom glasačkom mestu prisutni organizatori i glasači. Razlika u odnosu na tradicionalno glasanje je u tome da organizatori nemaju kontrolu nad uslovima glasanja već samo prate regularnost izbornog proces. Kod ovog tipa glasanja osim toga što se glasanje izvodi upotrebom elekronskog uređaja nema razlike u odnosu na tradicionano glasanje. Glasač nema nikakvu drugu autonomiju u toku glasanja, kao ni mogućnost glasanja sa udaljene lokacije.

Postoje različiti načini organizacije elektronskog glasanja u zavisnosti od vrste elektronskog glasanja koju je potrebno organizovati. Ovi načini poznati su kao šeme glasanja. Svaka od šema predstavlja niz algoritama na osnovu kojih se sprovodi proces e-glasanja. Takođe šeme definišu i niz pravila i protokola kojima se definiše kako će elektronsko glasanje biti obavljeno. Same šeme grupisane su prema metodama na kojima je se zasniva kreiranje, prenos, snimanje i obrada e-glasova, kao i po tome na koji način je organizovana identifikacija glasača[195].

- Miks-net šema. Ova šema predstavlja kriptografsku primitivu čija je namena da oformi komunikacioni kanal koji će pružiti osobinu anonimnosti, slično osobini nedodirljivog komunikacionog kanala, između dve krajnje tačke. Ova mreža se sastoji od povezanog niza elektronskih uređaja (miks-eva) sa ciljem da obezbede anonimnost pošiljaoca poruke. Postoji veći broj vrsta i načina korišćenja mix-net šema, ali sve one dele isti koncept i određena zajednička svojstva. U prvom koraku učesnici u anonimnoj komunikaciji šalju svoje kriptovane poruke do miks servera. Nakon što primi određeni broj poruka ovaj server menja redosled pristiglih poruka na slučajan način i šalje ih dalje. Upravo iz ovog razloga i nosi naziv miks server. Svaki sledeći server na koji poruke tokom svog puta do odredišta naiđu će uraditi isti postupak promene redosleda poruka. Proces miksovanja se u osnovi sastoji od dva koraka. U prvom koraku će se pristigle poruke obrađivati kriptografskim algoritmom u zavisnosti od tipa miksovanja. U drugom koraku ide spomenuto nasumično mešanje poruka. Kada poruka izađe iz miks oblasti, ona će do primaoca doći u potpuno čitljivom obliku. Na ovaj način je sakrivena veza između ulaznih i izlazni poruka, dok sadržina poruke ostaje nepromenjena.
- Šeme sa homomorfnim kriptovanjem. Metod homomorfnog kriptovanja ogleda se u postojanju algebarske operacije nad šifratima koja za posledicu ima algebarsku operaciju nad polaznim čitljivim podacima. Sama vrsta ovih algebarskih operacija zavisi od kriptografskog algoritma. Kod homomorfnih šema za e-glasanje, glasač

[195]Pilipović, D., Starčević, D., „Pregled šema za elektronsko glasanje“, Info M, Broj 51, str. 19-25, 2014.

kriptuje svoj glasački listić javnim ključem izborne komisije, a nakon toga glas se šalje izbornoj komisiji u virtuelnu glasačku kutiju. Nakon toga izborna komisija obrađuje sve glasačke listiće odjednom ne proveravajući njihov sadržaj. To praktično znači da ako korišćeni kriptografski sistem ima osobinu aditivnog homomorfizma, izborna komisija će uraditi sabiranje kriptovanih glasačkih listića. Pošto je sada zbir glasačkih listića kriptovan, potrebno je da izborna komisija svojim privatnim ključem skine enkripciju i onda objavi rezultat u javnosti. Na ovaj način je zadržana privatnost glasača jer ni jedan glasački listić nije prebačen u čitljivu formu, već je od svih glasačkih listića izračunat zbir dok su još u kriptovanom stanju. Dekriptovan je samo zbir koji je sam po sebi anoniman.

- Šeme zasnovane na potpisu na slepo. U ovako organizovanoj komunikaciji predajnik i prijemnih koriste zajednički entitet pomoću koga se poruka prenosi. I predajnik i prijemnik imaju poverenja u pomenuti entitet koji im obezbeđuje sigurnost u komunikaciji. U ovoj šemi postoje četiri modula: registrator, virtuelno glasačko mesto (eng. pollster), validator i brojač. Registrator je odgovoran za registraciju birača pre početka glasanja. Virtuelno glasačko mesto pomaže biraču da završi sve računske i ostale proceduralne korake. Validator će proveriti da li je birač stvarno registrovan i onemogućiti dvostruko glasanje. Brojač će prikupljene glasačke listiće prebrojati i tako dobiti izborni rezultat.
- Šeme zasnovane na biometriji. Šeme za e-glasanje zasnovane na biometriji glasača koriste biometrijske karakteristike za identifkaciju glasača. Ovo je od velikog značaja naročito kod udaljenog tipa e-glasanja, jer predstavlja dosta dobar način da se utvrdi da na udaljenom mestu, sa druge strane veze, stoji upravo osoba koja se tako predstavlja[196]. Biometrijski sistemi za identitetsku proveru glasača analiziraju njegove fizičke karakteristike, ali i karakteristike ponašanja. Da bi neke ljudske karakteristike kvalifkovali kao biometrijske, one moraju biti univerzalnog tipa, jedinstvene, nepromenljive (vremenski i prostorno) takođe one moraju biti merljive. Najpoznatija fizička karakteristika u biometriji je otisak prstiju, koja se čak uspešno koristila i pre početka elektronske obrade u policijskom radu. U ostale biometrijske karakteristike mogu se ubrojiti izgled oka, crte lica, otisak šake, itd. Neke od karakteristika ponašanja su potpisivanje, način govora, dinamika hoda itd. Krajnja biometrijska karakteristika, koja bi bila odlična po mnogim osobina, je analiza DNK lanca osobe, ali ona još uvek nije dovoljno jeftina i jednostavna za implementaciju. Dva pokazatelja koja se najčešće koriste za prikazivanje preciznosti su FRR i FAR. FRR (false rejection rate) predstavlja procenat pogrešnog odbijanja biometrijskog sistema u odnosu na ukupan mogući broj uspešnih provera identiteta. Pogrešno odbijanje se događa kada pravog glasača biometrijski sistem ne prepoznaje zbog nedovoljnog podudaranja ulaznih biometrijskih podataka sa podacima u bazi podataka svih glasača, te mu tako pogrešno odbije identifkaciju. FAR (false acceptance rate) predstavlja procenat pogrešnog prihvatanja biometrijskog sistema u odnosu na ukupan mogući broj pokušaja sa nevalidnim biometrijskim podacima. Pogrešno prihvatanje se događa

[196]Paunović, S., „Biometrijski sistemi za utvrđivanje identiteta“, Međunardna konferencija i izložba Infotech 2013, Aranđelovac, Srbija., 2013.

kada lažnog glasača biometrijski sistem prepoznaje kao pravog glasača, na osnovu biometrijskih podataka u bazi podataka koji su slični ulaznim biometrijskim podacima. Kod e-glasanja postoje dva slučaja pogrešnog prihvatanja. U prvom slučaju, lažni glasač koristi tuđe pravo glasa. drugom slučaju glasača prepoznaju kao neku drugu osobu, ali takođe sa pravom glasa. Ovaj glasač nije oštećen po pitanju prava glasa, ali će druga osoba za koju je zamenjen biti pogrešno odbijena.

Celokupna organizacija e-glasanja nije ni malo lak posao. Sama činjenica da je potrebno akcenat staviti na udaljeno glasanje dodatno komplikuje celi proces. Takođe veći broj vrsta kao i šema elektronskog glasanja dodatno otežavaju proces odabira istih prilikom kreiranja sistema e-glasanja. Kako bi se kreirao najefikasniji sistem za potrebe e-glasanja zasnovanog na odabiru najefikasnije vrste i šeme e-glasanja u tu svrhu mogu se upotrebiti različiti okviri (framework). Cilj framework-a je da se kroz njega ispita ceo proces e-glasanja kao i da se na taj način uoče eventualni nedostaci koji bi mogli uzrokovati neuspeh u poslednjih fazama izbora. Postoji veći broj framework-a koji su se razvijali zajedno sa procesom razvoja e-glasanja.

TAM (Technology Acceptance Model) framework– zasniva se na teoriji da verovanja utiču na stavove pojedinaca, pa je i njihovo ponašanje određeno tim veorvanjima. U ovom framework-u izvajaju se dve determinante kojima je ponašanje pojedinaca određeno. Prva determinanta predstavlja predviđenu korist na osnovu koje pojedinac dobija informaciju na koji način će nova tehnologija uticati na povećanje njegovih dostignuća. Druga determinanta predstavlja predviđenu lakoću usvajanja nove tehnologije, kao i koliko će nova tehnologija biti shvaćena kao olakšanje života i rada. Ovakav framework ima puno širu primenu, i na taj način e-glasanje je samo jedan od domena. Praktično ovim framework-om može se posmtrati uvođenje bilo koje nove tehnologije namenjene korišćenju od strane širokih narodnih masa.

TOE (Technology Organization Environment) framework – zasniva se na ideji da sami proces impelmentiranja i prihvatanja novih tehnoloških inovacija zavisi od udruženih konteksta tehnologije, organizacije i samog okruženja. Kroz ova tri skupa faktora framework u isto vreme definiše kako ograničenja tako i mogućnosti za tehnološke inovacije.

EKD (Enterprise Knowledge Development) framework – zasniva se na modelovanju tri oblasti: organizacionih ciljeva, fizičkih procesa, i na kraju softverskog sistema koji sadrži prve dve stavke. Ovo praktićno znači da će prosec razvoja krenuti od samog modelovanja cilje, preko procesa pa do finalnog softvera. Na ovakav način procesi se modeluju na osnovu unapred definisanih ciljeva, dok se softver modeluje na osnovu ciljeva i procesa. Ovakv princip omogućava evaluaciju sistema u svakoj od fazi modelovanja. Celokupan proces mora biti ispraćen adekvatnim dokumentovanjem.

ANT (Actor Network Theory) framework – zasniva se na ideji da je mrežna teorijska postavka most između tehnoloških i društvenih mreža. Ovakva veza mora biti uzeta sa svim prednostima koje donosi, ali u isto vreme i sa svim manama. Tehnološke mreže odlikuju se nepostojanjem ljudskih entiteta, i zasnovanošću na radu baza podataka, servera, računarskih komponenti. S dtuge strane kod društvenih mreža obrnut odnos. Svaka mreža prema ovom framework-u može biti globalna i lokalna, a

sve funkcionalnosti između njih se zovu posrednici. Ako se ovaj framework posmatra kao crna kutija onda je on apstraktna teorija ili konkretna tehnologija čija pripadajuća mreža aktera nije vidljiva. Sa procesom stavljanja nečega u crnu kutiju idu zajedno fenomeni kompozicije, translacije i delegacije.

Sami proces modelovanja i kreiranja protipova sistema koji se mogu testirati i evaluirati jako je bitan i predstavlja napor u razvoju rešenja za e-glasanje. Potrebno je razumeti sve potrebe naručilaca i krajnjih korisnika softverskog podsistema za e-glasanje, pa se zbog toga izrada prototipova nudi kao odličan pristup. Korisnici (organizatori e-glasanja, birači) softvera za e-glasanje često su odlični u komentarisanju i kritikovanje prototipskih modela softvera, dok sve apstraktnije od toga nije zanimljivo za većinu njih. Prototipovi softvera poboljšavaju komunikaciju između korisnika i developera softverskog rešenja. Uključujući korisnike u izradu prototipova dobijaju se upućeni korisnici u budući rad softvera, kao i entuzijazam kod usvajanja novog softverskog rešenja. Sve su to kritične i bitne polazne osnove za izradu softverskog podsistema za e-glasanje kao najvažnijeg dela za realizovanje atributa „elektronsko“ kod e-glasanja.

Sistemi za e-glasanje datiraju još od vremena bušenih kartica tačnije od 1965. godine kada su se pojavili prvi sistemi za glasanje nalik e-glasanju zasnovani na bušenim karticama. Kreirani su kao prirodni nastavak glasačkih listića od papira a trebali su da olakšaju i ubrzaju celi proces glasanja. U Sjedinjenim Američkim Državama se ovakav sistem koristio od 1965. godine pa čak sve do 2000. godine, kada se desio poznati problem u prebrojavanju glasova za predsedničke izbore u državi Floridi[197]. Prvobitno su to bile *Votomatic* mašine licencirane od strane *IBM*-a, a kasnije su došle njihove kopije[198]. Moglo bi se reći da su ove mašine bile začetnici elektronskog glasanja, ali samo u slučaju kada je bušene kartice sa glasovima prebrojavao elektronski sistem povezan sa računarom.

Sistem sa optičkim skeniranjem počeo je sa korišćenjem šezdesetih godina prošlog veka u SAD. Glasački listići su popunjavani na uobičajen način a prebrojavanje se izvodilo ubacivanjem u uređaj koji je optičkim senzorom prepoznavao kako je listić popunjen. I dalje su upotrebi, npr. na predsedničkim izborima 1996. u SAD je ovakav sistem koristilo oko 25% registrovanih glasača[199]. Glasač na optičkom skeneru mora da ili spoji dve tačke ili da svoj glas unese popunom odgovarajućeg polja. Što se tiče sistema bojanja glasova, mogu se razlikovati da metoda brojanja. Prvi metod je centralno orijentisan, dok se kod drugog metoda glasovi broje na biračkom mestu. Kod centralanog metoda brojanja, nakon glasanja svaki od glasova se prosleđuje u centralni registar gde se vrši samo brojanje glasova. Na ovakav način glasač nema povratnu informaciju o tome koji je rezultat glasanjau momentu glasanja. Što se tiče obrade glasova na biračkom mestu u ovom metodu odmah nakon glasanja glas se obrađuje i

[197]Federal Election Commision, Punch Card Voting Device, Available on: http://www.fec.gov/pages/punchrd.htm, date: 12.01.2017.
[198] Pilipović, D., „Pregled šema za elektronsko glasanje“, Opus citatum.
[199]Bellis, M., „The History of Voting Machines“, online article, Available on: http://inventors. about. com/library/weekly/aa111300b.html,

glasač dobija informaciju o tome da li je pre svega njegov glas evidentiran i koji je trenutni rezultat glasanja. Na ovakav način glasač može dobiti informaciju ukolko je došlo do greške u glasanju. U ovakvim slučajevima kada dođe do neke greške glasaču se daje mogućnost da opet glasa. Ovo je upravo možda i glavna prednost brojanja glasova na biračkom mestu u odnosu na brojanje u centralnom registru. Što se tiče optičkih šema elektronskog glasanja postoji nekoliko šema koje su u upotrebi. Neke od njih su SureVote, Pret-a-Voter, Scratch&Vote, Punchscan, Scantegrity i ThreeBallot. Svaka od njih sami proces glasnja kao i brojanja glasova obavlja ne određeni i unapred definisani način. Primera radi Pret-a-Voter razdvaja glasački listić u dva dela. Na levom delu listića imena kanditata, dok se na desnoj strani nalaze prazna polja. Prazno polje služi kako bi glasač uneo svoj izbor.

Scratch&Vote šema elektronskog glasanja slična je Pret-a-Voter šemi. Razlika između ove dve šeme je u tome što se na desnoj strani nalazi barkod i površina za grebanje. Nakon obavljenog glasanja glasač predaje desni deo listića izbornoj komisiji koja se nalazi na mestu glasanja. Zadatak komisije je da pogleda stanje u kome se nalazi površina za grebanje. Ukoliko je površina netaknuta to znači da je listić validan. Nakon utvrđivanja validnosti glasačkog listića, pomenuta površina se uklanja i glasač skenira bar kod koji se nalazi ispod zaštite. Nakon uspešno obavljenog skeniranja glasač ubacuje deo listića sa markerom dok levi deo zadržava za sebe.

U Punchscan šemi elektronskog glasanja glasački listić sastavljen je iz dva dela. Ovoga puta listić je podeljen horizontalno na gornji donji deo. Na gornjem delu glasačkog listića nalaze se imena glasača i pridruženi kod. Na donjem delu nalaze se svi kodovi kao i na gornjem delu samo što su ovog puta dati u naizmeničkom redosledu. Druga strana glasačkog listića sadrži samo donji deo. Na prvoj strani na delu koji se preklapa postoji rupa.

Scantegrity je šema kreirana je tako da daje skup poboljšanja u odnosu na Punchscan šemu elektronskog glasanja. Kod ove šeme na glasačkom listiću nalazi se ime kandidata i kod koji je raspoređen u naizmeničnom poretku. Prilikom glasanja, a nakon markiranja polja uz kandidata za koga se glasa glasač vrši skeniranje gornjeg dela glasačkog listića na optičkom skeneru. Na donjem delu listića nakon dobijene informacije o uspešnom skeniranju glasač upisuje jedinstveni kod svog kandidata na donji deo listića koji zadržava za sebe. Na kraju izbornog dana objavljuju se lista glasačkih listića, serijski broj i kod listića. Na osnovu ove liste glasač može da proveri da li je njegov glas regularno upisan ili je došlo do manipulacija glasovima. Glasaču je ostavljena mogućnost da podnese zalbu izbornoj komisiji ukoliko njegov glas nije pravilno upisan. Problem koji se ovde javlja jeste u tom slučaju glasač izbornoj komisiji mora da otkrije svoj izbor kandidata za koga je glasao. Na ovakav način narušava se osnovni princip glasanja a to je tajnost glasanja.

ThreeBallot je jedinstveni glasački sistem bez implementiranih kriptografskih zaštitnih mehanizama. Sistem glasanja zasnovan je tako da glasač dobija tri glasačka listića sa jedinstvenim identifikatorom. Kako bi uspešno glasao glasač mora da označi polja pored imena svog kandidata na dva listića dok na trećem mora da označi sve kandidate za koje neće da glasa tako da jedino pored njegovog kandidata ostane

neoznačeno polje. Nakon procesa označavanja glasač je u obavezi da skenira sva tri listića. Ukoliko je proces skeniranja završen validno glasač dobija povratnu informaciju o tome da li su ili nisu listići označeni na pravi način. Ukoliko je celi proces prošao validno glasač uzima jedan tri listića kao dokaz o uspešno izvršenom glasanju. Zapravo kao sami dokaz on ne dobija konkretan listić već njegovu kopiju. Kao i u prethodnim šemama glasanja na kraju izbornog dana objavljuje se spisak svih glasačkih listića u cilju provere regularnosti brojanja.

EVM (Electronic Voting Machine) se sastoji se od dva dela povezana dugačkim kablom. Prvi deo se nalazi u glasačkom prostoru i na njemu se nalazi niz tastera pored odštampane liste stranaka ili kandidata. Drugi deo je kod predsednika izborne komisije i on dozvoljava svakom biraču da iskaže svoje preference, te se onda tu skupljaju glasovi[200].

DRE (Direct Recording Electronic) uređaji su elektronski uređaji kreirani u svrhu realizacije elektronskih izbora. Ovi uređaji postavljaju se na lokacijama koje su definisane pre samih izbora i koje predstavljaju glasačka mesta. Glasački listić ovog puta dat je u virtuelnoj reprezentaciji na ekranu uređaja, tako da se celokupni proces obavlja virtuelno. Svaki ovako kreirani virtuelni glas se pamti u memoriju ovog uređaja. Na ulazu ovog uređaja za potrebe glasanja mogu se nalaziti posebno dizajnirani tasteri, numeričke tastature, dok se kao standardni izlaz koriste ekrani, zvučni signali i glasovna obaveštenja. Sa razvojem tehnologije i upotrebe pametnih uređaja DRE uređaji razvijeni u kombinaciji sa ekranom osetljivim na dodir, pa se pomoću ovog ekrana obavljaju i ulazne i izlazne funkcije. Proces glasanja obavlja se tako što glasač na dan glasanja dolazi na izborno mesto, i nakon provere podataka od strane komisije glsača bira svoju opciju i informacija o odabranom kandidatu se smešta u memoriju uređaja. Kao i u pretodnim slučajevima kad se radi o centralnom načinu brojanja glasova na kraju izbornog dana, sa DRE uređaja se dobija rezultat izbora. Ukoliko je DRE uređaj postavljen lokalno bez povezivanja sa centralnom bazom memorija na kojoj su smešteni rezultati glasanja mora biti uklonjena iz uređaja nakon završenog glasanja. Ukoliko jedno glasačko mesto zahteva veći broj ovakvih uređaja obično se nakon završenog glasanja memorije sa svih uređaja stavljaju u jedan DRE uređaj koji će vršiti sumiranje glasačkih listića i generisanje rezultata izbora. Prva zemlja koja je krenula ozbiljno u upotrebu ovih uređaja je SAD, te je od 1980. godine prvi put dostupnost prešla 1% da bi se povećavala za duplo svakih četiri godine (izuzev 1992. kada procent ostao skoro isti) i tako na predsedničkim izborima 2012. taj procenata je iznosio oko 40% birača[201]. Druga zemlja koja se posebno ističe je takođe sa američkog kontinenta. U pitanju je Brazil koji je prvi put uveo DRE uređaje na izborima 1996. godine za trećinu glasača, dve godine kasnije za dve trećine glasača i od 2000. godine pa na dalje izbori idu u potpunosti preko spomenutih uređaja[202].

[200] Election Comission of India, FAQs – Electronic Voting Machine, Available on: http://eci.nic.in/eci/eci.html, date: 10.01.2018.

[201] ProCon.org, Voting Systems & Use: 1980-2012, Available on: http://votingmachines.procon.org/view.resource.php?resourceID=000027, date: 12.09.2016.

[202] Brunazo. F., „Computerization of voting in Brazil“, Available on: http://noleakybuckets.org/brasil-history.html, date:12.01.2017.

Slično stanje je u susednoj Venecueli[203]. U Belgiji se ovim uređajima koristi oko 45% glasača za sve nivoe i vrste izbora: gradske, regionalne, federalne i evropske. Slično je u Francuskoj, ali u kojoj se procenat korišćenja može promeniti od izbora do izbora jer lokalne izborne komisije mogu da upotrebe ili ne upotrebe DRE mašine što one autonomno odlučuju. Izborne komisije biraju sa liste sertfikovanih uređaja[204]. U Finskoj se zbila zanimljiva kombinacija udaljenog Internet glasanja i upotrebe DRE uređaja 2008. godine za tri opštine. Probna glasanja za manja područja su se odigrala takođe u Italiji i Norveškoj, dok su se u Kazahstanu koristili belaruski uređaji u tri navrata za izbore na nivou cele države. U Kanadi ne postoji standard za e-glasanje na nivou države, ali se za razne forme e-glasanja odlučuju pojedini gradovi i provincije[205].

O uvođenju elektronskog glasanja u izborni sistem Republike Srbije kao i u izborni sistem zemalja okruženja pokreću se razne inicijative u poslednjih nekoliko godina. Jedna od inicijativa u Republici Srbiji bilo je uvođenje e-glasanja putem web aplikacije na sajtu Republičke izborne komisije. Ideja je bila da se u okviru aplikacije glasač identifikuje preko imena i prezimena, matičnog broj i šifre. Ovakav sistem još uvek nije zaživeo kako na lokalnom tako ni na nivou cele države. Da bi e-glasanje zaživelo, potrebno je celokupan posao uraditi tehnički i bezbednosno perfektno, a još važnije je izgraditi poverenje građana da institucije svoj posao obavljaju nezavisno i profesionalno. Takođe, ako ne dođe do promene u funkcionisanju administracije i RIK-a (Republička izborna komisija), ne može se govoriti da će Srbija moći da implementira digitalno glasanje[206].

Slična inicijativa uvođenje e-glasanja u BiH pokrenuta je kako bi se na lokalnim izborima sproveo pilot projekat na reprezentativnom i statistički relevantnom broju. Međutim, prepreke već u startu postoje. Što se tiče uvođenja elektronskog glasanja na svim biračkim mestima, tu bi mogao nastati problem s obzirom na to da će za to biti neophodno obezbediti najmanje 20 miliona KM. Prema nekim istraživanjima opremanje biračkog mesta za potrebe elektronskog glasanja, zavisno od modela e-glasanja, koštalo bi od tri do šest hiljada KM. Ukoliko se cena opremanja jednog biračkog mesta pomnoži sa ukupnim brojem birališta dobija se ukupna cifra koja iznosi između 15 i 30 miliona KM. Iako je cena previsoka izračunavanja pokazuju da bi se uloženi novac delom vratio već nakon prvih izbora organizovanih na taj način. Ako se pogledaju finansijski aspekti uvođenjem elektronskog sistema glasanja, umesto

---

[203] Embassy of the Bolivarian Republic of Venezuela to the U.S (2012). The Venezuelan VENEZUELA'S 2012 PRESIDENTIAL ELECTIONS - A model of transparency and democracy, Available on: http://venezuela-us.org/live/wp-content/uploads/2009/08/08-31-12-FS-Elections-2012-Long.pdf, date: 12.01.2018.

[204] Jordi Barrat i Esteve, Ben Goldsmith and John Turner, „International Experience with E-Voting", International Foundation for Electoral Systems (IFES), 2012.

[205] Laronde, P., „Technologies in the Voting process: An Overview of Emerging Trends and Initiatives (Research Note)", Available on: http://www.elections.ca/content.aspx?section=res&dir=rec/tech/note&document=index&lang=e, date: 18.01.2018.

[206] Nenad Zorić, „Elektronsko glasanje u Srbiji, realnost ili fantastika", Dostupno na: https://rs.sputniknews.com/komentari/201704071110672860-sve-o-elektronskom-glasanju1/, datum pregleda: 01.02.2018.

biračkih odbora, na biračkim mestima bi bilo potrebno samo tehničko osoblje. Na ovakav način smanjenje izdataka u domenu ne plaćanja biračkih odbora iznosilo bi oko oko 4.500.000 KM po izbornom ciklusu[207].

4.1.2 Elektronska participacija (e-participacija)

E-participacija predstavlja novi komunikacioni kanal kreirna radi lakšeg i efikasnijeg uključivanja građana u demokratske procese. Postoji veći broj definicija e-participacije. Generalno posmatrano e-participacija se može definisati kao interakcija između građana i političkog sektora ali i između građana i administrativnog sektora vlasti, bazirana na upotrebi ICT. Na ovakav način cilj je uključiti građane u politički proces putem određenih umreženih softvera, prvenstveno preko Interneta. E-participacija može uključiti građane različitog profila, a njen potencijal za promenu tekućeg stanja je veliki. Smer učešća može da krene od vrha (top-down pristup), što je inicijativa od strane državnih organa, ali i odozdo (bottom-up pristup), gde se građanski sektor angažuje da dopre do pojedinih administrativnih sektora.

Zainteresovane strane za učešće u procesu e-participacije nalaze se na različitim novima vlasti i građana. U sami proces interakcije putem e-participacije obično su uključeni političari, ministri, narodni poslanici, državna uprava i agencije, nevladine organizacije i udruženja građana. Nije retkost da se u domen e-participacije uključi i privredni sektor. Bilo kako bilo najvažniji korisnici e-participacije trega da budu građani. E-participacija kao takva treba građanima da omogućiti veće učešće u digitalnom društvu i vlasti kroz učestvovanje u političkim procesima i transformaciji vladinih servisa u digitalne servise.

S obzirom da e-participacija predstavlja deo e-demoktarije i s obzirom na činjenicu da učesnici e-participacije mogu biti različiti i u sklopu e-participacije mogu se izdvojiti različite interakcije.

- G2C (government-to-citizen) interakcija se ostvaruje ukoliko se e-participacija posmatra kao javni proces koji treba realizovati pomoću ICT rešenja i na taj način ista ponuditi građanima na slobodnu upotrebu,
- G2E (government-to-education) interakcija predstavlja proces u kome građane treba ohrabriti i osposobiti kako bi aktivno učestvovali u elektronskim procesima.
- C2G (citizen-to-government) interakcija nastaje ako inicijativa potiče od građanstva, a u proces komunikacije su pored građana uključeni i predstavnici vladinog sektora i javne uprave.
- C2C (citizen-to-citizen) interakcija predstavlja upotrebu ICT servisa sa ciljem omogućavanja međusobne rasprave ili dogovora između građana.

[207] Nezavisne novine, „Elektronsko glasanje krupan zalogaj za BiH“ Dostupno na: https://www.rtvbn.com/377696/Elektronsko-glasanje-krupan-zalogaj-za-BiH, datum pregleda: 1.02.2018.

Posmatrano iz ugla ICT razna rešenja se mogu izdvojiti u cilju kreiranja i korišćenja e-participacije. U ovu svrhu mogu se izdvojiti razne vrste aplikacija, web orijentisanih servisa, softvera složenijeg domena kao i softverskih dodatka. Bilo kako bilo svi ovi servisi su tu radi kreiranja efektivnog i efikasnog kanala za komunikaciju između državnih ustanova, ostalih organizacija i pre svega građana. Bitno je napomenuti da je akcenat na umrežavanju građanstva putem računarskih mreža gde celokupan saobraćaj i prenos podataka ide preko TCP/IP javne mreže. Softverska platforma koristi ICT kanale da dopre do svih aktera u komunikaciji kako bi u proces participacije uključila njihova stanovišta i uopšte neposredno komunicirala sa njima radi njihovog učešća u procesu grupnog odlučivanja. Dodatno, ovakvi softveri čuvaju, obrađuju i prikazuju podatke koje su dobijeni na taj način za interne potrebe. Ovde spadaju vesti, blogovi, forumi, GiS odeljci, itd. U principu rešenja koja imaju veću sadržinsku vrednost za sami proces e-participacije su sledeća:

- ePanel – web aplikacija koja okuplja odabranu grupu eksperata i aktera da bi izrazili stavove o temi u ograničenom vremenskom intervalu.
- ePeticije – oblik peticije koja se nalazi na web sajtu ili portalu i koju potpisuju građani samostalno imenom i sopstvenom adresom e-pošte ili preko autorizovanog modula. Ovakve peticije mogu postavljati i sami građani a rezultat se šalje ciljnom adresantu e-poštom.
- eKonsultacije – način promišljanja, savetovanja i traženja rešenja sa građanima kroz intezivnu interakciju u kojoj oni daju formalni odgovor na postavljeno pitanje o aktuelnoj temi, za šta dobijaju potvrdu o izboru. Ovakav vid e-participacije se može posmatrati kao dopuna klasične javne rasprave licem u lice.

Postoje brojne rasprave o tome koliki će biti krajnji uticaj ICT u bližoj ili daljoj budućnosti na kvantitet i kvalitet učešća građana u političkim procesima. S jedne strane određeni broj analitičara predviđa da će e-participacija zadobiti veće poverenje građana nego njena offline varijanta u vidu papirnih anketa i intervjua. Takođe zagovornici ove ideje tvrde da će sve većim i većim učešćem građana u procesu e-participacije doći do transparentne i odgovorne vlasti. Uz to, doći će do formiranja stabilnih online zajednica koje će veoma uticati na društvo. Sa druge strane, protivnici ove ideje tvrde će takav neposredan uticaj e-građana dovesti do preterane žurbe u procesu odlučivanja, ispoljiće se psihologija mase, a gomila poluistina, dezinformacija i spinova će uništiti razuman politički dijalog. Međutim jedno je sigurno a to je da e-participaciju ne treba posmatrati kao samo čisto tehničko, brzo i jeftino rešenje, jer će se tako iz vida izgubiti globalna slika društvenog vladanja i pravednosti.

4.2 Elektronska uprava (e-Uprava)

Servisi elektronske uprave u okviru javnih privrednih društava i državnih organa uvode se kako bi u mnogim sferama društva olakšali poslovanje, ubrzali proces razmene informacija i smanjili potencijalne troškove. Ovakvi servisi trenutno su zastupljeni do nivoa lokalnih samouprava i aktivno se radi na njihovom popularizovanju i široj upotrebi od strane ljudi kojima su namenjeni. Koncept e-Uprave radi na uvođenju elektronskih usluga koje su usmerene ka zadovoljenu potreba fizičkih i pravnih lica. Ovako koncipirane usluge trebalo bi da budu infiltrirane u svaki segment javnog sektora. Samim uvođenjem elektronskih servisa e-Uprave javne službe imaju efikasniji, transparentniji i odgovorniji odnoso prema potrebama građana i privrede. Posmatrano iz ugla državnih ili vladinih organa i agencija uticaj ICT odrazio se na nova softverska rešenja koja su u upotrebi u procesu komunikacije kako između pojedinačnih vladinih sektora tako i između vladinih sektora i građana. Vladini sektori koji koriste ovakve servise jednim imenom se nazivaju e-vlada ili e-uprava. E-uprava generalno posmatrano predstavlja transformaciju unutrašnjeg i spoljašnjeg javnog sektora kroz upotrebu ICT u cilju optimizacije dostupnosti vladinih servisa građanima. Ukoliko se e-Uprava posmatra kroz digitalno društvo može se krenuti od pojašnjenja istog. Digitalno društvo je društvo ili zajednica koja je napredovala u usvajanju i integraciji digitalne tehnologije u svakodnevni život i rad kod kuće. Upravo sa te strane posmatrano, e-Uprava predstavlja razvoj i primena politike, zakona i propisa neophodnih za podršku funkcionisanja društva, kao i e-vlade. Pojam e-Uprave ima korene u pokušajima mnogih zemalja da modernizuju vladin sektor kao odgovor na osećaj nezadovoljstva građana[208]. Kao takva e-Uprava se može posmatrati kao upotreba ICT tehnologija od strane vlade sa ciljem unapređenja dostupnosti servisa i informacija, ohrabrenja građanja ka njihovom aktivnom učešću u procesu donošenja odluka, kao i kreiranja odgovornijih, transparentnijih i efikasnijih vladinih sektora. U ovom procesu kao akteri mogu se izdvojiti tri glavne strane: vlada, fizička lica (građani) i pravna lica (privreda). Posao ICT tehnologija primenjenih u sklopu elektronskih servisa e-Uprave jeste da poveže ove tri strane, s toga se mogu izdvojiti sledeći poslovni modeli e-uprave[209]:

- Government-to-Government (G2G) model se odnosi na komunikaciju između različitih nivoa i organizacija javne administracije i uprave. Primera radi u ovaj model može se svrstati komunikacija između lokalne samouprave i nadležnih ministarstava, saradnja policija različitih država u okviru Interpola, itd.
- Government-to-Citizen (G2C) model se odnosi na usluge različitih državnih organa prema građanima. U ovaj model spada izdavanje ličnih dokumenata, prijava poreza, vađenje različitih uverenja, itd.

[208] Oakley K, „What is e-governance?“, Integrated Project 1: e-Governance Workshop, Strasbourg, 2002.

[209] Kalinić Z., Ranković V. „Razvoj e-uprave na lokalnom nivou – Ocena sadašnjeg stanja i mogućnosti unapređenja”, Tematski zbornik: Stanje i perspektive ekonomskog razvoja grada Kragujevca, Univerzitet u Kragujevcu-Ekonomski fakultet, str. 365-383, 2014.

- Government-to-Business (G2B) model se odnosi na komunikaciju između javne admistracije ili državnih službi sa jedne strane i poslovnih subjekata ili organizacija sa druge strane. U ovaj model spada registracija privrednog društva, prijava i odjava radnika, plaćanje poreza, itd.
- Government-to-Employee (G2E) model se odnosi na komunikaciju i servise koje državni organi pružaju svojim zaposlenim, u cilju unapređenja poslovanja.

Servisi e-Uprave kreirani za potrebe komunikacije između pomenuta tri aktera moraju obezbediti određeni nivo sigurnosti zavisno od nivoa upotrebe ličnih podataka korisnika. Takođe pored implementiranog stepena zaštite podataka servisi moraju raditi na odgovarajući način i moraju biti intuitivni za korišćenje. S obzirom da su ovi servisi a posebno G2C servisi veoma često u upotrebi od strane ljudi različitog nivoa poznavanja ICT oni se moraju implementirati tako da prosečan korisnik može neometano da ih koristi.

Evropska komisija definiše e-upravu kao skup alata i sistema koji uz pomoć informaciono komunikacionih tehnologija omogućavaju bolje javne usluge stanovništvu i privrednim društvima. U Evropskoj komisiji se pod e-upravom podrazumeva struktura koja koristi digitalne alate i sisteme da bi pružila bolje usluge stanovništvu i privrednim društvima. Na nivou Evropske unije usluge koje se pružaju kroz e-upravu omogućavaju ljudima da se slobodnije kreću (iz poslovnih ili privatnih razloga) i da efikasnije obavljaju poslove iz domena javnih usluga van matičnih zemalja[210]. Modeli e-Uprave se razlikuju od regiona do regiona i svaki od njih se treba prilagoditi specifičnim potrebama vlade i građana za koje se kreira. Na primer e-Uprava će biti različita u Nemačnoj, Mađarskoj ili USA. Sami procesi kreiranja će biti slični ali normativi, pretpostavke od kojih se kreće sa izradom servisa kao i razvojna strategija će se veoma razlikovati. Svi servisi e-Uprave sagledani u ovom istraživanju su online servisi, jer moraju biti dostupni građanima 24 časa dnevno. Korišćenje u realnom vremenu obezbeđuje korisnicima prenosivost i vremensku nezavisnost upotrebe ovih servisa. Kao i većina zemalja i Republika Srbija poseduje portal e-Uprave putem koga su građanima i kompanijama obezbeđeni različiti elektronski servisi. Kako bi koristili servise e-Uprave korisnici portala moraju kreirati korisnički nalog i/ili koristiti digitalne sertifikate u cilju autentifikacije. Pojedini servisi zahtevaju upotrebu oba načina autentifikacije kako bi korisnik mogao da ih koristi.

Autentifikacija korisnika na portalu e-Uprava putem korisničnog naloga zahteva kreiranje istog. Ukoliko se budući korisnik odluči za ovakav način autentifikacije korisnički nalog se kreira popunjavanjem registracione forme. Pored osnovnih polja sličnih većini registracionih formi ove forme sadrže i polje za unos javnog matičnog broja građana. Ovaj broj je bukvalno jednini osetljiv podatak o budućem korisniku. Na osnovu ovog broja sistem prikuplja podatke o korisniku i iste upoređuje sa podacima koje je korisnik uneo u okviru registracione forme. Posle uspešne registracije korisnik mora izvršiti verifikaciju i aktivaciju svog naloga putem linka koji dobije na svoju

[210] eGovernment & Digital Public Services, European Commission, Information Society Portal. Available at: http://ec.europa.eu/information_society/activities/egovernment/ index_en.html, date: 27.10.2017.

email ardesu. Ovakvim načinom registracije korisnika portal zadržava pravo prikupljanja i obrade informacija o svojim korisnicima. Informacije koje se najčešće prikupljaju su ime domena sa koga je pristupano kao i vremenski parametri pristupa. Kako bi se izvršila adekvatna zaštita portala e-Uprava sav saobraćaj ka ovom portalu se prati. Na ovakav način se sprečava svaki mogući napad usmeren protiv portala ili računarskog sistema na kome portal radi.

Autentifikacija putem digitalnih sertifikata kao što je i ranije napomenuto zahteva upotrebu dodatnog hardvera u formi čitača lične karte ili dodatne kartice u zavisnosti od izdavaoza sertifikata. U trenutku kada proces logovanja počne čitač kartica mora biti povezan sa uređajem sa koga se vrši logovanje, i kartica mora biti ubačena u čitač. Prednost ovakvog načina autentifikacije je veća sigurnost korisničkih podataka sa kojima sistem operira. Sa druge stane mana ovakvog načina logovanja su dodatni troškovi korisnika u vidu kupovine čitača kartice i digitalnog sertifikata. Ovakav komad hardvera i softvera predstavlja električni pasoš koji omogućava osobama, računarima ili organizacijama da razmenjuju informacije sigurno putem mreže korišćenjem već pomenute PKI infrastrukture.

Svi servisi portala e-Uprava Republike Srbije koji su u upotrebi između vlade i građana, vlade i kompanija i vladinih agencija međusobno, navedeni su u tabeli 2. Neparne kolone u tabeli predstavljaju ime kategorije servisa. Parne kolone u tabeli predstavljaju odnos broja e-servisa u okviru kategorije i ukupnog broja servisa koje kategorija nudi. Činjenica koju je bitno istaći jeste da su u svim kategorijama mogu razlikovati tri grupe e-servisa: e-servisi, obrasci dokumenta i informacije. Pojedini servisi dostupni na portalima e-uprave kako Republike Srbije tako i drugih zemalja u okruženju ne mogu se uvek okarakterisati kao elektronski jer određeni broj njih nema mogućnost izvrešenja celokupne operacije posredstvom informaciono komunikacionih tehnologija. Ovakvi servisi u nekim slučajevima nude podnošenje zahteva za pružanje različitih usluga ili za izdavanje dokumenata elektronskim putem, dok se za konkretnu uslugu korisnik mora javiti konkretnoj poslovnici državnih organa. U pojedinim slučajevima elektronska usluga pruža samo osnovne informacije o postupku pribavljanja konkretnog dokumenta ili načinu pružanja konkretne usluge, dok se za sve ostalo korisnik Portala mora obratiti konkretnoj državnoj upravi ili lokalnoj samoupravi. Ovi servisi omogućavaju korisniku da putem portala preda recimo zahteve za različite tipove dokumenata, izvrši plaćanje poreza, saobraćajnih kazni, pronađe posao i još mnogo toga. Kao što se iz tabele može videti neke od kategorija su navedene u okviru portala ali njihovi servisi još uvek nisu implementirani. Putem druge grupe servisa korisnici mogu preuzeti obrasce dokumenata koje je potrebno da popune i predaju u papirnoj formi odgovarajućem organu vlade ili lokalane samouprave. Ovakav način poslovanja smanjuje gužve na šalterima i u kancelarijama opština i uprava, jer korisnik dolazi sa popunjenom dokumnetacijom i svim potrebnim pratećim dokumentima. Treća grupa obezbeđuje informacije korisnicima o različitim vladinim proceduram, pravnim propisima ili daje instrukcije korisnicima o načinu popunjavanja potrebnih dokumenata i zahteva, kao i predaje istih.

Tabela 2. Servisi elektronske uprave u Republici Srbiji

e-Uprava Republike Srbije					
Građani (G2C)		***Privreda (G2B)***		***Uprava (G2G)***	
Ime kategorije	Broj e-servisa/ Ukupan broj servisa	Ime kategorije	Broj e-servisa/ Ukupan broj servisa	Ime kategorije	Broj e-servisa/ Ukupan broj servisa
Porodica	24/43	Poslovanje	10/52	Usluge državnih organa	4/12
Zravlje	5/22	Životna sredina i prostorno planiranje	13/16		
Saobraćaj	5/37	Uvoz/Izvoz	2/4		
Stanovanje i životna sredina	56/68	Saobraćaj	3/9		
Poslovanje	6/11	Zdravlje	11/62		
Sport i omladina	1/1	Katastar	4/4		
Katastar	3/32	Rudarstvo	0/0		
Vanredni događaji	2/2	Grad Beograd	14/60		
Poljoprivreda i vodoprivreda	0/0	Javni pozivi	0/10		
Obrazovanje	2/7	Javne nabavke	7/8		
Dokumenta	65/110	Finansije	1/1		
Rad	7/45	Obrazovanje	1/1		
Finansije	3/12	Statistika	1/4		
Javni red i mir	22/29	Sport i omladina	0/2		
Osobe sa invaliditetom	9/40	Energija	0/2		
Ljudska prava	8/14	Turizam	0/0		
Turizam	0/1	Vodoprivreda poljoprivreda	0/0		
Grad Beograd	18/81				
Javni pozivi	0/47				
Ukupno	236/602	Upupno	67/235	Ukupno	4/12

Kako su u potpuno implementirane elektronske servise pobrojani smo oni čija usluga počinje i završava se elektronskim putem potrebno je istaći da postoji značajan broj onih kod kojih se primera radi zahtev može podneti elektronskim putem, dok se ostatak usluge obavlja na već ustaljeni način. Ovakvi servisi posebno su prisutni kod grupe servisa koji pripadaju privredi.

G2B domen se fokusira na interakciju između vlade i privrednog društva preko računarskog okruženja. Jedan od najranijih primera G2B interakcije je putem elektronske razmene podataka (EDI), koji predstavlja standardizovan metod za deljeljenje dokumenata. EDI tehnologija se koristi za transakcije kao što je online nabavka proizvoda od strane privrednih društava i vlada, sa prednostima kao što su smanjeni troškovi transakcija i povećana operativna efikasnost. Cilj G2B je smanjenje opterećenja poslovanja, obezbeđivanje pristupa informacijama na jednom mestu i omogućavanje digitalne komunikacije koristeći jezik e-poslovanja (XML). Kada su upitanju korisnici G2B servisa prijavljivanje na sistem pomoću korisničkog naloga nije dovoljno. Za uspešno korišćenje ovih servisa pravna lica moraju koristiti digitalne sertifikate i digitalni potpis. Neki od predstavljenih servisa koji su zastupljeni na portalu e-Uprave u cilju zadovoljenja potreba korisnika vrše redirekciju istog na druge web portale na kojima će korisnik pronaći ono što mu je potrebno. Neki od takvih portala su i portali koji pružaju druge e-usluge sa određenom namenom, kao na primer Portal javnih nabavki i Portal poreske uprave. Nezavisni portali kao što su ovi krerirani su kako bi grupisali slične servise iz jedne određene oblasti. Na ovaj način portali poput ovih su najkompaktniji, a korisnici bi mogli brzo pronaći željenu uslugu ili informacije. Sa strane vlade, administrativni posao je mnogo lakši sa nezavisnim portalima.

Podela servisa u okviru Portla e-Uprave Crne Gore obavljena je na fizička lica, pravna lica i upravu. Ovakva podela odgovara podeli servisa na Portalu e-Uprava Republike Srbije. Kategorije servisa kao i broj elektronskih servisa naspram ukupnog broja servisa na Portalu e-Uprave Crne Gore date su u Tabeli 3. Posmatrajući Tabelu 3 i Tabelu 2 može se ustanoviti da na Portalu e-Uprave Crne Gore ima manje kategorija servisa u delu fizičkih i pravnih lica dok u delu uprave ima jedna kategorija više nego što je to slučaj sa Portalom e-Uprave Republike Srbije.

Tabela 3. Servisi elektronske uprave u Crnoj Gori

e-Uprava Crne Gore					
Fizička lica		***Prvana lica***		***Uprava***	
Ime kategorije	Broj e-servisa/ Ukupan broj servisa	Ime kategorije	Broj e-servisa/ Ukupan broj servisa	Ime kategorije	Broj e-servisa/ Ukupan broj servisa
Poslovanje	4/6	Poslovanje i rad	10/15	Registri	3/3
Dokumenti	44/69	Dokumenti	23/25		
Zdravlje	0/0	Zdravlje	0/0		
Uređenje prostora, izgradanja objekata	3/3	Turizam	8/10		
Statistička istraživanja podataka	0/0	Unapređenje prostora, izgradnja objekata	1/1		
Javne nabavke	0/0	Javne nabavke	0/0		
Obrazovanje	5/24	Obrazovanje	11/11	Zahtevi/ Uverenja	8/19
Finansije	5/6	Finansije	1/1		
Rad	1/16	eLicence	3/28		
Turizam	8/8	Statistička istraživanja podataka	0/3		
Prijave građana	8/11	Uvoz / Izvoz	0/0		
Ukupno	78/143	Ukupno	57/94	Ukupno	11/22

Pristup e-Uprava Portalu Crne Gore omogućen je kako anonimnim korisnicima tako i registrovanim korisnicima. Anonimnim korisnicima omogućeno je korišćenje usluga državne uprave na informativnom nivou. Praktično anonimnki korisnici se putem portala mogu informisati o propisanim procedurama za dobijanje dokumenta, mogu pronaći kontakt podatke vladinih institucija zaduženih za realizaciju samih proceura kao i druge informacije. Pristup portalu je organizovan na istovetan način kao svim ostalim javnim web portalima. Registrovani korisnici kao što je to slučaj i sa ostalim portalima državne uprave u zemljama okruženja mogu biti fizička lica, pravna lica, zaposleni u javnoj upravi, kao i ovlašćeni službenici nadležnih institucija. Registrovani korisnici u procesu autentifikacije koriste kvalifikovane digitalne sertifikate izdate od nadležnih sertifikacionih tela. Za razliku od Republike Srbije u Crnoj Gori postoji jedno sertifikaciono telo i to je Pošta Crne Gore. Poslove izdavanja sertifikata obavlja jedno sertifikaciono telo, pri se poslovi registrovanja sertifikacionih tela obavljaju

takođe pred jednim registracionim telom. S tim u vezi Pošta CG-CA obavlja poslove provere identiteta korisnika u postupcima upravljanja sertifikatima kao što su prvo izdavanje sertifikata, obnova sertifikata, opoziv sertifikata[211].

Portal e-Građani Republike Hrvatske u osnovi ima istu namenu kao Portal e-Uprava već pomenutih zemalja. Ovaj portal sastoji se od tri podsistema (državni portal koji predstavlja javni deo sistema, osobni korisnički pretinac i nacinalni sistem za identifikaciju u auntentifikaciju)[212]. Osobni korisnički pretinac radi na Android, iOS i Windows monilnim platformama. Sve usluge na Portalu e-Građani su podeljene u tri grupe a popis usluga prikazan je u Tabeli 4.

Tabela 4. Servisi elektronske uprave u Republici Hrvatskoj

e-Građani Republike Hrvatske					
Dostupne e-usluge u sistemu e-građani		***Ostale e-usluge***		***Popis e-poruka u Osobnom korisničkom pretincu***	
Ime kategorije	Broj e-servisa	Ime kategorije	Broj e-servisa	Ime kategorije	Broj e-servisa
Pravna država i sigurnost	10	Pravna država i sigurnost	28	Stanovanje i okolina	1
Porodica i život	3	Porodica i život	1	Prava potrošaca	1
Odrastanje i obrazovanje	4	Odrastanje i obrazovanje	9	Zdravlje	13
Saobraćaj i vozila	3	Saobraćaj i vozila	2	Finansije i porezi	10
Aktivno stanovništvo	1	Aktivno stanovništvo	5	Aktivno stanovništvo	1
Finansije i porezi	2	Branitelji	1	Poslovanje	2
Zdravlje	5	Finansije i porezi	2	Saobraćaj i vozila	5
Rad	7	Zdravlje	5	Odrastanje i obrazovanje	1
Poslovanje	4	Poslovanje	21	Rad	17
Stanovanje i okolina	3	Prava potrošača	6	Porodica i život	1
		Stanovanje i okolina	12	Pravna država i sugurnost	12
Ukupno	42	Ukupno	92	Ukupno	64

[211] Žaklina Spalević, Bojan Milisavljević, Miloš Ilić, „Pravni aspekti razvoja Elektronske uprave u Republici Srbiji“, Zbornik radova Međunarodni naučni skup Sinergija, 2017.
[212] Središnji državni portal – O sistemu e-Građani, Dostupno na: https://gov.hr/e-gradjani/o-sustavu-e-gradjani/1584, datum pregleda: 27.01.2018.

Prve dve grupe nude elektronsko izvršenje usluga, dok treća grupa predstavlja spisak e-poruka u okviru servisa koji služi za pružanje informacija i obaveštavanje korisnika putem e-poruka. Proces pristupa servisima zasnovan je na korišćenju autentifikacionih sertifikata koji se mogu dobiti od ovlašćenog sertifikacionog tela.

Broj ovlašćenih sertifikacionih tela koja su zadužena za izdavanje digitalnih sertifikata u cilju prijavljivanja i korišćenja usluga na Portalu e-Građani[213] je znatno veći nego što je to slučaj sa brojem sertifikacionih tela u Crnoj Gori i Republici Srbiji. Pored većeg broja sertifikacionih tela proces dobijanja digitalnog sertifikata i dalje se zasniva na ličnom odlasku u poslovnicu sertifikacionog tela. Još jedan od potencijalnih nedostataka jeste i taj da je podnošenje zahteva i izdavanje uverenja putem sistema e-Građani moguće samo za one dokumente za koje se sudska taksa ne naplaćuje.

U Republici Srpskoj Portal e-Srpska je portal elektronskih servisa nastao kao jedna od reformi javne uprave. Na ovom portalu usluge su podeljene na usluge za građane i usluge za privredu. Sve ponuđene usluge su pretežno informativnog karaktera, bez mogućnosti elektronskog izvršenja samih usluga. Ono što je karakteristično za Republiku Srpsku jeste da jedino savet ministara ima operabilnu e-Upravu, dok građanima ovakvi servisi nisu dostupni. Problem sa e-Upravom nastao je zbog neusaglašenosti i loše komunikacije državnih organa čija je saradnja neophodna kako bi ovakav sistem mogao funkcionisati. Neusaglašenost je proistekla zbog toga što su pojedini organi javne uprave razvili odvojene informacione sisteme i infrastrukture unutar sopstvenih organizacija. Ovakva organizacija pojedinih organa javne uprave povećava vreme potrebno za izvršenje elektronskih servisa jer nepostojanje centralnog sistema dovodi do velikog broja repliciranja podataka i funkcionalnosti koji se nalaze u drugim servisima. Takođe javlja se i nekompatibilnost jer je svaki pojedinačni sistem nabavljen za specifičnu namenu. Uvođenjem zasebnih sistema povećavaju se troškovi nabavke i održavanja ovakvih sistema jer zahtevaju specifičnu veštinu IT stručnjaka. Ovakav pristup realizaciji elektronskih servisa u okviru javne uprave doveo je do toga da 70 institucija treba da krene da funkcioniše i deli podatke međusobno kako bi sistem e-Srpska ponudio adekvatne servise građanstvu. Neke pretpostavke sa aspekta tehničkog rešenja jesu da bi za celokupnu realizaciju sistema bilo potrebno oko 2 godine. Ipak Vlada Republike Srpske radi na rešavanju ovog problema, čemu u prilog govori i činjenica postojanja sertifikacione agencije čije je zaduženje sertifikacija saobraćaja u okviru elektronskih servisa. Poslovi sertifikacije povereni su Agenciji za informaciono društvo Republike Srpske (AIDRS). Ova agencija na osnovu Zakona o elektronskom potpisu i Zakona o Vladi Republike Srpske imenovana je nosiocem poslova elektronske sertifikacije. Na osnovu dobijenih poslova pružanja usluge serifikacije agenicija je kreirala infrastrukturu javnih kriptografskih ključeva. Pomenuta sertifikacija je dostupna isključivo organima republičke uprave. Svoj rad AIDRSCA je zasnovala na rešenju kompanije Entrust. Ovo rešenje zasnovano je na dva sertifikaciona tela: AIDRS Root CA server i AIDRS Issuing CA server[214].

---

[213] Lista prihvaćenih verodajnica, Dostupno na: https://gov.hr/e-gradjani/lista-prihvacenih-vjerodajnica/1667, datum pregleda: 20.01.2018.

[214]Agencija za informaciono društvo Republike Srpske, Dostupno na: https://www.aidrs.org/sr/aidrs/aidrsca/opste-informacije/, datum pregleda: 20.01.2018.

Pored svih pomenutih e-usluga za građane i pravne korisnike koji se kreiraju na nivou države, različite usluge e-uprave sprovode se na opštinskom nivou. Ovakvi portali implementirani na lokalnom nivou obezbeđuju informacije i e-servise značajne samo za konkretan grad ili određenu opštinu. Neke od e-usluga slične su uslugama dostupnim na portalu elektronske vlade, ali na taj način administracija takvih usluga je mnogo lakša i brža. Korisnici mogu naći određene informacije, različite šablone dokumenata, ili mogu mnogo brže podneti različite vrste elektronskog zahteva. Zbog tih činjenica svaki grad mora imati portale koji pružaju ovakve usluge.

Kao i svaki doment primene ICT u elektronskom poslovanju i e-vlada ima svoje prednosti i mane. Opšta ideja koja stoji iza e-Uprave jeste da građani mogu da naručuju različite vrste dokumenata od kuće, koristeći samo računar i pristup internetu, pruža veliki broj prednosti. Jedna od možda najupečatljivijih prednosti jeste da građani mogu doći do svih vrsta dokumenta bez čekanja u redu. Pored uštede u vremenu, za građane to znači uštedu novca, transparentnost i pravičnost funkcionisanja javne uprave i poboljšanje kvaliteta usluge. Za zaposlene u javnoj upravi korišćenje usluga e-uprave to znači jednostavniji i efikasniji način rada. Iz ugla ekonomije znači smanjenje troškova komunikacije i transakcija. Iz ugla državnih službi servisi e-Uprave i njemu slični portali predstavljaju način eliminisanja korupcije i zloupotrebe, primera radi u postupku javnih nabavki[215].

Na osnovu potreba i stepena razvoja, različite zemlje imaju različit indeks razvoja e-Uprave (EGDI). Na osnovu izveštaja UNPACS (United Nations Public Administration Country Studies) studije iz 2014.godine, najveći EGDI indeks ima Republika Korea, i on iznosi 0.9462. Na osnovu istog izveštaja EGDI indeks Republike Srbije iznosi 0.5472. Poređenjem EGDI indeksa Republike Srbije za 2012. godinu i već pomenutog indeksa za 2014. godinu može se utvrditi da je stepen razvoja za 2014. godinu manji, s obzirom da je u 2012. godini iznosio 0.6312. Ovaj indeks predstavlja nivo razvoja elektronske administracije i odnosi se na merenje kapaciteta i spremnost zemalja da koriste elektronsku upravu. Na osnovu indeksne vrednosti Republika Srbija se nalazi u grupi zemalja sa visokim EDGI. Ova grupa ima granične vrednosti između 0,50 i 0,75, tako da je vrednost EGDI naše zemlje blizu donje granice, što je jako bitno naglasiti. Ako uporedimo EGDI Republike Srbije sa bivšim jugoslovenskim republikama, možemo videti da Makedonija i Bosna i Hercegovina imaju nižu vrednost EGDI, 0.4720 i 0.4707 respektivno. Slovenija, Crna Gora i Hrvatska imaju veću vrednost EGDI, 0.6506, 0.6346 i 0.6282, respektivno. Svaka od pomenutih zemalja je imala niži EGDI u 2012. godini. Ove informacije pokazuju da trend smanjenja EGDI nije prisutan samo u Republici Srbiji. Jedno od mogućih objašnjenja za smanjenje EGDI-a može se dobiti iz gornje tabele. Sa ove tabele može se uočiti da se samo 39.21% i 28.51% svih G2C i G2B usluga primenjuju elektronski. Broj servisa koji su u potpunosti orijentisani elektronskom izvršavanju mora biti povećan.

[215] Kreca M., Vaskovic J. „Analysis of the current state of E-government services in Serbia“, In Proceedings of ITC Conference and Exhibition Infotech, Aranđelovac, 2013.

Drugi problem su e-usluge za građane koje se primenjuju samo u nekim gradovima, ili za koje građanin mora da sadrži digitalni sertifikat i čitač kartica. Neke od njih su e-usluge za naručivanje ličnih dokumenata ili rezervisanje termina za registraciju automobila. Drugi problem je broj korisnika interneta. Prema izveštaju UNPACS-a iz 2014. godine 48.10% građana u Republici Srbiji koristi Internet. Ovo je samo 7,2% više nego u 2012. Godini. Očigledna je i disproporcija između broja žena korisnika i broja korisnika muškaraca, kao i disproporcije između mladih i starih korisnika. Mnogi stariji zaposleni teško prihvataju korišćenje takvih usluga. Istovremeno, mnoge opštine nemaju IT stručnjake za razvoj e-usluga na nivou opštinske administracije i edukovanje drugih zaposlenih.

Usluge koje e-uprava pruža građanima, privrednim društvima, javnim službenicima, državnoj upravi i agencijama putem interneta i mobilnih veza osjetljive su na različite pretnje. Pretnje sigurnosti mreže se stalno menjaju i povećavaju. Takođe stalno se otkrivaju ranjivosti kako u sistemima koji si duže vremena u upotrebi tako i na novouspostavljenim sistemima, a na rešenjima za suprotstavljanje takvim pretnjama stalno se radi. Mere za obezeđenje mrežne sigurnosti iz ugla sprečavanja neovlašćenih upada zasnivaju se na firewall-u i proxy serverima, antivirusnim softverima, softverima za internet bezbednost, anti-malwaru, enkripciji podataka i saobraćaja, kao i na poboljšanju računarske arhitekture[216]. Tipičan šablon napada sastoji se od dobijanja pristupa korisničkom nalogu, dobijanja privilegovanog pristupa, kao i na korišćenju računara žrtve u vidu platforme za lansiranje drugih napada.

Svaka od zemalja na putu razvoja elektronske uprave mora da usvoji niz različitih strategija, zakona i podzakonskih akata. Jedan od dokumenata kojim se uređuje pravac implementiranja i razvoja elektronske uprave je i Strategija razvoja koja se definiše za period on nekoliko godina i koju obično prati akcioni plan sa njeno sprovođenje[217]. Strategija razvoja elektronske uprave u Republici Srbiji doneta je za period od 2015-2018. godine. U okviru nje definisan je i akcioni plan za sprovođenje ove strategije za period 2015-2016. godine. Doneta strategija zajedno sa akcionim planom definiše elektronsku upravu kao sistem informaciono komunikacionih tehnologija koje pružaju mogućnosti građanima i privredi da komuniciraju i poslovno sarađuju sa javnom upravom, koristeći elektronske medije (internet, mobilni telefon, pametne kartice, kioske itd.).

Glavni ciljevi Strategije u oblasti razvoja eUprave, a gledano iz ugla javne uprave, su svakako obezbeđivanje tehničke podrške za kvalitetno upravno odlučivanje na svim nivoima sistema javne uprave. Takođe, e-Uprava mora odgovoriti na potrebe javnosti za pristupačnim, pouzdanim i transparentnim uslugama. Pružanje usluga mora biti prilagođeno potrebama građana i pravnih lica, a ne isključivo javnoj upravi. Tako je Akcionim planom za sprovođenje reforme javne uprave u okviru „Mere 1.1“ planirano uspostavljanje elektronskih registara organa i drugih subjekata i zaposlenih u sistemu

[216] Singh S., Karaulia S, „E-governance: information security issues“, In Proceedings of the International Conference on Computer Science and Information Technology, pp.120-124, Pattaya, 2011.
[217] Žaklina Spalević, Bojan Milisavljević, Miloš Ilić, Opus citatum.

javne uprave, ova mera je istovremeno jedan od ciljeva Akcionog plana za sprovođenje Strategije razvoja e-Uprave koji glasi: „Uspostavljanje osnovnih elektronskih registra povezanih sa drugim informacionim sistemima državnih organa, organa autonomne pokrajine i jedinica lokalne samouprave“[218].

Ključni zakoni važni za razvoj e-Uprave doneti su u periodu od 2006-2010. godine, i to su Zakon o elektronskom potpisu[219], Zakon o zaštiti podataka o ličnosti[220], Zakon o elektronskoj trgovini[221], Zakon o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju[222], Pravilnik o izdavanju vremenskog žiga[223], Zakon o elektronskim komunikacijama[224], Uredba o posebnim merama zaštite tajnih podataka u informaciono-telekomunikacionim sistemima[225]. Izmene i dopune pojedinih pobrojanih zakona donete su naknadno u skladu sa potrebama u domenu primene. Prijavljivanje na sistem Portala e-Uprava, sertifikacija, podnošenje zahteva, distribucija elektronskih dokumena, kao i regulisanje prava i obaveza korisnika portala definisani su ovim setom zakona.

Jedan od takođe veoma važnih zakona a za čije je donošenje bilo potrebno doneti sve prethnodne jeste i Zakon o elektronskoj upravi[226]. Nacrt ovog zakona trenutno je u procesu razmatranja i usvajanja. Ovim zakon se uvodi korišćenje državnog cloud sistema. Ovaj cloud sistem namenjen je organima u elektronskoj upravi. On je zapravo deljeni i skalabilan skup resursa zasnovan na tehnologijama virtualizacije. Pored claud-a uvodi se i elektronska pisarnica. Informaciono komunikacioni sistem koji predstavlja elektronsku pisarnicu trebalo bi da omogući automatizaciju poslova koji se obavljaju ručno. Neki od tih poslova su poslovi prijema, otvaranja, pregledanja i raspoređivanja pošte. Tekođe putem e-pisarnice će se vršiti i poslovi evidentiranja predmeta, združivanja akata, kao i dostavljanje istih unutrašnjim organizacionim jedinicama i sve to u elektronskom obliku. Takođe se uvodi i mogućnost elektronskog upravnog postupanja u upravnim stvarima elektronskim putem. Za bezbednost korišćenja celokupnog sistema zadužen je CERT (centar za bezbednost informaciono-komunikacionih sistema). Članom 12 definisano je uspostavljanje i vođenje registara. Ovim članom definisano je da svi Registri i evidencije u elektronskom obliku moraju

[218] Strategija razvoja elektronske uprave u Republici Srbiji za period od 2015-2018. godine i akcioni plan za spovođenje Strategije za period od 2015-2016. godine, Dostupno na: http://www.mduls.gov.rs/doc/Strategija%20razvoja%20eUprave%20sa%20AP%202015-2018.pdf

[219] Zakon o elektronskom potpisu, Opus citatum

[220] Zakon o zaštiti podataka o ličnosti, Sl. glasnik RS", br. 97/2008, 104/2009 - dr. zakon, 68/2012 - odluka US i 107/2012.

[221] Zakon o elektronskoj trgovini, Opus citatum.

[222] Zakon o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju, Opus citatum.

[223] Pravilnik o izdavanju vremenskog žiga, Opus citatum.

[224] Zakon o elektronskim komunikacijama, Sl. glasnik RS", br. 44/2010, 60/2013 - odluka US i 62/2014.

[225] Uredba o posebnim merama zaštite tajnih podataka u informaciono-telekomunikacionim sistemima, Sl. glasnik RS", br. 53 od 20/2011.

[226] Nacrt zakona o elektronskoj upravi – Teks propisa, Dostupno na: http://www.paragraf.rs/dnevne-vesti/210917/210917-vest19.html, datum pregleda: 02.02.2018.

da se nalaze na serverima koji su stacionirani na prostoru Republike Srbije. Isključivost od ovog člana mogu imati samo nalozi za elektronsku komunikaciju organa zaduženih za poslove van Republike Srbije[227]. Članom 15 ovog nacrta Zakona definiše se uspostavljanje i vođenje Metaregistara[228]. Metaregistri obezbeđuju interoperabilnost registara i evidencija u elektronskom obliku. Podaci koje sadrže metaregistri vezani su za registre i evidencije koji se nalaze u elektronskom obliku. Praktično metaregistri će sadržati informacije o tome kada su pojedini registri ili evidencije uspostavljenji, koje podatke sadrže kao i koji organi im pristupaju i sa kojim privilegijama pristupa. Svaki od metaregistra će sadržati i infomraciju o tome da li se podaci u nekom registru ili evidenciji mogu pravno ustupiti, kao i na koji način se ovi podaci mogu koristiti. Možda jedan od najbitniji delova ovog nacrta zakona jeste i definisanje upotrebe elektronskog plaćanja u okviru portala elektronske uprave. Ovo praktično znači da će za one poslove za koje su ranije korisnici morali da uplate taksu i dokaz o uplati prilože nadležnom organu sada biti data mogućnost da sve odradi elektronski bez odlaska u filijale i čekanja u redu[229]. Ovakav pristup obezbediće mogućnost celokupnog izvršenja usluga za usluge koje zahtevaju plaćanje nadoknada. Upravo je plaćanje nadoknada za izdavanje dokumenta ili bilo kakvog drugog vida taksi najveći kamen spoticanja e-Uprave kako u Republici Srbiji tako i u zemljama okruženja. Ovo se možda najbolje vidi na primeru Hrvatske kao što je ranije navedeno, čiji servisi samo iz tog razloga nisi operativni do kraja.

Ukoliko pomenuti set Zakona zajedno sa Nacrtom Zakona o elektronskoj upravi uporedimo sa sličnim zakonima u zemljama okruženja možemo uvideti da je deo njih u zemljama okruženja donet i ranije. Primera radi Zakon o elektronskim komunikacija Crne Gore[230] donet je 2014 godine. Odredbe ovog zakona su slične odredbama Nacrta Zakona o elektronskoj upravi Republike Srbije. Set Zakona na kojima je bazirano donošenje ovog zakona istovetan je sa zakonima u Republici Srbiji. Ukoliko uporedimo Republiku Hrvatsku sa Republikom Srbijom možemo uvideti da pored sličnog seta donesenih zakona u Republici Hrvatskoj je donesen i zakon o Elektronskim komunikacijama. Što se tiče Republike Srpske broj usvojenih zakona na kojima se bazira rad elektronske uprave manji je nego što je to slučaj u Republici Srbiji[231]. S tim u vezi Republika Srpska još uvek nema donet Zakon o elektronskoj upravi.

Poređenjem nivoa implementiranih elektronskih servisa u okviru Portala elektronske uprave kao i seta donesenih zakona Republike Srbije i zemalja okruženja može se uvideti da je broj potpuno implementiranih servisa na sličnom nivou izuzevši Republiku Srpsku gde su servisi informativnog karaktera. Sve posmatrane zemlje još uvek imaju problema u realizaciji servisa za koje je potrebno plaćanje neke nadoknade, što svedoči o tome da Zakon o elektronskom novcu i Zakon o elektronskom plaćanju

[227] Ibidem, član 12.
[228] Ibidem, član 15.
[229] Ibidem, član 24.
[230] Zakon o elektronskim komunikacijama Crne Gore, Službeni list Crne Gore, broj 32/2014,
[231] Spisak zakona RS, Agencija za informaciono društvo Republike Srpske, Dostupno na: https://www.aidrs.org/sr/legislativa-i-standardizacija/zakoni/, datum pristupa: 05.10.2017;

nisu naišli na veliku primenu od strane državnih organa ili nisu dovoljno kvalitetno ispratili moguća tehnička rešenja. Podatak o tome da su zemlje okruženja većinu zakona potrebnih za rad elektronske uprave zajedno sa Zakonom o elektronskoj upravi donele ranije nego što je to slučaj sa Republikom Srbijom u poređenju sa trenutnim stanjem e-servisa svedoči o tome da bez obzira na činjenicu da Zakon o elektronskoj upravi Republike Srbije još uvek nije donet broj implementiranih servisa uveliko parira zemljama okruženja. Donošenjem ovog zakona očekuje se jačanje elektronskih servisa i njihove primene.

5
Elektronski servisi u službi vlade i građana

Razvoj elektronskih servisa različite namene i ciljne grupe građana daleko prevazilazi servise orijentisane samo na komunikaciji vlade i građana. Tačnije servisi e-Uprave se mogu smatrati čak i servisima novijeg datuma u odnosu na e-servise koji su u upotrebi bilo od strane građana ili od strane državnog sektora. Ovakvi servisi u pojedinim slučajevima nisu dostupni građanima za aktivno korišćenje već ih vlada primenjuje u cilju monitoringa građana i obezbeđenja bezbednije životne okoline. S druge strane postoje i e-servisi koji nisu kreirani od strane državnih organa ili u službi državnih organa već su kreirani od strane privatnih kompanija ili samih građana. Primera radi različiti vidovi aplikacija koriste se u procesu obrazovanja mladih, s obzirom da oni pripadaju informatičkoj eri pa samim tim veoma lako prihvataju tehnologije i uče korišćenjm istih[232]. Bilo kako bilo svaki od servisa kreiranih na ovakav način zauzima značajno mesto svakodnevnom životu i radu ljudi.

5.1 Elektronski nadzor osuđenika

Kako bi se na najuspešniji mogući način realizovalo izvršenje vanzavodskih sankcija i mera uveden je sistem monitorniga lica korisnika ovakvog programa. Uređaji za elektronsko praćenje koji su u upotrebi pružaju podatke o kretanju osuđenih lica, njihovoj trenutnoj lokaciji, kao i o tome da li su napustili unapred definisani prostor boravka. Izuzetno ovi uređaju mogu vršiti kontrolu konzumiranja alkohola ili narkotika. Neki sistemi obezbeđuju praćenje u okviru unapred definisanih i ograničenih područja, i mogu se koristiti u situacijama praćenja osobe pre suđenja ili tokom izvršenja kazne.

Različiti tipovi uređaja za praćenje razvijeni su tokom godina, pri čemu je svaka naredna generacija unapređivana u pogledu funkcionalnosti i prenosivosti u odnosu na prethodnu. Generalno uređaju za praćenje mogu biti kreirani u dva oblika. Prvi oblik sistema za elektronski nadzor čine aktivni sistemi. Ovi sistemi zahtevaju da pojedinac u našem konkretnom slučaju osuđenik nosi transmiter u obiku nanogice koji konstantno emituje signal do prijemnika. Uobičajeno prijemnik je povezan sa telefonskom linijom. Ovako povezani uređaj obaveštava vlasti ukoliko dodje do prekida signala bilo zbog udaljavanja korisnika od bazne stanice ili uništavanja uređaja. Takođe su razvijene varijante koje koriste mobilnu opremu koja omogućava praćenje pozicije pojedinačnog uređaja, omogućavajući na taj način vlastima utvrđivanje lokacije osućenika, kao i da li on sme ili ne sme biti na tom mestu. Ovo je posebno značajno ukoliko je osuđeniku dozvoljeno kretanje do posla ili određenih organizacija, na takav način može se utvrditi da li je osuđeno lice promenilo rutu kretanja. Aktivni sistemi se mogu koristiti i za ograničavanje pristupa osuđenog lica drugim licima. Primera radi ukoliko se radi o praćenju lica osuđenih za kućno nasilje ili drugi vid uznemiravanja sistem će obavestiti vlasti ukoliko se osuđenik približio licu

[232] S. Minić, Ž. Spalević, A. Gadžić, Edukativne igre kao savremeno sredstvo za učenje, Teme, Vol. 35, No. 4, pp. 1677 - 1689, Dec, 2011.

pod zaštitom. Takođe svrha nadgledanja se može postići u određenoj meri postavljanjem uređaja za nadgledanje na autobuske i železničke stanice tako da se pojedinac može pratiti do i sa posla[233].

Drugi oblik sistema za praćenje naziva se pasivni sistem. Kod ovih sistema nosioci uređaja za praćenje se povremeno kontaktiraju telefonom kako bi se osiguralo da je osuđeno lice u perimetru u kome mu je kretanje dozvoljeno. Najčešći način potvrđivanja prisustva jeste povezivanje uređaja sa telefonom. Na ovakav način obezbeđuje se sto posto samopouzdanja. Različite tehnologije bi se mogle implementirati kako bi se obezbedili pasivni sistemi. Na primer, u pasivnim sistemima pored sistema za proveru glasa može se vršiti biometrijski otisak prsta ili skeniranje mrežnice. Neke druge tehnike zahtevaju od prekršioca da odgovori na pejdžer, sa tehnologijom caller-ID koja potvrđuje lokaciju pojedinca. Međutim, svi pasivni sistemi ograničeni su činjenicom da oni ne pružaju trenutno obaveštenje o kršenju lokacije ili stanja u intervalima između poziva.

Elektronske nanogice kao što je već rečeno se najčešće koriste kod izdržavanja kazni u sistemu van zatvorskog izdržavanja. Najčešće se koriste u kombinaciji sa baznom stanicom koja radi na principu radio frekvencije i koja je kreirana sa tradicionalnom telefonskom linijom. Izveštaji prosleđeni od strane bazne stanice najčešće se prate od strane agencija zaduženih za praćenje osuđeni lica, dok u pojedinim jurisdikcijama treću stranu predstavljaju državne agencije za sprovođenje zakona. Posmatrano iz ugla tehnologije izrade elektronska nanogica je cvrst i vodootporan upređaj koji se ne može ukloniti sa noge osuđenog lica. Po pitanju parametra koji se prate može se razlikovati veći broj tipova elektronskih nanogica. Neke od njih kao što je recimo *ExacuTrack One* prate kretanje osuđenog lice pomoću kombinacije različitih tehnologija za praćenje lokacije. Veći broj tehnologija se kombinuje kako bi sistem u svakom trenutku imao informaciju o lokaciji praćenog lice, pri čemu na tačnost podataka ne sme da utiče okolina u kojoj se lice nalazi (visoke zgrade, vožnja u vozilu ili boravak u zatvorenom prostoru). Kako bi se obezbedila postojanost sistema i manji utrošak energije po pitanju baterije a samim tim dobilo i na manjim dimenzijama uređaja dodatno se može ugraditi podsistem u kući, na poslu ili školi osuđenog lice. Pomoću ovog podsistema nanogica prilikom ulaska lica u prostoriju prelazi iz GPS moda praćenja u radio frekventni mod. Kada osoba napusti oblast pokrivenosti ovog podsistema nanogica iznova prelazi u GPS mod. Za razliku od većine GPS sistema za praćenje *ExacuTrack One* omogućava iscrtavanje rute kretanja nadgledanog lica pomoću Microsoft® MapPoint® and Bing™ softvera. Takođe nadzornik može pomoću ovog uređaja poslati nadgledanom licu glasovnu poruku i na taj način ga upozorita da je izasao iz oblasti u kojoj mu je dozvoljeno kretanje. Drugi model nanogice je SCRAMx nanogica koja se pomoću trake pričvršćuje za korisnika. Zadatak ovog uređaja je da tokom perioda nošenja preračunava nivo alkohola u krvi korisnika, i to na bazi isparenja sakupljenih na površini kože. Nanogica čuva očitane vrednosti i u tačno predefinisano vreme iste šalje

[233] Johnson T. „Monitoring device trial hailed a success“, Corrective Services Bulletin, 1(466), 6, 1999.

putem radio frekvencije do bazne stanice. Očitavanje alkohola, kao i dijagnostički podaci dalje idu na detaljnu analizu i kreiranje izveštaja. Bazna stanica takođe poseduje i LCD displej putem kojeg korisnik dobija poruke[234]. Najveći nedostatak ovakiv sistema za praćenje alkoholnih zavisnika i osuđenika jeste što sama nanogica ne registruje samo etil alkohol koji se koristi u svakodnevnoj konzumaciji već registruje sve vrste alkohola. Ovo praktično znači da će uređaj pored alkohola za konzumiranje registrovati i alkohol iz parfema kao i sredstava za čišćenje. Kako bi se izbeglo lažno alarmiranje i potencijalna šteta naneta kažnjenom licu usled interferencije, sve pristigle podatke posmatraju obučeni zaposleni. Oni svoje odluke i zaključke da li je merenje dobijeno na osnovu konzumnog alkohola ili neke druge vrste alkohola donose pre svega na osnovu analize grafikona koji se kreiraju od dobijenih podatka.

Ovakvi i slični tipovi uređaja za praćenje osuđenih lica mogu prikupljati veliki broj podataka kako o kretanju osuđenog lica tako i o njegovom fizičkom stanju, načinu organizacije vremena, navikama i ponašanju. Korisna informacija mogla bi se dobiti obradom prikupljenih podataka na osnovu čega bi se mogli kreirati profili ponašanja određene kategorije osuđenika. Takođe rana predikcija ostvarenosti uslova za ponavljanje istog ili sličnog dela u mnogome može pomoći oko sprečavanja istog. Kako bi sve ovo bilo moguće nad prikupljenim podacima mogu se primeniti razni mehanizmi data mininga. Ovo praktično znači da ukoliko sistem poseduje parametre pod kojima je došlo do izvršenja prekršajnog ili krivičnog dela, na osnovu poklapanja vrednosti parametara iz prošlosti i trenutnih vrednosti parametara može se predvideti buduće ponašanje. Kako bi se predikcija mogla obaviti prikupljene vrednosti posmatranih parametara moraju se klasifikovati prema krivičnom delu. Ovakav princip potrebno je primeniti iz prostog razloga jer predikcija mogućnosti ponavljanja istog krivičnog dela će zavisiti od različitih parametra za različita krivična dela. U nekim slučajevima vrednost zavisnog parametra zavisiće od jednog nezavisnog parametra, dok će u nekim slučajevima vrednost zavisnog parametra biti uslovljena odnosom većeg broj nezavisnih parametra. U oba slačaja mašinsko učenje se može primeniti kao način realizacije predikcije. Tačnost predikcije zavisiće od veličine seta podataka na kome je bazirano obučavanje predikcionog modela. Zapotrebe predikcije ponavljanja krivičnog dela definisane su hipoteza i cost funckija i predstavljene jednačinama 1 i 2 respektivno[235].

$$h_\theta(\mathrm{x}) = \theta^T x = \theta_0 x_0 + \theta_1 x_1 + \theta_2 x_2 + \ldots + \theta_n x_0 \qquad (1)$$

$$J(\theta_0, \theta_1, \ldots, \theta_n) = \frac{1}{2m} \sum_{i=1}^{m} (\mathrm{h}_\theta(\mathrm{x}^{(\mathrm{i})}) - \mathrm{y}^{(\mathrm{i})})^2 \qquad (2)$$

[234] Barton M, „The scram tether, How it works and how it doesn't", Law Office of Barton Morise, Available at: http://michigancriminalattorney.com/scram-tether-works/, date: 05.02.2018.

[235] Spalević, Ž., Ilić, M., Spalević, P., „ Electronic monitoring devices and data processing. In Proceedings of 2nd International scientific conference of IT and Business Related Research – Synthesis, Belgrade, pp. 242-247, 2015.

U datim jednačinama $\theta_1, \theta_2, ..., \theta_n$ su parametri hipoteze, dok su $x_1, x_2, ...x_n$ podaci iz baze podataka na osnovu kojih hipoteza dovodi do zaključka. Bitno je istaći da parametri $\theta_1, \theta_2, ..., \theta_n$ nisu individualni parametri već parametri predstavljeni u vidu n+1 dimenzionalnog vektora *θ*. U drugoj jednačini parametar *m* predstavlja broj trening uzoraka. Na osnovu reprezenatacije parametara, cost funkcija biće predstavljena sa *J(θ)*. Cost funkcija predstavlja linearnu regresiju nad podacima. Pseudo algoritam za gradient descent je predstavljen jednačinom 3. Gradient descent služi kao metod za minimizaciju cost funkcije.

$$\text{Repeat}\{$$

$$\theta_j := \theta_j - \alpha \frac{\partial}{\partial \theta_j} J(\theta) \qquad (3)$$

$$\}$$

Kod izračunavanja jednačine 3 najvaznije je da se vrednosti $\theta_1, \theta_2, ..., \theta_n$ simultano update-uju, sa svakom iteracijom po *j*. Ukoliko ne dolazi do simulatanog obnavljanja vrednosti parametra, na kraju algoritma njihove vrednosti neće biti tačne. Razvojem algoritma jasno se uočava da u svakoj od narednih faza učestvuje izračunata vrednost iz prethodne što i jeste glavni razlog simultanog obnavljanja vrednosti sa svakom iteracijom. Zavisno od parametara gradient descent će figurirati kao veći ili manji korak u minimizacionom procesu. Drugi deo jednačine 3 može se drugačije predstaviti kao u jednačini 4, s obzirom da α predstavlja stopu učenja.

$$\frac{\partial}{\partial \theta_j} J(\theta) = \frac{1}{m} \sum_{i=1}^{m} (\mathrm{h}_\theta(\mathrm{x}^{(\mathrm{i})}) - \mathrm{y}^{(\mathrm{i})}) x_j^{(\mathrm{i})} \qquad (4)$$

Konačni algoritam za izračunavanje gradient descenta dobija se kada se jednačina 4 zameni u jednačini 3. Ovaj algoritam predstavljen je u jednačini 5.

$$\text{Repeat}\{$$

$$\theta_j := \theta_j - \alpha \frac{1}{m} \sum_{i=1}^{m} (\mathrm{h}_\theta(\mathrm{x}^{(\mathrm{i})}) - \mathrm{y}^{(\mathrm{i})}) x_j^{(\mathrm{i})} \qquad (5)$$

$$\}$$

Ukoliko se algoritam primeni za prva tri parametra dobiće se izgled jednačina 6-8. Zanimljiva je činjenica da svaki korak u gradient descentu korsiti ceo trening skup. Karakter *i* u superskriptu kod *x* ne predstavlja vrednost stepena već vrednost indeksa. Kombinacijom indekasa dobija se konkretna vrednost podatka iz baze podataka.

$$\theta_0 := \theta_0 - \alpha \frac{1}{m} \sum_{i=1}^{m} (\mathrm{h}_\theta(\mathrm{x}^{(\mathrm{i})}) - \mathrm{y}^{(\mathrm{i})}) x_0^{(\mathrm{i})} \quad (6)$$

$$\theta_1 := \theta_1 - \alpha \frac{1}{m} \sum_{i=1}^{m} (\mathrm{h}_\theta(\mathrm{x}^{(\mathrm{i})}) - \mathrm{y}^{(\mathrm{i})}) x_1^{(\mathrm{i})} \quad (7)$$

$$\theta_2 := \theta_2 - \alpha \frac{1}{m} \sum_{i=1}^{m} (\mathrm{h}_\theta(\mathrm{x}^{(\mathrm{i})}) - \mathrm{y}^{(\mathrm{i})}) x_2^{(\mathrm{i})} \quad (8)$$

Nakon izračunavanja cost funckije mora se pronaći njena minimalna vrednost, jer će upravo takva cost funkcija dati najbolju linearnu regresiju. U zavisnosti od složenosti problema u samom procesu izračunavanja predikcionih vrednosti može uticati veći broj hipoteza. Takođe moguće je pre početka samog procesa izvršiti skaliranje vrednosti ukoliko se početne vrednsoti jako velike. Kada se završi sa izračunavanjem gradiet descenta i minimizacijom cost funkcije, vrednost parametara dobijene cots funkcije se mogu uporediti sa parametrima u hipotezi. Najpogodnije je ceo proces obavljati specijalizovanim alatima, jer ovakvi alati nude i različite mogućnosti reprezenatacije podataka, cost funkcije i hipoteze u vidu 2D i 3D dijagrama. Na ovakav način znatno lakše se mogu uočiti nedostaci ili greške u izračunavanju ili polaznim hipotezama.

Ovakav način upotrebe prikupljenih podataka značajno može umanjiti broj povratnika koji kaznu za izvršeno krivično delo izvršavaju uz elektronsko praćenje van postorija zavoda. Primera radi, na osnovu putanje kretanja, otkucaja srca ili nivoa alkohola kao i udaljenosti osuđenog lica od štićenog objekta ili lica organi reda mogu ustanoviti da postoji mogućnost da osuđeno lice ponovi prekršaj. Na osnovu izvedenih zaključaka isti organi mogu blagovremenom akcijom osuđeno lice sprečiti u pokušaju izrvšenja dela. Izvršenje kazni van zavoda uz elektronsko praćenje regulisano je odgovarajućim zakonskim odredbama. Zakonski okviri koji se primenjuju u ovakvim slučajevima definisani su u okviru Zakona o izvršenju vanzavodskih sankcija i mera[236]. Vanzavodske sankcije i mere propisane ovim zakonom mogu se izreći u slučaju krivičnog, prekršajnog ili bilo kog drugog sudskog postupka. S obzirom da se ove kazne izvršavaju van kontrolisanih uslova zavodskih prostorija, a u okviru zajednice potrebno je za svako lice definisati način izvršenja, položaj lica u postupku kao i način sprovođenja nadzora tokom izvršenja. Ovim zakonom se definišu dve situacije u kojima se može primenjivati mera elektronskog nadzora: kućni zatvor i kućni pritvor.

Kućni zatvor je kazna, krivična sankcija koju sud izriče presudom kojom se okončava krivični postupak. To je modalitet izvršenja kazne zatvora. Ona se umesto u zatvoru izvršava u prostorijama u kojima osuđeni stanuje. Ona suštinski, iako ne formalno, za osuđeno lice, predstavlja posebnu kaznu lišenja slobode iz razloga što

[236] Zakon o izvršenju vanzavodskih sankcija i mera, Službeni glasnik RS, br. 55/2014.

menja njen način i mesto izvršenja. Članom 45. Krivičnog zakonika[237] predviđena je kazna kućnog zatvora:

- U slučaju kada se učiniocu krivičnog dela izrekne kazna zatvora do jedne godine i ukoliko sud na osnovu procene ličnosti učinioca, njegovog ranijeg života, držanja posle učinjenog dela kao i na osnovu stepena krivice donese odluku o izvršenju iste u prostojima u kojima stanuje.
- Lice koje me propisana kazna zatvora u okviru prostorija u kojma stanuje napuštanje istih može se vršiti samo u slučajevima propisanim Zakonom o izvršenju krivičnih sankcija. Ukoliko dođe do samovoljnog napuštanja prostorija jednom u trajanju više od 6 sati ili dva puta u ukupnom trajanju do 6 sati sud može smatrati da je došlo do povrede služenja kazne u stambenim prostorijama i može odrediti da se ostatak kazne zatvora izvrši u zavodu za izvršenje kazne zatvora.
- Ograničenje nemogućnosti određivanja izvršenja kazne zatvora u prostorijama u kojima stanuje propisano je za lica koja su osuđena za krivično delo protiv braka i porodice, a koja žive sa oštećenim licima u istom domaćinstvu.

Kućni pritvor je mera za obezbeđenje prisustva okrivljenog tokom trajanja postupka, koju sud izriče rešenjem, tokom postupka. Ova mera se odnosi na zabranu napuštanja prostorija stanovanja, zabranu korišćenja telefona, interneta kao i primanja gostiju. Dužina trajanja kućnog pritvora propisuje se na vremenski period za koji se proceni da postoji potreba, a najduže do pravnosnažnosti presude. Donošenjem pravosnažne presude lice može biti oslobođeno ili se može uputiti na izdržavanje krivične sankcije koja se sastoji u lišenju slobode. U oba slučaja mera kućnog pritvora se prekida i stupa na snagu mera izrečena presudom. Ova mera regulisana je odredbama Zakonika o krivičnom postupku[238].

I u jednoj i u drugoj situaciji sud u odluci rešava da li se mera kućnog zatvora i kućnog pritvora izvršava sa ili bez elektronskog nadzora. Ukoliko se izrekne izvršenje mere uz elektronski nadzor tada se oprema za elektronski nadzor aktivira odmah posle dostavljanja odluke koju je sud doneo o primeni ove mere. Propisana su prava i obaveze osuđenika koji izdržava kaznu zatvora u prostorijama u kojima stanuje. Jedno od prava dato osuđeniku je i pravo da van prostorija u kojima stanuje i izvršava kaznu može boraviti najviše 2 časa dnevno, u periodu od 13 do 17 časova. Tokom izvršenja ove mere Poverenik može bez najave da vrši proveru da li se osuđeni nalazi u prostorima u kojima stanuje.

Članom 17 Zakona o izvršenju vanzavodskih sankcija i mera definisana su pravila nadzora nad izvršenjem mere kućnog protvora[239]. Ovim članom definiše se da je za postavljanje uređaja za elektronski nadzor zadužena poverenička služba. Uređaj za lociranje okrivljenog mora biti neškodljiv po zdravlje i za njegovo postavljanje zaduženo je stručno lice. Takođe postoji obaveza davanja uputstva o načinu rada

[237] Krivični zakonik, Opus citatum, član 45.
[238] Zakonik o krivičnom postupku, „Službeni glasnik RS“, br. 72/2011, 101/2011, 32/2013, 45/2013 i 55/2014.
[239] Zakona o izvršenju vanzavodskih sankcija i mera, Opus citatum, član 17.

uređaja osuđenom licu. Za upravljanje uređajem za daljinsko praćenje kretanja okrivljenog zadužena je poverenička služba. Istim članom definisano je i postavljanje uređaja za nadzor lica u slučaju izrečene mere kućnog zatvora.

Lice koje se nalazi pod elektronskim nadzorom može napustiti prostorije u kojima služi kaznu zatvora ili pritvora vanzavodskim izdržavanjem samo u slučajevima defnisanim članom 24 Zakona o izvršenju vanzavodskih sankcija i mera. Prema ovom članu za svako napuštanje prostorije u kojima lice stanuje isto prethodno mora podneti molbu direktoru Uprave za izvršenje krivičnih sankcija. Odlukom direktora uprave osuđenom se dozvoljava ili ne napuštanje prostorija. Isto tako ukoliko prestanu razlozi navedeni u zahtevu ili je lice prekršilo utvrđena pravila napuštanja prostorija direktor može opozvati odluku o dozvoli napuštanja prostorija[240].

Izricanje kazni kućnog zatvora ili kućnog pritvora uz elektronski nadzor nije neubičajena sudska praksa u Republici Srbiji. Generalno ovakve mere najčešće se izriču mlađim licima koja su recimo još uvek u obrazovnom procesu pa im se na taj način pruža mogućnost da isti nastave i da na taj način održe svakodnevni korak sa spoljim svetom. Takođe ovakve mere često se izriču odgovronim licima kompanija ili vlasnicima istih u postupcima koji ih terete za privredni kriminal. Navedena lica iako osuđena za razna prekršajna i krivična dela svakako se ne mogu uvrstiti u istu grupa sa licima osuđenim za ubistva, silovanja, trgovinu ljudima, robom i narkoticima. Iz rog razloga potpuno je opravdana ovakva praksa. Da praksa elektronskog nadgledanja nije novina i da se u svetu primenjuje duži niz godina svedoče i primeri širom sveta. Primera radi u Švedskoj prosečno 3000 osuđenih osoba godišnje služi kaznu kućnog zatvora uz elektronski nadzor. Sistem elektronskog nadzora u provinciji Buenos Aires počeo je sa primenom još 1997. godine. Podaci pokazuju da je za prvih deset godina primene bilo 910 muškaraca pod nekom vrstom elektronskog nadzora. Sistem elektronskog nadzora i praćenja u ovom provinciji je relativno mali i obuhvata oko 300 osuđenika istovremeno[241]. Što se tiče SAD-a izdržavanje kazne vanzavodskih prostorija uz elektronski nadzor primarni je način. Statistika zavoda za pravosuđe SAD-a (Bureau of Justice Statistics) pokazuje da je 1998 godine bilo 19677 osuđenika sa merom elektrosnkog nadzora. Ovakva kazna smatra se daleko blažom od zatvorske, ali u isto vreme težom od uslovne[242]. U novije vreme broj osuđenika koji kaznu služe pod nekom vrstom elektronskog nadzora je premašio 5 miliona. Kao primer važnosti ovakvog sistema može se uzeti sudska praksa suda u Severnoj Karolini. U maju 2013. godine sud je nakon 4 godine zatvora licu osuđenom zbog seksualnog prestupa drugog stepena odredio meru puštanja iz zatvora uz elektronsko praćenje pomoću GPS

[240] Zakona o izvršenju vanzavodskih sankcija i mera, Opus citatum, član 24 i član 27.
[241] Tella, R, Schargrodsky, E., „Criminal recidivism after prison and electronic monitoring“, National Bureau Of Economic Research. 1050 Massachusetts Avenue, Cambridge, MA 02138
[242] Bonczar, T., Glaze, L.E. „Correctional Populations in the United States“, 1998, Bureau of Justice Statistics, US Department of Justice, Washington DC. 1999.

nanogice[243]. Činjenica da je osoba seksualni prestupnik i povratnik dodatno je učvrstila odluku da ovakva osoba mora biti pod stalnim elektronskih nadzorom[244].

Pored prednsoti koje elektronski nadzor donosi u pogledu socijalizacije osuđenika i napora da neometano nastave sa svakodnevnim životom i radom ovakva način izdržavanja kazni donosi dodatne prednosti. Jedna od prednosti jeste i ekonomska ušteda u pogledu manjeg broja zatvora i njihovog održavanja. Primera radi korišćenje elektronskog nadzora u SAD košta između 5.50$ i 10$ dnevno, dok izdržavanje zatvorske kazne košta 100$ do 160$ dnevno. Takođe osuđenici pod elektronskim nadzorom mogu neometano nastaviti sa svojim poslom pa im se na takav način korišćenje uređaja može naplatiti. Iz ugla maloletnih prestupnika ovo je prilika da neometano nastave sa svojim obrazovanjem i svakodnevnim životnim navikama, a da opet sa druge strane uz određena ograničenja razumeju težinu preestupa koji su napravili. Primera radi nakon uvođenja elektronskog nadzora u jednoj od zemlja broj maloletnih prestupnika u jednom od centara za izdržavanje kazne se smanjio sa 94 dnevno na 45 dnevno. Smanjenje je rezultat upićivanja osuđenika na izdržavanje kazne elektronskim nadzorom[245].

5.2 Elektronsko praćenje poštanskih usluga

Razvoj poštanske industrije može se posmatrati kao jedan je od najvećih i najbitnijih momenata u razvoju ljudskog društa iz ugla trgovine i prenosa robe. Tokom poslednjih dvadeset godina značajni koraci su napravljeni u cilju unapređenja poštanskih servisa i povećanju poverenja korisnika u online poštanske usluge. Razvoj digitalne industrije i informaciono komunikacionih tehnologija svakako se odrazio i na razvoj poštanskih servisa koji su danas dostupni građanima. U jednoj od studija objavljenoj od strane Universal Postal Union (UPU) navedeno je da postoji 55 različitih eloktronskih poštanskih servisa. Svi oni su trenutno u upotrebi širom sveta[246]. Različiti poštanski servisi koji su u ponudi građanima rade na različite načine, i zahtevaju upotrebu različitih tehničkih rešenja. Jedan od servisa takozvana brza kurirska služba je globalni brend koja služi za dostavljenje pošiljki od pošiljaoca do primaoca na najbrži mogući način. Pošte u više od 200 zemalja širom sveta nude ovakve servise za dostavljanje dokumenta i robe. Pored poštanskih kompanija u vlasništvu države razvio se veliki broj sličnih privatnih kompanija za brzu dostavu dokumenta i robe. Ključna stvar kod ovakvih servisa jeste da se dostava završi u unapred definisanom periodu vremena, kako bi potrošači bili zadovoljni.

---

[243] Brief for Respondent at 1, Grady v. North Carolina, No. 14-593 (Feb. 4, 2015).

[244] Bodi, A. „Monitoring for Life: Satellite Surveillance of Ex-Offenders“, American Criminal Law Review, Available at: http://www.americancriminallawreview.com/aclr-online/monitoring-life-satellite-surveillance-ex-offenders/, date: 05.02.2018.

[245] Stacey L. Sklaver, „The Pros and Cons of Using Electronic Monitoring Programs in Juvenile Cases“, Juvenile Justice Committee Newsletter, No.5. Washington, D.C.: American Bar Association.

[246] Corredera, D. „Measuring postal e-services development“, A global perspective. UPU, Berne, 1-20, 2012.

Drugi vid servisa koji se pojavio sa upotrebom elektronskih servisa u poštanskim uslugama jeste i elektronsko praćenje pošiljki. Ovakva usluga jako je bitna jer obezbeđuje informaciju o trenutnoj lokaciji paketa, pa se na osnovu toga može utvrditi tačno vreme pristizanja paketa. Potrebne informacije se prikupljaju počevši od sortiranja paketa, skladištenja u polaznom i usputnim skladištima pa sve do trenutka dostavljanja primaocu. Primaoc i pošiljaoc putem ovog vida servisa online mogu pratiti paket kroz lokaciju u usputnim skladištima ili putem GPS tehnologije na vozilu u kome se paket nalazi[247]. Dokaz da je ovakav sistem praćenja pošiljki jako popuparan je i broj korisnika ovog sistema. Primera radi sa pojavom ovog sistema broj korisnika u periodu od 1995. godine do 1999. godine bio je 3,3 miliona dnevno. Rad ovakvih servisa znatno je napredovao sa pojavom web portala koji nude isključivo usluge praćenja pošiljki bez obzira o kojoj se kompaniji radi[248]. Neke kompanije su otišle i korak dalje pa u okviru svog sistema za dostavu pošiljki nude klijentima pored informacije o vremenu kada je paket dostavljen i vizualni pregled digitalnog postpisa primaoca. Ovakva vid praćenja paketa najčešće je u upotrebi kada su poslovni subjetki akteri u procesu razmene pošiljki.

Najčešće sami proces praćenja paketa zasnovan je na jednistvenom broju koji se dodeljuje svakom paketu prilikom preuzimanja paketa od strane klijenta. Ovaj broj najčešće je alfanumerički kod i ovaj kod se sastoji od trinaest alfanumeričkih karaktera. Svaki broj je podeljen u tri grupe karaktera od kojih svaka predstavlja jedinstvenu oznaku. Prva grupa se sastoji od dva karaktera i predstavlja tip pošiljke. Druga grupa se sastoji od devet alfanumeričkih karaktera i predstavlja originalni broj pošiljke. Poslednja treća grupa sastoji se od dva alfanumerička karaktera koji predstavljaju zemlju odakle je paket poslat. Primera radi brojevi pošiljki mogu izgledati ovako: EE123456785US, RR123456785US i CP123456785US. Poslednja dva karaktera označavaju da je pošiljka poslata iz Amerike. Broj pošiljke se nakon dodeljivanja šalje primaocu putem SMS-a ili maila u zavisnosti od toga kako je pošiljaoc naglasio. Takođe pored samog paketa vreće i kontejneri u kojima se paketi prenose imaju jedinstveni identifikacioni kod. Ovaj kod sastoji se od sedamnaest alfanumeričkih karaktera podeljenih u četiri grupe. Prvih šest karaktera predstavljaju originalni broj vreće ili kontejnera. Sedmi karakter predstavlja tip vreće ili kontejnera, dok karakteri od osam do dvanaest predstavljaju ZIP kod poštanske ispostave odakle se pošiljka šalje. Poslednjih pet karaktera predstavljaju ZIP kod pošte primaoca. Ovakav način označavanja veoma je bitan kod pošiljki koje se distribuiraju između pošiljaoca i primaoca koji su u različitim državama ili na različitim kontinentima.

Kao zamena za obeležavanje pomoću već pomenutih kodova u novije vreme pojavljuje se i obeležavanje paketa pomoću RFID (Radio Frequency Identification) mikročipova. Ovaj čip se može postaviti na paket koji se šalje, vreću za pakete, kontejner za pakete, vozilo za prevoz paketa i druge ibjekte čije je kretanje potrebno pratiti. Sistemi zasnovani na RFID su pasivni i prenos podataka se vrši samo kada se

[247] Esser, M., „Industry Developed Temperature Tracking Device for Packages May Have Climate Metrology Applications“, NIST Tech Beat, 2011.

[248] Basu, S. „10 Package Tracking Websites for Alternative Ways to Track Your Shipments. Aveilable at:http://www.makeuseof.com/tag/10-package-tracking-websitesalternative-ways-track-shipments/, date: 26.12.2015.

ovaj čip približi radaru. Radar ili čitač emituje radio signale koji aktiviraju RFID čip, koji nakon toga prenosi informacije putem unapred definisane radio frekvencije. Ove informacije je prihvataju i prenose do centralne baze podataka[249]. Ovakav način praćenja paketa korišćen je u malom broju slučajeva kod praćenja određenog broja pisama i pošiljki. Međunarodna poštanska korporacija trenutno prati kretanje paketa i poštanske sandučiće pomoću RFID u više od 50 zemalja. Takođe postoje i RFID sistemi uz pomoć kojih je u potpunosti automatizovan ceo proces dostave pošiljki, počevši od prijema pošiljki preko razvrstavanja pa se do dostave. Ovakav sistem je uspešno testiran na poštanskim sandučićima u Korei. Još jedna upotreba RFID je umesto poštanskih marki. Kako bi se zadržala tradicionalna vrednost poštanskih marki RFID čip je umetnut na tradicionalnu potansku marku. Ovakva simbioza otvorila je mogućnosti za poboljšanje kvaliteta poštanskih usluga kao i prostor za razvoj novih servisa[250].

Poštanske usluge u vidu slanja paketa veoma često bivaju iskorišćene u nelegalne svrhe. Kako bi korisnicima pružile što je moguće kvalitetniju uslugu i obezbedile svoje meso na tržištu poštanske kompanije kako one u valsništvu države tako i u privatnom vlasništvu sve manje obaraćaju pažnju na sadržinu paketa. U najvećem broju slučajeva pošiljaocu se veruje na reč kada je upitanju sadržaj paketa koji se šalje. Tačnije pošiljaoc je u obavezi da prijavi tačan sadržaj paketa kao i njegovu vrednost. Činjenica da poštanski službenici ne proveravaju sadržaj paketa otvara mogućnosti za razne zloupotrebe. U najupečatljivije kategorije svrstavaju se slanje narkotika i ilegalnih lekova, slanje oružja i municije, kao i dostava robe koja je predmet trgovine u delu sive ekonomije. Svakoga dana lica koja je bave zloupotrebom profesionalnosti poštanskih usluga pronalaze načine kako da svoje ilegalne aktivnosti sprovedu u delo. Primera radi ljudi koji se bave dilovanjem narkotika iste pakuju u manja pakovanja u vidu lekova ili bilo kakvih drugih predmeta i šalju poštom na odgovarajuće adrese radi dalje distribucije. Jedan od primera distribucije narkotika putem poštanskih servisa zabeležen je u Filadelfiji. Dva brata vršila su distribuciju metamfetamina putem Express pošte između dva grada. Distribucija je vršena pakovanjem u narkotika u unutrašnjost cevi. Inspektori su istragom ustanovili da su dileri za potrebe slanja koristili U.S mail kao i druge privatne transportne kompanije[251].

Poštanski ispektori kao i jedinica za narkotike San Dijega uhapsli su čoveka koji je za potrebe distribuiranja anabolic steroids, ketamina i drugih zabranjenih supstanci koristio U.S poštu. Okrivljeni je porudžbine primao putem Interneta, dok je za distribuciju koristio brzu poštu i prioritet poštu kao dva servisa U.S. pošte. Ovo lice dnevno je distribuiralo robu u vrednosti od 5000 dolara, dok se broj stalnih korisnika kretao oko 300[252].

---

[249] Stanivuković, B., Marković, D. „RFID u funkciji poštanske marke–čipovanje poštanskih pošiljaka“, In XXXII Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – PosTel, 2. i 3. Decembar 2014, pp. 3-14, Beograd.

[250] Spalević, Ž., Ilić, M., Palević, M. „Electronic tracking of postal services“, in Proceedings of 3rd the International Scientific Conference on ICT and e-Business Related Research - Sinteza 2016, Belgrade, pp. 479-485.

[251] IDTA. „Illegal Drugs and Trafficking. Annual Report of Investigations“, United States Postal Inspection Service. pp. 26-28. 2002.

[252] Ibidem

Nakon što je rekreaciona upotrebe marihuane postala legalna u nekoliko zemalja učestala je praksa slanja paketa sa marihuanom iz zemalja u kojima je njena upotreba dozvoljena u zemlje u kojima nije. U pojednim slučajevima ovaj narkotik je upakovan u vakum kese ili dobro uvijene pakete kako bi se sprečilo širenje mirisa. Tokom 2014 godine poštanski inspektori su zaplenili preko 40 hiljada kilograma ovog narkotka upakovanog i poslatog putem nekog od servisa pošte[253].

Kao što je već navedeno još jedan od tipova zloupotrebe poštanskih servisa je i slanje oružja i municije. U najvećem broju slučajeva oružje i municija se pakuje tako da podseća na neki uobičajeni objekat određene težine i zapremine. Takođe opis paketa koji se daje zaposlenom poštanske kompanije prilikom predaje paketa obično ukazuje na metalni bojekat. Na ovakv način opravdano je reagovanje metalnog detektora prilikom provere paketa. Ukoliko je komad otužja koji se šalje veliki on se najčešće rastavlja pa pojedinačni delovi se šalju na istu ili različite adrese. Kupac će pojedinačne delove preuzeti na unapred definisanim adresama. Jedan od primera u Sijetlu pokazuje dva brata koja su uhapšena i proglašena krivim zbog slanja oružja na Tajland. Jedan od braće živeo je na Tajlandu dok mu je drugi brat slao oružje iz delova. U jednoj od pošiljki za koju je navedeno da se nalaze metalna kućišta za elektronske komponente nalazili su se saržeri za pištolj kalibra .45. Veruje se da je ova grupa odgovorna za više od 240 pošiljki zabranjenog oružja[254].

U Kanadi su otkriveni kriminalci koji su koristili putem poštanskih servisa ilegalno distribuirali pištolje, granate, pancirne prsluke, municiju i opasne hemikalije. Pemenuta militara oprema je bilo u komadu ili rastavljena dopremana u Kanadu iz inostranstva[255].

Da je slanje pomenutih dobara putem poštanskih kompanija zabranjeno govori i podatak da je Zakonom o poštankim ulugama decidno navedeno koji predmeti i materije se ne smeju slati u vidu pošiljke[256]. U zabranjene pošiljke spadaju:

- opasne i štetne materije, kao i predmeti čiji prenos ugrožava zdravlje i život ljudi. U ovu grupu spadaju i druge poštanske pošiljke, poštanska postrojenja i transportna sredstva i oprema. Izuzetak su materije čiji je prenos dozvoljen pod uslovima i na način koji je utvrđen zakonom.
- opojne droge, izuzev u slučajevima kada su primalac i pošiljalac ovlašćeni za promet drogom ili pak imaju ovlašćenje za njihovo korišćenje.
- žive životinje, izuzev u slučajevima kada je ovakav prenos regulisan posebnim uslovima za obavljanje poštanske delatnosti.
- druga roba i predmeti čiji je prenos zabranjen zakonom i drugim propisima.

---

[253] Goudie, C., Marcoff, B., „Mailing marijuana: Officials report spike in pot-laden packages“, Eyewitness News.
[254] Brock, T., „Two brothers plead guilty to illegally shipping gun parts to Thailand“. 2013.
[255] Bronskill, J. „Criminals using Canada Post to transport illicit goods — including a rocket mlauncher — RCMP report says“, National Post.
[256] Zakon o poštanskim uslugama, Opus citatum, član 29.

Slobodno se može reći da u poslednju kategoriju zabranjenih pošiljki spadaju oružje i municija jer je nihova distribucija zabranjena zakonima i pod zakonskim aktima koji regulišu ovu oblast. U cilju što efikasnije borbe sa ovakvim vidom zloupotrebe servisa građana i kriminalim aktivnostima radnici poštanskih ispostava i pripadnici policijskih snaga moraju raditi zajedno. Ovo praktično znači se zakonskim regulativama službenicima na prijemu paketa moraju dati veća ovlašćenja u pogledu provere sadržine paketa. Na ovakav način paketi sumnjivih lica će uz pristustvo organa raduženih za poslove provere bit provereni ili prilikom same predaje ili u nekom od momenata sortiranja. Naravno da broj pošiljki koji se pošalje tokom dana, kao i zalaganje radnika za što efikasnijim prijemom ne ostavljaju prostora za proveru svakog paketa, ali ukoliko takva mogućnost postoji i primenjuje se u praksi manji broj prestupnika će se odvažiti na ovakav korak.

5.3 Elektronski servisi u turizmu

Razvoj informaciono komunikacionih tehnologija poslednjih decenija ostavio je uticaj na veliki broj oblasti svakodnevnog života i rada ljudi. S tim u vezi sa razvojem ICT razvijali su se i servisi dostupni u turističkoj industriji. Softwerska rešenja 20-veka primenjena u turističkoj industriji često se nazivaju e-turizam. U turističkoj industriji sve je više usluga koje se pružaju turistima, a zasnivaju se na upotrebi Interneta kao glavnog komunikacionog kanala. Upotreba specijalizovanih softverskih aplikacija kompatibilnih sa modernim elektronskim uređajima, interakcija između građana i turističkih organizacija otvaraju jednu novu dimenziju u turizmu. Generalno sve aplikacije se mogu svrstati u nekoliko kategorija[257]:

- Aplikacije za planiranje prevoza. Ove aplikacije se baziraju na pružanju informacija o konkretnom letu ili trenutnoj lokaciji vozila u drumskom saobraćaju. Putnici dobijaju informacije direktno od kompanije koja pruža usluge ili drugih korisnika aplikacije. Na ovakav način korisnici mogu u realnom vremenu imati informaciju o tome koliko je recimo autobus koji čekaju udaljen od njihove stanice, ili da li je došlo do kašnjenja leta i koliko kašnjenje iznosi. Takođe ovakve aplikacije se koriste za razmenu infomacija između korisnika o različitim vidovima prevoza na konkretnim turističkim destinacijama.
- Aplikacij za planiranje odmora. Korisnik sa Interneta preuzima aplikaciju uz pomoć koje će dobiti sve neophodne informacije. U većini slučajeva ove informacije sadrže podatke o znamenitostima, atrakcijama, hotelima i restoranima, najboljem načinu putovanja do same destinacije itd. Prednosti ovakvih aplikacija su višestruke, posebno zbog činjenice da u najvećem broju slučajeva ovakve aplikacije nude mogućnost pretrage informacija vezanih i za mnoge druge destinacije. Na ovakav način korisnik u svakom trenutku ima na raspolaganju najnovije informacije

[257] G. Bendon, S. Hundson, „Our mobile future: how smartphones will transform visiting experiences“. Horizon Digital Economy Research, London, 2010

u vezi sa nekom destinacijom. Takođe, pored informacija o postojećim destinacijama, aplikacije se ažuriraju i informacijama o novim destinacijama koje su dodate u bazu podataka sistema od momenta poslednjeg ažuriranja.

- Turistički vodiči. Generalno se sastoje od online vodiča koji sadrži informacije i preporuke o restoranima, šoping centrima, turističkim atrakcijma, noćnim klubovima itd. Ove aplikacije su zamena za papirne turističke vodiče uz veliku pogodnost zasnovanu na stalnom obnavljanju informacija. Takođe u najnovije informacije o konkretnom turističkom lokalitetu često dolaze i različiti komentari posetioca i kritičara.
- Aplikacije u službi kompanija. Veoma važni servisi u okviru e-turizma jesu i aplikacije za pretragu i rezervaciju letova, smeštaja, ulaznica za različite turističke atrakcije i znamenitosti. Ranije je proces pronalaženja željenog hotela u mnogim slučajevima bio u najmanju ruku iscrpljujući i vremenski zahtevan. Prelazak sa tradicionalnog načina rezervisanja smeštaja na rezervisanje pomoću online aplikacija donelo je velike prednosti kako potencijalnim turistima, tako i konkretnim davaocima usluga. Koliko je online rezervacija smeštaja postala popularna govori i podatak da veliki broj hotela ima sopsteve sisteme elektronske rezervacije u okviru svojih web portala. Pored toga, sve je veća prisutnost samostalnih servisa koji pružaju usluge pronalaženja i rezervacije smeštajnih kapaciteta. Samostalni online servisi su sprega između hotelijera i potencijlalnih gostiju. Putem ovih servisa se hotelijerima nudi isključivo mogućnost oglašavanja. Celokupan proces pretrage između smeštajnih kapaciteta koji zadovoljvaju zahteve korisnika sistema kao i sama rezervacija se obavljaju nezavisno od hotelijera. Uvođenje online rezervacije smeštaja smanjilo je probleme koji se javljaju pod uticajem ljudskog faktora, povećalo preciznost, doslednost i ažuriranost informacija.

Svi pomenuti tipovi aplikacija moraju pored pomenutih funkcionalnosti moraju obezbediti određeni stepen zaštiti. Zavisno od toga o kojim aplikacijama se radi, kao i od podataka koje korisnik unosi razlikovaće se se stepen implementirane zaštite. Primera radi aplikacije koje pružaju informacije o konkretnim lokalitetima kao i konkretnim atrakcijama koje korisnik posećuje ne moraju imati složene enkripcione algoritme u pozaditi za zaštitu podataka koje obezbeđuju, iz prostog razloga jer kod ovih aplikacija korisnik ne unosi svoje lične podatke. Posebna pažnja na zaštitu ličnih (osetljivih) podataka korisnika usmerena je kod aplikacija koje zahtevaju iste. Ovo su primera radi servisi za rezervacijurezervaciju karata za avio, drumski, železnički i vodeni saobraćaj, kao i za rezervaciju smeštaja i ulaznica za pojedine atrakcije. U velikom procentu kod ovakvih servisa pored unosa ličnih podataka od korisnika se zahteva i unos broja kreditnih ili debitnih kartica u cilju provere validnost bankovnog računa. Ne retko korisnik putem samih servisa vrši plaćanje dela iznosa konkretne rezervacije ili celokupni iznos. Nivo implementirane sigurnosti servisa koji zahtevaju unos broja kreditnih kartica i plaćanje istim na svojim portalima mora biti na najvećem mogućem nivou. U cilju što efikasnijeg rada i klijenti i turistički servisi moraju dati svoj doprinos. Generalno sigurnosni mehanizmi implementirani su na klijentskoj strana, u komunikaciji između klijentske i serverske strane i na strani samog servisa. Na klijentskoj strani od korisnika servisa se zahteva kreiranje naloga na konkretnom

servisu. Prilikom kreiranja naloga pored ličnih podataka od korisnika se zahteva i kreiranje šifre za logovanje. Korisnik bi trebalo da samu šifru kreira tako da se razlikuje za različite servise kao i da se menja nakon određenog perida vremena. Takođe prilikom korišćenja pogodnosti koje servis nudi korisnik mora voditi računa o bezbednosti mreža sa koje pristupa samom servisu. Takođe korisnik mora voditi računa da u bilo kojoj situaciji ne postane žrtva phishing i pharming napada. Ovo praktično znači da korisnik mora proveriti validnost poruka koje dobija u svakoj situaciji kada se od njega zahteva unos ličnih podataka i podataka o kreditnim karticama koje koristi za dati servis[258].

Komunikacija između klijenta i servera kao i sami prenost podataka moraju biti zaštićeni. Ovo se obezbeđuje implementiranje sigurnosnih protokola. Sigurnosti mehanizmi u konekciji između klijentske i serverske strane pomenutih servisa istovetni su sigurnosnim mehanizmima baziranim na TCP/IP protokolu objašnjenom u odeljku elektronskog bankarstva. Što se tiče zaštite podataka na strani samog servisa, tačnije kompanije koja poseduje servis stavljen u službu građana zaštita se zasniva na adekvatnom radu sa podacima korisnika kao i njihovom adekvatnom čuvanju. Čuvanje ličnih korisničkih podataka regulisano je Zakonom o zaštiti podataka o ličnosti[259]. Ovim zakonom definisano je da se zaštita podataka o ličnosti obezbeđuje se svakom fizičkom licu. Zaštita podataka o ličnosti ne sme biti izuzeta zbog državljanstva, rase, godina života, pola, jezika, veroispovesti, političkog ili drugog uverenja, nacionalne pripadnosti, socijalnog statusa, imovinskog stanja, obrazovanja, društvenog položaja ili drugih ličnih svojstava[260].

Prema Evropskom zakonu o zaštiti podataka svi servisi koji rade sa ličnim podacima korisnika moraju obezbediti mehanizme koji će sprečiti neautorizovani pristup i zloupotrebu ličnih podataka njihovih korisnika[261]. Mnogi od servisa radi adekvatne zaštite a u skladu sa ovim zakonom definišu sopstvene pravilnike. Najčešće se u njima navodi da isključivo autorizovano osoblje ima pristup bazi podataka koja sadrži lične podatke korisnika. Podaci sa platne kartice se obično u sistemu čuvaju do maksimano deset dana nakon boravka korisnika. Nakon toga ovi podaci se ili brišu ili heširaju u sistem radi zaštite od mogućih prevara. Ovakav metod podrazumeva pamćenje podataka o kreditnoj kartici, ali bez poslednje četiri cifre broja kartice.

Pored konkretnih zakonskih regulativa propisanih ovim zakonom kao i Zakonom o zaštiti potrošača svedoci smo velikog broja zloupotreba i problema koji nastaju upotrebom elektronskih servisa. Jedan od primera neadekvatnog rada sa ličnim podacima korisnika jesu i problemi koji su se javili u korišćenju portala u vlasništvu Hippo hotela u Velikoj Britaniji. Ovaj servis je kao potvrdu uspešne rezervacije

---

[258] Ilić, M., Spalević, Ž., Veinović, M., Spalević, Ž. „Electronic services for tourist destination reservations“, Zbornik radova 15. Međunarodno naučno-stručnog Simpozijuma INFOTEH, Jahorina, vol. 15, pp. 621-626, 2016.

[259] Zakon o zaštiti podataka o ličnosti, „Sližbeni glasnik RS“, Opus citatum

[260] Ibidem, član 1.

[261] Boillat, P., Kjaerum, M. „Handbook on European data protection law“, Publications Office of the European Union, Belgium, 2014.

smeštaja klijentima slao link ka samoj potvrdi. Link je u svom pozivu sadržao veliku količinu ličnih podataka i podataka o vremenu boravka. Web strana koja je sadržala podatke o rezervaciji nije vršila bilo kakvu autentifikaciju korisnika, kako bi se utvrdilo da li osoba može da pristupi podacima. Otvaranje strane zasnivalo se na ID broju klijentovog naloga koje je takođe bio prosleđen u okviru linka. Ukoliko bi zlonamerni korisnici došli u posed ovakvog linka, sa vrlo malo izmena ID broja mogli bi da pristupe i nalozima drugih korisnika[262]. Sa aspekta sigurnsoti pojavio se drugi problem na server strani. Tačnije server je imao podršku samo za SSLv2, SSLv3, i TLSv1.0. Nije postojala podrška za novije protokole kao što su TLSv1.1 or TLSv1.2. Takođe nije postojala podrška za Perfect Forward Secrecy. Ovakve ranjivosti sistema mogu ostaviti na hiljade korisnika opasno izloženih napadu.

Krajem 2015 godine korporacija Hajat objavila je da su gosti ovog hotelskog lanca bili pod napadom. Sprovedena istraga pokazala je da su kompjuterski sistemi bili pod napadom PoS (Point-of-Sale) malvera čiji je cilj bio neovlašćeni pristup podacima sa platnih kartica (ime vlasnika, broj platne kartice, datum isteka i verifikacioni kod). Najveći procenat napada bio je usmeren pre svega na kartice kojima je vršeno plaćanje u restoranima, plaćanje spa tretmana, parkinga kao i prilikom plaćanja smeštaja na recepcijama. Ukupno 250 hotela bilo je pogođeno ovim malverom. Sa stanovišta internet plaćanja ukradeni podaci su neophodni za korišćenje bilo koje kartice[263].

Pored hotelskog lanca Hajat, pod sličnim napadom bio je i sistem Mandarin Oriental hotelskog lanca u 2013. godini. Broj napadnutih platnih kartica iznosio je oko hiljadu [264]. Lanac hotela sad već izabranog predsednika Amerike Donalda Trampa (Donald Trump) napadnut je počevši od februara 2015. godine. Napad je registrovan tako što su banke uočile isti šablon prevara na računim svojih klijenata koji su bili gosti ovog hotelskog lanca. Veza između svih ovih hotela koja je i dovela do napada jeste sistem za vođenje hotela kompanije White Lodging Services Corporation. Ovaj sistem koji je služio za sve poslove u okviru hotela od prijavljivanja gostiju do svih tipova plaćanja nije imao odgovarajući stepen zaštite.

Veliki broj problema javlja se prilikom različitih rezervacija. Najizraženiji problemi jesu lažne rezervacije ili plaćanje. Ovakvi problemi se dešavaju kada hoteli ili avio kompanije ne dobiju nikakvu potvrdu o rezervaciji i plaćanju smeštaja ili leta, dok kompanije koje se bave posredništvom tvrde da je celokupan proces rezervacije prošao neometano. Veoma često ove kompanije imaju posebne propise kojima ne prihvataju bilo kakvo vraćanje novca. U tom slučaju pored neprijatnosti u toku putovanja turisti vrlo često ostaju i bez svog novca.

---

[262] Helme, S. „Hotel Hipo Insecure, so I've herd", Available at: https://scotthelme.co.uk/hotel-hippo-insecure/, date: 15.06.2017.

[263] Sheppard, S. „Notifies Customers Of Malware Activity", Available at: http://newsroom.hyatt.com/news-releases?item=123450, date: 20.06.2017.

[264] Vaas, L. „Mandarin Oriental hotel chain confirms credit card breach", Naked Security by Sophos. Available at: https://nakedsecurity.sophos.com/2015/03/06/mandarin-oriental-hotel-chain-confirms-credit-card-breach/, date: 12.12.2017.

Drugi veoma frekventan problem jeste dobijanje smeštaja koji gost nije rezervisao. Kako servisi za rezervaciju jedino na osnovu komentara i pritužbi korisnika mogu prikupiti informacije o stvarnom stanju smeštaja koji je dat u ponudi veoma često se događa da korisnik dobije smeštajnu jedinicu koja je u daleko lošijem stanju od stanja prikazanog na web portalu servisa. Tako na primer, gosti umesto sobe sa dva odvojena ležaja mogu dobiti sobu sa jednim ležajem za dve osobe, ili sobu čiji su higijenski uslovi jako loši. Materijal (slike, video, tekstualni opis) na kome je baziran prikaz smeštaja u okviru web portala za rezervatiju smeštaja obično datira iz vremena kada je smeštajna jedinica prvi put otvorena.

Grčka policija je u saradnji sa Interpolom otkrila veliku prevaru širom Grčkih letovališta u kojoj su oštećeni izgubili na hiljade eura. Prevara se odigrala kroz četiri lažna web portala za rezervaciju smeštaja. Vlasnici portala su za obavljene rezervacije naplatili depozit, zatim rezervacije u poslednjem trenutku otkazali i zadržali novac. Turisti su o otkazivanju rezervacije saznali tek po dolasku u hotel. Ovakva prevara je uspela jer su rezervacije zaista bile obavljene pa su turisti proverom sa osobljem hotela dobili informacije da su njihove sobe rezervisane. Uplata depozita je izvršena direktno na bankovni račun, a ne posredsvom sistema za rezervaciju, što je u mnogome olakšalo prevaru[265]. Veoma je važno da korisnici portala provere gde su portali koje koriste registrovani i koliko dugo su u funkciji. Portali koji su učestvovali u prevari bili su registrovani u proseku oko godinu dana, što je kratak period[266].

Jedan od vidova prevare sa smeštajem jeste i rezervacija jeftinijeg hotela za mnoge veće sume novca. Ovakvi hoteli imaju obično ista imena kao hoteli visoke kategorije. Turisti prilikom rezervacije na osnovu imena i opisa hotela zaključuju da se radi o hotelu koji zaista žele da rezervišu. Turisti koji obave rezervaciju obično u sklopu nje dobijaju i uslugu organizovanog prevoza do hotela. Taksi prevoz ih umesto u hotel visoke kategorije odvodi u hotel pod istim imenom, ali daleko lošijeg kvaliteta.

Pretplata cene smeštaja kao vid prevare događa se prilikom takozvanih specijalnih ponuda. Naime putem određenih portala vlasnici hotela kreiraju korisničke naloge putem kojih vrše rezervaciju svojih smeštajnih kapaciteta još pre početka sezone[267]. Prilikom pretrage hotela ovako rane rezervacije kod drugih korisnika portala ostavljaju utisak atraktivnosti smeštaja. Vlasnik hotela u sezoni otkazuje pojedine rezervacije i objavljuje smeštajnu jedinicu kao slobodnu po većoj ceni od prvobitne. Ovako slobodna smeštajna jedinica publikuje se kao specijalna ponuda i za ovakve ponude se obično zahteva uplata celog iznosa novca. Kod ovakvih ponuda ukoliko cena nije

[265] Žaklina Spalević, Kosana Vićentijević, „Challenges of forenic accounting in tourist industry“, Second International Thematic Monograph - Thematic Proceedings: Modern Management Tools and Economy of Tourism Sector in Present Era, pp.230-239, 2017.

[266] Žaklina Spalević, Željko Spalević, „Terorizam kao prijetnja hotelijerstvu“, International Thematic Monograph – Thematic Proceedings: Modern Management Tools and Economy of Tourism Sector in Present Era, pp. 520 - 528, Dec, 2016

[267] Miloš Ilić, Žaklina Spalević, „Primena elektronskih servisa u turizmu“. International Thematic Monograph - Thematic Proceedings: Modern Management Tools and Economy of Tourism Sector in Present Era, pp. 336-344, 2016.

uvećana izostavljen je određeni broj usluga koje su inače uključene u cenu smeštaja. Postoje servisi koji se bave samo prikupljanjem i publikovanjem ovakvih ponuda.

Kod servisa za rezervaciju ili kupovinu karata za avio ili drumski saobraćaj dešavaju se propusti kada prevoznička kompanija promeni vreme i dan polaska ili otkaže polazak, a putnik ne bude obavešten o konkretnoj promeni. Ovakva promena može uzrokovati niz drugih problema u organizaciji puta. Primera radi, ukoliko korisnik putuje sa presedanjem moraće da otkaže ostatak putovanja kao i smeštaj. Zbog kasnog otkazivanja putnik sigurno neće dobiti povraćaj novca koji je dat kao depozit. U najvećem broju slučajeva moraće da plati pun iznos karti kompanijama kojima je morao da otkaže aražman.

Razvoj e-turizam servisa svakako nije oblast u stagnaciji. Pored sigurnostih mehanizama koji se stalno unapređuju velika požnja usmerena je ka primeni cloud computing-a. Cloud computing (računarstvo u oblaku) je skup standardizovanih IT performansi, isporučenih korisnicima putem interneta, na bazi samoposluživanja i plaćanja po korišćenju. E-turizam servisi bazirani na cloud-u nude mogućnosti deljenja informacija između turista, državnih i privatnih turističkih agencija, hotela, osiguravajćih kuća itd. Jedan od vidova upotrebe cloud turizma mogu biti mobilne aplikacija za deljenje informacija o turističkim destinacijma. Na primer, ovakav sistem se zasniva na korišćenju javnog cloud-a. Samoj cloud infrastrukturi pristupa se pomoću nekog od elektronskih uređaja u cilju prenosa informacija na cloud. Servis je organizovan tako da korisnici dodaju informacije o lokaciji na kojoj se nalaze, kao što su naziv lokacije, informacije o hrani i piću, različitim aktivnosti koje lokacija nudi, događajima i svojim utiscima. Informacije mogu da budu u vidu multimedijalnih poruka, slika i zvuka. Obaveštenje o novo dodatoj informaciji se od strane cloud servisa prosleđuje svim korisnicima ovog servisa. Korisnik, nakon primanja obaveštenja o novoj informaciji, može uz pomoć preuzete aplikacije na svom uređaju da pogleda sve detalje. Analizom podataka koji se šalju u okviru ovog servisa, državne agencije za kontrolu rada turističkih agencija, prevoznika i hotela mogu dobiti više informacija o eventualim problemima. Iz tog razloga ove agencije su takođe korisnici ovog servisa. Turističke agencije mogu dodati na cloud informacije o novim turistima u vidu odabranog prevoznika, smeštaja, kao i dnevnih planiranih aktivnosti. Ovakve informacije se putem obaveštenja prosleđuju prevoznicima, hotelima i turističkim vodičima koji na osnovu ovih informacija mogu dalje organizovati svoje aktivnosti u cilju pružanja što kvalitetnije usluge.

Upotreba cloud computing-a u sprezi sa alatima zasnovanim na GIS (Geographic Information System) i web servisima može biti još jedan od načina promovisanja turističkog potencijala u cilju povećanja broja turista. Na ovakav način kreira se giscloud platforma, koja je zapravo WebGis servis koji pruža turistima besplatne informacije o konkretnom području ili turističkoj destinaciji. Servisi poput ovih baziraju se na privatnim podacima internet korisnika koji su dobrovoljno ustupljeni na korišćenje. Generalna ideja jednog ovakvog servisa je da on bude dostupniji svakodnevnim korisnicima web tehnologija. Iz toga razloga servis može biti povezan sa različitim društvenim mrežama (Facebook, Twiter), platformama za deljenje slika (FlickR, Panoramio) kao i platformama da deljenje video (Youtube, Vimeo).

U upotrebi e-turizam servisa baziranih na colud-u izdvajaju se dva tipa korisnika: turisti kao korisnici servisa kojima su informacije namenjene, i svi ostali korisnici koji kreiraju i dobrovoljno ustupaju na korišćenje sadržaje o nekom području. Svakom od korisnika koji dostavlja sadržaj servisu pruža se mogućnost da pored deljenja svojih utisaka u vidu komentara, slika i videa, konkretne sadržaje poveže sa interaktivnom mapom područja ili konkretnog objekta (hoteli, restorani, atrakcije) za koje su sadržaji vezani. Primera radi vlasnici restorana mogu putem ovakvog servisa reklamirati svoje restorane. Snaga ovakvih servisa zasniva se na dostupnosti prostornih podataka i informacija koje oni nose. Deljenje prostornih podataka od strane korisnika sistema je glavna karakteristika koja može dovesti do unapređenja njihovog kvantititeta i kvaliteta. Organizacija podataka u okviru web portala ili bloga treba takođe da bude što kvalitetnija kako bi korisnici što lakše došli do potrebnih informacija. Informacije mogu biti podeljene u grupe, primera radi:

- turistički objekti restorani i hoteli;
- mesta za obilazak;
- transport;
- kulturno nasleđe;
- mape grada.

Pored same pretrage i pregleda informacija, jedna od kvalitetnih funkcionalnosti koju bi portal trebao da ima jeste i ponuda plana obilaska konkretnog mesta. Ovakav plan bi trebao da ponudi korisniku interaktivnu mapu obilaska najvažnijih atrakcija, mesta za izlazak, restorana, zajedno sa mapom gradskog prevoza. Na ovakav način turisti koji su ograničeni vremenom boravka ili su neodlučni u pogledu dnevnog plana aktivnosti mogu dobiti adekvatne predloge. Servis bi mogao kreirati planove na osnovu parametara koje odabere korisnik. Neki od parametara mogu biti deo grada u kome se korisnik nalazi, vreme koje želi da provede u obilasku, doba dana, itd. Veoma je važno da bi inicijativa za kreiranje ovakvih servisa trebala bi da potekne od turističkih organizacija nekog mesta kao i od resornog Ministarstva trgovine turizma i telekomunikacija svake od zemlja koja ima turističke potencijale. U cilju što kvalitetnije implementacije veći broj organizacija (IT sručnjaci, geografi, turizmolozi, lokalna samouprava) i pojedinaca treba da uzme učešće.

5.4 Sistemi nadgledanja saobraćaja

Svakodnevna putovanja kako javnim prevozom tako i sopstvenim postala su neraskidivi deo svakodnevnog života i rada ljudi. Zbog sve većeg broja prevoznih sredstava zagušenje saobraćaja postalo je značajan problem. Svaki grad može izdvojiti određene ulice ili blokove koji predstavljaju usko grlo u saobraćaju. Saobraćajne nesreće postale su česta pojava na svim vrstama puteva. Kako bi smanjio broj saobraćajnih nesreća i kako bi unapredio saobraćaj veliki broj zemalja uveo je kamere za nadgledanje ulica i saobraćajnica. Ovako koncipirano nadgledanje najpre je

postavljeno na rasksnicama koje predstavljaju usko grlo saobraćaja, a kasnije i na manje frekventnim putevima. Praćenje saobraćaja kao i obrada video zapisa dobijenih sa postavljenih kamera treba da omoguće aktivno unapređenje kontrole saobraćaja, obradu informacija o konkretnoj saobraćajnoj nesreći kao i unapređenje sudskih procesa u ovom domenu. Sposobnost praćenja i prikupljanja podataka o saobraćaju, korišćenjem relevantnih sistema nadzora može pomoći razumevanju mehanike saobraćajne mreže. Napredovanje sistema za monitoring saobraćaja širi se na prikupanje video snimaka ne samo sa saobraćajnih kamera već i sa javnih kamera na prodavnicima, hotelima, poslovnim prostorima, a sve u cilju što većeg broja uglova iz kojih se konkretan prostor može snimiti. Kako bi se obezbedila bolja obrada video strima izvlačenje korisnih informacija i kreiranje paterna ponašanja u saobraćaju koriste se data mining tehnike. Pored video snimka koji je nezamenljiv u procesu obrade, u kreiranje paterna mogu se uključiti i informacije o vremenskim uslovima, brzini vozila, dužini traga kočenje, itd. Kvalitet video snimka kao i opseg pokrivenosti kamere u mnogome zavisi kako od kvaliteta kamere tako i od njene pozicije nad saobraćajnicom. Primera radi ukoliko je kamera na većoj visini imaće veći opseg pokrivenosti pa će određeni prostor moći da se obradi sa manje kamera. U isto vreme rezolucija ovih kamera mora biti daleko veća nego kamera koje imaju manji opseg pokrivnosti.

Kao što je već navedeno data mining tehnike mogu se koristiti u obradi prikupljenih informacija dobijenih iz video snimaka. Ovako koncipirane tehnike omogućavaju istraživačima analizu velikih skupova podataka veoma brzo i efikasno. Premenom data mining tehnika kao što su asocijaciona pravila, klasifikacija, predikcija, klasterizacija i analiza outlier-a mogu se kreirati paterni u struktuiranim podacima[268]. Svaka od ovih tehnika može izvući i označiti entitet koji je specifičan za konkretno istraživanje. Izvlačenjem entiteta identifikuje se konkretan patern iz podataka kao što su tekst, slike, video i audio materijali. U cilju što kvalitetnije klasifikacije podataka, tačnije u cilju kreiranja što efikasnijeg klasisifikatora najpre se vrši predobrada podatka. Predobrada je bukvalno transformacija podataka kojom se otklanjaju nepotrebne informacije, šumovi i ostale nesavršenosti videa. Ovakve nesavršenosti obrađuju tehnike za obradu slika. Na osnovu novodobijenih podataka veoma je lako izvršiti obuku klasifikatora kako bi u obradi videa pravio razliku između uobičajenih scena u saobraćajnim snimcima, kao što su vozila, semafori ili pešaci. Za ovakav tip klasifikacije principal component analysis daje kvalitetne rezultate, jer će frejmovi sličnih slika imati slične osobine. Tehnike koje su u upotrebi za klasterizaciju podataka grupišu podatke sa sličnim karakterisitka u klastere sa ciljem minimizacije ili maksimizacije unutar klasterske sličnosti. Primera radi ovakve tehnike mogu se koristiti za identifikovanje kritičnih mesta na saobraćajnicama gde se nesreće događaju na sličan način. Ovo je posebno značajno ukoliko je procenat saobraćajnih nesreća na tom delu puta jako veliki. Zbog nestruktuirane prirode video podataka predobrada korišćenjem image processing-a ili computer vision-a je podrazumevana kako bi se dobio struktuirani format karakteristika bitnih za dalju obradu. Za razliku od klasičnog obrađivanja video

[268] S. Nagesh, „Roll of Data Mining in Cyber Security“, Journal of Exclusive Management Science, vol. 2/2013, pp. 1.

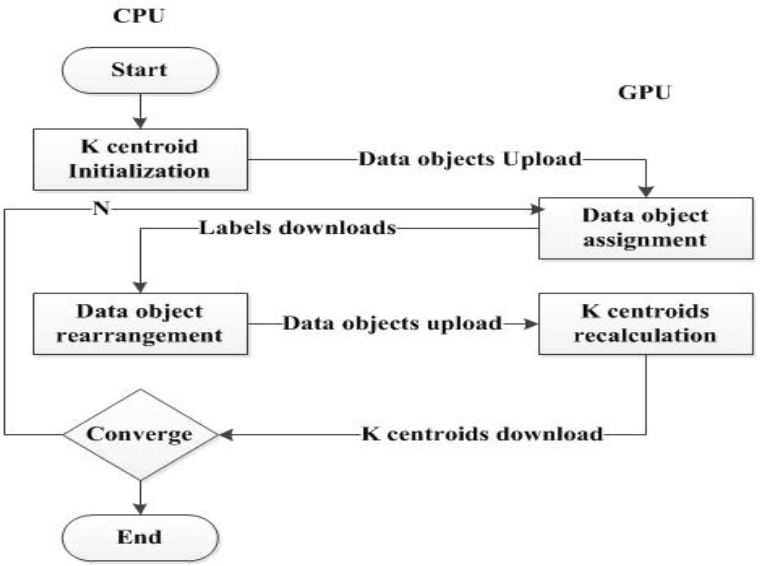
zapisa, gde lice zaduženo za obradu mora pregledom snimka ustanoviti bitna mesta za konkretan događaj koji se obrađuje, upotrebom algoritama za prepoznavanje paterna takva mesta se automatski označavaju. U samom algoritmu za prepoznavanje paterna ovakva mesta se unapred definnišu pa algortiam u toku obrade vrši prepoznavanje poklapanja šablona sa konkretnom situacijom. Primera radi ukoliko hoćemo da vršimo praćenje konkretnog automobila na određenim delovima puta snimljenog sa više kamera, definisaćemo kriterijum u okviru algoritma za prepoznavanje uzorka na osnovu osobina automobila koji se prati[269]. Kada su svi marketi postavljeni, algoritam klasterizacije može da se pokrene. Zavisno od potreba veći broj klasterizacionih algoritama sa različitim kriterijumima klasterizacije može se definisati u procesu obrade videa.

Jedan od algoritama klasterizacije koji se može koristiti za pronalaženje abnormalnosti u videu je k-means algoritam. Ovaj algoritam kreira klastere tako što minimizuje rastojanje između klastera. Kada su upitanju video podaci k-means radi sa segmentima video podataka. Ovo praktično znači da recimo video obrađen i kompresovan pomoću H.264 dekodera mora biti podeljen u segmente nakon čega će sami segmenti biti klasterizovani. Tako dobijeni klasteri predstavljaju vezu između segmenata. U ovom kontekstu segmenti se generišu sa svakim frejmom[270]. Na početku izvršenja k-means algoritam počinje sa k random odabranih centroida koje predstavljaju centre klastera. Svaki elekment koji je potrebno rasporediti u klastere raspoređuje se u klaster čijoj je centroidi najbliži. Nakon toga algoritam pomera centre klastera u prostoru kako bi minimizovao rastojanje između centroide i segmenata u kreiranom klasteru[271]. Minimizacija se izvršava iterativno ponavljanjem dva koraka sve do trenutka dok se ne dostigne kriterijum za prekid. Pomenuta dva koraka mogu se definisati na sledeći način:

1. Za svako p ∈ P odrediti njegov najbliži centar iz skupa {c1, . . . , ck}. Podeliti P u k seta C1, . , Ck tako da svako Ci sadrži sve tačke čiji je najbliži centar ci. Ovako definisano P predstavlja ulaznu instancu, dok Ci predstavlja klastere.
2. Za svaki klaster Ci odrediti njegovu centoridu C(Ci), tačnije optimalni centar klastera. Nakon toga postaviti ci = C(Ci) za svako $1 \leq i \leq k$.

[269] D. Saravanan, S. Srininvasan, „Video Image Retrieval Using Data Mining Techniques“, Journal of Computer applications, vol. 5/2012, pp. 39-42.
[270] D. Dailey; F.Cathey; S. Pumrin, „An algorithm to estimate mean traffic speed using uncalibrated cameras“, IEEE Transactions on Intelligent Transportation Systems, vol.1/2000, pp. 97-108
[271] Spalević, Ž., Ilić, M., Arsić, N. „Legal aspects of data mining algorithms for stream processing in traffic surveillance“, Journal of criminalistics and law, Academy of criminalistic and police studies, Belgrade – The Republic of Serbia, Num. 1, pp. 57-79, 2016.

Kako je k-means algoritam iterativan i kako je u obradi videa brzina veoma bitan faktor ove dve osobine se sukobljavaju. Iz tog razloga kako bi se klasterizovanje video podataka ubrzalo k-means algortam se može implementirati tako da se izvršava na GPU[272]. Za samu video kompresiju mogu se iskoristiti prednosti grafičkog procesora, nakon čega se mogu klasterizovati video segmenti na GPU takođe. Motivacija je usmerena ka redukovanju broja operacija. Tačke podataka koje je potrebno klasterizovati su sačuvane u vidu tekstura, dok se rastojanje svake od tačaka podataka od svake centroide izračunava paralelno. Izračunata rastojanja se dodeljuju u bafer od strane fragment programa. Nakon toga se trenutno rastojanje bafera upoređuje sa rastojanjem koje se dobija od narednog fragmenta. Upisivanje rastojanja u bafer se nastavlja sve dok se izračunavanje rastojanja za sve centroide ne završi. Rezultat ovakvog procesa je ubrzanje procesa klasterizacije između 1,5 i 3 puta u poređenju sa iterativnim postupkom implementiranim na CPU. Najbolje performase se dobijaju kada se deo procesa izvršava na GPU a deo procesa na CPU. Na ovakav način koriste se najbolje performanse CPU i GPU arhitekture. Sa slike 3 može se videti sprega između CPU i GPU na način da se složene operacije izvršavaju na GPU, dok se izvršenje manje složenih operacija obavlja na CPU.



Slika 3. Okvir k-means algoritma zasnovan na GPU aghitekturi

Ovakvim načinom klasterizacije ukoliko se klasterizuje video određenog dela puta, objekti koji su na više video zapisa ustaljeni (zgrade, saobraćajni znaci, rasveta,..) koncentrisaće se u klaster sa odgovarajućim osobinama. Segmenti ili frejmovi koji

[272] A. Shalom; M. Dash; M. Tue, „K-means Clustering Using Accelerated Graphics Processors“, Proceedings of 10th International Conference DaWak, Turin, Italy, 2008, pp. 166-175.

sadrže neuobičajene objekte neće se pojaviti u ni jednom klasteru. Takvi segmenti će predstavljati outlajere za koje je naknadnim procesom potrebno utvrditi koje deo snimka predstavljaju i šta je zapravo predstavljeno tim snimkom. Na ovakav način mogu se kreirati paterni saobraćajnih nezgoda na kritičnim delovima puta, a sve u cilju pronalaženja rešenja za korekciju saobraćajnice u cilju povećanja bezbednosti.

Pored sagledavanja nedostataka saobraćaja u cilju povećanja bezbednosti informacije dobijene iz video zapisa mogu se koristiti i od strane sudskih organa u procesu prekršajnog ili krivičnog gonjenja pojedinaca. Korišćenje video i tonskih zapisa kao dokaza u sudskom procesu praksa je koja se razlikuje od zemlje do zemlje. Većina sudova u SAD pridaje istu važnost digitalnim dokazima kao i tradicionalnim. Studije pokazuju da ukoliko je poroti prikazan video zapis kao dokaz počinjenog dela optuženi će u većini slučajeva biti proglašen krivim, što nije slučaj ukoliko takav dokaz ne postoji. Međutim samo prikazivanje videa nije dovoljno. Tačnije potrebna je potvrda sertifikovanih agencija ili pojedinaca o autentičnosti samog videa. Koliko je monitoring saobraćajnica i objekata u SAD postao uobičajena praksa svedoči i podatak angažovanja vlasti nakon događaja od 11. septembra na postavljanu kamera. Primera radi odeljenje državne bezbednosti je zaključno sa krajem 2016. godine na teritoriji Čikaga postavilo kamere za nadzor na svakoj raskrsnici. Ovakav potez pojedine organizacije za zaštitu privatnosti građana videle su kao narušavanje privatnosti . Međutim ukoliko je video nadzor sproveden od strane policije ili pravnog sistema u cilju detektovanja, praćenja i sprečavanja kriminalnih aktivnosti smatra se da zaštita privatnosti nije narušena. Policijske organizacije ovakav način monitoringa posmatraju kao legitiman alat u borbi protiv kriminalnih aktivnosti, uključujići i terorizam.

Pored SAD-a upotreba video nadzora od strane organa za sprovođenje zakona i antiterorističkih jedinica veoma je zastupljena u UK. Izvođenje digitalnih dokaza u pravosudnom sistemu UK-a veoma je fleksibilno, s obzirom da primera radi orginalni video zapis nije obavezujući kao dokaz. Ovo praktično znači da ukoliko original ne postoji, sud će prihvatiti kopiju digitalnog dokaza ili čak kopiju kopije. Ovo je potpuno prihvatljivo čak i ako je original uništila baš osoba koja je napravila kopiju, i to u procesu pravljenja iste. Sama činjenica da je prezentovani dokaz kopija a ne original može uticati na njegovu težinu, ali nikako na samu prihvatljivost. Ovo je u najvećem broju slučajeva praksa kada se kao digitalni dokaz izvode kopije slika ili elektronskih dokumenata. Ukoliko korisnik slika kao dokaza dokaže na sudu da su zaista kopije originala sudija će uputiti porotu da oni trebaju ovakav dokaz smatrati odgovarajućim.

U Indiji sudovi imaju ozbiljne implikacije u slučajevima u kojima se tužilaštvo oslanja na elektronske dokaze posebno one u kojima se audio i video zapisi na CD/DVD prezentuju na sudu. Primera radi antikorupcioni slučajevi su generalno bazirani na elektronskim dokazima prosleđenim sudu na CD/DVD. Obavezujuće je da ovakvi dokazi imaju odgovarajući sertifikat kako bi bili uzeti u obzir. Praktično za svaki izvedeni digitalni dokaz mora se obezbediti garancija autentičnosti. Bez odgovarajuće garancije celokupan sudski proces zasnovan na elektronskim zapisima,

kao i na video zapisima dovodi do odbacivanja dokaza[273]. Originalni video i audio snimci se prema članu 65B(4) zakona o dokazima moraju čuvati od bilo kakvog oštećenja ili uništenja u suprotnom izdavanje sertifikata o autentičnosti dokaza nije moguće čak ni uz svedočenje stručnjaka.

Zbog sve većeg broja prevara sa osiguranjem, kao i namernog izazivanja saobraćanih nesreća u cilju ostvarivanja finansijske koristi sudovi u Ukrajni uveli su praksu prihvatanja video zapisa sa kamera na saobraćajnicama i kamera u automobilima kao adekvatnog dokaznog materijala. Član 85-2 Zakona o krivičnom postupku defniše da svaki video zapis snimljen u periodu pre suđenja može biti upotrebljen na sudu. Prema ovom članu snimanje video zapisa može se koristiti prilikom inspekcije, pretrage i rekonstrukcije događaja i okolnosti kao i kod drugih istražnih radnji. Učesnici u istražnim radnjama moraju biti informisani pre početka snimanja da će isto biti korišćeno u cilju sprovođenja istražnih radnji. Procedure obrade video zapisa i drugih digitalnih dokaza prilikom prikazivanja u istražnom postupku kao i izvođenju dokaza na sudu definisane su članom 85-1 Zakona o krivičnom postupku. Narušavanje prava privatnosti jedno je od pitanja na osnovu kojeg se najčešće baziraju pokušaji osporavanja digitalnog video dokaza ili umanjenje njegove težine.

Sudska praksa Republike Srbije pokazuje da su misljenja oko primene video zapisa u formi dokaza pred sudom podeljena. Osnovni sud u Valjevu primera radi odbacio je kao dokaz snimak iz super marketa na kome se vidi kako zaposleno lice uzima novac iz kase. Obrazloženje za odbijanje ovakvog dokaznog materijala bazirano je na činjenici da zaposleni nije znao za postojanje kamere, kao ni da nije dao bilo kakvu saglasnost da bude sniman. S tim u vezi snimak može poslužiti isključivo vlasniku u cilju potvrđivanja ličnih sumnji u poštenje zaposlenog[274]. U drugom slučaju apelacioni sud u Beogradu potvrdio je presudu Višeg suda u Beogradu K. Po1. br. 258/10 od 18. 07. 2012, na osnovu video meterijala snimljenih telefonom kao i audio zapisa telefonskih razgovora. Sa druge strane video zapisi sa kamera na automobilu koje snimaju saobraćaj nisu uobičajen dokaz na sudu. Video snimci kao takvi u dokaznom postupku se mogu uzeti samo ukoliko su snimljeni od ovčašćenih lica tokom postupka istrage, privođenja ili prikupljanja dokaza. Zakonom o bezbednosti saobraćaja definisane su situacije u kojim se video zapis može koristiti kao dokazni materijal.

Jedan od primena je u slučaju kada policijski službenik ili nadležni inspekcijski organ putem video zapisa ili fotografja utvrdi da je načinjen prekršaj nepropisnog parkiranja ili zaustavljanja vozila. U ovakvom slučaju na osnovu snimljenog stanja službeno lice može doneti rešenje u elektronskom obliku o uklanjanju vozila. Lice koje vrši uklanjanje vozila dobija predmetno rešenje u elektronskog obliku i dužno je

[273] Electronic Evidence/Digital Evidence & Cyber Law in India, Available at: https://www.linkedin.com/pulse/electronic-evidence-digital-cyber-law-india-adv-prashant-mali- date: 08.02.2018.

[274] Court practice –online bulletins, Available at: http://www.sudskapraksa.com/sudske-odluke-presude-pravna-shvatanja.-najveca-baza-sudske-prakse-u-srbiji.html.

postupiti po istom[275]. U ovakvom slučaju video zapis ili fotografija se definišu kao verodostojna isprava kojom se dokazuje izvršenje prekršaja ukoliko se na njima mogu jasno videti vozilo koje je izvršilo prekršaj, registarski broj tog vozila, kao i bitna obeležja samog prekršaja[276]. Postavlja se pitanje zašto na isti način kreirani video zapisi ili fotografije fizičkih lica dobijene sa kamere vozila ne mogu biti dokaz u sudskom postupku.

Upotreba video sistema za praćenje saobraćaja nailazi na sve veću primenu organizacija zaduženih za unapređenje bezbednosti saobraćaja, kao i pravosudni organa. Razmatranje video zapisa sa kamere autmobila privatnog lica ili privatnih kamera na objektima kao dokaznog materijala svakako treba uvesti kao sudsku praksu u Republici Srbiji. Potpuno je suprotno zdravorazumskom razmišljanju da optuženi za krađu ili saobraćajni prekršaj bude oslobođen iako postoji video snimak na kome se vidi celokupno delo samo zato jer on nije bio upoznat sa postojanjem kamere.

5.5 Servisi e-vlade u borbi protiv terorizma

Servisi e-vlade kao što je navedeno u prethodnim poglavljima imaju veoma značajnu ulogu u svakodnevnom životu i radu ljudi. Pored servisa koje građani koriste u cilju komunikacije sa vladinim sektorom postoje i servi koje isključivo koriste zaposleni u državnoj upravi. Ovakvi servisi koriste se u cilju povećanja bezbednosti države, vlade i njenih građana. Ovo praktično znači da će zaposleni koristiti mrežu elektronskih servisa za blagovremeno uočavanje potencijalnih opasnosti od terorističkih ili bilo kakvih drugih napada. U slučajevima kada se radi o sprečavanju tradicionalnih napada policijske snage u okviru zemlje ili na granična policija na državnim granicama mogu nadgledati sumnjive osobe i sprečiti potencijalne napade oslanjajući se na informacije prikupljene sa biometrijskih dokumenata i informacije o šemama prethodno izvedenih napada[277]. Biometrijska dokumenta uvedena su kao obavezna u mnogim zemljama sveta. Svrha njihovog uvođenja i korišćenja jeste veći stepen bezbednosti građana i njihov zaštita od krađe identiteta. Različita biomertijska dokumetna koriste se za različite namene. Svaki od dokumenta ima specifičnu arhitekturu i koristi neku vrstu biometrije. S tim u vezi različiti vladini servisi zahtevaju korišćenje različitih biometijkih dokumenta. Primera radi biometrijski pasoš sadrži RFID čip na kome ase nalaze sve potrebne informacije: broj pasoša, datum izdavanja i datum važenja, zemlja izdavalac, ime i prezime osobe, pol, nacionalnost, datum rođenja, tip dokumenta, digitalna slika vlasnika pasoša, otisak prsta i skenirana

[275] Zakon o bezbednosti saobraćaja, „Službeni glasnik“, br. 41/2009, 53/2010, 101/2011, 32/2013 - odluka US, 55/2014, 96/2015 - dr. zakon i 9/2016 - odluka US, član 296

[276] Ibidem, član 322.

[277] Spalević, Ž., Ilić, M., Spalević, Ž. „Electronic government in the fight against terrorism“. In Proceedings of 3rd the International Scientific Conference on ICT and e-Business Related Research - Sinteza 2016, Belgrade, pp. 518-525, 2016.

zenica oka. Na osvnovu ovih podataka u procesu provere mogu se kreirati novi kako bi se utvrdilo da li je lice koje poseduje ovakvu putnu ispravu zaista i njen vlasnik, tačnije da li je putna isprava original ili ne. Primera radi na osnovu digitalne slike lica mogu se dobiti informacije kao što su rastojanje između očiju, pozicija nosa, položaj brade, itd. Drugi biometrijski podatak je otisak prsta za koji je karakteristično da ne postoje dva lica sa istim otiskom. U najvećem broju slučajeva za kreiranje biometrijskog dokumenta uzima se otisak prsa samo sa jedne ruke. Međutim nije redak slučaj zemalja koje na čip biometrijskog dokumenta upisuju dva otiska prsta svaki sa po jedne ruke. U skup ovih zemalja spada i Nemačka.

Pored digitalne slike lica i otiska prsta u cilju unapređenja sigurnosti biometrijskih dokumenata na sami čip se može upisati više biometrijskih podataka. Jedan od dodatnih biometrijskih podataka je struktura zenice oka. Prednost uvođenja ovakvog biometrijskog podatka jeste preciznost i pouzdanost. Primera radi skeniranje zenice oka je deset puta tačnije u odnosu na otisak prsta. Istraživanja su pokazala da kod skeniranja zenice oka može doći do lažnog poklapanja jednom u 2 miliona skeniranja, dok kod otiska prsta jedno lažno poklapanje dolazi na 100 hiljada skeniranja. Posmatano sa stanovišta fiziologije čoveka otisak prsta je stalno izložen mehaničkim oštećenjima, dok se zenica oka zaštičena rožnjačom. Dodatna pogodnost je i ta što za konkretno skeniranje oka savremeni skeneri mogu raditi na određenoj udalenosti od oka.

Sve je veći broj primera biometrijskih dokumenata sa većim brojem biometrijskih podataka osobe. Jedno od itraživanja prikazalo je upotrebu skenirane zenice i otiska prsta kao biometrijskih podataka na kojima se zasniva provera[278]. Cilj je bio kreirati sistem za skeniranje zenice oka bez prislanjanja istog do samog skenera. Praktično ovaj sistem može vršiti skeniranje oka bez obaveze da osoba mora prekinuti pomeranje oka. Drugi primer biometrijskih dokumenta sa većim brojem biometrijskih podataka jeste pasoš sa otiskom prsta i EEG (Electroencephalogram) tehnologijom. Ekperimentalni rezultati su pokazali visoke performanse primene ovakvog sistema, znatno više u poređenju sa sistemom zasnovanim samo na jednom biometrijkom podatku bilo otisku prsta bilo EEG-u.

Biometrijski podaci na putnim ispravama moraju obezbediti visok stepen sigurnosti ali u isto vreme sami sistem provere mora biti maksimalno efikasan. Ovo praktično znači da provera na graničnim prelazima mora biti organizovana tako da se zadržavanje i gužve maksimalno umanje. Ukoliko je neka osoba sumnjva i ukoliko sistem utvrdi nelogičnosti u biometrijkim podacima dodatna provera se može sprovesti, u suprotnom osoba nastavlja svoje putovanje. Ubrzanje provere može se organizovati na osnovu automatskog sistema za proveru. Primera radi dok zaposleni na graničnom prelazu vrši proveru dokumenta automatski sistem za prepoznavanje lica može vršiti poređenje slika prikupljenih sa kamera na granici i onih u dokumentu. Ukoliko ne dodje do poklapanja slika ili do poklapanja podataka o osobi i slike u

[278] Counter, P. „The Biometric Upgrade: SRI International Introduces IOM PassPort SL“, Available at: http://findbiometrics.com/thebiometric-upgrade-sri-international-introducesiom-passport-sl/, date: 25.02.2016.

dokumentu takva osoba se upućuje na detaljan pregled kako bi se ustanovilo o čemu je reč. Jedan od primera zloupotrebe biometrijskih dokumenta desio se na međunarodnom aerodromu John F. Kennedy u Njujorku. Naime putnik je kontroli pokazao validan pasoš i vizu ua ulazak u zemlju. Ime i slika u samom dokumentu su se poklapali dok je dodatna provera otiska prsta pokazala da lice pokušava da uđe u zemlju na osnovu vize koja pripada njegovom bratu blizancu koji nije imao kriminalni dosije ili kršenje imigracionih pravila. Nakon detalje provere inicirane nepolapanjem otiska prsta službenici aerodroma su ustanovili da je privedeno lice ranije hapšeno zbog slikanja vojne baze. Pored toga on je tokom zadnjeg boravka u SAD produžio samo vreme boravka pa je zbog toga deportovan van granica zemlje[279].

Ponekad otkrivanje sumnjivog ili traženog lica na granici između dve zemalja ne mora obavezno značiti njegovo hapšenje. Ovakvo lice može se dodati u program praćenja i prisluškivanja kako bi se pomoću njega došlo do osoba koje su ne višem nivou kriminalne organizacije. S tim u vezi vlasti mogu organizovati praćenje lokacije mobilnih telefona u posedu ovih lica kao i praćenje njihovih kako dolaznih tako i odlaznih poziva. Mnogo puta ovakve akcija donesu znatno bolje rezultate u odnosu na hapšenje pojedinaca. S tim u vezi vlada SAD-a kreirala je katozvanu bazu terorista Terrorist Screening Database (TSDB). Ukoliko je osoba registrovani terorista ili ukoliko postoji opravdana sumnja da može biti uključen u terorističke aktivnosti naći će se u ovoj bazi[280]. Pre nego što se osoba doda u samu bazu agencija zadužena za ove poslove mora obaviti detaljnu proveru kako bi bila sigurna da je osoba zaista potencijalno opasna. Prema pravilniku nominacija za upisivanje u TSDB bazu ne može biti zanovana na etičkim, rasnim, religiskim ili nacionalnim principima. Tačnije svako izražavanje slobodnog govora u domenu religije, rasnih problema, štampe itd ne može biti povod za upisivanje lica u ovu bazu jer su ovakva prava zagarantovana prvim amadmanom ustava SAD-a. Kako bi se izbegli problemi sa pogrešno upisanim osobama postoji poseban program putem koga osoba može proveriti da li je njeno ime na listi i zašto je na listi. Na takav način ukoliko je greškom upisana može podneti prigovor nakon čega će program na osnovu podataka o licu ustanoviti da li je lice greškom upisano. Ukoliko je lice greškom upisano isto će biti izbačeno sa liste. Iako deluje veoma jednostavno ovo ipak nije jednostavan proces. Sami proces od podnošenja prigovora do dobijanja odgovora i eventualnog uklanjanja sa liste traje prosečno oko 67 data. Praktično za vreme tog perioda licu je zabranjen izazak i zemlje bilo ono zaista sumnjivo ili ne. U mnogim slučajevima prigovor se odbacuje a zbog samog pokušaja pomeranja sa liste lice biva prebačeno na viši nivo bezbednosti. U nekim slučajevima ukoliko se ustanovi da lice od momenta dodavanja na listu do momenta podnošenja prigovora nije imalo aktivnosti okarakterisane kao opasne za društvo, isto može biti prebačeno na niži nivo bezbednosti ali svakako neće biti biti ukljonjeno sa liste.

---

[279] Homeland Security, „Enhancing Security Through ‚Biometric Identification“. Available at: https://www.dhs.gov/xlibrary/assets/usvisit/usvisit_edu_biometrics_brochure_english.pdf , date: 12.02.2018.

[280] TSC, „Terrorist screening center, Federal Bureau of Investigation“, Available at: https://www.fbi.gov/about-us/nsb/tsc/, date: 02.02.2018.

Servisi koji se nalaze u službi državnih organa bazirani na upotrebi informaciono komunikacionih tehnologija, a usmereni ka povećanju bezbednosti građana a samim tim i cele zemlje svakako su u upotrebi svakodnevno. Na unapređenju ovakvih servisa kao i biometrijskih ličnih dokumenta svakodnevno se radi kako bi se smanjila mogućnost zloupotrebe istih. Svaka od zemlja trebalo bi da u skladu sa svojim mogućnostima razvije mehanizme zaštite ličnih podataka svojih građana.

6
Kriminalne aktivnosti bazirane na informaciono komunikacionim tehnologijama

Pogodnosti koje nudi Cyber prostor u vidu brže komunikacije, razmene informacija, e-trogivne, obavljanja poslova od kuće, anonimnosti u radu veoma često znaju da budu stavljenje u drugi plan. Kao i svaka inovacija, značajan pronalazak i tehnologija, a kako je istorija pokazala i cyber prostor je iskorišćen za širenje nelegalnih i kriminalnih aktivnosti. Sama pogodnost korišćenja Interneta bez ličnog kontakta i otkrivanja identiteta upravo je dovela i do jednog od najvećih problema. Naime, teško je na Internetu utvrditi nečiji pravi identitet (*On the Internet nobody knows you are a dog*, je tekst ispod čuvene karikature objavljene u u Newyorker-u, 5. jula 1993. godine, na kojoj je naslikan pas koji surfuje Internetom). Pitanje identiteta za određenu grupu korinisnika danas se rešava elektronskim potpisom i raznim sistemima identifikacije. Međutim za ostale korisnike problem identiteta je i dalje nerešen. Tačnije za korisnike koje žele da otkriju svoj identitet ova mogućnost postoji, dok oni koji žele da ostanu anonimni takođe to mogu postići.

Bitno je naglasiti da je izuzetno brz napredak računarske tehnologije, a posebno u poslednje dve decenije, pored velikih prednosti doneo i mogućnosti izvršenja postojećih krivičnih dela u drugačijem obliku kao i nove oblike krivičnih dela. Upravo zbog toga, a reagujući na ovu pojavu, u zakonodavstvima pojedinih zemalja se negde pre, a negde kasnije definišu nova krivična dela i preduzimaju se različite mere protiv ove vrste kriminala koji sve više uzima maha. Kompjuterski kriminal je postao deo svakodnevnog života i rada ljudi. Korisnici računara i interneta svakodnevno se svesno ili nesvesno susreću ili učestvuju u nekom obliku komjuterskog kriminala. O raširenosti, težini i opasnosti kompjuterskog kriminala u dovoljnoj meri ukazuje podatak da je u SR Nemačkoj 1992. godine registrovano 12.435 slučajeva tog pojavnog oblika kriminala, od čega kompjutersku prevaru čini 2.485 slučajeva. Prema jednom izvoru iz 1999. godine, u Velikoj Britaniji je zbog softverskog piratstva kompjutersko tržište godišnje gubilo 7 milijardi funti[281].

Definicija kompjuterskog kriminala ima mnogo, u zavisnosti sa kog aspekta isti posmatramo. Međutim, opšteprihvaćena definicija bi mogla biti da kompjuterski kriminal predstavlja svaki oblik kriminalnog ponašanja pojedinaca i grupa u kojem se kao objekt izvršenja javljaju računari, računarski podaci, računarski sistemi i mreže. Takođe kao oblik kriminalnog ponašanja mogu se javiti računarski proizvodi u materijalnom ili elektronskom obliku. Drugim rečima, to je nezakonita upotreba informaciono-komunikacionih tehnologija, gde se zloupotrebom savremenih tehnologija protivpravno stiče materijalna ili neka druga korist.

Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, definisan je pojam visokotehnološkog kriminala. Ovaj zakon stupio je na snagu 2005. godine. Prema ovom zakonu visokotehnološkim kriminalnom smatra se svako vršenje krivičnih dela kod kojih se kao objekt ili sredstvo izvršenja javljaju računari u bilo kom obliku, elektronski podaci, kao i računarski proizvodi u meterijalnom ili elektronskom obliku [282].

---

[281] Brvar, B., „Pojavne oblike zlorabe računalnika“, Revija za kriminalistiko in kriminologijo, ISSN 0034-690X, vol. 33, no. 2. pp. 92–104.

[282] Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, „Službeni glasnik RS“, br. 61/2005 i 104/2009

U praksi su najizraženiji neki oblici visokotehnološkog kriminala, i to: povreda intelektualne svojine, piraterija, kompjuterska krađa i pranje novca. Povreda intelektualne svoje i autorskog prava detaljno je obrađena u prvom poglavlju ovog rada. Što se tiče piraterije u smislu kompjuterskog kriminala ona predstavlja izuzetno rasprostranjeno kompjutersko krivično delo. Osnovna karakteristika piraterije odnosi se na korišćenje i umnožavanje softverskih programa koji prethodno nisu nabavljeni na legalan način. Razlozi za pribegavanje pirateriji softvera kreću se od prkošenja zakonu pa sve do ostvarivanja imovinske dobiti. Generalno u zavisnosti do motiva i načina realizovanja piratskog napada može se razlikovati pet osnovnih vrsta softverske piraterije[283]:

- piraterija krajnjeg korisnika.
- višestruka upotreba klijent-servera,
- Internet piraterija,
- snimanje na hard disk,
- falsifikovanje softvera.

Kompjuterska krađa može se posmatrati kao oblik krivičnog dela u kome je došlo do otuđenja tuđe pokretne stvari kako u cilju njenog korišćenja tako i u cilju sticanja novčane koristi daljim otuđenjem. Pod samim pojmom krađa može se podvesti krađa računara i njegovih komponenti, krađa razne vrste robe, podataka, lozinki, zloupotreba platnih kartica. Kompjuterska krađa predstavlja trenutno predstavlja radnju koja je jako opasna po društvo u celini, dok su procene stručnjaka da će još intezivnije rasti. Rast kompjuterske krađe očekuje se sa porastom stepena upotrebe elektronske trgovine[284].

Kada je reč o pranju novca, treba reći da je Skupština Republike Srbije 18. marta 2009. godine usvojila Zakon o sprečavanju pranja novca i finansiranja terorizma[285]. Zakonom se propisuju radnje i mere koje se preduzimaju radi otkrivanja i sprečavanja pranja novca i finansiranja terorizma, čime je ujedno prestao da važi prethodni Zakon o sprečavanju pranja novca iz 2005. godine. Prema ovom Zakonu u sastavu Ministarstva nadležnog za poslove finansija obrazuje se Uprava za sprečavanje pranja novca, čiji je rad orijentisan ka praćenju novčanih tokova. Praktično uprva će prikupljati, obrađivati, analizirati i dostavljati podatke nadležnim organima. Svi poslovi uprave treba da budu orijentisani na sprečavanje i otkrivanje pranja novca i korišćenje istog u cilju finansiranja terorizma. Zakon je širi u odnosu na prethodni i po pitanju saradnje sa pravosudnim organima i učešćem advokata u postupku. Cilj zakona jeste sprečavanje štetnih posledica po rad organa i organizacija nadležnih za borbu protiv pranja novca, finansiranja terorizma i drugih oblika kriminala, a pre svega organizovanog i finansijskog kriminala i korupcije.

---

[283] Dragičević D.,Kompjuterski kriminalitet i informacijski sustavi", IBS – Informatov Biro Sustav d.o.o., Zagreb, 2004, pp. 19-25.

[284] Žaklina Spalević, „Krivična odgovornost pravnih i fizičkih lica na polju elektronskih komunikacija i elektronske uprave prouzrokovana cyber kriminalom", Doktorska disertacija, Pravni fakultet za privredu i pravosuđe, Univerzitet privredna akademija, Novi Sad, 2012.

[285] Zakon o sprečavanju pranja novca i finansiranja terorizma, „Službeni glasnik RS", br. 20/2009, 72/2009, 91/2010 i 139/2014.

U Krivičnom zakoniku Rusije postoji tipologija izvršioca ovih krivičnih dela koja po svojim karakteristikama predstavlja model razgraničenja praktično održiv i u sadašnjem trenutku. To su[286]:

- lica koja ostvaruju neautorizovani pristup računarskoj informaciji ili podatku samostalno;
- lica koja prema prethodnom dogovoru ili u organizovanoj grupi na ovaj isti način ostvaruju pristup računarskoj informaciji ili podatku;
- lica koja do ovakvih podataka i informacija dolaze iskorišćavanjem svog položaja ili službene dužnosti;
- lica koja imaju pristup računaru, sistemima ili mrežama, ali neovlašćeno ostvaruju isti u cilju pribavljanja nedozvoljenih podataka ili informacija narušavajući pravila iskorišćavanja računarskog sistema ili mreže;
- lica koja su kreirala, koriste ili distribuiraju vrednosne programe.

Kompjuterski kriminal, iz godine u godinu, postaje sve napredniji i efikasniji. Najveći broj napada usmeren je ka pravnim licima i velikim kompanijama. Kao što veliki broj primera iz prakse pokazuje meta napada su najčešće lični i osetljivi podaci kojima se može trgovati na crnom tržištu, ili na osnovu kojih se može steći bilo kakav vid imovinske koristi. Nisu retkost ni slučajevi da su upravo zaposleni odgovorni za sigurnosne incidente. S tim u vezi kompanije bi trebale uvesti skup određenih pravila kojima bi se osigurale ili zaštitile meterijalne i intelektualne vrednosti same kompanije. Takođe preporuka stručnjaka je da bi korporacije i institucije trebalo da uvedu sigurnosne politike koje bi pokrivale kako podizanje nivoa sigurnosti informacionog sistema tako i njihovih korisnika.

Sigurnosna politika predstavlja skup jasno definisanih pravila kojima su pokrivena područja u informacionom sistemu podložna napadu. Cilj sigurnosne politike je minimizacija štete nad informacionim sistemom koja je nastala kako namernim tako i nenamernim delovanje. Minimizacija štete moguća je samo definisanjem sigurnosne politike vezane za informacioni sistem koji se štiti. Sigurnosna politika korporacije ili institucije prilagođava se potrebama i nije jednaka za sve.

6.1 Cyber kriminal kao globalna pretnja svetskom poretku

Taman kada su nastale neke svodne definicije kompjuterskog kriminala pojavio se novi fenomen, tzv. cyber kriminal. Cyber kriminal predstavlja uniju skupova računarskog, digitalnog, e-Kriminala, Web kriminala, kriminala koji obuhvata napad na računarske mreže, krađu podataka, napada na sisteme, povredu autorskih prava, itd. Naime, cyber kriminal podrazumeva kriminal koji se odnosi na bilo koji oblik kriminala koji se može izvršavati sa kompjuterskim sistemima i mrežama, u kompjuterskim sistemima i mrežama ili protiv kompjuterskih sistema i mreža. To je, u

[286] Крылов В.В. „Информационные компьютерные преступления: Учебное и практическое пособие“, – М.: Инфра-М – Норма, 1997. – 285 с.

suštini, kriminal koji se odvija u elektronskom okruženju. Ako se pod kompjuterskim sistemom podrazumeva svaki uređaj ili grupa međusobno povezanih uređaja kojima se vrši automatska obrada podataka ili bilo kojih drugih funkcija, onda je jasno da bez njih i kompjuterskih mreža nema cyber kriminala. On je kompleksan i čak ga smatraju kišobran terminom koji pokriva raznovrsne kriminalne aktivnosti uključujući napade na kompjuterske podatke i sisteme, napade vezane za računare, sadržaje ili intelektualnu svojinu. Pri tome se kompjuterske mreže, odnosno informaciono-komunikaciona tehnologija pojavljuje u višestrukoj ulozi, odnosno kao: cilj napada, alat, okruženje i dokaz u dokaznom postupku[287].

Naime, cyber kriminal je takav oblik kriminalnog ponašanja kod koga je cyber prostor okruženje u kome se kompjuterske mreže pojavljuju kao sredstvo, cilj, dokaz i/ili simbol ili okruženje izvršenja krivičnog dela. Pri tome se pod cyber prostorom podrazumeva ili vrsta zajednice sačinjene od mreže kompjutera u kojoj se elementi tradicionalnog društva nalaze u obliku bajtova i bitova ili prostor koji kreiraju računarske mreže. Termin cyber prostor prvi je upotrebio William Gibson u naučnofantastičnoj noveli Neuromancer 1984. godine[288]. Cyber prostor je veštačka tvorevina koja zahteva visoku tehničku opremljenost, dobru informacionu infrastrukturu i koji je ničija i svačija svojina, u kome paralelno koegzistiraju virtuelno i realno i kod koga je komunikacija kolektivna. U takvom okruženju je izuzetno teško govoriti o nacionalnim razmerama kriminala i društvenoj opasnosti, bar ne u konvencionalnom smislu reči. Iz tog razloga se cyber kriminal svrstava u najizrazitiji oblik transnacionalnog kriminala protiv koga ni borba ne može biti konvencionalna, posebno što društveni, socijalni i ekonomski kontekst ovog kriminala nije istovetan sa klasičnim transnacionalnim kriminalom, jer za cyber prostor važe druga pravila, a što pokazuje Globalna studija o organizovanom kriminalu (Global studies on organized crime) Centra za prevenciju od međunarodnog kriminala i Instituta Ujedinjenih Nacija za istraživanje inter-regionalnog kriminala.

Interesantno je razmotriti kako se u susednoj Hrvatskoj teoretičari bave problematikom terminološkog određivanja ovog oblika kriminala. U Hrvatskoj literaturi termin i sama konvencija Saveta Evrope br. 185 prevedena je kao Konvencija o kibernetičkom kriminalu, mada reč kibernetika, engl. cybernetics nije sinonim reči cyber. Pojedini autori navode: Kibernetiku bi najkraće mogli definirati kao sustavno proučavanje komunikacije i upravljanja u organizacijama svih vrsta, a za cyber još ne postoje precizne definicije[289]. Hrvatski Rječnik stranih riječi navodi: Cyber je prvi element u riječima koji označava što vezano uz svet prividne stvarnosti koji nastaje pomoću računara.

---

[287] Žaklina Spalević, „Krivična odgovornost pravnih i fizičkih lica na polju elektronskih komunikacija i elektronske uprave prouzrokovana cyber kriminalom“, Opus citatum. str. 181.

[288] “Cyberspace. A consensual hallucination experienced daily bybillions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data. Like city lights, receding

[289] Deutsch, K. W. „The Nerves of Government“, Monels of Political Communication and Control, 2nd ed. New York, 1966., p. 76.

Prema Enciklopediji cyber kriminala navodi se da FBI i Nacionalni centar za kriminal belih kragni Sjedinjenih Američkih Država (National White Collar Crime Center) otkrivaju i prate sledeće oblike:

- upade u kompjuterske mreže;
- industrijsku špijunažu;
- softversku pirateriju;
- dečju pornografiju;
- bombardovanje elektronskom poštom;
- njuškanje password-a;
- prerušavanje jednog računara da elektronski liči na drugi, kako bi se moglo pristupiti sistemu koji je pod restrikcijama;
- krađu kreditnih kartica.

Zavisno od tipa počinjenih dela, cyber kriminal može biti:

- politički, koji čine: cyber špijunaža, haking, cyber sabotaža, cyber terorizam i cyber ratovanje;
- ekonomski, koji čine: cyber prevare, haking, krađa Internet usluga i vremena, piratstvo softvera, mikročipova i baza podataka, cyber industrijska špijunaža, prevarne Internet aukcije (neisporučivanje proizvoda, lažna prezentacija proizvoda, lažna procena, nadgrađivanje cene proizvoda, udruživanje radi postizanja veće cene, trgovina robom sa crnog tržišta, višestruke ličnosti);
- proizvodnja i distribucija nedozvoljenih i štetnih sadržaja, koji čine: dečja pornografija, pedofilija, verske sekte, širenje rasističkih, nacističkih i sličnih ideja i stavova, zloupotreba žena i dece;
- manipulacija zabranjenim proizvodima, supstancama i robama, i to: drogom, ljudskim organima, oružjem;
- povrede cyber privatnosti, koji čine: nadgledanje e-pošte, spam, phiching, prisluškivanje, snimanje pričaonica, praćenje e-konferencija, kačenje i analiza cookies;

Pored navedene klasifikacije cyber kriminala koja je prema svemu priloženom jako raznolika što ukazuje na ozbiljnost problema sprečavanja ovakvih aktivnosti u cyber kriminal se mogu uvrstiti i računarski virusi, odnosno njihova proizvodnja i distribuiranje, kao i ceo skup nedozvoljenih i štetnih sadržaja od dečje pornografije do rasturanja verskih, rasističkih i sličnih sadržaja. Posebno su brojna dela diseminacije nedozvoljene robe ili pružanje nedozvoljenih usluga. Tome treba dodati i cyber sabotaže i terorizam, kao i krađu Internet vremena, usluga, indentiteta i razne zloupotrebe kreditnih kartica.

6.1.1 Cyber ratovanje i cyber oružje

Sa globalnim širenjem Interneta, komercijalizacijom i povećanjem broja njegovih korisnika, naglo je porastao i broj pretnji prema korisnicima, te je zahtev za bezbednošću postao najbitniji. Budući da ovaj zahtev nije bio inherentno uključen u osnove mreže, ostvaruje se njenim neprekidnim naknadnim nadograđivanjem, poput uvođenja novih metoda kriptovanja sadržaja i saobraćaja. Nažalost, to nije otklonilo osnovne nedostatke mreže koji su omogućili rast cyber kriminala i cyber ratovanja. Nedostaci sadržani u arhitekturi cyber prostora (ugrađeni u njegovu osnovu) predstavljaju okolnost koja u značajnoj meri doprinosi cyber ratovanju, s obzirom da je iste moguće zloupotrebiti bez obzira na stepen njegovog tehnološkog razvoja.

Pored nedostataka sadržanih u arhitekturi cyber prostora, nedostaci koji proizilaze iz nesavršenosti hardvera i softvera, takođe predstavljaju okolnost koja doprinosi cyber ratovanju. Decentralizovana struktura Interneta obezbeđuje potencijal za širenje, ali ga istovremeno čini podložnim na mnoge vrste napada. Podaci u cyber prostoru se na svom putu ka odredištu kreću kroz različite sredine (npr. etar, optički, koaksijalni i parični kablovi), pri čemu se stalno preusmeravaju u ruterima i čvorištima čiji broj zavisi od lokacije konačnog odredišta. Zapis podataka se na svom putu do odredišta više puta konvertuje iz jednog oblika u drugi (npr. analogno-digitalna konverzija, opto-elektronska konverzija, modulacioni postupci). S tim u vezi, Internet je zasnovan na principima samoregulacije i bezuslovnog poverenja pri paketskom prenosu podataka pri čemu paketi koji putuju do istog odredišta ne moraju putovati istom trasom, pa tako potencijalni napadači relativno lako mogu zaobići standardni način regulacije njegovog saobraćaja.

Cyber ratovanju u velikoj meri pogoduju i nedostaci koji omogućavaju nekriptovani pristup podacima u cyber prostoru. Razvoj metoda i tehnika šifrovanja otežava mogućnost upada napadača u komunikaciju, ali ga ne sprečava u potpunosti. Svetski pretraživači, Internet-provajderi i bezbednosne agencije u svim državama sveta imaju zakonski regulisan pristup Internet-saobraćaju koji se odvija u nadležnosti tih država.[290] Pored toga svi komercijalni davaoci usluga i servisa, poput javnih *e-mail* provajdera, *Web* pretraživača i sajtova za društveno umrežavanje imaju potpuni pristup ličnim podacima i konverzaciji svojih korisnika. Svaki korisnik tih servisa ili softvera mora s tim da se složi prilikom otvaranja naloga. Zloupotrebu ovih podataka sprečava samo interna politika kompanije i savest administratora.

Dostupnost informacija na raznim nivoima pogoduje razvoju tehnika prisluškivanja saobraćaja, koje je naročito zastupljeno u bežičnim komunikacijama. Čak je i kompanija *Google* u mnogim državama godinama neovlašćeno preuzimala velike količine privatnih podataka u bežičnom prenosu prilikom snimanja fotografija za projekciju ulica (*Google Street*) za svoj servis *Google Maps*. Iako je kompanija na

[290] Zakon o elektronskim komunikacijama, Opus citatum, članovi 128.i 129.

zvaničnom blogu objavila da je napravila grešku,[291] sudski organi nekoliko država pokrenuli su istrage o ovom slučaju, a neki su i zabranili tu aktivnost.[292] Da bi se sprečio neovlašćen pristup informacijama koriste se razne metode obezbeđivanja saobraćaja, poput enkripcije i upotrebe sertifikata zaštite. Njihov nedostatak je povećavanje troškova poslovanja i neprimenljivost od strane svih korisnika Interneta. Njihova primena nije dovoljna, jer su u upotrebi mnoge metode prikrivenog praćenja aktivnosti korisnika, poput korišćenja raznih vrsta špijunskih programa.[293]

Značajnom okolnošću koja doprinosi cyber ratovanju smatraju se i nedostaci u dizajnu hardvera i softvera. Isti alati, sredstva i metode koje koriste počinioci krivičnih dela u oblasti cyber kriminala i cyber terorizma koriste se i za cyber ratovanje. Zahtevi za uštedom u proizvodnji, tokovi *outsourcing*-a i migracija softverskog inženjerstva i proizvodnje u zemlje Istoka i zemlje u razvoju uzrokuju da se softver i hardverske komponente masovno proizvode širom sveta.[294] Reprezentativan primer iskorišćavanja slabosti hardvera i softvera u vojnopolitičke svrhe jeste dizajniranje i podmetanje računarskog crva *Stuxnet*, koji je ciljano napadao specifične Siemens elektronske uređaje namenjene za automatizovanu industrijsku kontrolu u nuklearnim postrojenjima. Iako je njegovo prisustvo otkriveno u više država sveta, stručnjaci su utvrdili da je njegov osnovni cilj bila nuklearna centrala u izgradnji u gradu Bušer u Iranu.[295] Više nezavisnih analitičara je po načinu dizajna ovog softvera i prirodi njegovog delovanja procenilo da je on verovatno proizvod specijalnih cyber jedinica Izraela i SAD,[296] a što ukazuje na činjenicu da se okolnosti koje doprinose cyber ratovanju mogu posmatrati i sa

[291] Google je dao neubedljivo obrazloženje da je došlo do neovlašćenog prikupljanja podataka sa bežičnih mreža. Zvaničnici Nemačke, Kanade i SAD smatraju da taj postupak nije bio slučajan i zadržale su pravo na pokretanja sudskog procesa protiv kompanije. David Kravets, „Lawyers Claim Google Wi-Fi Sniffing Is Not an Accident", Wired.com.

[292] John Ribeiro, „Google faces privacy investigation in Canada", Computer World, Available at: https://www.cio.com/article/2417788/legislation/google-faces-privacy-investigation-in-canada.html, date: 18.02.2018.

[293] Tokom istraživanja mogućnosti snimanja elektromagnetnih promena nastalih usled aktivnosti računara pomoću radio-antene, student doktorskih studija na *Security and Cryptography Laboratory at the Swiss Ecole Polytechnique Federale de Lausanne* (EPFL) u Švajcarskoj testirali su 11 različitih modela tastatura povezanih sa računarom USB kablom ili ugrađenih u laptop računare. Praćenjem elektromagnetnih promena na udaljenosti od 20 metara bilo je moguće otkriti šta su korisnici računara kucali na tastaturama. Praćenje aktivnosti korisnika moguće je ostvariti i na monitorima računara. Oprema koja se koristila za praćenje aktivnosti na računaru. Available at: http://news.bbc.co.uk/2/hi/technology/7681534.stm, date: 10.02.2018.

[294] Defense Science Board, Report of the Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software, U.S. Department of Defense, pp. 19, 2007; Available at: http://www.acq.osd.mil/dsb/reports/ADA486949.pdf, date: 19.2.2013.

[295] Lolita. C. Baldor, Stuxnet, Iran Computer Attack, Linked to Wealthy Group or Nation, The Huffington Post, Available at: http://www.sandiegouniontribune.com/sdut-computer-attacks-linked-to-wealthy-group-or-nation-2010sep26-story.html, date: 02.02.2018.

[296] Mark Clayton, „Stuxnet malware is 'weapon' out to destroy…Iran'Bushehr nuclear plant?", The Christian Science Monitor, Available at: https://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant, date: 03.02.2018.

vojnostrategijskog aspekta. Iako je računarski crv *Stuxnet* bio namenjen dejstvu na nuklearno postrojenje, isti je našao put i do drugih civilnih sistema.

Širenje računarskog crva *Conficker* imalo je obrnuti smer – sa civilnih na vojne informacione sisteme. Isti je koristio postojanje bezbednosnih propusta *Microsoft* operativnih sistema i stvarao prikrivene virtuelne *bootnet* mreže kojima napadač upravlja sa distance. Iako nije dizajniran za napad na vojne sisteme, usled primene identičnog operativnog sistema u vojnim i civilnim računarskim sistemima došlo je do njegovog širenja u vojnim sistemima francuske mornarice – *Intramar*,[297] britanske ratne mornarice (uključujući ratne brodove i podmornice) – *NavyStar*[298] i na nekoliko stotina računara u računarskim mrežama nemačke vojske. Bez obzira na odsustvo katastrofalnih posledica, ovaj slučaj pokazuje potrebu pažljivog balansiranja zahteva za bezbednošću i njihovih troškova u skladu sa nacionalnim doktrinama i intenzitetom postojećih bezbednosnih rizika.

Imajući u vidu da među državama čije kompanije proizvode hardver i softver ima mnogo vojno-političkih suparnika, očekivana je pojava mešanja politike u postupak same proizvodnje. Autori softvera mogu ostaviti prikrivene propuste koje je teško otkriti kako bi ih kasnije zloupotrebili protiv korisnika njihovih programa. Poznati su mnogi primeri dodatno ubačenog softvera za koji čak ni kompanije nisu znale da se nalazi u njihovim proizvodima. Već duži vremenski period postoje indicije da je u *Microsoftov* operativni sistem *Windows* namerno ubačeno nekoliko tajnih *backdoor* sigurnosnih propusta u dogovoru sa bezbednosnim službama američke vlade,[299] što ova kompanija zvanično negira. Postoje ozbiljne optužbe da je to učinjeno i sa operativnim sistemima otvorenog koda, kao što su *OpenBSD* i neke *Linux* distribucije.[300] S druge strane, postoje snažna nastojanja američke vlade da se ovakva mogućnost i zvanično ozakoni.[301] Zbog toga je izuzetno bitno da se za primenu u vojnim, državnim i strateškim infrastrukturnim sistemima koristi namenski projektovan softver. Iako ovaj zahtev iziskuje dodatno vreme i troškove u cilju razvoja, uvođenja u operativnu primenu, obuke osoblja i održavanja, primene posebnih mera zaštite, to je neophodno učiniti da bi se obezbedili pouzdanost i bezbednost istih.

---

[297] Kim Willsher, French fighters planes grounded by computer virus, The Daily Telegraph, http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html, date: 02.02.2018.

[298] Lewis Page, „MoD networks still malware-plagued after two weeks“, The Register, Available at: http://www.theregister.co.uk/2009/01/20/mod_malware_still_going_strong/, date: 15.02.2018.

[299] J. Reavis, Microsoft, the National Security Agency and backdoors, Network World on Security, Available at: http://www.networkworld.com/newsletters/sec/0927sec2.html, date: 12.03.2013.

[300] Robert McMillan, „Former Contractor Says FBI Put Back Door in OpenBSD“, PC World, Available at: https://www.pcworld.com/article/213751/former_contractor_says_fbi_put_back_door_in_openbsd.html, date: 15.02.2018.

[301] Charlie Savage, „U.S. Tries to Make It Easier to Wiretrap the Internet“, The New York Times, Available at: http://www.nytimes.com/2010/09/27/us/27wiretap.html?pagewanted=1&_r=1&hp, date: 08.02.2018.

Sve vojne komunikacije u cyber prostoru su u osnovi ranjive onoliko koliko je ranjiv i sam cyber prostor. S tim u vezi, pripadnici iračkog pokreta otpora i avganistanski pobunjenici su dugo vremena koristili obične laptopove i jeftin softver *SkyGrabber* čija je osnovna namena preuzimanje komercijalnog satelitskog saobraćaja, da bi pratili i preuzimali vojne bežične komunikacije sa američkih vojnih bespilotnih letelica tipa *Predator* i *Reaper*, čiji je zadatak nadgledanje, televizijsko snimanje i uništavanje ciljeva na zemlji sa daljine.[302] Podaci sa letelica prenosili su se cyber prostorom do komandnih centara i bili su kriptovani isključivo na putu od letelice do centara na Zemlji. Iako je američka vojska primetila ovaj propust tokom bombardovanja Republike Srpske i SR Jugoslavije, nije preduzela mere za njihovo otklanjanje tokom kasnijih sukoba jer je smatrala da protivnici u Iraku i Avganistanu tehnološki nisu u stanju da otkriju i iskoriste ovu slabost. U vreme incidenta, neke letelice bile su opremljene najnovijim kamerama visoke rezolucije tipa *Gorgon Stare*, sposobnim da centralnoj komandi istovremeno šalju po deset različitih video prenosa. Ove letelice proizvodi specijalizovano privredno društvo za vojne tehnologije *General Atomics Aeronautical Systems Inc.* u San Dijegu po ceni od 10 do 12 miliona dolara po komadu. Navedeni program *SkyGrabber* proizvodi ruski programer i u SAD košta svega 26 američkih dolara, a može se besplatno nelegalno preuzeti širom Interneta. Posledica ovog incidenta je brz razvoj bezbednijih bežičnih veza sa bespilotnim letelicama. Ipak, bez obzira na nove tehnologije komunikacije borbenih letelica sa komandnim centrima, u slučaju presretanja i izmene komunikacionog saobraćaja u bilo kom smeru postoji realna mogućnost uticaja na njihova borbena dejstva.

Shodno iznetom, okolnosti koje doprinose cyber ratovanju – koje možemo posmatrati sa društvenog, tehnološkog i vojnostrategijskog aspekta, su od izuzetnog značaja za shvatanje same prirode cyber ratovanja u savremenom geostrateškom pozicioniranju i velike moći njegove evolucije i razvoja. Pre svega, to se ogleda u kapacitetima za ostvarivanje dejstva na protivnika i posledicama dejstva na cilj. Međutim, kao karakteristična disruptivna vojna tehnologija, može se očekivati da će ono brzo evoluirati u nove, znatno opasnije i razornije forme.

U cilju spoznaje prirode cyber oružja potrebno je napraviti analogiju sa vatrenim oružjem. Američko Ministarstvo odbrane definiše pojam "oružje" kao: "sredstvo namenjeno da ubije, povredi ili onesposobi ljude ili da ošteti ili uništi materijalna sredstva". Nakon opaljenja iz vatrenog oružja metak prolazi kroz vazduh i pogađa metu, razarajući je. Oružje, samo po sebi, ne stvara štetu, već mu je namena da dopremi sredstvo uništenja (metak) do mete. Sredstvo uništenja ne može da načini štetu, sve dok se ne ispali iz vatrenog oružja. Na kraju, ni oružje, ni metak nisu opasni sve dok ih borac ne uzme u svoje ruke, napuni oružje mecima i opali ih. U cyber ratu, maliciozni kod, računarska instrukcija ili podatak su sredstvo uništenja i imaju ulogu metka. Računarski hardver je sredstvo kojim se taj "metak" stvara i doprema do cilja napada. Operater koji koristi informacione sisteme, odnosno programer koji piše programe kojima se preduzima cyber napad je borac.

[302] Charles Arthur, „SkyGrabber: the $26 software used by insurgents to hack into US drones“, Guardian, Available at: http://www.guardian.co.uk/technology/2009/dec/17/skygrabber-software-drones-hacked, date: 08.02.2018.

Prema tome, tri elementa su osnovica cyber napada: softver, hardver i napadač. Svaki od njih je bitan ratnom pravu za regulisanje ratnih sukoba. Oni se moraju upotrebljavati u skladu sa principima prava oružanih sukoba, a činjenica da se koriste za borbena dejstva čini ih legitimnim ciljevima napada. Međutim, prihvatanje činjenice da informacije, programi, računarski sistemi i celokupna cyber infrastruktura mogu biti oružje ne znači da oni jesu oružje u svakoj situaciji. Oni su statusno neutralni, jer služe za prenos svih informacija, mirnodopskih ili napadačkih. Nije ista upotreba informatičkih sredstava za direktan cyber napad i u slučaju obezbeđenja pratećih funkcija ratovanja, poput komunikacija, logistike, u obaveštajne svrhe ili za pasivnu odbranu. U prvom slučaju oni su oružje, a u drugom sredstva vođenja rata. Kao sredstva koja omogućuju ratna dejstva, informacioni sistemi i infrastruktura doprinose sposobnosti vođenja rata i njihovo onesposobljavanje ili uništenje u pojedinim situacijama može dovesti do značajne vojne prednosti. U tom svetlu, napad na neprijateljske informacione sisteme nije u suprotnosti sa ratnim pravom. U novijoj istoriji NATO savez je u nekoliko navrata upotrebio ovakvo objašnjenje, poput bombardovanja Radio televizije Srbije 1999. godine ili Libijske državne televizije 2011. godine. Međutim, cyber ratovanje omogućava asimetričnost dejstava, pa se ovakvo tumačenje može podjednako primeniti u slučaju napada na informacione resurse malih država i velikih sila.

Primena cyber ratovanja neće ukinuti vođenje rata fizičkom silom, ali će značajno promeniti prirodu vođenja sukoba koji se permanentno vode u stanju mira, bez zvanične objave rata. Međutim, nepravilno ponašanje učesnika pri aktivnostima sa informacionim tehnologijama u cyber prostoru, zbog neznanja ili zbog neprimenjivanja bezbednosnih procedura i smanjene odgovornosti, na jednostavan način omogućava protivniku da pokreće i ostvaruje dejstva čije posledice mogu imati ekvivalent napada fizičkom silom. O tome svedoči ogroman interes vojno dominantnih svetskih sila da razviju sredstva, metode, tehnike i vlastite kapacitete za cyber ratovanje, kao i napori na razvoju novih vrsta cyber oružja.

6.1.2 Dark web

Statistika pokazuje da oko 1,6 milijardi ljudi širom planete svakog dana koristi Internet kako bi proverili svoj profil na Facebooku, Twiteru, nekom od mail account-a, pogledali video na YouTube-u, ili jednostavno vršili pretragu u cilju pronalaženja različitih informacija[303]. Pomenute aktivnosti korisnika spadaju u domen korišćenja takozvanog površinskog (*eng. surface*) dela weba. Pod pojmom površinskog weba spada sve ono što se može indeksirati korišćenjem javnih web pretraživača kao što su Google, Yahoo, Bing, itd[304]. Ovi pretraživači korišćenjem robota za indeksiranje

[303] M. Mitrović, „Mračne tajne globalne mreže“, Nova energija, Dostupno na: http://www.novaenergija.net/mracne-tajne-globalne-mreze/, datum: 10.02.2018.

[304] Bright Planet, „Clearing up confusion – deep web vs. dark web“, Available at: https://brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/, date: 10.02.2018.

obilaze sve dolazne i odlazne linkove sa trenutno posmatrane stranice i na taj način kreiraju mapu povezanosti stranice sa ostalim stranicama. Na ovakav način pretraživači imaju evidenciju o tome koje stranice je korisnik posećivao kao i koliko vremena je proveo na konkretnoj stranici.

Pored ovakvog vida praćenja veliki broj društvenih mreža posredno ili neposredno prati aktivnosti kako svojih korisnika, tako i internet korisnika uopšte. Ovde se izdvajaju različite situacije. Jedna od njih je kada korisnik poseti stranicu koja sadrži dodatak koji služi da se stranica lakše deli na društvenim mrežama, i koji se najčešće javlja u vidu Share ili Like dugmeta. Dodatak tada beleži koju je stranicu posećivao konkretni korisnik i informaciju o tome šalje na server društvene mreže, koji onda ukrštanjem podataka može da sazna gotovo sve o korisniku, naročito zbog toga što već ima veliki broj njegovih ličnih podataka. Ovakav vid praćenja aktivnosti internet korisnika krši jedan od osnovnih principa zaštite podataka o ličnosti – srazmernost obrade podataka u odnosu na svrhu za koju se podaci prikupljaju. Posebno je interesantno da do ukrštanja podataka dolazi bez obzira da li su korisnici ulogovani na društvenu mrežu ili ne. Takođe i slučajna ili kratkotrajna poseta određenoj društvenoj mreži može dovesti do toga da se instalira „tracking" kolačić, koji potom, posetom drugoj stranici na kojoj je bio prisutan dodatak za društvene mreže, može da otkrije podatke korisnika mreže kao što su IP adresa, Internet pretraživač koji koristi ovakav korisnik i stranica koja se posećuje[305].

Nasuprot površinskom delu weba koji je indeksiran, dubinski deo (*eng. deep*) obuhvata deo web stranica na Internetu koje nisu indeksirane. Ovo zapravo znači da su stranice koje pripadaju deep web-u samostalne i da nema linkova koji bi ih povezivali međusobno. Upravo zbog ovakvih karakteristika javni pretraživači ne mogu da pristupaju stranicama koje pripadaju deep web-u. Pristup se obavlja samo pomoću korišćenja specifičnog softvera, konfiguracije, ili uz ovlašćenje vlasnika stranice, često koristeći nestandarde komunikacione protokole. Ovakva organizacija deep web-a nudi visok stepen privatnosti svojim korisnicima pa je iz tog razloga veoma često u upotrebi od strane ljudi koji ne žele da njihova aktivnost na Internetu bude praćena. Broj stranica, a samim tim i količina podataka koji se mogu naći na deep web-u znatno su veći nego što je to slučaj sa površinskim delom web-a. Ne postoje tačni podaci o tome koliko puta je veći deep web od površinskog dela weba. Niko pouzdano ne zna kolika je veličina deep weba, zato što retko ko ima pristup gotovo svemu što se tu može naći. Dakle, to je jedan univerzum sajtova na kojima se mogu pronaći informacije, ponude, slike, zvučni i video zapisi o stvarima sa kojima se veliki broj korisnika površinskog weba nikada nije susreo[306]. Prema nekim istraživanjima odnos proporcija ove dve internet sfere jeste da površinski deo zauzima oko 4%, dok deep web zauzima oko 96% globalne mreže. Anonimnost koja se pruža korisnicima deep web-a iskorišćena je kao

[305] M. Stojković, „Fejsbuk i praćenje korisnika putem dodataka za društvene mreže", PravoIKT Serbian ICT Law resource, Dostupno na: http://pravoikt.org/fejsbuk-i-pracenje-korisnika-putem-dodataka-za-drustvene-mreze/, datum: 10.02.2018.

[306] Steve, „Surface web, deep web, dark web -- What's the difference?", CambiaResearch, Available at: https://www.cambiaresearch.com/articles/85/surface-web-deep-web-dark-web----whats-the-difference, date: 10.02.2018.

vid zaštite za širenje različitih ilegalnih aktivnosti, što je dovelo do izdvajanja jednog njegovog dela. Ovaj deo deep web-a i interneta uopšte naziva se dark web.

Veliki broj ljudi vođen informacijama dobijenim iz različitih medija, kao i određenog broja internet članaka, foruma i blogova izjednačava termine deep i dark web. Jedina sličnost između ova dva dela interneta je anonimnost korisnika i nemogućnost indeksiranja od strane javnih web pretraživača. Za pristup i jednom i drugom delu Interneta potreban je poseban softver koji omogućava anonimnost podataka i IP adrese korisnika. Jedan ovakav softver poznat je pod imenom Tor (eng. *The Onion Router*). Osnovna namena ovog softvera je da posluži kao gateway ka ovom delu Interneta. Kako bi sakrio adresu internet korisnika Tor vrši preusmeravanje signala preko gotovo 6000 servera[307]. Kako bi se stvorila privatna i zaštićena veza unutar Tor mreže, klijentska aplikacija inkrementalno izgrađuje vezu između izvorišta i odredišta paketa podataka, a koja se sastoji od kriptovanih veza između nasumično odabranih serverskih stanica. Ova veza nastaje u koracima, tako da pojedinačni server zna samo od kojeg servera je dobio pakete i kojem serveru ih treba proslediti. To se postiže korišćenjem posebnog ključa za enkripciju u svakom koraku. Jednom kada je veza uspostavljena njome je moguće prenošenje različitih vrsta podataka korišćenjem različitih programskih paketa[308]. Pored Tor-a koji se koristi u najvećem broju slučajeva kada je upitanju primera radi deljenje fajlova, I2P (*Invisible Internet Project*) mrežni nivo se koristi kako bi se obezbedila anonimna komunikacija između aplikacija. Ovaj sloj podržava niz protokola i aplikacija. Svaka uspostavljena konekcija između dva korisnika se štiti posebnom enkripcijom. Poređenje funkcionalnosti i sigurnosti koju nude Tor i I2P pokazalo je da je I2P znatno otporniji na napade izvedene analizom protoka podataka[309]. Freenet je još jedno od sličnih rešenja koje je znatno prostije i znatno pristupačnije za upotrebu od širokih narodnih masa. Pristup ovom servisu je obezbeđen putem pretraživača, dok u pozadini aplikacija obebeđuje konekciju. Sami korisnik može odabrati nivo zaštite prilikom pristupa mreži. Celokupna komunikacija i deljenje fajlova se obavlja putem P2P, i svakog puta kada se uspostavi konekcija nova putanja je kreirana. Iz ovog raloga svako ponovno otvaranje stranica iziskuje više čekanja nego što je to slučaj sa prethodno pomenutim tehnologijama.

Razlika između deep i dark web-a je velika počevši od veličine jednog i drugog dela Interneta pa sve do sadržaja koji oni nude. Deep web obuhvata uglavnom web sajtove koji nisu zlonamerni, kao što su primera radi email nalozi, servisi za čije je korišćenje potrebno platiti kao što je Netflix, kao i sajtovi kojima se pristupa kroz logovanje putem online forme. Jednostavno na deep webu se nalaze strane koje nisu indeksirane, odnosno označene tako da se ne mogu pronaći uz pomoć običnih alata za

[307] Zoran Čekerevac, Zdenek Dvorak, and Petar Čekerevac, „Da li je „tamni internet" dubok i taman?", FBIM Transactions, str. 1-12, 2016.

[308] Cydney Grannan, „What's the Difference Between the Deep Web and the Dark Web?", Encyclopedia Britannica, Available at: https://www.britannica.com/demystified/whats-the-difference-between-the-deep-web-and-the-dark-web, date:10.02.2018.

[309] Leon Mergen, „On anonymous networking in Haskell: announcig Tor and I2P for Haskell", Luctor et Emergen. Available at: https://leonmergen.com/on-anonymous-networking-in-haskell-announcing-tor-and-i2p-for-haskell-f1e30f52294f, date: 15.02.2018.

pretraživanje. Ovakve web strane spadaju pod domenom deep weba, jer im je nemoguće pristupiti bez posebne dozvole, a takođe ih pretraživači neće vratiti kao rezultat pretrage. Praktično ukoliko bi pretraživač mogao da vrati ovakve web strane kao rezultate pretrage to bi značilo da neko može da pristupi gmail nalogu određene osobe prostom pretragom prema imenu osobe[310].

Pored upotrebe od strane običnih korisnika deep web često koriste i programeri različitih kompanija, koje eventualno žele da testiraju kreirane web sajtove pre nego što ih učine dostupnim za indeksiranje i pristup sa strane površinskog interneta. Kao osobe koje stalno imaju potrebu za pronalaženjem informacija do kojih se ne može doći pretragom površinskog interneta deep web koriste i novinari. Takođe, deep web pruža mnogo veću anonimnost, pa iz tog razloga ljudi u totalitarističkim zemljama kao što je Severna Koreja koriste deep web kako bi zaobišli sigurnosne sisteme i ograničenja u dostupnosti informacija koje im je Vlada postavila u pogledu korišćenja Interneta[311]. Korišćenjem deep web-a državljani ovih zemalja ostvaruju međusobnu komunikaciju, informišu se o dešavanjima širom sveta, i u isto vreme informišu ostatak sveta o dešavanjima u svojoj zemlji. Dark web se može posmatrati kao mali deo deep weba koji je zbog anonimnosti koju nudi svojim korisnicima postao popularan kod zlonamernih korisnika. Pristup ovom delu Interneta kao što je već navedeno je gotovo identičan pristupu deep web-u. Iz domena korisnika dark web-a poznato je da ovom delu Interneta pristupaju samo korisnici koji tačno znaju šta traže i kako najefikasnije da pronađu stranice koje su im potrebne. Upotreba dark web-a povezuje se sa raznim ilegalnim aktivnostima kao što su hakovanje, dečija pornografija, razni oblici ilegalne trgovine uključujući trgovinu drogom i oružjem, prostitucija i tako dalje.

6.2 Ilegalne aktivnosti u cyber prostoru

Veliki broj istraživanja u kojima se posmatraju aktivnosti korisnika dark web-a, kao i sve ono što se može pronaći pristupom njegovim stranicama nesumljivo polazi od stranice pod nazivom *Put Svile (eng. Silk Road)*. Ovo je bila čuvena stranica na kojoj su korisnici jednostavnim klikom mogli da poruče bilo koju vrstu opijata koja im je potrebna, uključujući i različite vrste kako dozvoljenih tako i zabranjenih lekova. Osnivač i vlasnik bio je Ross Ulbrich 29. godišnji programer, koji se predstavljao pod pseudonimom pirat Roberts (*eng. Dread Pirate Roberts*). Od 2011. godine do 2013. godine on je stvorio imperiju vrednu 1,2 milijarde dolara[312]. Zanimljiva i pomalo zastrašujuća činjenica jesta da je ovaj sajt funkcionisao kao bilo koji drugi portal za online kupovinu. Sva poručena roba bi stizala posredstvom kurirskih službi na kućnu ili dogovorenu adresu.

---

[310] CARNet, „Tor - mreža za anonimnost“, CarNet-Hrvatska akademija i istraživačka mreža. str. 1-15, 2007.

[311] Marija Mitrović, „Mračne tajne globalne mreže“, Opus citatum

[312] Kim Zetter, „How the Feds Took Down the Silk Road Drug Wonderland“, Wired, Available at: from: www.wired.com/2013/11/silk-road/, date: 10.02.2018.

O upornosti ljudi koji se bave ovakvim vidom kriminala svedoči i podatak da je samo mesec dana nakon hapšenja Ulbricha i gašenja portala, portal postao ponovo aktivan na dark web-u, ovoga puta u verziji 2.0. Sajt je veoma brzo doživeo ekspanziju. Prema podacima FBI-a imao je prosečno oko 150.000 aktivnih posetilaca i zarađivao je mesečno oko 8 miliona dolara od prodaje robe i usluga. Nakon godinu dana rada sajt je ugašen, dok je administrator Blake Benthall uhapšen[313]. Od trenutka gašenja sajt nije bio aktivan svega sat vremena, nakon čega je opet pokrenut i nastavio je sa radom, ovoga puta u verziji 3.0. Ova činjenica pokazuje jačinu dark web-a i postojanost portala koji se na njemu nalaze[314].

Sajt The Armory, je jedan u nizu specijalizovanih sajtova za trgovinu vatrenim, tupim i oštrim oružjem kojim se mogu naneti povrede opasne po život. Prodaja oružja i municije obavlja se na sličan način širom drugih sajtova, od kojih neki garantuju isporuku širom planete, i to pod parolom "Dostavljamo globalno, jer svi imaju pravo da se zaštite"[315]. Na raspolaganju je bukvalno sve, od pištolja do eksploziva C4. Isporuka se vrši u posebnim pakovanjima, tako da mogu da prođu rendgensku kontrolu. Takođe veoma često se oružje pakuje u igračke, ali i u različite druge instrumente i električne uređaje[316].

Postoje primeri koji pokazuju da je dark web savršeno mesto za Cyber kriminal. Ovo je jedinstveno mesto gde u isto vreme korisnici mogu postati vlasnici različitih vrsta malvera, ali takođe i žrtve istih. Za distibuciju malvera koriste se svi poznati metodi phishing-a i pharming-a. Jedna velika grupa malvera koji se mogu naći na dark web-u su CryptoLocker malveri. Ovi malveri nakon pristupa fajlovima žrtve vrše kriptovanje istih. Nakon kriptovanja fajlova, žrtva biva redirektovana na stranicu na kojoj se od nje traži da izvrši plaćanje ukoliko želi da povrati kontrolu nad svojim podacima. Veoma često su zahtevi za plaćanjem kao i informacije potrebne da bi se izvršila transakcija ispisani na maternjem jeziku žrtve. Uloga Tor-a u ovakvim transakcijama jeste da hostuje sajtove za plaćanje u cilju izvršenja plaćanja pomoću bitcoin-a koji su veoma česta valuta plaćanja usluga na dark web-u[317].

---

[313] James Cook, „FBI Arrests Former SpaceX Employee, Alleging He Ran The 'Deep Web' Drug Marketplace Silk Road 2.0", Business Insider, Available at: https://www.businessinsider.com.au/fbi-silk-road-seized-arrests-2014-11, date: 11.02.2018.

[314] K. Knibbs, „Silk Road 3 Is Already Up, But It's Not the Future of Darknet Drugs", Gizmodo, Available at: http://gizmodo.com/silk-road-3-is-already-up-butits-not-the-future-of-da-1655512490, date: 11.02.2018.

[315] Marko Luković, "Deep internet - Droga, ubistva, pornografija - šta se sve krije u crnoj web rupi?", Before After, Maj 2014, Available at: http://www.beforeafter.rs/tehnologija/deep-internet/, date:12.02.2018.

[316] N1, „Darknet - mračna strana surfovanja internetom", N1 SCI-TECH portal Zagreb, Dostupno na: http://rs.n1info.com/a50647/Sci-Tech/Sve-o-Deep-Web-ili-Darknetu.html, date: 10.02.2018.

[317] Vincenzo Ciancaglini, Marco Balduzzi, Robert. McArdle, and Martin Rosler, „Below the Surface: Exploring the Deep Web", Trend Micro, pp. 1-48

Cyber kriminalci na dark web-u često nude hakerske uluge u najam. Primera radi kineska grupa Hidden Lynx tvrdi da ima do sto profesionalnih cyber lopova, među kojima ima i onih koji su upali u računarske sisteme Google-a, Adobe-a i Lockheed Martina. U zavisnosti od složenosti posla i rizika koji on nosi, tarife su u opsegu od nekoliko desetina do nekoliko hiljada dolara. Nude se različite usluge od ispravljanja ocena u školama, preko krađi pristupnih šifri za različite naloge, do prisvajanja osetljivih podataka privrednih društava ili organizacija.

Klijenti koji iz bilo kojih razloga imaju potrebu da angažuju plaćene ubice, mogu zadovoljiti svoje potrebe stupanjem u kontakt preko dark web-a. Jedan od primera prikazuje osobu, navodno verifikovanog plaćenika "sa osmogodišnjim iskustvom" koji nudi usluge isključivo za plaćenje unapred u Bitcoin-ima[318]. U kontaktu sa ovakvim osobama dozvoljeno je samo razmenjivanje informacija o žrtvi. Zahteva se da cela komunikacija, kao i svaki kontakt email-om moraju biti kriptovani. U slučaju da bilo koji deo komunikacije nije kriptovan, biće obrisan. Portali koji nude ovakve tipove uluga veoma često navode da su njihovi članovi bivši vojnici i plaćenici Legije stranaca. Ovakvi portali posvećuju veliku pažnju zaštiti komunikacije i tajnosti klijenata. Od informacija o meti prema kojoj će delovati, ovi online plaćenici zahtevaju ime, kućnu i adresu na kojoj im se nalazi radno mesto, što više fotografija i podataka o tome s kim žrtva živi, registarski broj, opis i sliku vozila koje koristi.

U zavisnosti od dogovora, tim ubica navodi da pripreme za posao, putovanje, lociranje i praćenje mete zahtevaju oko dva meseca, pri čemu troškovi kupovine avionske karte, oružja i smeštaja, po njihovim tvrdnjama, nisu uračunati u cenu samog ubistva. Jedan od portala pod nazivom *C'thulu* nudi odabir načina ubistva od regularnog, preko mučenja i silovanja, do bombaškog napada. Cene usluga su u rasponu od 3.000 dolara do 180.000 dolara u zavisnosti od odabrane kategorije i društvenog položaja žrtve. Cena se naravno razlikuje od toga da li je osoba koju treba ubiti pojedinac nepoznat široj javnosti ili se radi o javnoj ličnosti, političaru, pripadniku organa reda, itd.

Na dark web-u se veoma često obavlja trgovina falsifikovanim novcem, menicama, čekovima, kao i drugim hartijama od vrednosti. Stranice koje nude trgovinu falsifikovanim novcem navode različite vrste garancija u vidu opisa postupka kreiranja koji pokazuje da je kako tvrde prodavci falsifikovani novac kreiran na identičan način kao i pravi novac. Dostupne su praktično sve valute koje se isplati falsifikovati. Kvalitet falsifikovanih novčanica kao i količina koja se prilikom jedne transakcije može nabaviti variraju od slučaja do slučaja. U ovakvim transakcijama, najčešći pariteti su da se za 600 pravih američkih dolara mogu se dobiti 2.500 falsifikovanih, a za 500 pravih eura 2.000 falsifikovanih. Sve transakcije se obavljaju uz obećanje da kupljene novčanice mogu proći standardne provere, uključujući i onu ultraljubičastim svetlom[319]. U velikom broju slučajeva se naravno plaćanje za falsifikovani novac odvija u Bitcoin-ma.

---

[318] Marko Luković, "Deep internet - Droga, ubistva, pornografija - šta se sve krije u crnoj web rupi?", Opus citatum

[319] Vijesti online, „Tamni internet: Tu su hakeri, prodavci ljudskih organa, oružja", Dostupno na: http://www.vijesti.me/techno/tamni-internet-tu-su-hakeri-prodavci-ljudskih-organa-oruzja-828308, date: 10.02.2018.

Postoji i nekoliko sajtova na dark web-u koji tvrde da se bave prodajom pasoša i ličnih dokumenata. Cena ovakvih usluga zavisi od zemlje za koju se dokumenta izrađuju, kao i od samog prodavca. Validnost ovakvih dokumenata je teško proveriti, posebno kada se radi o državljanstvima. Ovakvi servisi mogu i biti kreirani u domenu prevare za emigrante koji žele da na bilo koji način dođu do državljanstva zemlje u kojoj se nalaze. Cena recimo pasoša, vozačke dozvole i lične karte za Australiju iznosi 800 eura na portalu pod nazivom Fake ID. Na istom portalu najskuplja dokumenta su za USA, a najjeftinija za Maleziju[320].

Ukradene informacije o bankarskim nalozima, brojevima kreditnih kartica, online aukcijama, takođe se mogu kupiti. Atlantik karding je lokacija na dark web-u na kojoj se mogu kupiti informacije o tuđim kreditnim karticama, adresama i sličnim privatnim informacijama. Cene se kreću između 5 i 80 dolara. Kvalitet informacija zavisi od cene. Sa druge strane, prodaja naloga se vrši na jedan od dva načina. Prvi način podrazumeva kupovinu pojedinačnog naloga, za koji su date detaljne informacije o količini sredstava na njemu. Drugi način podrazumeva kupovinu veće količine naloga od kojih je određeni broj verovatno validan. Prvi način je daleko isplativiji, jer kupac uvidom u količinu sredstava na računu ima veće garancije da će uložena sredstva povratiti i dodatno zaraditi. Pored toga, postoji i ponuda kupovine fizičkih platnih i kreditnih kartica različitih banaka[321].

Postoji veći broj primera gde su kao predmet sticanja zarade korišćena deca. Tokom 2011. godine Europol je u koordinaciji sa trinaest agencija različitih zemalja uhapsio 184 osobe osumnjičene za zlostavljanje dece i širenje dečije porrnografije u vidu slika[322]. Slična akcija sprovedena je u Velikoj Britaniji. U ovoj akciji uhapšeno je 650 ljudi, koji su optuženi za različine vidove zlostavljanja dece, od posedovanja slika, pa čak i do konkretnih slučajeva podvođenja[323]. Na teritoriji Severne Irske u 2015. godini uhapšeno je 37 osoba pod optužbom da su se na Tor-u bavile distribucijom dečije pornografije i pedofilijom[324].

Postoje podaci da su pripadnici grupe Islamska država Irak i Levant upravo korištenjem dark weba osigurali naoružanje za napade u Parizu i Briselu. Organizacije kao što su ISIL i Al-Kaida koriste dark web za aktivnosti koje nisu direktni napadi putem interneta, ali su u funkciji osnovnih ciljeva i posredna su sredstva terora i terorizma. Jedan od vidova korišćenja interneta u terorističke svrhe odnosi se na vrbovanje i regrutovanje novih snaga, uglavnom mlađe populacije, širenjem propagandnih materijala kao što su video snimci u kojima opisuju ciljeve za koje se bore, načine borbe i značaj njihovog rata. Određen broj ljudi se pronalazi u tome i želi

[320] Vincenzo Ciancaglini, Marco Balduzzi, Robert. McArdle, and Martin Rosler, „Below the Surface: Exploring the Deep Web“, Opus citatum

[321] Vincenzo Ciancaglini, Marco Balduzzi, Robert. McArdle, and Martin Rosler, „Below the Surface: Exploring the Deep Web“, Opus citatum

[322] Europol, „Operation Rescue“, Europol, 2014, Available at: www.europol.europa.eu/content/operation-rescue, date: 18.12.2017.

[323] BBC, „Child abuse image investigation leads to 660 arrests“, BBC News, Available at: www.bbc.com/news/uk-28326128, date: 15.02.2018.

[324] BBC, „50 arrests in NI online abuse images probe in past year, say police“, BBC News, 2015, Available at: www.bbc.com/news/uk-northern-ireland-31896685, date: 15.02.2018.

da im se priključi. Pored regrutovanja novih članova dark web servisi u funkciji terorizma veoma često se koriste za ostvarivanje sigurne komunikacije. Ovakva komunikacija je nalik društvenim mrežama i forumima, sa razlikom da je praćenje ovakvog vida komunikacije gotovo nemoguće. Takođe teroristi koriste dark web za ostvarivanje finansiranja svojih organizacija, pranje novca, kupovinu oružja municije i eksploziva. Sve pomenute aktivnosti kao i u ranijim primerima zloupotreba interneta najčešće se obavljaju u bitcoin-ima ili drugim vidovima kriptovanih valuti[325]. Jedan od terorističkih web sajtova pod nazivom Alneda.com identifikovan od strane vlade US predstavljao je sebe kao „Centar za Islamističke studije i istraživanje". Ovaj sajt obezbeđivao je informacije o Al kaidi. Teroristički članovi sajta koriste ga u cilju deljenja motivacionih poruka, priča i opisa operacija. Za masovne medije i ljude koji nisu članovi oni obezbeđuju analize i komentare skorašnjih događaja na stanicama koje su javno dostupne[326]. Primera radi Azzam.com poziva Muslimane da putuju u Pakistan i Avganistan u borbi protiv „Jewish-backed American Crusaders". Drugi web sajt Qassam.net apeluje na davanje donacija za kupovinu AK-47 pušaka.

Pored pomenutih ilegalnih aktivnosti korisnika dark web-a postoje i veoma bizarnije stvari koje se mogu pronaći u ovom delu Interneta. Jedna od takvih stvari je i trgovina ljudskim organima. Prema pojednim web sajtovima na dark web-u primera radi bubreg se može kupiti za 200.000$, srce za 120.000$, jetra za 150.000$, a par očiju za 1.500$. Takođe različiti proizvodi za negu lepote na bazi ljudske kože ili tkiva mogu se kupiti[327]. U ovom delu web-a mogu se naći stranice koje sa temama o različitim fetišima. Neki od sadržaja su snimci ili fotografije poslednjih trenutaka putnika u avinoskoj nesreći, zatvorenika na dan njihove egzekucije (primera radi egzekucija električnom stolicom u Teksasu), ili pornografski materijali u kojima žene gaze male životinje štiklama[328].

Veliki broj ilegalnih aktivnosti u cyber prostoru usmeren je kao otvoreni napad na kompanije, vlade pojedinih zemalja kao i na obično stanovništvo. Upotreba dark weba u realizaciji ovih aktivnosti nije obavezujuća, ali je u mnogim slučajevima prisutna. Neki od različitih registrovanih napada navedeni su u nastavku.

Računarski virus pod nazivom Malissa napravio je štetu u iznosu od 80 miliona dolara kompanijama u Severnoj Americi. Virus je kreiran tako da koristi Microsoft Outlook adresar u računaru zaraženog korisnika i da se pošalje na prvih pedeset adresa iz adresara. Na ovakav način veliki broj korisnika biva brzo inficiran jer i ne sluti da je sadržina maila opasna. Pored samog umnožavanja i slanja zadatak virusa bio je da kreira takozvana zadnja vrata za druge crve kao što su *The Love Bug, Anna Kournikova, i MyDoom*[329].

---

[325] G. Weimann, „Terrorist Migration to the Dark Web", Perspectives on terrorism, vol. 10, no. 3, 2016.
[326] Thomas L. Timothy, „Al Qaeda and the Internet: The danger of cyberplanning", Parameters, vol. 33, Num 1, pp. 112–123, 2003.
[327] Joel Falconer, „Mail-order drugs, hitmen & child porn: A journey into the dark corners of the deep web". Insider, Available at: http://thenextweb.com/insider/2012/10/08/mail-order-drugs-hitmen-child-porn-a-journey-into-the-dark-corners-of-the-deep-web/, date: 15.02.2018.
[328] Marija Mitrovic, „Mračne tajne globalne mreže", Opus citatum.
[329] U.S. Department of Justice, „Creator of Melissa Computer Virus Pleads Guilty to State and Federal Charges", Press Release, 2002.

U februaru 2000. godine cyber teroristi su napali web sajtove Amazona, eBay-a, Yahoo-a i drugih renomiranih kompanija. Ovi web sajtovi bili su pod DoS napadom nekoliko sati. Sledeći ozbiljniji DoS napad registrovan je 2002. godine kada je trinaest root servera širom sveta napadnuto. Funkcionalnost ovih servera bila je zadužena za kreiranje mape Interneta. Za razliku od napada izvedenog 2000. godine ovaga puta napad nije uzrokovao prestanak rada servera i usporenje Internet saobraćaja.

Takođe u 2000. godini računarski virus pod nazivom *IloveYou* za samo nekoliko sati oborio je email naloge miliona računara širom sveta. Ukupna ekonomska šteta napadnutih poslovnih kompanija iznosila je između 6 i 10 miliona dolara[330].

Da cyber napad može biti toliko dobro organizovan i izveden svedoči i činjenica da je 2000. godine Japanska policija utvrdila da je softver za praćenje policijskih automobila kako onih obeleženih tako i neobeleženih neovlašćeno korišćen od strane Aum Shinryko kulta. Od početka špijuniranja pa sve do otkrivanja kult je primio poverljive podatke o praćenju sa 115 automobila. Da nevolja bude još veća sami sistem je izdradio pomenuti kult kao firma pod izvođač druge softverske kompanije. Detaljnija istraga je pokazala da je kult radio kao podizvođač i za mnoge druge kompanije. Sve kompanije za koje je kult radio kreirale su softver za osam Japanskih kompanija i deset vladinih agencija. Sama činjenica da su radili kao podizvođači obezbedila im je anonimnost. Svaki od kreiranih softvera potencijalno je ugrožen činjenicom da je u isti kult imao mogućnost da ubaci virus kako bi kasnije aktivirao cyber napad[331].

Tokom 2004. godine računarske mreže i računari u samim mrežama u okviru NASA-e, Lockheed Martin-a, Redstone Arsenal-a, Sandia National Laboratorija kao i nekoliko drugih postrojenja bile su pod cyber napadom. Ovi napadi bili su deo velikog napada pod nazivom „*Titan Rain*“. Titan Rain je bio jedna možda od najvećih napada tog vremena. Pored kompromitovanja vojnih sistema i poverljivih podataka sami napad ostavio je zadnja vrata kao mogućnosgt upada drugih hakera i spijunskih organizacija. Ovakav vid infiltriranja u sistem značajno je opasniji od klasičnih cyber napada u kojima hakerska grupa deluje samostalno.

Međunarodni Olimpijski komitet, Ujedinjene Nacije i sedamdeset drugih kompanija i organizacija bile su napadnute u 2006. i 2008. godini. Ovaj napad poznat je kao „*Operation Shady Rat*“. Pretpostavlja se da iza ovih napada stoji vlada Narodne Republike Kine.

Lanac prodavnica prehrambenih proizvoda Hannaford Bros bio je meta cyber napada u 2007. godini. Ovaj napad izveo je Albert Gonzales. U ovom napadu ukradeno je više od 4.2 miliona brojeva kreditnih i debitnih kartica, kao i drugih osetljivih podataka klijenata. Napad je izveden tako što je grupa hakera predvođena Albertom inficirala server kompanije računarskim maleverom. Nakon napada ukradeni podaci

[330] Melanie Lee, Lucy Hornby, „Google attack puts spotlight on China's "red" hackers“, Reuters - Technology news, 2010.
[331] Gabriel Weimann, „Cyberterrirism? How real is the threat“, Special Report 119, United States Institute of peace, pp. 1-12, 2004.

prodati su na aukciji organizovanoj na sajtu Shadowcrew.com. Godinu dana kasnije kompanija za prenos novca i plaćanje Heartland Payment System izgubila je više od 140 miliona dolara u phising napadu sprovedenom od strane tima takođe predvođenog Gonzalesom. O ova dva napada više od 100 miliona brojeva kartica je ukradeno. Joše veće posledice od samih ekonomskih gubitaka po Heartland kompaniju jesu narušavanje ugleda i gubitak poverenja klijenata. Za ove i slične napade Gonzales je proglašen krivim i osuđen na 20 godina zatvora.

Tokom 2007. godine web portali Estonske vlade i servisi elektronske uprave bili su pod jednim od najpasnijih napada nakon Titan Rain-a. Napadači su primenili najrazličitije tehnike u cilju obaranja ovih sajtova. Ping floods i botnets su samo neke od primenjenih tehnika. Sama složenost napada kao i način na koji su izvedeni ukazivala je na to da Ruska vlada stoji iza hakerskih grupa angažovanih u ovim napadima. Međutim kao i u većini napada ova sumnja nikada nije potvrđena.

U julu 2009. godine US i Južna Korea bile su pod serijom koordinisanih cyber napada. Ciljne mete ovih napada bili su web sajtovi državnih i vladinih institucija, funansijskih i novinskih agencija. Registrovani cyber napadi bazirani na DDoS metodu napada imali su širok spektar važnih ciljeva. Neki od njih su banke, online mediji, servisi elektronske uprave, itd[332]. Tokom napada pristup ovim servisima bio je otežan ili čak nemoguć. Broj otetih računara za potrebe izvođenja napada iz *Symantecs security Technology Response Group, National Inteligence Servise* i *Vietnamese computer security researchers* iznosio je 50.000, 20.000 i 166.000 respektivno.

Iransko nuklearno postrojenje u Natanz bilo je pod napadom cyber-crva pod nazivom Stuxnet tokom 2010. godine. Zadatak ovog crva bio je da uništi nuklearne centrifuge Tahran-a. Ovaj crv se raširio računarskom mrežom i inficirao više od 60.000 računara. Krajnji efekat ovog napada bilo je ugrožavanje Iranskog nuklearnog programa i njegovo vraćanje dve godine unazad. Iranska vlada bila je uverena da iza napada stoje računarski stručnjaci angažovani od strane Izraelske i US vlade. Međutim celokupna istraga nije uspela da razotkrije počinioce.

Plazstation Network i Sony Online Entertainment bili su pod cyber napadom u 2011. godini. U ovim napadima 77 miliona korisničkih naloga je ukradeno. Pored ličnih podataka ukradeni su i podaci o kreditnim i debitnim karticama korisnika. Ukupna procenjena šteta bila je između jedne i dve milijarde dolara. Sami napad trajao je 24 dana, pre nego što je otkriven. Tokom trajanja napada počinioci su bili u mogućnosti da se loguju kao validni korisnici i da na taj način kompromituju podatke.

Modularni računarski malver pod imenom Skywiper ili Flamer iskorišćen je za potrebe napada na računarske sisteme zemalja Bliskog Istoka tokom 2012. godine. U vreme napada napadnuti računari radili su na operativnom sistemu Microsoft Windows. Sami malver širio se na dva načina ili putem lokalne mreže ili putem USB memorije. U ovom napadu preko 1000 računara je inficirano. Sami inficirani računari bili su vlasništvo kako pojedinaca tako i obrazovnih institucija, vlade, i kompanija.

[332] Digital Attacks Map, „What is a DDos attack“, Available at: http://www.digitalattackmap.com/understanding-ddos, date: 18.02.2018.

Istraga je utvrdila da je ovaj malver korišćen za potrebe špijunaže. Bio je dizajniran tako da vrši beleženje audio snimaka, aktivnost na tastaturi, screenshots, mrežni saobraćaj, pa čak i konverzacije na Skype-u.

Takođe u 2012. godini veliki broj cyber napada bio je usmeren protiv računarskih mreža US-a, Katara, Saudijske Arabije i Izraela. U ovim napadima sistemi banaka sa bili meta napada. Kao počinioc napada optužena je Iranska vlada jer se smatralo da je to odgovor na cyber napad US protiv Irana u 2010. godini.

Kao što je već naglašeno cyber napadi podrazumevaju svaki oblik upotrebe računara i računarskih mreža u cilju bilo kakvog organizovanja terorističkih napada. U jednom od računara koji su korsitili pripadnici Al Kaide a koji je zaplenjen tokom borbi u Avganistanu pronađeni podaci o elektronski kontrolisanim sistemima brana, vodosnabdevanju, nuklearnim postrojenjima kao i US i Evropskim stadionima. Ovo je samo još jedna od potvrda da cyber prostor može biti iskorišćen kao sredstvo istraživanja, planiranja i koordinisanja napada koji će kasnije biti izvedeni na tradicionalni način.

Kao i mnoge druge zemlje sveta ni Republika Srbija kao ni bivše Jugoslovenske republike nisu imune na cyber pretnje[333]. Tako su 2008. godine hakeri sa kosova lansirali određeni broj napada na web sajtove u vlasništvu Republike Srbije, uključujući web sajt predsednika Srbije i nekoliko ministarstava. Najizrazitiji napadi bili su DoS i DDoS napadi[334]. U DDoS napadu 2014. godine nakon incidenta na fudbalskoj utakmici sa Albanijom veliki broj web sajtova Srpskih medija bio je oboren. Ovi portali bili su nedostupni nekoliko sati. Pored web portala medija, web portali zvaničnih institucija takođe su napadnuti. U ovom napadu lični podaci miliona građana Republike Srbije su ukradeni iz baze podataka Agencije za privredne registre. Pored ličnih podataka email adrese zvaničnika ministarstava takođe su bile preuzete[335].

Tokom 2014. godine DD4BC hakerska grupa otkrivena je na prostoru Bosne i Hercegovine. Ova grupa najpre je lansirala DDoS napade protiv određenog broja novinskih portala kao što su buka.com, istinito.com e-novine, federalna.ba, fena.co.ba, kurir.rs i blic.net. Nakon DDoS napada grupa je tražila isplatu u Bitcoinima. Ukoliko bi napadnuti novinski portal odbio plaćanje grupa bi izvršila novi mnogo snažniji DDoS napad. Istraga je pokazala da je DD4BC grupa razvijala softver sa ciljem istraživanja slabosti digitalni novčanika i kriptovaluta, posebno Bitcoin-a[336].

---

[333] Žaklina Spalević, Božidar Banović, Miroslav Vrhovšek, „Cyber Crime in the States of Western Balcan“, TTEM - Technics Technologies Education Management, Vol. 8, No. 2, pp. 886 - 895, Jun, 2013.

[334] Nikola Milošević, “Case of the cyber war: kosovo conflict”, Inspiration,org, Available at: http://inspiratron.org/blog/2014/07/01/case-cyber-war-kosovo-conflict/, date: 18.02.2018.

[335] Ivana Milatović, „Serbia’s efforts to respond to cyber security threats”, OSCE, Available at: http://www.osce.org/serbia/170361, date: 18.02.2018.

[336] OCCRP, „Bosnia and Herzegovina: crackdown on 'cyber blackmail' group“, Available at: https://www.occrp.org/en/daily/4793-bosnia-and-herzegovina-crackdown-on-cyber-blackmail-group, date: 18.02.2018.

Telekom Hrvatska jedan od vodećih provajdera mobilne telefonije u Hrvatskoj pretreo je cyber napad u 2015. godini. Problem napada je otklonjen nakon deset sati, ali su korisnici tokom tog vremena bili ugroženi. Ne postoje tačne informacije koliko korisničkih podataka kompromitovano ovim napadom[337].

Web portali elektronske uprave vlade Crne Gore, nekoliko državnih institucija kao medija u službi ove vlade bili su pod serijom cyber napada i tokom 2017. godine. Povećanje broja napada vidljivo je i u poređenju između broja napada tokom 2016. godine i 2012 godine. U brojkama ukupan broj napada tokom 2016. godine iznosio je 200 napada na web sajtove državnih institucija, online prevara i zloupotreba ličnih podataka, dok je ukupan broj napada po istim kategorijama u 2012. godini iznosio samo šest napada. Ozbiljnost napada tokom 2016. i 2017. godine ogleda se u tome da su napadi usmereni ka špijunaži i sabotaži državne informaciono komunikacione infrastrukture. Takođe zabeležen je veliki broj slučajeva phishing-a usmerenog protiv civilnog stanovništva[338].

Mete cyber napada veoma često su i web servisi, računarske mreže, kompanije i pojedinci orijetisani bavljenju turizmom kao i širenju ove grane industrije. Kao i u većini drugih napada i u cyber napadima protiv turizma najučestaliji su DoS i DDoS napadi. Prekidi u komunikaciji ili nedostupnost web servisa pomoću kojih se turisti informišu o konkretnoj turističkoj destinaciji, lokalitetu ili smeštajnom kapacitetu mogu imati za posledicu velike ekonomske gubitke. Pored remećenja rada ovih servisa ovakvi napadi mogu kreirati otvoreni prostor za ubacivanje različitih vrsta malwera i računarskih virusa. Ukoliko je primera radi napadnut web servis čija funkcionalnost uključuje i online plaćanje različitih rezervacija računarski virusi mogu obezbediti napadaču mogućnost krađe ličnih podataka posetioca portala. Ovakva aktivnost napadača može ostati neprimećena kako tokom samog napada tako i nakon što kompanija koja je vlasnik portala uspostavi ponovnu kontrolu nad portalom. Tokom organizacije olimpijskih igara u Riu 2015 godine određeni broj web portala različitih organizacija koje su bile u direktnoj vezi sa organizovanjem samih igara i smeštaja gostiju napadnute su DDoS napadom. Ovaj napad je trajao nekiko meseci, a jačina napada se povećavala kako su se igre približavale. Tokom vremena trajanja napad se kretao u opsegu od nekoliko 10Gbps do nekoliko 100Gbps. Najveća jačina napada iznosila je 540Gbps. Zahvaljujući merama za ublažavanje ovakvih napada predviđenim od strane Brazilskih profesionalaca za informatičku bezbednost koje su podrazumevale migraciju servisa Olimpijski komitet je uspeo da očuva svoje sisteme[339].

---

[337] Eduard Kovach, „Site of nato croatia hacked and defaced by teamp0ison“, Softpedia, Available at: http://news.softpedia.com/news/Site-of-NATO-Croatia-Hacked-and-Defaced-by-TeaMp0isoN-262429.shtml, date: 18.02.2018.

[338] Dusica Tomović, „Montenegro on alert over new cyber attacks“, BalkanInsight, Available at: http://www.balkaninsight.com/en/article/montenegro-govt-on-alert-over-new-cyber-attacks-02-21-2017, date: 18.02.2018.

[339] David Bisson. „The 5 Most Significant DDoS Attacks of 2016“, The State Of Security, Available at: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/5-significant-ddos-attacks-2016, date: 18.02.2018.

Neki od zabeleženih slučajeva cyber napada orijentisanih na krađu ličnih podataka korisnika, kao i na krađu podataka o platnim karticama već su opisani u prethodnim poglavljima kao neki od nedostataka elektronkih servisa primenjenih u turizmu. Cyber napadi mogu biti usmereni i ka potpuno autonomnim sistemima koji za zadatak imaju kontrolu različitih procesa. Napadi na ovakve sisteme mogu prouzrokovati katastrofe velikih razmera u kojima mogu stradati mnogi životi. Ovakvi sistemi su zastupljeni u kontroli avio saobraćaja, rutiranju brodskih kontejnera, kao i u domenu skladištenja i obrade toksičnog otpada. Jedna od vodećih osiguravajućih kompanija Allianz identifikovala je i sastavila listu od šest najvećih trenutnih rizika po avio industriju. Svi identifikovani rizici dolaze od strane cyber terorizma i upotrebe dronova. Prema ovoj kompaniji postoje velike mogućnosti da teroristi iskoriste sisteme bazirane na računarima u avionu kako bi preuzeli kontrolu i usmerili avion na putanju koju oni odaberu. Šanse sa ovakve napade su svakog dana sve veće s obzirom na činjenicu da je iz dana u dan kontrola aviona sve više bazirana na računarskim sistemima[340]. Cyber otmicom aviona na letovima ka popularnim destinacijama putnici u avionu bili bi prepušteni volji napadača. Razmere ovakvih napada mogu biti katastrofalne od klasične otmice aviona sa putnicima, do korišćenja aviona za obrušavanje na druge mete. Cyber napadi takođe mogu biti lansirani u simbiozi sa tradicionalnim napadima kako bi ovakvi napadi imali još veće posledice. Primera radi ometanje komunikacija u vanrednim situacijama ili napadima na hotelske komplekse mogu srečiti adekvatno informisanje gostiju o ozbiljnosti situacije. Zakasnelo alarmiranje može uzrokovati stradanjem ljudi. U cilju stvaranja panike upadom u sigurnosni sistem mogu se ostvariti uslovi za lažno aktiviranje različitih alarmnih sistema ili lažno informisanje gostiju o mogućem napadu.

Najviše krivičnih dela u oblasti visokotehnološkog kriminala u Srbiji se vrši kombinovanim napadima, upotrebom tehničkih metoda, malicioznih softvera i tehnika socijalnog inženjeringa[341]. Radi se o kriminalu počinjenom na računaru i mreži, ali i u oblasti radiodifuzne, mobilne tehnologije, telekomunikacija. U odnosu na pre nekoliko godina, broj krivičnih dela sajber kriminala je u porastu, a prognoze su da će uvećanjem elektronskih sistema plaćanja rasti i dalje. U Srbiji se dešavaju različiti napadi, kako u domenu online plaćanja tako i u oblastima koje mogu svrstati u kategoriju kriminalnih prevara. Kriminalci rade tako što preuzmu rad nad serverom nekog sajta za plaćanje aražmana putem interneta, koji korisnik često koristi. Kasnije se korisniku prikazuje sajt koji je identičan kao original i preko koga korisnik kreće u standardni postupak pretraživanja, rezervacija ili online plaćanja različitih aranžmana. Osobe ili organizacije koji stoje iza sajtova na taj način prikupljuju podatke i dalje ih koriste. Ovi podaci se najčešće koriste van teritorije zemlje iz koje je pokradeni korisnik. Najranjiviji faktor je čovek i bez njegove saradnje retko koja prevara može

[340] David Baker, „Tourism and Terrorism: Terrorists Threats to Commercial Aviation Safety & Security“, International Journal of Safety and Security in Tourism/Hospitality, Vol 1, No. 12, pp. 1-19. 2015.

[341] Žaklina Spalević, Miloš Ilic, Željko Spalevic, „Cyber terrorism as a threat to tourism development“, International scientific conference on economics and management Eman 2017: Globalization challenges, Ljubljana, Slovenia, pp.862-868, 2017.

uspeti. Ljudi često veruju u spam mejlove o nagradnim putovanjima ili jako povoljnim ponudama u kojima se nudi atraktivan smeštaj ispod svake realne cene. Ne tako retko mogu se pronaći i sajtovi koji prikupljaju i objavljuju samo ovakve ponude, od kojih su većina lažne. Sve u svemu svaki pojedinac, pravno lice, institucija moraju voditi računa o svojim podacima kao i o tome kakvom portalu pristupaju i koje se informacije od njih traže.

6.3 Pravna regulativa na polju cyber ratovanja

Postojeći nacionalni i međunarodni pravni režimi regulišu primenu krivičnog prava na polju obaveštajnih i vojnih operacija. Cyber operacije se, u zavisnosti od situacije, istovremeno mogu naći u područjima kriminala i obaveštajnih aktivnosti. Ta okolnost komplikuje izbor aktivnosti država u unutrašnjim i međunarodnim odnosima, s obzirom na zahtev da prema napadačima istovremeno treba različito postupati. Čak i u slučaju da cyber napad ima isključivu prirodu cyber ratovanja i da ni po čemu ne zadire u područje kriminala i obaveštajnih aktivnosti, nedostatak regulativa i zajedničkih međunarodnih kriterijuma i propisa u oblasti cyber ratovanja bitno otežava izbor nadležnog prava i legalnog postupanja države, jer neki akt cyber ratovanja može biti[342]:

- zakonita državna aktivnost (u skladu sa Poveljom UN i odlukama Saveta bezbednosti UN),
- nezakonita aktivnost koja po svom intenzitetu i posledicama ne daje povoda za primenu oružane sile kao akta samoodbrane,
- akt agresije, koji daje pravo napadnutoj strani da preduzme proporcionalan oružani odgovor (npr. napad na važan infrastrukturni sistem sa posledicama materijalnog uništenja ili smrtnim posledicama) ili čak stanje rata u kojem se međusobno masovno sukobljavaju oružane snage protivničkih strana u skladu sa pravom oružanih sukoba.

U cilju davanja odgovora na pitanje da li cyber napad ima isključivu prirodu cyber ratovanja, odnosno da li predstavlja akt agresije, jedna grupa autora polazi od Rezolucije UN prema kojoj je agresija definisana kao "upotreba oružane sile od strane neke države protiv suvereniteta, teritorijalnog integriteta ili političke nezavisnosti druge države", pri čemu Savet bezbednosti, na osnovu date formulacije, određuje da li cyber napad predstavlja akt agresije ili ne. Međutim, s obzirom da pomenuta formulacija nabraja oblike agresije u koje uključuje "invaziju ili napad oružanim snagama, vojnu okupaciju, aneksiju putem upotrebe sile" preduzetu protiv strane države, "upotrebu bilo kakvog oružja" protiv strane države, kao i napad na oružane snage druge države, procena prirode cyber napada može ići od krajnosti da je svaki cyber napad akt agresije, do stava da to nije nijedan, jer njihovo dejstvo nije kinetičko, pa ne predstavljaju primenu fizičke sile. Shodno tome, navedena formulacija ne pruža odgovor na pitanje da li je cyber napad akt agresije.

[342] Žaklina Spalević, „Krivična odgovornost pravnih i fizičkih lica na polju elektronskih komunikacija i elektronske uprave prouzrokovana cyber kriminalom“, Opus citatum.

Druga grupa autora smatra da kvalifikaciju prirode cyber napada treba izvesti na osnovu posledica, a ne vrste napada[343], jer upotreba biološkog i hemijskog oružja pokazuje da primena kinetičke sile ne mora da bude kriterijum za procenu prirode napada i posledice dejstva. S tim u vezi, cyber napad sa smrtnim posledicama ili uništenjem fizičkih objekata treba da se smatra aktom upotrebe sile. Priroda cyber ratovanja je veoma kompleksna i čini da mnoge oblike cyber napada uopšte nije moguće otkriti, a da u većini slučajeva nije moguće utvrditi ko su njegovi počinioci. Pri tom, cyber napadači mogu biti državni organi, ali i ne moraju.

I pored činjenice da cyber napad ne povređuje državnu bezbednost, teritorijalni integritet i političku nezavisnost bukvalnim prolaskom kroz informacione komunikacije do cilja, jedan od najvećih problema državne nadležnosti u cyber prostoru proizilazi upravo iz činjenice da digitalni podaci u razdvojenim paketima informacija prelaze neprimetno preko državnih granica. Svaka država ima nadležnost na vlastitoj teritoriji, ali postoje i izuzeci, na primer, u slučaju kada se primenjuje na diplomate stranih država. Nadležnost nad tim licima po nacionalnom principu imaju njihove matične države, čak i kada se oni fizički ne nalaze na njihovoj teritoriji. U praksi postoji još jedan, bezbednosni princip suverenosti, koji se shvata kao "princip nadležnosti u kome nacije mogu uzeti za pravo da kazne stranu državu za određeno ponašanje van svoje teritorije, koje je usmereno protiv njene bezbednosti, teritorijalnog integriteta i političke nezavisnosti". Ovaj princip, koji je po svojoj formi pogodan za primenu u situacijama cyber ratovanja nije usvojila međunarodna zajednica, ali ga pojedine države zloupotrebljavaju po "pravu jačeg".

U stručnoj javnosti postoje predlozi da se u oblast regulisanja cyber ratovanja uvede i treće stanje, tzv. "stanje drugačije od rata" koje je po svojoj prirodi između rata i mira, pa samim tim dozvoljava istovremenu primenu prava oružanih sukoba, krivičnog prava i ljudskih prava[344]. Bez obzira na mnoštvo suprotstavljenih stavova, u međunarodnoj zajednici postoji inicijativa da se započne izgradnja međunarodne regulative, koja je otpočela nastojanjem da se definišu zajednički stavovi i usvoji zajednička taksonomija u ovoj oblasti, čiji su inicijatori SAD i Rusija.

Razlog za ovo leži u činjenici da sve veći broj cyber napada, sakriven pod velom kriminala, predstavlja svojevrstan oblik međudržavne agresije. S obzirom da nemaju prirodu rata, na kriminalna dela se ne može primeniti pravo oružanih sukoba. Međutim, ovakve situacije kriju latentnu opasnost po izbijanje međudržavnih sukoba. Kao primer mogu poslužiti mnogobrojni nacionalno obojeni sukobi u cyber prostoru: izraelsko-palestinski, rusko-estonski, rusko-gruzijski, rusko-kirgistanski, srpsko-albanski, indijsko-pakistanski, severnokorejsko-američki, jermensko-azerbejdžanski i drugi. Svi

---

[343] Доктрина информационной безопасности Российской Федерации, No. Pr-1895, Совет Безопасности Российской Федерации, Available at: http://www.scrf.gov.ru/documents/5.html, date: 3.3.2013.

[344] Karl Rauscher, Andrey Korotkov, „Working Towards Rules for GoverningCyber Conflict“, Russia-U.S. Bilateral on Critical Infrastructure Protection, East-West Institute, pp.36-37, Available at: http://www.ewi.info/working-towards-rules-governing-cyber-conflict, date: 18.02.2018.

ovi sukobi su se odvijali u formi kriminalnih akata u cyber prostoru, ali suštinski su oblik međunacionalnih informacionih sukoba u cyber prostoru. Iako su im posledice bile niskog intenziteta i privremenog karaktera, ovi sukobi u cyber prostoru nisu izolovani i predstavljali su deo šireg područja sukoba između pomenutih država (nacionalnih zajednica), pa su stoga imali potencijal da prerastu u oblik sukoba većeg intenziteta. Takvu opasnost potenciraju najave vojnih zvaničnika SAD i Rusije da će cyber napade ekvivalentne oružanom napadu smatrati oružanom agresijom na koju će odgovoriti vojnim sredstvima u skladu sa nacionalnom doktrinom.[345]

Asimetričnost dejstava u takvim sukobima je realna, tako da se na cyber napade mogu uputiti vojni odgovori fizičkom silom, ali i obrnuto[346]. Pokrenuti cyber napadi mogu biti uzrok eskalacije sukoba, ali i posledica prethodnog akta agresije. Imajući u vidu specifičnu prirodu cyber ratovanja, mala je verovatnoća međudržavnih ili unutrašnjih državnih ratnih sukoba koji će se odigrati isključivo u cyber prostoru, ali to ne znači da takvih sukoba neće biti u budućnosti. Skoro svi savremeni sukobi u nekom obliku uključuju aktivnosti u cyber prostoru. Cyber ratovanje se idealno uklapa u koncepte mrežnocentričnog i asimetričnog ratovanja, a posebno na stanja odnosa koja se nalaze između rata i mira. Ta okolnost uslovljava prihvatanje postojanja i drugih stanja političkih odnosa, poput stanja "drugačijeg od rata" koje prihvata istovremeno postojanje i stanja rata i stanja mira u toku nekog sukoba. Takođe, može se očekivati da nastanu i novi oblici sukoba koji će se razlikovati od tradicionalnih sukoba u kojima se sukobljava jedna ili više država na jednoj i jedna ili više država na drugoj strani. Pored ovakvih linearnih sukoba mogu se očekivati i novi oblici kompleksnih, distribuiranih oblika sukoba u kojima je moguć rat "svih protiv jednog" ili "jednog protiv svih" u kojima učesnici nisu nužno državni subjekti, već to mogu biti svi, od pojedinaca do mreže grupa pojedinaca. Predlozi za uspostavljanje novih oblika stanja u odnosima među državama predstavljaju pokušaj da se omogući primena postojeće pravne regulative oružanih sukoba u cyber prostoru, običajnog prava, međunarodnog krivičnog prava i drugih oblika prava, kako po pitanju njihovog sadržaja, tako i po pitanju istovremenosti primene na konkretan cyber incident ili napad.

Kao i kompjuterski kriminal i cyber kriminal iziskuje odgovarajuću pravnu regulativu. Od prvih pojavnih oblika početkom 90-ih godina do danas mnoga su međunarodna tela posvetila pažnju ovom kriminalu. Pored međunarodne, sve je učestalija i nacionalna regulacija cyber kriminala, odnosno nekih od njegovih oblika. Paralelno sa tim i samoregulacija pokušava da se izbori sa ovom pojavom, što znači da se i sama regulacija odvija na više koloseka. Zanimljivo je da se mnogo više aktivnosti dešava na međunarodnom u odnosu na nacionalni i samoregulacioni plan. To je donekle i prirodno s obzirom na karakteristike dela i svojstva kriminalaca koji se njima bave. Najznačajniji i najbrojniji međunarodni akti doneti su u okviru Evropske unije.

---

[345] Siobhan Gorman, Julian Barnes, „Cyber Combat: Act of War“, Available atvor: http://www.rootsaction.org/news-a-views/108-cyber-combat-act-of-war- , date: 15.02.2018.

[346] International Strategy For Cyberspace, The White House, Available at: https:// obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, date: 19.02.2018.

Godine 1998. pod vođstvom *Urliha Sieber*-a sa Univerziteta u Virzburgu izrađena je posebna Studija o pravnim aspektima kompjuterskog kriminala u Informacionom društvu (*Legal Aspects of Computer-related Crime in the Information Society-COMCRIME study*) koja je obuhvatala i osnove cyber kriminala, kao višeg oblika. Ovaj akt u kombinaciji sa dokumentima sa Lisabonskog sastanka Evropskog saveta 2000. godine na kome je istaknut značaj tranzicije u konkurentnu, dinamičnu i na znanju zasnovanu ekonomiju predstavlja smernice za aktivnosti vezane za razumevanje fenomena cyber kriminala. Akcioni plan (*eEurope Action Plan*) iz iste godine vezan je za aktivnost obezbeđenja sigurnosti mreže i uspostavljanja saradnje zemalja članica i njihovog zajedničkog pristupa cyber kriminalu do 2002. godine. Iste godine donosi se i predlog Pravnog okvira odlučivanja vezanog za napade na informacione sisteme (*Proposal for a Council Framework Decision on attacks against information systems*). Godinu dana kasnije dokument je dopunjen sa nedozvoljenim pristupom informacionim sistemima i nedozvoljenim ometanjem sistema i podataka. Godine 2000. doneta je i Direktiva o eletronskom poslovanju (*Directive on electronic commerce*) u kojoj se posebna pažnja posvećuje problemu zloupotreba. Ta je godina i dalje plodna, jer se donosi čitav set različitih akata od Odluke Saveta o sprečavanju dečje pornografije na Internetu, Konvencije o međusobnoj pomoći u krivičnoj materiji do Preporuke o strategiji za novi Milenijum u zaštiti i kontroli kompjuterskog kriminala. Potom sledi akt kojim treba da se obezbedi sigurnije Informaciono društvo kroz sigurnost informacione infrastrukture i borbe protiv kriminala vezanog za kompjutere (*Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*)[347].

Tako je 1996. godine započela Zajednička akcija protiv rasizma i ksenofobije, a 1997. doneta je Preporuka o anonimnosti subjekata na Internetu i Deklaracija o globalnim računarskim mrežama. Godine 1998. sačinjen je Predlog o okvirima sprečavanja seksualne eksploatacije i trgovine ljudima. Par godina kasnije donosi se i poseban akt vezan za cyber kiminal (*Communication on Cybercrime*). Nešto manje bile su aktivnosti OECD-a, Ujedinjenih Nacija i Saveta Evrope. Još 1983. godine, u okviru OECD-a usvojena je Studija o međunarodnoj primeni i harmonizaciji krivičnog prava vezanog za problem kompjuterskog kriminala i zloupotreba. Tri godine kasnije izašla je minimalna lista u okviru dokumenta *Kriminal vezan za kompjutere: analiza i pravna politika,* a 1999. godinu je obeležio ceo set priručnika za sigurnost informacionih sistema kojima se uspostavljaju pravila i osnov njenog postizanja.

Savet Evrope je krajem 1998. godine objavio početak pripreme na donošenju Konvencije o cyber kriminalu, čiji predlog je aprila 2000. godine pušten u proceduru javne rasprave. Ona je danas jedan od najznačajnijih dokumenata koji su, pored evropskih zemalja, prihvatili i Japan, Sjedinjene Američke Države, Kanada, Južna Afrika. Konvenciju, koja je stupila na snagu u julu 2004. godine, prate brojni dokumenti doneti u okviru Saveta: *Trust and Security in Cyberspace: The Legal and Policy Framework for Addressing Cybercrime* (*2002*), *Cyber-Rights & Cyber-Liberties,*

[347] Žaklina Spalević, „Krivična odgovornost pravnih i fizičkih lica na polju elektronskih komunikacija i elektronske uprave prouzrokovana cyber kriminalom“, Opus citatum, str. 186.

Advocacy Handbook for NGOs (*2003*), *Racism Protocol to the Convention on Cybercrime* (*2003*), *The Protocol to the Cybercrime Treaty* (*2002*), *Additional Protocol to the Cybercrime Convention Regarding "Criminalization of Acts of a Racist or Xenophobic Nature Committed through Computer Networks", Report Revised draft of the Protocol on Racist Speech* (*2000*), *Background Materials on the Racist Speech Protocol, Draft Protocol on Racist and Zenophobic Speech: Prelimiary draft* (*2001*), *Second Protocol on Terrorism* (*2002*).

Pomenuti akti su u ime državne zajednice Srbije i Crne Gore potpisani u Helsinkiju 7. aprila 2005. godine. Naime, u radu 26. Konferencije ministara pravde Saveta Evrope, dana 7. aprila 2005. godine u Helsinkiju, Zoran Stojković, tadašnji Ministar pravde u Vladi Republike Srbije, je u ime državne zajednice Srbije i Crne Gore potpisao Građansko-pravnu konvenciju o korupciji i Drugi dodatni protokol uz Evropsku konvenciju o međusobnom pružanju pravne pomoći u krivičnim stvarima. U radu pomenutog skupa učestvovala je i delegacija Ministarstva pravde Republike Crne Gore, predvođena ministrom koji je u ime državne zajednice Srbije i Crne Gore potpisao Konvenciju o cyber kriminalu, u vezi sa kriminalizacijom akata rasističke i ksenofobične prirode učinjene preko kompjuterskih sistema. Učesnici konferencije razgovarali su i o napretku postignutom u borbi protiv terorizma, socijalnim aspektima pravde, posebno o socijalnoj misiji krivično-pravnog sistema, a razmotrili su i Evropsku povelju o zatvorima.

Uspostavljanje saradnje između pravosudnih organa, industrije, raznih organizacija i asocijacija posebno se potencira od 1997. godine, kada je u Vašingtonu održan sastanak ministara pravde i policije zemalja G8 i kada je utvrđeno 10 tačaka Akcionog plana borbe protiv cyber kriminala među kojima je posebno mesto posvećeno saradnji sa industrijskim sektorom koji dizajnira, razvija i proizvodi komponente globalnih mreža, ali i koji treba da bude odgovoran za izgradnju i primenu tehničkih standarda sigurnosti. Time je *pružena ruka* proizvođačima specijalizovanih hardverskih i softverskih proizvoda namenjenih sigurnosti. Komisija Evropske unije je donela Odluku o posebnom programu razvoja (*EU R&D Framework Programme, Internet Action Plan*, *Programs STOP i Daphne*) koji ima za cilj da utvrdi pravce borbe protiv pojedinaca i grupa okupljenih oko zloupotreba elektronskog poslovanja u okviru koga su brojni subjekti potencijalne i stvarne žrtve. Možda najznačajnija aktivnost kojom se pokušava operacionalizovati saradnja među ovim akterima je formiranje Foruma Evropske unije koji obuhvata razne agencije, provajdere Internet usluga, operatore telekomunikacija, organizacije za ljudska prava, predstavnike korisnika, tela za zaštitu podataka i sve druge zainteresovane koji žele da se uspostavi saradnja u borbi protiv cyber kriminala na evropskom nivou. Forum treba da omogući[348]:

- razvoj dvadestčetvorosatne veze između državnih organa i industrije;
- definisanje standardnih zahteva za koje provajderi treba da obezbede informacije o korišćenju Interneta;
- izgradnju i primenu etičkog kodeksa sa definisanjem dobrih poslovnih običaja svih aktera, a posebno u međusobnim odnosima između državnih organa i industrije;

[348] Žaklina Spalević, „Krivična odgovornost pravnih i fizičkih lica na polju elektronskih komunikacija i elektronske uprave prouzrokovana cyber kriminalom“, Opus citatum, str. 189.

- podspešivanje razmene informacija o trendovima kriminala visokih tehnologija između različitih partnera, posebno u okviru industrije;
- uspostavljanje posebnih koncerna za razvoj novih tehnologija;
- razvoj menadžment mehanizama kojima se pruža zaštita, olakšava identifikacija i savladavaju pretnje vezane za informacionu infrastrukturu;
- uspostavljanje čvršćih oblika ekspertske saradnje između različitih međunarodnih organizacija, tela i asocijacija npr. Saveta Evrope i G8;
- razvoj principa saradnje (*Memorandum of Understanding*, *Codes of Practice in line with the legal framework*).

Naš cyber prostor nije ostao nedodirnut mnogim od oblika cyber kriminala. Za svega nekoliko godina popeli smo se visoko na rang listi opasnih i nesigurnih područja sa akterima kojima raste ugled u cyber podzemlju. Međutim, jedna grupa ovih počinilaca izgubila je predznak kriminalaca i svrstana je u heroje iako su njihove aktivnosti uveliko prevazilazile takve kvalifikacije. S druge strane, nespremnost pravosuđa i uspavanost prava olakšali su prelazak ovih pojedinaca u sferu *čistog* kriminala. To je ohrabrilo i mnoge druge koji su iz faze bojažljivih pokušaja prešli u drske i samosvesne kriminalce ubeđene da im niko ništa ne može. Takvu atmosferu prekinulo je nekoliko prijava istražnim organima koji pokušavaju da se uhvate u koštac sa novim oblicima kriminala i njima, često, nerazumljivim aktivnostima. Počele su i prve istrage i prikupljanje dokaza, a i prve tužbe našle su se pred sudovima u Beogradu, Pančevu i Nišu.

Nažalost, brojne su nedaće sa kojima se sreću sudije, tužioci i advokati zbog niskog nivoa, čak i elementarnog znanja informatike što umnogome otežava i produžuje postupke koji, inače, iziskuju brzinu i spremnost da se u delićima sekunde spasu dokazi i identifikuju počinioci. Iako je pravna praznina koja je postojala u krivičnom zakonodavstvu popunjena izmenama i dopunama Krivičnog zakona Republike Srbije sa delima protiv bezbednosti računarskih podataka, to nije bilo dovoljno (preuzeta su rešenja Predloga Krivičnog zakonika SRJ iz 1999. godine, bez dopunjavanja sa novim krivičnim delima i oblicima inkrimnisanog ponašanja). Suočili smo se sa nekonzistentnošću sa drugim delima i sankcijama.

Iako je ekspertski tim Saveta za državnu upravu Vlade Republike Srbije i UNDP-a u novembru 2002. godine izradio prvu verziju posebnog, *lex specialis,* Zakona o cyber kriminalu, isti još uvek nije donet. Poseban propust je što se u odredbe o organizovanom kriminalu nisu uvrstili i oblici cyber kriminala. Svemu ovome treba dodati i probleme u radu pravosudnih i policijskih organa, uvreženog mišljenja o nedodirljivosti izvršilaca, nepostojanja saradnje sa međunarodnim organizacijama, telima i asocijacijama, kao i nacionalnim institucijama drugih zemalja, zatim nepostojanje posebnih specijalizovanih jedinica za istragu, specijalizovanih sudova za presuđivanje i serioznosti u radu provajdera, kao i neuspostavljanje saradnje između subjekata koji bi trebalo da se izbore sa ovom pojavom.[349]

[349] Vasić D.,"Zakonska zaštita elektronskih informacija i komunikacija u Srbiji - kritički osvrt na stepen normativne uređenosti", Srpska politička misao, ISSN 0354-5989, vol. 57, br. 5-6, str. 135-146, 2008.

6.4 Analiza kaznenog zakonodavstva za kompjuterski i cyber kriminal

Ozbiljnost problema koji predstavljaju kompjuterski i cyber kriminal obrađena je i odredbama velikog broja zakonskih i pod zakonskih regulativa. Takođe kao što je već napomenuto ranije postoji i veliki broj konvencija koje se bave ovom tematikom. Predmetne konvencije su potpisale mnoge zemlje kako članice Evropske Unije tako i zemlje koje to nisu. Različita zakonodavstva na različite načine definišu pojam cyber kriminaliteta, saglasno usvojenoj politici krivičnog gonjenja i konkretnim prilikama, karakteristikama i stepenu razvoja svakog pojedinačnog društva. Na međunarodnom planu, usvajanjem Konvencije Saveta Evrope o cyber kriminalu, učinjen je napor da se određeni delikti i pojmovi sistematizuju i pravno definišu kako bi se izvršila harmonizacija nacionalnih zakonodavstava u cilju efikasnije borbe protiv cyber kriminaliteta.[350]

6.4.1 Konvencija Saveta Evrope o cyber kriminalu

Činjenica da su Konvenciju potpisale i pojedine zemlje koje nisu članice Saveta Evrope ukazuje na to koliki je značaj ovog pravnog akta i kolika su očekivanja da se napravi krupan iskorak u suzbijanju ove vrste kriminaliteta.

Konvencija sadrži četiri poglavlja koja se odnose na značenje i upotrebu određenih termina, na mere koje je potrebno preduzeti na nacionalnom nivou u okviru procesnog i materijalnog zakonodavstva, na odredbe o standardima međunarodne saradnje i na završne odredbe.

Pored propisivanja krivičnih dela koja bi trebalo predvideti nacionalnim zakonodavstvom i njihovim elementima, Konvencija daje instrukcije i u pogledu nekih drugih instituta materijalnog krivičnog prava, tako da je propisano da svaka članica treba da usvoji takve legislativne i ostale neophodne mere da bi se u njenom nacionalnom pravu kao krivično delo okvalifikovalo namerno pomaganje ili podstrekivanje na izvršenje nekog od prestupa definisanih Konvencijom, sa namerom da se takav prestup učini.[351]

Pored toga, Konvencija propisuje obavezu država potpisnica da se reguliše i odgovornost pravnih lica za krivična dela koja su njome propisana, a koja učini fizičko lice koje ima određenu funkciju u pravnom licu.[352] Ovime se misli kako na zaposlene u okviru pravnog lica tako i na odgovorna lica i rukovodeći organ. Konačno, i potpisnice

---

[350] Convention on Cybercrime, ETS No.185, Budapest, 23.XI 2001.
[351] Ibidem, Član 11
[352] Ibidem, Član 12

se obavezuju da sankcije i mere koje se izriču prema izvršiocima krivičnih dela treba da budu efikasne, proporcionalne i da obuhvate i sankciju lišenja slobode.[353]

Od naročitog značaja za međunarodnu saradnju i podizanje nivoa efikasnosti u otkrivanju i progonu izvršilaca krivičnih dela jeste član koji predviđa ustanovljenje mreže tipa 24/7 u svim zemljama potpisnicama.[354] Ovom odredbom je definisana da svaka članica treba da odredi mesto za kontakt koje će biti dostupno 24 sata dnevno, svih 7 dana u nedelji, kako bi omogućila momentalnu pomoć u istragama i procedurama u vezi sa krivičnim delima koja se odnose na kompjuterske sisteme i kompjuterske podatke ili u prikupljanju dokaza za krivična dela u elektronskom obliku. Ova vrsta pomoći bi trebalo neposredno da omogući davanje tehničkih saveta, čuvanje podataka u skladu sa odredbama Konvencije, kao i prikupljanje dokaza, davanje informacija pravnog karaktera i lociranje osumnjičenih lica.

6.4.2 Kazneno pravno zakonodavstvo cyber kriminala u Nemačkoj

U Nemačkoj kakoda je reč o krivično pravnom regulisaanju kompjuterskog kriminala koristi se pristup dopune postojećih zakona. Korpus modernog krivičnog prava u Nemačkoj, u vezi sa kompjuterskim kriminalitetom svodi se na sledeće pravne izvore:[355]

- Drugi Zakon o sprečavanju privrednog kriminaliteta;[356]
- Zakon o autorskom delu.

Pomenutim zakonima su u korpus nemačkog krivičnog prava uvedena sledeća krivična dela u oblasti cyber kriminala:

- Krađa podataka;[357]
- Kompjuterska prevara;[358]
- Kompjutersko falsifikovanje;[359]
- Neovlašćeno menjanje podataka;[360]
- Ometanje rada računara;[361]
- Zaštita autorskog prava na računarskim programima.[362]

---

[353] Ibidem, Član 13.
[354] Ibidem, Član 34
[355] Sieber U., „Responsibility of Internet Providers", University of Würzburg, 2005. Available at: http://www.iura.uni-muenchen.de/sieber; date: 11.10.2011.
[356] Zweites Gesetz zur Bekampfung der Wirtschaftskriminalitat, 2.WiKG;
[357] Ibidem, Član 202a.
[358] Ibidem, Član 263a.
[359] Ibidem, Član 269.
[360] Ibidem, Član 303a.
[361] *Computersabotage,* Član 03b, WiKG.

Ukoliko uporedimo nemačko zakonodavstvo sa smernicama koje su date u Konvenciji o cyber kriminalu, vidimo da je u velikoj meri već sada nemačko zakonodavstvo usaglašeno sa relevantnom evropskom legislativom. Zatim, nemački sudovi imaju značajno, gotovo tridesetogodišnje iskustvo u rešavanju slučajeva vezanih za cyber kriminalitet. Nemačkom zakonodavstvu preostaje još da krivično-pravno sankcioniše sam neovlašćeni pristup. Takođe potrebno je detaljnije i funkcionalnije zaštititi pravilno funkcionisanje računara, u smislu kažnjavanja različitih DoS napada.[363] Sama prisutnost DoS napada dovoljan je svedok činjenici da ova oblast nije dovoljno zaštićena.

6.4.3 Kazneno pravno zakonodavstvo cyber kriminala u Austriji

Austrijsko krivično zakonodavstvo nije sadržalo posebne odredbe u pogledu cyber kriminaliteta sve do 1987. godine.[364] Jedini propis u kome su bile sadržane odredbe vezane za pojam kompjuterskih zloupotreba bio je Zakon o zaštiti podataka iz 1978. godine. Međutim, zaštita pružena ovim propisom odnosila se samo na lične podatke građana čuvane u javnim službama i ustanovama ovlašćenim za njihovo prikupljanje. Drugi kompjuterski podaci nisu uživali nikakvu zaštitu, te su stoga pravna lica bila izložena nesmetanim i neinkriminisanim cyber napadima koji su im nanosili velike štete u normalnom poslovanju. Na predlog austrijskog ministarstva pravosuđa 1985. godine, predložena je dopuna krivičnog zakonodavstva. Nažalost, predlog je samo delimično prihvaćen, tako da su konačnom izmenom *Strafgesetzbucha* uneta samo krivična dela Oštećenja podataka i Prevarne zloupotrebe obrade podataka.[365] Novi Krivični zakon stupio je na snagu 1988. godine.

Ukoliko se uporedi zakonodavni sistem Nemačke i Austrije može se zaključiti da su austrijski i nemački stručnjaci sarađivali, budući da su obe zemlje otprilike u isto vreme, na sličan način razmatrale reformu krivičnog sistema u pogledu obuhvatanja krivičnih dela kompjuterskog kriminaliteta.

Za razliku od nekih drugih zemalja koje su posebno inkriminisale kompjutersku sabotažu, poput Nemačke, Japana, Brazila, Poljske i Kanade, Austrija se odlučila da na slučajeve krađe ili oštećenja tehničke osnove (hardvera) primeni postojeće inkriminacije (Krađa, Teško oštećenje podataka) i da uvede novu inkriminaciju u vidu krivičnog dela Oštećenje podataka[366]. U zavisnosti od toga kolika je načinjena šteta srazmerno je definisana i kazna.[367]

---

[362] Zakon o autorskom delu, Član 106 i 108.

[363] Schmölzer G.,"Internet i kazneno pravo", *prevod u Hrvatskom ljetopisu za kazneno pravo*, 1997, vol. 4 2/97, str. 891-897.

[364] Dragičević D., „Kompjutorski kriminalitet i računalni sustavi", Opus citatum.

[365] StrafGesetzbuch, StGB, Član 126 i 148. StGB.

[366] Ibidem, Član 127, 126, 126a, 126a st.2.

[367] Dragičević D., „Kompjutorski kriminalitet i računalni sustavi", Opus citatum, str. 169.

Krivično delo Prevarne zloupotrebe obrade podataka obuhvata kompjutersku prevaru i falsifikovanje putem programa, unosa, brisanja ili izmene podataka, kao i svako drugo delovanje kojim se utiče na tok obrade podataka. Za ponavljanje krivičnog dela, kao i za počinjenu veću štetu predviđena je i stroža kazna.

Ono što iznenađuje u austrijskom pristupu materiji je nedostatak sankcionisanja dela Neovlašćenog pristupa i Kompjuterske špijunaže (Neovlašćenog pribavljanja podataka), kao što je to učinjeno u Nemačkoj, Sjedinjenim Američkim Državama, Kanadi, Velikoj Britaniji, itd. Ipak, treba spomenuti da, iako ta dela nisu deo krivičnog zakona, ona jesu regulisana, zakonom iz sfere trgovačkog prava (Zakonom protiv nelojalne konkurencije) sa svim posledicama koje to sa sobom nosi (specifičnosti građanskog u odnosu na krivični postupak)[368].

Za očekivati je da će austrijski krivični sistem teško odgovoriti na izazove kompjuterskog kriminaliteta ukoliko uskoro ne sankcioniše i preostala krivična dela vezana za kompjuterski kriminalitet, pogotovo dela Neovlašćenog pristupa i Neovlašćenog pribavljanja tuđih podataka.

6.4.4 Kazneno pravno zakonodavstvo cyber kriminala u Francuskoj

Republika Francuska je dana 23. novembra 2001. godine potpisala Konvenciju o cyber kriminalu i ratifikovala je 10. januara 2006. godine, sa dodatnim Protokolom o ksenofobiji i rasizmu. Pravni propisi su usklađeni sa ovom Konvencijom, a problematika cyber kriminala je regulisana Krivičnim zakonikom (*Code Penal*), Zakonom o intelektulanoj svojini (*Code de la Propriete Intellectuelle*) i Zakonikom o krivičnom postupku (*Code de Procedure Penal*).[369]

Krivični zakonik Republike Francuske u oblasti pitanja zaštite automatske obrade podataka (tekst se nalazi u zakonu pod nazivom *Loi Godfrain* od 5. januara 1998. godine) inkriminiše radnje menjanja i brisanja računarskih podataka, a zaprećena je zatvorska kazna do jedne godine i novčana kazna u iznosu do 15.000 evra.[370] Uništavanje podataka inkriminisano je i zaprećena je zatvorska kazna do dve godine i novčana kazna do 30.000 evra; inkriminisano je ometanje funkcionisanja obrade podataka, a propisana je kazna zatvora do tri godine i kazna do 45.000 evra, kao i protivpravna prodaja podataka kaznom do tri godine zatvora i novčanom kaznom do 45.000 evra. Protivpravno umnožavanje podataka sankcionisano je identičnom kaznom.[371]

---

[368] Žaklina Spalević, „Krivična odgovornost pravnih i fizičkih lica na polju elektronskih komunikacija i elektronske uprave prouzrokovana cyber kriminalom“, Opus citatum, str. 212.

[369] Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries for assisting Computer Security Incident Response Teams (CSIRTs), str. 47.

[370] Krivični zakonik Republike Francuske, Član 323 st. 1,

[371] Ibidem, Član 323-1 stav 2, 323-3, 323-4.

Prikupljanje istorijskih, statističkih i naučnih podataka, bez ovlašćenja od strane njihovih vlasnika, predviđeno je kao krivično delo, sa zaprećenom sankcijom do tri godine zatvora i novčanom kaznom do 45.000 evra. Zloupotreba podataka u svrhe za koje nisu dati regulisano je kao krivično delo, sa kaznom zatvora do pet godina i novčanom kaznom do 300.000 evra.

Prodaja ličnih podataka predstavlja krivično delo, a predviđena je kazna zatvora do jedne godine i novčana kazna do 15.000 evra. Javno objavljivanje ličnih podataka bez ovlašćenja, neobezbeđivanje poverljivih tehničkih podataka i fabrikovanje lažnih podataka je krivično delo predviđeno u zakonu *Code des P&T* u čl. L. 39-31, za koje je predviđena kazna zatvora do jedne godine i novčana kazna do 75.000 evra.[372]

Krivična dela iz oblasti elektronskog poslovanja, vezana za zloupotrebu i falsifikovanje platnih kartica nalaze se u Zakonu o monetarnoj politici i finansijama (*Code monetaire et Financier*), u tekstu akta pod nazivom *LSQ* od 15. 11. 2001. godine.[373] Za ova krivična dela predviđena je kazna zatvora do sedam godina. Neovlašćena enkripcija podataka definisana je kao krivično delo u Krivičnom zakoniku za čije činjenje je zaprećena kazna do jedne godine zatvora i novčano do 45.000 evra.

Delo odbijanja predaje ključa za dekripciju inkriminisano je u čl. 11. Zakona o telekomunikacijama (*L. Telecom* 29. 12. 1990. godine), sa modifikacijama od 10. jula 1991. godine. Ukoliko se radi o pokušaju izbegavanja predaje šifre u cilju izbegavanja istrage, zaprećena kazna je do 30.000 evra i pet godina zatvora, a u slučaju pokušaja ograničavanja istrage kazna je do 75.000 evra, a takođe i pet godina zatvora.[374]

U francuskom zakonodavstvu, zloupotreba dece u pornografske svrhe inkriminisana je u nekoliko članova Krivičnog zakonika. Krivično delo gledanja dečje pornografije i registracija u nameri pribavljanja sadržaja sa dečjom pornografijom inkriminisano je u članu 227-23 Krivičnog zakonika i kažnjava se kaznom od tri godine zatvora i 45.000 evra. Širenje pornografskog materijala putem mreže je krivično delo sa zaprećenom kaznom do pet godina zatvora i novčanom kaznom do 75.000 evra. Posedovanje fotografija sa sadržinom dečje pornografije je krivično delo, a zaprećena kazna za činjenje istog je takođe do pet godina zatvora i novčana kazna do 75.000 evra.

Za dela organizovanog kriminala u oblasti dečje pornografije predviđena je kazna do 10 godina zatvora i do 500.000 evra novčane kazne. Krivično delo širenja pornografskih predstava u kojima učestvuju lica koja se predstavljaju kao maloletna sankcionisano je kaznom do tri godine zatvora i novčano 75.000 evra.[375]

Krivična dela vezana za širenje rasne, verske i etničke mržnje i netrpeljivosti, takođe su regulisana u Krivičnom zakoniku, gde je kao krivično delo predviđeno podsticanje na izvršenje ovih krivičnih dela, a kazna je novčana do 45.000 evra i zatvorska kazna do pet godina zatvora. Za negiranje ratnih zločina i pozivanje na terorizam predviđena je istovetna kazna, odnosno do pet godina zatvora i novčana kazna do 45.000 evra.

---

372 Ibidem, Član 226-17 do 226-20,

373 Zakon o monetarnoj politici i finansijama Republike Francuske, Član 35-40,

374 Zakon o telekomunikacijama, Član 434-15-2 stav 2,

375 Krivični zakonik Republike Francuske, Opus citatum, Član 227-23 stav 3, 227-3 stav 4, 227-4

Izazivanje rasne mržnje predviđeno je kao krivično delo sa kaznom zatvora do jedne godine i novčanom kaznom do 45.000 evra. Izazivanje zločina protiv čovečnosti je predviđeno, takođe, u čl. 24. sa zaprećenom kaznom do jedne godine zatvora i 45.000 evra. Kleveta na osnovu rasnih razlika kao krivično delo i uvreda na osnovu rasnih razlika su krivična dela čije se kazne kreću do jedne godine zatvora i 45.000 evra novčano.[376]

Krivična dela protiv ličnosti i dostojanstva, takođe se nalaze u Krivičnom zakoniku. Krađa identiteta predviđena je kao krivično delo sa zaprećenom kaznom do pet godina zatvora i 75.000 evra.[377] Obične pretnje i pretnje smrću inkriminisane su čl. 222-17, a predviđene su kazne od šest meseci do tri godine zatvora, kao i novčane kazne od 45.000 do 75.000 evra. Iznošenje privatnih podataka o ličnosti je krivično delo sa predviđenom kaznom do jedne godine zatvora i 45.000 evra novčano. Narušavanje ugleda je krivično delo sa istovetno predviđenom kaznom. Nasuprot tome, kleveta je kao krivično delo predviđena sa kaznom zatvora do pet godina i novčanom kaznom do 45.000 evra. Najzad, otkrivanje poslovne tajne je krivično delo, a predviđena je kazna zatvora do jedne godine i novčana kazna do 45.000 evra.[378]

Krivična dela protiv imovine, takođe su sadržana u Krivičnom zakoniku, a najznačajnije krivično delo za cyber kriminal predstavlja pretnja oštećenjem ili uništenjem imovine sa predviđenom kaznom do 6 meseci zatvora i novčanom kaznom do 7.500 evra. Krivična dela vezana za prevare sa platnim karticama inkriminisana su kao prevare vezane za korišćenje lažnih platnih kartica i plaćanja na Internetu, a zaprećene kazne za takve aktivnosti iznose do pet godina zatvora i 350.000 evra.[379]

U francuskom Zakonu o zaštiti intelektualne svojine sadržana su krivična dela vezana za zaštitu intelektualne svojine u koje spadaju različiti programi, žigovi, dizajn i slično. Takođe je dodatno sankcionisano i ponavljanje (izvršenje u povratu) krivičnih dela iz ove oblasti, kao i kvalifikovan oblik ukoliko izvršilac krivičnog dela korsti neki specifičan poslovni ili privatni odnos sa žrtvom.[380] Za pomenuta krivična dela su zaprećene kazne do tri godine zatvora i novčane kazne do 300.000 evra. Zakon predviđa sankcionisanje povratništva ili korišćenje specifičnog položaja ili odnosa koji izvršilac koristi, a kazne se u tom slučaju udvostručuju. Kazna za organizovane kriminalne grupe koje čine krivična dela vezana za zaštitu intelektualne svojine je do pet godina zatvora i 375.000 evra. [381]

Analiza strukture i organizacije državnih organa Republike Francuske u čijoj nadležnosti se nalazi sprečavanje i suzbijanje cyber kriminala, kao i krivično-materijalnih propisa koji u Francuskoj regulišu ovu oblast, značajna je sama po sebi, pošto se radi o državi u kojoj su začete ideje o slobodi, jednakostima i pravima čoveka i zemlji koja je u mnogo čemu kolevka demokratije.

---

376 Ibidem, Član 23-24, i član 29-33.
377 Ibidem Član 434-23.
378 Ibidem, Član 226 st. 1 i 2, 226-8, 226-10 i 226-13.
379 Ibidem, Član 323-12 I 313-2.
380 Ibidem, Član 335-1, 335-2 i 335-3, 716-9 i u čl. 521-4.
381 Zakon o zaštiti intelektualne svojine Republike Francuske, Član 335-9.

Republika Francuska je danas država u kojoj se neguje ovo istorijsko nasleđe i istovremeno konstantno razvija savremeno društvo, a sprečavanje i suzbijanje cyber kriminala i zaštita informacionog sistema u toj zemlji su regulisani uz puno uvažavanje ovih principa.

Struktura državnih organa koji se bave sprečavanjem Cyber kriminala ustanovljena je na sistematičan način i pruža adekvatan okvir za uspešnu borbu protiv ovog fenomena na teritoriji Republike Francuske. Osim toga, uloga Republike Francuske i njenih državnih organa u borbi protiv ove vrste kriminala jasno je uočljiva i na međunarodnom planu.

Krivično-pravna regulativa, takođe, pruža efikasne okvire za sprečavanje ove pojave. Oštra kaznena politika koja se ogleda u visini zaprećenih zatvorskih kazni, kao i zaprećenim novčanim kaznama predstavlja i svojevrstan faktor odvraćanja od izvršenja krivičnih dela iz ove oblasti.

6.4.5 Kazneno pravno zakonodavstvo cyber kriminala u Republici Srbiji

Prvi pokušaj da se u našoj zemlji, bar u jednom delu, zakonski reguliše ova oblast učinjen je donošenjem Zakona o zaštiti podataka o ličnostima,[382] maja meseca 1998. godine, čime se naša država priključila onim zemljama koje su pitanje zaštite privatnosti zakonski regulisale u skladu sa svetskim standardima.

Drugi važan zakon kao element zaštite od cyber kriminaliteta jeste Zakon o autorskim i srodnim pravima,[383] donet u maju mesecu 1998. godine, kojim je regulisana zaštita kompjuterskih programa.

Najznačajniji pomak učinjen je tokom 2003. godine kada je u Zakonu o izmenama krivičnog zakona Republike Srbije, a koji je objavljen u Službenom glasniku Republike Srbije, br. 39/03, predviđena grupa krivičnih dela protiv bezbednosti računarskih podataka, i to:[384]

- prvo krivično delo je Neovlašćeno korišćenje računara i računarske mreže koje učini onaj ko ošteti, prikrije, neovlašćeno izbriše ili na drugi način učini neupotrebljivim računarski podatak ili program;
- drugo krivično delo je Računarska sabotaža i isto čini onaj ko 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 koji su od značaja za državni organ, javnu službu, ustanovu, privredno društvo ili organizaciju;

---

382 Zakon o zaštiti podataka o ličnosti, Opus citatum.

383 Zakon o autorskim i srodnim pravima, Opus citatum.

384 Žaklina Spalević, „Krivična odgovornost pravnih i fizičkih lica na polju elektronskih komunikacija i elektronske uprave prouzrokovana cyber kriminalom“, Opus citatum, str. 224

- treće delo je Pravljenje i unošenje računarskih virusa koje čini onaj ko napravi računarski virus u nameri da ga unese u tuđi računar ili računarsku mrežu, kao i onaj ko unese računarski virus u tuđi računar ili računarsku mrežu i time prouzrokuje štetu;
- četvrto delo je Računarska prevara koju čini onaj ko unese netačan podatak ili ne unese kakav važan podatak 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;
- peto delo je Ometanje funkcionisanja elektronske obrade i prenosa podataka i računarske mreže koje čini onaj ko neovlašćenim pristupom elektronskoj obradi podataka ili računarskoj mreži izazove zastoj ili poremeti funkcionisanje elektronske obrade podataka ili mreže;
- šesto delo je Neovlašćeni pristup zaštićenom računaru ili računarskoj mreži koje čini onaj ko kršeći mere zaštite neovlašćeno pristupi računaru ili računarskoj mreži;
- sedmo delo je Sprečavanje i ograničavanje pristupa javnoj mreži koje čini onaj ko neovlašćeno sprečava ili ometa pristup javnoj računarskoj mreži.

U oblasti borbe protiv visokotehnološkog kriminala, u Srbiji je najznačajniji pomak učinjen osnivanjem specijalizovanih organa na nivou policije, tužilaštva i suda Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, koji je stupio na pravnu snagu 26. jula 2005. godine, a čije su poslednje izmene i dopune stupile na snagu 24. decembra 2009. godine.

Primećujemo ipak da je navedenim zakonskim propisom stvarna nadležnost posebnog tužilaštva postavljena suviše usko, odnosno da pojedina krivična dela koja bi po svojoj prirodi trebalo da se nalaze u nadležnosti specijalizovanog organa gonjenja ostaju van njegovog domašaja. Konkretno, radi se o krivičnom delu Prikazivanje pornografskog materijala i iskorišćavanje dece za pornografiju i krivičnom delu Falsifikovanje i zloupotreba platnih kartica. Ukoliko se uzmu u obzir elementi počinilaca ovih krivičnih dela i mogući načini njihovog izvršenja, posebno da se distribucija sadržaja uglavnom vrši preko Interneta, kao i da su pribavljanje relevantnih identifikacionih podataka za izradu lažne platne kartice, kao i sama izrada i korišćenje nezamislivi bez upotrebe specifičnih elektronskih uređaja i programa koji po svojoj prirodi i nameni jesu računari i računarski program, vidi se da je veliki propust učinjen činjenicom da se krivično gonjenje učinilaca ovakvih krivičnih dela i dalje nalazi u okviru organa gonjenja opšte nadležnosti.

Rešenja drugih evropskih zemalja koja regulišu ovu oblast su mnogo stroža i vode računa o prirodi ovih krivičnih dela, društvenoj opasnosti koju predstavljaju i zaštitnom objektu, pri čemu je i samo posedovanje ovakvih materijala krivično delo, a kao pozitivan primer može se uzeti Norveška čija regulativa je otišla korak dalje i sankcioniše i samo pristupanje Internet sajtovima sa ovakvim sadržajem.

Pored krivičnopravnih odredaba materijalnog karaktera koje sadrži Krivični zakonik Republike Srbije, oblast pravne zaštite prava intelektualne svojine u okviru borbe protiv visokotehnološkog kriminala regulisana je i Zakonom o posebnim

ovlašćenjima radi zaštite prava intelektualne svojine.[385] Ovim zakonom predviđena je odgovornost za privredne prestupe i prekršajna odgovornost pravnih lica za povredu prava intelektualne svojine. U pravcu kontrole proizvodnje, prometa, upotrebe i držanja robe, kao i pružanja usluga kojima se povređuje pravo intelektualne svojine, posebna ovlašćenja poverena su pojedinim ministarstvima kroz inspekcijske službe (tržišna i turistička inspekcija pri Ministarstvu trgovine, turizma i usluga, poreski inspektorat i policija pri Ministarstvu finansija, itd).

Ekspertski izveštaj Saveta Evrope[386] o usklađenosti domaćeg zakonodavstva u krivičnopravnoj oblasti sa zahtevima Konvencije o cyber kriminalu pruža preciznu sliku o merama koje je neophodno preduzeti u pravcu stvaranja optimalnog pravnog okvira za suzbijanje visokotehnološkog kriminaliteta. Ukratko, opšta ocena jeste da domaće zakonodavstvo samo delimično ispunjava zahteve Konvencije, odnosno da je budućom reformom krivičnog zakonodavstva neophodno uskladiti propise sa obavezom koju je država preduzela. Ova obaveza naročito dobija na značaju ako se ima u vidu da je Narodna skupština, marta meseca 2009. godine, ratifikovala Konvenciju i time postala deo unutrašnjeg pravnog poretka.

Potrebno je ukazati na činjenicu da je Konvencija doneta i usvojena 2001. godine, a aktuelni Krivični zakonik Republike Srbije stupio na snagu 1. januara 2006. godine, iz čega proizilazi da je bilo sasvim dovoljno vremena da se usvoje nova i unaprede već postojeća rešenja u domaćem zakonodavstvu na način koji bi omogućavao veću usklađenost i samim tim efikasniju primenu.

Tako npr. domaće zakonodavstvo definiše niz pojmova koji spadaju u oblast visokotehnološkog kriminala, kao što su računarski podatak, računarska mreža, računarski program, a da pri tom ne sadrži definiciju osnovnog hardvera, odnosno računara, što može dovesti do problema u praktičnoj primeni zakona, jer je nejasno da li pojam računara obuhvata samo osnovnu procesorsku jedinicu ili, pored nje, i sve periferne uređaje i uređaje za skladištenje podataka.

Pored ovoga, teško je ustanoviti koji još oblici savremenih računarskih sistema mogu biti uključeni u pojam računara (palmtop uređaji, mobilni telefoni najnovije generacije koji koriste operativne sisteme i podržavaju iste oblike komunikacije i prenosa podataka kao i računari).

Na osnovu stanja pozitivnog zakonodavstva u Republici Srbiji, a imajući u vidu činjenicu da je visokotehnološki kriminal novi pojavni oblik kriminaliteta, možemo da konstatujemo da je država preduzela značajan i odlučan korak u pravcu konstituisanja specijalizovanih organa, kao i usvajanja odgovarajućih pravnih propisa, prevashodno materijalne prirode, koji predstavljaju osnov za efikasno krivično gonjenje počinilaca krivičnih dela sa područja visokotehnološkog kriminala[387].

---

[385] Zakon o posebnim ovlašćenjima radi zaštite prava intelektualne svojine, *Službeni glasnik RS,* broj 46/06, 104/2009.

[386] Skrlec B., Grecke M., „Usklađenost KZ i ZKP Republike Srbije sa zahtevima Konvencije Saveta Evrope o visokotehnološkom kriminalu", *Expert report,* Council of Europe, October 2007.

[387] Žaklina Spalević, „Krivična odgovornost pravnih i fizičkih lica na polju elektronskih komunikacija i elektronske uprave prouzrokovana cyber kriminalom", Opus citatum, str. 226.

S druge strane, neophodno je veoma ozbiljno analizirati primedbe i preporuke koje dolaze od stručnih lica angažovanih na poslovima otkrivanja i gonjenja cyber kriminala i izvršiti korekciju i dopunu materijalnog i procesnog zakonodavstva, koja bi omogućila postizanje optimalnih rezultata u borbi protiv sveprisutnijeg cyber kriminaliteta.

6.4.6 Kazneno pravno zakonodavstvo cyber kriminala u bivšim Jugoslovenskim republikama

Prema mišljenju većine stručnjaka, promene u pravnom poretku trebaju biti evolutivne, a ne revolucionarne. Internet je u tehničkom smislu definitivno revolucija, ali u pravnom, a posebno u vezi sa kompjuterskim i cyber kriminalom, reč je ipak o evolutivnoj promeni.

Iz tog razloga ne iznenađuje da se, kada se govori o odgovornosti pružaoca Internet usluga u Hrvatskoj, ista razmatra u okviru propisa generalne prirode, kao što je Kazneni zakon iz 1998. godine, sa svojim izmenama i dopunama, te *leges speciales*, u zavisnosti o kojim povredama je reč, Zakon o autorskom pravu i odredbe Zakona o obaveznim odnosima.

Članovi Kaznenog zakona inkriminišu ponašanja kvalifikovana kao krivična dela u članovima 2. do 6. Konvencije o cyber kriminalu. Naime, krivično delo Oštećenje i upotreba tuđih podataka (čl. 223) pokriva krivična dela Neovlašćenog pristupa i Oštećenja, izmene i uništenja podataka, sadržana u čl. 2 i 4. Konvencije.

Što se tiče čl. 3. Konvencije o cyber kriminalu i krivičnog dela Neovlašćeno presretanje podataka (*Illegal Interception*), u teoriji se smatra da iako čl. 223. Kaznenog zakona ne sadrži odredbe o kompjuterskoj špijunaži, postoji dovoljno postojećih inkriminacija kojima se može sankcionisati ovakvo ponašanje u svojim pojavnim oblicima, kao npr. inkriminacije o izdavanju i neovlašćenom pribavljanju poslovne tajne (čl. 295 KZ), odavanju službene tajne (čl. 132 KZ) ili odavanju državne tajne (čl. 144 KZ). Potom, krivično delo Nedozvoljena upotreba ličnih podataka (čl. 133 KZ) pokriva kako prikupljanje, obrađivanje i korišćenje ličnih podataka građana, tako i njihovo korišćenje suprotno zakonom dozvoljenoj svrsi njihovog prikupljanja.

Zatim, i glava krivičnih dela protiv imovine dopunjena je inkriminacijama koje, takođe, mogu poslužiti za sankcionisanje nekih zloupotreba Interneta. Tako su tu navedena kao inkriminacije sledeća dela:

- Povreda prava autora ili umetnika izvođača;
- Neovlašćena upotreba autorskog dela ili izvođenja umetnika izvođača;
- Oštećenje i upotreba tuđih podataka.
-

Ovo poslednje krivično delo je posebno interesantno, jer je reč o sasvim novom krivičnom delu kojim se zaštićuju automatski obrađeni podaci ili kompjuterski programi, a inkriminiše se i sam pristup njima pod uslovom da su zaštićeni posebnim merama, odnosno šiframa.

S obzirom da navedene inkriminacije pokrivaju veliki broj zloupotreba Interneta i računara, zakonodavac je mogao i trebao naći mesta i za sankcionisanje delovanja malicioznih programa, što bi direktno pomoglo i formiranju pravnog okvira za izražavanje odgovornosti proizvođača.[388]

Trebalo se naći mesta i za sankcionisanje neovlašćenog menjanja sadržaja tuđih Web stranica, kao i prezentaciju raznih štetnih sadržaja (dečja pornografija, zabrana veličanja nacističkih i fašističkih ideologija) odredbama koje imaju, recimo, Austrijanci.

Ovakav trenutni pravni režim u pogledu odgovornosti Internet provajdera smestio bi Hrvatsku, po *Sieber*-ovom tumačenju,[389] u grupu zemalja koje se u nedostatku specifičnih rešenja oslanjaju na svoje opšte krivične norme.

Sieber smatra da je upotreba opšteg sistema krivičnih normi i građanskopravnih normi dobro *vatrogasno* rešenje, ali da će načelo pravne sigurnosti, vremenom, ipak uticati na donošenje jasnih specijalnih rešenja, budući da je reč o pravno-tehničkoj problematici visoke složenosti koju je bolje zakonom čvrsto definisati nego ostaviti sudovima i opštim propisima. Razmatranja ovog nemačkog stručnjaka u svemu odgovaraju trenutnoj situaciji u Republici Hrvatskoj.

Početkom jula 2003. godine doneta je izmena Kaznenog zakona koja se primenjuje od 1. decembra 2003. godine. Pomenutom izmenom je čl. 223. doživio veliku izmenu, i tada je nosio naziv Povreda tajnosti, celovitosti i dostupnosti računarskih podataka, programa ili sistema i pokrivao, odnosno obuhvatao sve odredbe poglavlja Konvencije o tajnosti, nepovredivosti i dostupnosti podataka sačuvanih na računarima i samih računara. Kažnjiv je i sam pokušaj ovih krivičnih dela.

Ono što je bitno reći jeste da hrvatski pravni sistem prati i analizira promene u pravnim porecima zemalja istovrsnog pravnog okvira.

Pojavni oblici kompjuterskog kriminaliteta u zakonodavstvu Slovenije su koncentrisani u slovenačkom krivičnom zakoniku (*Kazenski zakonik*). Prvim reformama iz 1995. godine, kada je i donet novi Zakon o autorskom pravu, počeo je proces usvajanja kaznenopravnih standarda u kažnjavanju pojavnih oblika kompjuterskog kriminaliteta.

Godine 1999. novom reformom krivičnog sistema u slovenački krivični zakonik je uneto i krivično delo neovlašćenog pristupa kompjuterskom sistemu, kao i krivično delo neovlašćenog menjanja sadržaja, uništenja ili oštećenja podataka.[390]

---

[388] Dragičević D., „Kompjutorski kriminalitet i informacijski sustavi", Opus citatum., str .181 i 186.

[389] Sieber U., "Responsibility of Internet Providers", Opus citatum, pp. 35.

Iste godine izmenjen je i Zakon o autorskom pravu, a time i krivični zakon u koji su sada uključena i krivična dela vezana za povredu autorskog i srodnih prava.[391] Nakon pomenute promene, u krivično-pravni sistem uključena su bila i krivična dela vezana za neovlašćeno korišćenje autorskih dela, kršenje autorskog i drugih srodnih prava (čl. 158-160. *Kazenskog zakonika*). Zanimljivo je da je već tada u čl. 309. bila sankcionisana izrada i upotreba malicioznih programa koji mogu poslužiti za neovlašćeni pristup ili bilo koje drugo krivično delo vezano za upotrebu računara.

Prema nekim podacima, objavljenim u glasilu udruženja (BSA) i našem časopisu *Ekonomist*, Slovenija je, kao i većina ostalih bivših komunističkih zemalja, početkom devedesetih godina imala visoku stopu piratstva, negde oko 90%.[392] Očigledno je da su doneti propisi postigli svoju svrhu, budući da prema izveštaju BSA za 2001. godinu Slovenija ima manje od 60% nelegalnog softvera, dok veliki deo tog broja otpada na takozvano *meko piratstvo*, odnosno na korišćenje službenih licenci na većem broju računara od dopuštenog.

U ovom trenutku, Slovenija ispunjava gotovo sve zahteve Konvencije o cyber kriminalu. Ono što je još preostalo ispuniti su krivično-pravno sankcionisanje krivičnih dela usmerenih na ometanje normalnog rada kompjuterskih sistema i neovlašćeno presretanje podataka.

Državna agencija za istrage i zaštitu (SIPA) i ostale institucije u BiH nemaju mogućnost da se bore protiv Internet kriminala koji se javlja u vidu dečje pornografije ili krađe ličnih podataka. Situacija nije bolja ni kada je reč o entitetima i ministarstvima unutrašnjih poslova.

BiH je potpisnica Međunarodne konvencije o cyber kriminalu. Međutim, do sada u Krivični zakon BiH nisu ugrađena određena krivična dela koja se odnose na cyber kriminalitet, a koja su definisana Konvencijom, što ukazuje na neophodnost da se u Krivičnom zakonu BiH donese amandman u vezi sa cyber kriminalitetom.

U okviru Ministarstva unutrašnjih poslova Republike Srpske 2009. godine je formirano Odeljenje za visokotehnološki kriminal. Odeljenje radi na otkrivanju širenja verske i nacionalne mržnje posredstvom Interneta i zloupotreba platnih kartica, a za svaki slučaj koji ima elemente krivičnog dela ovo odeljenje predaje izveštaj tužilaštvu. Pomenuto odeljenje ima *uspešne* metode da locira i pronađe kreatore uvredljivih sadržaja, ali i posetioce istih. Međutim, ukoliko neko slučajno na Internetu pristupi serveru s dečjom pornografijom neće snositi krivicu, ali ako se *600 puta uloguje na taj server i snima sadržaj istog* postoje svi preduslovi da bude krivično gonjen. Ono što se, svakako, smatra bitnim jeste da policija može otkriti svaku osobu koja zloupotrebljava Internet, cyber kriminalca koji krade identitete da bi pljačkao bankovne račune, pedofile, kao i komentatore na forumima koji ostavljaju preteće poruke. Međutim, da bi policija mogla ući u trag svakom kriminalcu veoma je važno da cyber kriminal, odnosno hakerski upad bude prijavljen u najkraćem mogućem roku.

---

[390] Register predpisov Slovenije, *Ur.list RS,* št. 23/99, član 225.

[391] Dostupno na: *http://www.aas.si/pravni-viri/kzrs-fr1.htm*; datum pregleda: 12.10.2011.

[392] Dostupno na: *http://www.ekonomist.co.yu/magazin/ebit/12/por/slovenc.htm*; datum pregleda: 12.10.2011.

Pomenuto odeljenje za visokotehnološki kriminal u okviru Ministarstva unutrašnjih poslova Republike Srpske, pored svih oblika kriminala na tzv. cyber prostoru, odnosno Internetu, pokriva i zloupotrebe iz oblasti telekomunikacija, a bavi se i digitalnom forenzikom. Posebno bitnim smatra se podatak da je MUP Republike Srpske dostavio svoj predlog izmene Krivičnog zakona Ministarstvu pravde Republike Srpske. Od ishoda ovih izmena zavisiće odnos pravosudnog sistema prema delima cyber kriminala.

7
Opasnost upotrebe cyber prostora od strane mladih

Činjenica je da živimo u modernom informacionom dobu, u kome su računari i računarske komponente svima dostupni, pokazuje da su postali moćan alat koji je u stalnoj upotrebi u izvođenju kriminalnih aktivnosti. Kompjuter kao sredstvo koje obezbeđuje dostupnost i razmenu informacija u neslućenom obimu zauzeo je značajno mesto u gotovo svim sferama života savremenog čoveka, tako da bi bilo veoma teško uopšte pokušati da se na jednom mestu predstave sve njegove funkcije i načini na koje je izvršio uticaj na promenu života ljudi poslednjih decenija. Prema istraživanjima broj internet korisnika na kraju 2017. godine iznosio je 4,156,932,140. Ukoliko se ovaj podatak uporedi sa podatkom da je 2011. godine broj internet korisnika iznosio oko milijadru i po, uviđa se veliki rast. Najveći broj internet korisnika prisutan je na području Azije, što se može videti iz Tabele 5[393].

Tabela 5. Svetska upotreba interneta i populaciona statistika na dan 31.12.2017.

Regioni	Populacija (2018 Est.)	Internet korisnici 31 Dec 2017.	Penetration Rate (% Pop.)	Rast od 2000-2018	Internet korisnici %
Afrika	1,287,914,329	453,329,534	35.2 %	9,941 %	10.9 %
Azia	4,207,588,157	2,023,630,194	48.1 %	1,670 %	48.7 %
Evropa	827,650,849	704,833,752	85.2 %	570 %	17.0 %
Latinska Amerika/ Karibi	652,047,996	437,001,277	67.0 %	2,318 %	10.5 %
Bliski istok	254,438,981	164,037,259	64.5 %	4,893 %	3.9 %
Severna Amerika	363,844,662	345,660,847	95.0 %	219 %	8.3 %
Okeanija/ Australia	41,273,454	28,439,277	68.9 %	273 %	0.7 %
Svet Ukupno	7,634,758,428	4,156,932,140	54.4 %	1,052 %	100%

Od ukupnog broja internet korisnika na celom svetu broj internet korisnika u top 20 zemalja po broju internet korisnika iznosi 2,937,139,302, za šta se slobodno može reći da predstavlja više od polovine. U ovoj grupi zemalja Kina se izdvaja na prvom mestu sa 772,000,000 i rastom broja korisnika od 3,331% u periodu od 2000-2018. godine.

[393]World Internet Users and 2018 Population Stats (2018), Available at: https:// www.internetworldstats.com/stats.htm, date: 05.03.2018.

Nakon nje slede India, SAD, Brazil itd, dok je prva od zemalja Evropske Unije na ovoj listi Nemačka sa 79,127,551 internet korisnika i rastom od 229% u odnosu na 2000. godinu. Zanimljiv je podatak da od ukupnog broja internet korisnika u Kini broj korisnika koji koriste popularnu društvenu mrežu Facebook iznosi 1,800,000, dok u Nemačkoj ovaj broj iznosi 31,000,000.

Ukoliko se uporedi broj internet korisnika i broj korisnika facebook društvene mreže na prostorima bivših Jugoslovenskih Republika dobija se podatak da je najveći broj internet korinsnika kao i korisnika facebook društvene mreže u Srbiji, što se može videti u Tabeli 6.

Tabela 6. Broj Internet korisnika i Facebook korisnika na prostoru bivših Jugoslovenskih Republika u 2017. godini

Država	Broj Internet korisnika	Stopa penetracije %	Broj Facebook korisnika	Stopa penetracije %
Bosna i Hercegovina	2,628,846	69,3%	1,500,000	39,5%
Makedonija	1,503,315	72,2%	1,000,000	48,0%
Crna Gora	437,624	69,9%	320,000	51,1%
Srbija	5,885,816	67,1 %	3,400,000	38,7%
Slovenia	1,563,795	75,5%	910,000	43,9%
Hrvatska	3,133,485	74,4%	1,800,000	42,8%

Broj korisnika društvene mreže Facebook u Srbiji ne bi trebalo mešati sa stvarnim brojem korisnika sajtova za društveno umrežavanje koji je svakako manji, ali ipak govori da je ovaj fenomen široko rasprostranjen među domaćim korisnicima Interneta. Porast broja facebook korisnika u Srbiji između 2015 godine i 2018 godine bio je za gotovo milion. Ukoliko se uporedi broj internet korisnika i broj korisnika Facebook društvene mreže u Kini kao zemlji sa najvećim broj internet korisnika i zemljama pripadnicama bivših Jugoslovenskih Republika može se zaključiti da je ukupan broj internet korisnika u ovim zemljama daleko manji od broja internet korisnika Kine, dok samo Hrvatska ima isti broj Facebook korisnika kao Kina. Ovaj podataka pokazuje da je ova društvena mreža daleko popularnika na našim prostorima nego što se to slučaj sa prostorom Narodne Republike Kine.

Predmet mnogobrojnih istraživanja, diskusija i preporuka, kako šire javnosti tako i naučnika, vladinih i nevladinih organizacija, jeste problem zaštite privatnosti na sajtovima za društveno umrežavanje. Razlog ovako velike zainteresovanosti u cilju rešavanja ovog problema počiva na činjenici da se svakoga dana broj korisnika

društvenih mreža rapidno povećava[394]. Veliki broj njih gotovo da ne posvećuje pažnju bezbednosti informacija i podataka koje o sebi ostavljaju na ovakvim servisima. Ono što zabrinjava je da informacije koje se čuvaju na sajtovima za društveno umrežavanje mogu zauvek ostati tamo. Na ovakav način one su dostupne pojedincima različitih profila, zainteresovanim grupama i organizacijma. Način rada interneta i društvenih mreža organizovan je tako da informacija koja je jednom objavljena postaje u delićima vremena dostupna svima. Poseban problem jeste objavljivanje osetljivih podataka kao što je adresa stanovanja, fotografije sa porodicom i prijateljima, broj telefona, email adresa i slično.

Visokotehnološki kriminal karakteriše socijalni inženjering, navođenje ljudi aktivnom manipulacijom na odavanje podataka o sebi. Primera radi, *Gross* i *Acquisti* u svom istraživanju pokazuju da čak 82% aktivnih korisnika *Facebook*-a otkrivaju poverljive informacije o sebi kao što su datum rođenja, broj mobilnog telefona, adresu, političku i seksualnu orijentaciju i ime partnera. Do sličnih rezultata dolaze *Young* i *Quan-Hasse* istražujući ponašanje studenata u Kanadi. Rezultati pokazuju da neverovatnih 99,35% studenata koristi pravo ime u svojim profilima, 97,4% navodi ime škole koju su pohađali, 92,2% datum rođenja, 83,1% *e-mail* adresu, 80% ime grada u kome žive. Pored ovoga, gotovo svi studenti na profil postavljaju svoje slike (98,7%) i slike svojih prijatelja (96,1%). Ipak, studenti su nešto oprezniji kada je u pitanju davanje prave adrese (to čini samo 7,9%) ili broja mobilnog telefona (10,5%).

Ovako velika iskrenost korisnika sajtova za društveno umrežavanje se podstiče i od strane pružalaca ovih usluga koji ohrabruju objavljivanje ličnih podataka stvarajući iluziju njihove potpune bezbednosti. Da situacija nije baš toliko bezazlena, kao što to verovatno misli većina korisnika sajtova za društveno umrežavanje, svedoče brojne analize, vodiči i preporuke sa ciljem da se što bolje uredi ova oblast društvenog delovanja. Ali više od svega, o mogućnosti zloupotrebe podataka svedoče i konkretne sumnje, peticije javnosti, pa čak i tužbe protiv najpopularnijeg sajta za društveno umrežavanje, *Facebook*-a.

Prva velika rasprava na temu manipulacije ličnim podacima korisnika *Facebook*-a desila se nakon uvođenja kontraverznog sistema za reklamiranje pod nazivom *Beacon.* Uvedena u novembru 2007. godine, ova usluga bila je podešena tako da snima aktivnost svih *Facebook*-ovih korisnika na Internetu (kupovanje, prijavljivanje za različite usluge, itd.) i zatim te informacije prosleđuje listi prijatelja iz profila te osobe. Ideja je bila da se, preporučujući prijateljima usluge i proizvode koje koriste njihovi prijatelji, kompanije reklamiraju na jedan ličniji, personalizovaniji način. Nakon tužbe i pod pritiskom žalbi korisnika, samo dva meseca kasnije, *Beacon* usluga uz izvinjenje osnivača *Zuckerberg Mark*-a postaje opciona, da bi u septembru 2009. godine bilo objavljeno da će se u potpunosti ukinuti.

[394] Žaklina Spalević, Milan Počuča, Željko Bjelajac, Terrorist Activities and Internet Government with Focus on Importance of Prevention within a Family, TTEM - Technics Technologies Education Management, Vol. 8, No. 1, pp. 195 - 203, Mar, 2013.

Tokom 2009. godine *Facebook* je još dva puta bio predmet široke diskusije i pritužbi javnosti. Novu kontroverzu, februara 2009. godine, izazvala je najava od strane *Facebook*-a da će doći do izmene njihove politike vezane za privatnost podataka. Ono čime je ova najava posebno uzbudila javnost bio je jedan pasus čija se suština svodi na to da *Facebook* zadržava pravo na posedovanje ličnih podatka korisnika, čak i u slučaju da korisnik deaktivira svoj profil i obriše podatke sa njega. Međutim, nakon brojnih protesta i široke kampanje širom sveta i pretnje tužbom, kreatori *Facebook*-a su još jednom bili primorani da odustanu od nameravanih promena.

Mnogo ozbiljnije posledice po pitanje *Facebook*-ove politike privatnosti izazvala je tužba jedne kanadske nevladine organizacije koja se bavi politikom Interneta i javnim interesom (*Canadian Internet Policy and Public Interest Clinic* – CIPPIC) upućena Kancelariji poverenika za privatnost informacija Kanade (*Office of the Privacy Commissioner* – OPC). Ova organizacija iznela je pritužbe na politiku privatnosti podataka korisnika *Facebook*-a na više nivoa, od pritužbe na neovlašćeno prikupljanje podataka o rođenju korisnika do pritužbe na neovlašćeno davanje ličnih podataka korisnika trećim licima u svrhu reklamiranja. Kao odgovor na tužbu OPC je napravila više izveštaja i tokom marta 2009. godine dala je *Facebook*-u 20 preporuka vezanih za uklanjanje uočenih nepravilnosti vezanih za politiku privatnosti njihovih korisnika. Kao rezultat ovoga, *Facebook* je korigovao jedan deo svoje politike privatnosti koji se odnosi na *default*-no, odnosno standardno podešavanje sigurnosnih mehanizama na profilu, kao i u domenu oglašavanja, ali važan deo pritužbi koji se tiču aplikacija trećih lica, deaktivacije i brisanja profila, profila preminulih korisnika i ličnih informacija ne-korisnika, do danas je ostao nerešen.

Upravo su navedeni problemi stvorili potrebu za usvajanjem određenih standarda kada je u pitanju privatnost podataka korisnika sajtova za društveno umrežavanje. Jednu od najsadržajnijih analiza ove problematike sačinila je Evropska agencija za bezbednost mreže i informacija (*European Network and Information Security Agency* – ENISA). U izveštaju *Problemi bezbednosti i preporuke za online društvene mreže* iz 2007. godine potencijalne pretnje podeljenje su u sledeće kategorije:

- Pretnje po privatnost
- Tradicionalne opasnosti po mreže i bezbednost informacija
- Pretnje po identitet
- Drštvene pretnje

Na osnovu identifikovanih potencijalnih pretnji ista organizacija dala je i određene smernice u cilju povećanja bezbednosti kako samih korisnika interneta tako i njihovih podataka. Pomenute smernice podeljenje su u četiri grupe sa u zavisnosti od nivoa primene:

- Preporuke u oblasti vladinih regulatornih politika
- Preporuke za internet provajdere u domenu njihove poslovne politike
- Tehničke preporuke
- Preporuke u oblasi istraživanja i standardizacije.

Da ovo nije jedina organizacija koja se bavi problemima društvenog umrežavanja govori i podatak da je *Međunarodna radna grupa za zaštitu podataka u telekomunikacijama*, takozvana Berlinska grupa, objavila je svoj izveštaj i vodič o zaštiti privatnosti, kako za kreatore sajtova za društveno umrežavanje, tako i za same korisnike ovih aplikacija. U ovom izveštaju, poznatijem pod nazivom Rimski memorandum, posebno se ističu rizici po privatnost i bezbednost korisnika sajtova za društveno umrežavanje sa posebnim naglaskom na sledeće pretnje:

- na Internetu nema zaborava-podaci ostaju zauvek sačuvani;
- obmanjujuće poimanje *zajednice* stvara lažnu sliku sigurnosti;
- besplatnost usluge koja se plaća time što se lični podaci kasnije koriste u marketinške svrhe;
- sakupljanje podataka o kretanju na Internetu od strane provajdera usluga umrežavanja;
- rastuće potrebe da se refinansiraju usluge i ostvari profit mogu dalje ohrabrivati prikupljanje, obradu i upotrebu podataka o korisnicima;
- odavanje više ličnih podataka nego što korisnik misli da je dao;
- zloupotreba podataka iz ličnih profila od strane trećih lica;
- rizik krađe identiteta i moguće *otmice* profila od strane neautorizovanih trećih lica;
- upotreba veoma nesigurne infrastrukture;
- uvođenje standarda interoperabilnosti i interfejsa za kreiranje aplikacija (*API, Google*), u cilju tehničkog ujednačavanja različitih društvenih mreža.

Kada je reč o preporukama, treba spomenuti i istraživanje ranije pomenute kanadske nevladine organizacije (*Office of the Privacy Commissioner* – OPC) sprovedeno tokom 2008. godine, koje nakon identifikovanja, manje više, poznatih pretnji na sajtovima za društveno umrežavanje, daje čak 71 preporuku za poboljšanje zaštite privatnosti njihovih korisnika[395].

Treba spomenuti jedno od pionirskih istraživanja na ovu temu koje je sproveo Vlado Popović tokom 2001. godine na preko 1073 ispitanika. Već u ovoj ranoj fazi upotrebe Interneta u našoj zemlji, kako to pokazuju rezultati Popovićeve studije, tadašnji korisnici demonstriraju iznenađujuće veliku spremnost da ostave svoje lične podatke na Internetu. Ovde treba naglasiti da tada nisu postojali sajtovi za društveno umrežavanje, te se njihova otvorenost ne može shvatiti kao izraz neke vrste pomodarstva, već pre kao nepostojanje izražene svesti o potencijalnim opasnostima koje vrebaju na Internetu.

Pa tako, čak 75,7% ispitanika kaže da bi na Internetu ostavili podatke o godini svog rođenja, zanimanju (82,3%), polu (92,1%), itd. Polovina ispitanika je spremna da otkrije ime i prezime i *e-mail,* dok bi čak 22,4% otkrilo i kućnu adresu, a nešto manje i broj telefona (15,2%). Na sve ovo treba dodati i 14% onih koji su spremni da na nekom od sajtova ostave tako poverljiv podatak kao što je to matični broj.

---

[395] Spalević Ž. (2012). *Krivična odgovornost pravnih i fizičkih lica na polju elektronskih komunikacija i elektronske uprave prouzrokovana cyber kriminalom*, str 156

Istraživanje koje se direktno bavilo sajtovima za društveno umrežavanje sprovela je tokom 2008. godine Svetlana Jovanović sa saradnicima, a ticalo se studentske populacije u Srbiji i njihove upotrebe *Facebook*-a i *My Space*-a. Istraživanje je sprovedeno na uzorku od 1664 ispitanika i rezultati do kojih se došlo su slični onima koji se odnose na njihove kolege na Zapadu. Najzanimljivi nalaz je da samo 5% korisnika drži svoj profil sakriven za sve korisnike, dok čak 56% studenata dozvoljava da njihov profil vide svi korisnici *Facebook*-a, bilo da su na listi njihovih prijatelja ili ne. Broj (35%) onih koji na svojim profilima otkrivaju puno ime i prezime, datum rođenja, *e-mail* adresu ili broj telefona nije mali.

Umesto nekadašnjih, tradicionalnih zajednica, u savremeno doba postaje sve opravdanije govoriti o društvenim mrežama. Služeći se definicijom *Barry Wellma*-a možemo dodatno produbiti ovo shvatanje. On zaključuje da su *Zajednice*–mreže interpersonalnih veza koje obezbeđuju društvenost, podršku, informacije, osećaj pripadnosti i društveni identitet. Znači, za razliku od nekadašnjih zajednica koje su bile zasnovane na deljenju vrednosti i društvene organizacije, mreže se grade u vezi sa izborom i strategijama socijalnih aktera, bilo da su u pitanju pojedinci, porodice ili organizacije.

Ono što je takođe važno naglasiti, a tiče se kvaliteta veza koje se ostvaruju među socijlnim akterima je to da *slabe* veze često sa stanovišta aktera mogu imati veći značaj nego što ih imaju *jake* veze. Upravo su one izvor informacija, radnih karakteristika, komunikacije i slobodnog vremena.

Imajući ovakvo određenje društvenih mreža u vidu, ne čudi zašto se Internet, kao mreža svih mreža, savršeno nadovezao na već uspostavljenu mrežnu logiku društvenih odnosa. Internet je pogodan kako za održavanje *jakih* porodičnih, rođačkih ili drugih bliskih odnosa, tako i za sticanje i održavanje *slabih* veza koje bi se njegovim nepostojanjem u manjem ili većem broju prekinule.

Upravo u toj njegovoj karakteristici treba tražiti uslove za nastanak i ogromnu popularnost sajtova za društveno umrežavanje.

Sajtovi za društveno umrežavanje su paradigma današnjeg rizičnog društva. Budući da se na Internet projektuje društvo u svom virtulenom obliku, razumljivo je da se po toj analogiji u virtuelni svet Interneta projektuju i rizici realnog sveta. Međutim, pomenuti rizici po privatnost lica i podataka mogu se smanjiti na nekoliko nivoa.

Masovna upotreba interneta i društvenih mreža od strane mlađe populacije stvorila je prostora za ravoj internet pedofilije. Same pogodnosti cyber prostora nude pedofilima lako praćenje i nadgledanje dece, njihovih aktivnosti, igara koje igraju kao i vrste zabavnih sadržaja koje prate. Takođe cyber prostor nudi i izlaznu strategiju u domenu anonimnosti u slučaju kada je opsanost po dete otkrivena. O ozbiljnosti ovog problema svedoči i činjenica da će jednostavna pretraga reči *sex* na Google-u dati više rezultata pretrage nego ukoliko korisnik pretraži reč enciklopedija. Ovakvi podaci jako su alarmantni kako za samo društvo tako i za roditelje. Posedno se može reći da su podaci alarmatni za roditelje koji nemaju jasno poimanje ovog problema ili nisu svesni koliko je pedofilija u cyber prostoru zastupljena i koje posledice svega toga mogu biti.

Takođe veliki broj roditelja ne ume da prepozna prve oblike napada na svoje dete. Upotreba servisa u cyber prostoru otvorila je mogućnosti za skrivene zamke usmerene protiv pojedinaca, a naročito dece od strane osoba koje zloupotrebljavaju računare kao bi zadovoljile svoje perverzne potrebe. Imajaći sve navedeno u vidu postavlja se logično pitanje gde su deca sigurnija na ulici, u praku, dečijem igralištu ili na internetu? Razvoj računarstva i cyber prostora u mnogome su uticali na porodicu u celini, ostavivši posledice na samu srž poimanja porodice.

Kako je cyber prostor postao sastavni deo naših života, sastavni deo svake porodice može se reći da u velikoj meri zauzima osnovnu ćeliju socijalizacije. Sa aspektom cyber socijalizacije došle su i negativne posledice iste. Kada se u ove negativne posledice impliciraju na decu dolazi do formiranja različitih oblika zloupotrebe dece. Pored već pomenute pedofilije vrlo često se deca iskorišćavaju u domenu prodaje različitih proivoda, ispiranja mozga ili uvlačenja i različite sekte i kultne organizacije[396]. U svim slučajevima počinioci najčešće prilaze deci sa lepim pričama u domenu istog interesovanja kao i sa pokazivanjem velikog razumevanja za njihove „probleme“ ili prepirke. Najčešće pokazuju razumevanje i staju na stranu dece kada su prepirke sa roditeljima i drugovama u pitanju. Kada se radi o seksualnom zloupotrebljavanju počinitelji najpre predtavljaju sebe kao vršnjake potencijalne žrtve, i na taj način uspostavljaju nivo poverenja sa detetom kako bi isto ikoristili i krenuli u domen diskusije o seksu i seksulanim odnosima. U najvećem broju slučajeva dalja komunikacija se zasniva na razmeni fotografija, navođenju deteta na svlačenje ispred web kamere pa sve do ugovaranja vidjenja na nekom unapred odabranom mestu. Fotografije nastale na ovakav način veoma često završe na različitim portali za pedofiliju i internet pornografiju, što u slučaju otkrivanja istih ili njihovog deljenja putem društvenih mreža može ostaviti nesagledive posledice na dete. Ovo je tipična šema pedofilije primenjena u cyber prostoru[397]. Vrlo često fotografije ovako nastale fotografije bivaju iskorišćene i kao domen ucene kako same dece tako i roditelja pogotovu ukoliko se radi o imućnijoj i poznatijoj porodici.

Domen zaštite dece i mladih u cyber prostoru problem je sa kojim se suočavaju kako sami roditelji tako i organizacije, provajderi državne institucije. Poznata je činjenica da se samo društvo ne može osloniti na samokontrolu pojedinaca, pa se samim tim moraju sprovesti edukacioni programi koji će obuhvatiti kako populaciju mlađu od 18 godina, tako i odrasle interenet korisnike, roditelje, obrazovne institucije i organizacije koje se bave sprečavanjem ovakvih vidova kriminalnih aktivnosti. Nedostatak obrazovanja otežava mogućnost realnog sagledavnja problema, u suprotnom, bilo bi opšte prihvaćeno da je sajber prostor postao deo našeg svakodnevnog okruženja, i da je trenutni cyber prostor isti kao biranje između između stvarnih fizičkih okruženja, pri čemu ostaju sve srodne okolnosti i posledice,

[396] Palević M., Spalević Ž, Zloupotreba moći u Cyber prostoru, Zbornik radova "Zloupotreba moći" sa istoimene međunarodne konferencije, Udruženje za međunarodno krivično pravo, Intermex, 18-22 Jun, Tara, Srbija, pp. 326 - 344, 2014

[397] Minić S, Spalević Ž, Abuse of Computer Networks in Cyber Space: The Role of Family in the Modern Information Age, Teme, Vol. 38, No. 1, pp. 417 - 431, Mar, 2014

uključujući ključni problem a to je da se ovakav tip nasilja obično ne zaustavlja ako osoba jednostavno napusti okruženje, kao što je to slučaj sa fizičkim okruženjem.

Koliko je uloga roditelja značajna u zaštiti dece u cyber prostoro govori i podatak da su edukacioni kursevi i treninzi u najvećoj meri baš posvećeni roditeljima. Ne postoji bolja zaštita deteta i bolji način za njegovo usmeravanja u domenu korišćenja interneta nego što su to roditelji. Pravilna edukacija roditelja omogućava roditeljima potrebna saznanja kako da svoju decu bezbedno uvedu u digitalni svet i kako da im pomognu da prepoznaju i izbegnu neprijatna istustva koja cyber prostor sadrži. U skladu sa ovim stručnjaci su definisali određene sugestije predodređene roditeljima u cilju adekvatnog usmeravanja dece. Neke od sugestija pobrojane su u nastavku:

- Prva od sugestija odnosi se na kreiranje sigurnog profila svog deteta. Ovo podrazumeva zaštitu ličnih podataka iz ugla pravilnog odabira podataka koji će biti sadržane u informacijama o detetu.
- Učenje deteta u značaju korišćenja neutračne email adrese i korisničkog imena. Praktično email adresa ili korisničko ime kreirani za potrebe društvenih mreža recimo ne treba da otkrivaju ime i prezime deteta kao niti bilo šta što se može dovesti u vezu sa istim.
- Pristupne šifre uvek trebaju biti čuvane na sigurnom mestu.
- Deca trebaju biti naučena da otvaraju i odgovaraju na poruke pristigle samo od ljudi koji su im poznati iz okruženja van interneta.
- Detetu se mora pokazati kako da štiti i svoju privatnost, ali u isto vremene kao i da poštuje privatnost drugih.
- Detetu se mora pomoći da razlikuje tipove poruka koje mu mogu pristići od onih koje mogu biti napadne do poruka koje mogu izazvati neprijatna osećanja.
- Potrebno je da se roditelji socijalizuju sa ljudima iz dečije okoline, kako da drugarima svoje dece tako i sa njihovim roditeljima. Na ovakav način znatno brže se uočavaju potencijalni problemi kao i izmene u ponašanju deteta.
- Potrebno je objasniti detetu da ukoliko ga neko povredi to nije njegova krvica i da je potrebno da sa roditeljima otvoreno priča o tome.
- Potrebno je obučiti dete kako da koristi antivirusne programe i kako da proveri sigurnost podataka koje prebacuje ili kopira korišćenjem antivirusa.
- Kada se radi o korisničkim nalozima dobra praksa je da roditelji na računaru kreiraju korisnički nalog za svoje dete predefinisanim privilegijama u cilju što adekvatnijeg praćenja sadržaja koje dece prate.
- Možda najvažnija sugestija u svemu jeste razvijati odnos sa detetom tako da dete u roditelju vidi podršku i da o svim potencijalnim problemima priča sa njim, kao i da ga informiše o svemu čudnom što uoči kako u cyber prostoru tako i u realnom okruženju.

Pored roditelja velika uloga je i na provajderima cyber sadržaja. Provajderi usluga društvenog umrežavanja treba, takođe, pored želje za sticanjem profita, da misle i na one koji im taj profit posredno donose, odnosno na svoje korisnike. Ukoliko se mehanizmi za zaštitu ličnih podataka ne podignu na nivo zaista bezbednog boravka na sajtovima za društveno umrežavanje, korisnici će početi da traže alternativne načine za njihovo umrežavanje.

Ono što se već sada može uraditi jeste podizanje svesti korisnika sajtova za društveno umrežavanje, ali ne kroz pozive na bojkot sajtova za društveno umrežavanje, jer ti pozivi neće dati rezultata, već kroz stalno promovisanje lične brige o podacima koji se daju drugima na raspolaganje u onoj meri u kojoj se pojedinac brine da ne izgubi ličnu kartu ili svoj mobilni telefon.

Kada korisnici budu razumeli da su lični podaci koje ostavljaju u virtulenom prostoru Interneta vrlo realni i da se konsekvence njihove zloupotrebe mogu odraziti na njihove stvarne, a ne virtulene profile, biće daleko oprezniji po pitanju kome te podatke mogu poveriti na čuvanje, a kome ne.

8
Zaključak

Razvoj informaciono komunikacionih tehnologija i Interneta u celom svetu doveli su do krucijalnih izmena u načinu i brzini komunikacije. Sami uticaj ovakvog napretka može se videti u svim sferama društvenog života i rada ljudi. Ne može se a ne prepoznati činjenica da su naučna i tehnička dostignuća u ovoj oblasti stvorila i određeni broj problema. Problemi u oblasti primene informaciono kounikacionih tehnologija ogledaju se u primeni ovih tehnologija sa ciljem širenja različitih oblika visokotehnološkog kriminala. Kao što se u prethodnim poglavljima može videti pojam kompjuterskog ili visokotehnološkog kriminala može se tumačiti kao relativno novi oblik kriminalnog ponašanja. Kao sveobuhvatan pojam koji obuhvata sve ilegalne aktivnosti izvedene u ili upotrebom cyber prostora pojavio se pojam cyber kriminala. O ozbiljnosti pojave sve većeg broja kriminalnih aktivnosti u sajber prostoru svedoči i veliki broj studija koje se bave ovim problemom. Činjenica je da nekontrolisana i besciljna upotreba interneta prouzrokuje brojne opasnosti.

Zloupotreba interneta je često u direktnoj vezi sa krešenjem prava intelektualne svojine i autorskih prava, krađom ličnih podataka, napadom na web portale različitih organizacija i pojedinaca kao i pornografijom. Veliki broj servisa u cyber okruženju inicijalno definisan na zdravim osnovama kao način unapređenja poslovnog procesa ili komunikacije na daljinu iskorišćen je u domeu kriminalnih aktivnsti i narušavanja sigurnosti i stabilnosti kako pojedinaca tako i globalnog svetskog poretka. Evidentirani primeri zloupotrebe cyber prostora prikazani u ovom radu pokazuju da u današnje vreme gotovo da ne postoji oblast ljudskog interesovanja vezana za cyber prostor koja nije na neki način narušena i zloupotrebljena. Koliki je procenat zloupotrebe ili napada na neki konkretan servis ili oblast cyber prostora evidentiran zavisi kako od toga koliko je sama oblast atraktivna za cyber krminalce, kao i od toga koliko su cyber krimnalni vešti u prikrivanju svojih aktivnosti i ostvarivanju apsolutne anonimnosti. Ponekad posmatrano iz ugla žrtve stiče se utisak da službe za borbu protiv visokotehnološkog kriminala ni malo ne rade svoj posao, jer počinioci nikada ne budu otkriveni. Međutim žrtva nije upoznata sa kompleksnošću otkrivanja počinioca u cyber prostoru. Sami problem otkrivanja cyber krimnalaca pored metoda skrivenosti koje koriste uzrokovan je neadekvatnim ponašanjem i stepenom zaštite same žrtve.

Drugi problem koji se javlja jeste procesuiranje počinioca.Veoma često zbog globalnih razmera koje internet i cyber prostor zauzimaju jako je teško procesuirati osobu koja je nanela štetu korisnicima jedne države dejstvujući sa teritorije druge putem servisa ili posrednika hostovanih na teritoriji treće države. Pravne regulaive koje pokrivaju ovu oblast obično se definišu nakon što se konkretni slučajevi zloupotrebe evidentiraju. Takođe same regulative se definišu najpre na nacionalnom nivou, a tek kasnije se usklađuju sa međunarodnim normama i konvencijama. Takođe u slučajevima pravnog spora kako u domenu procesuiranja cyber kriminala, tako i domenu rešavanja sporova nastalih između kompanija ili pojedinaca potpisnika elektronskih ugovora i dokumenata veoma često se tešto utvrđuje nadležno sudstvo.

Pored adekvatne edukacije, i angažovanosti obrazovnih unstitucija, sudstva, internet provajdera i službi za bezbednost cyber prostora veoma je bitna svest korisnika o tome da sami moraju brinuti o svojoj zaštiti u cyber prostoru. Ukoliko sami korisnici ne vode računa o sadržaju koji posećuju, načinu na koji čuvaju i dele lične podatke, kao i o

sigunosti i pouzdanosti servisa koje koriste, svi napori institucija mogu samo donekle ublažiti potencijalni napad ali ga ne mogu izbeći. Ukolko se neadekvatno ponašanje korisnika u cyber prostoru posmatra iz domena pomenutih phishing napada koji su ustaljena šema za napade već godinama prosto zabrinjava činjenica da još uvek postoje korisnici koji odgovaraju unosom svojih podataka na ove ovakve mejlove.

Kako bi se celokupni cyber prostor kako u domenu weba tako i domenu elektronskih servisa dostupnih građanima, kompanijama i vladi unapredio i približio ostaje ulaganje napora kako IT stručnjaka, zakonodavstva, tako i ljudi u obrazovnom sistemu. Ovo praktično znači da pravni sektor treba da prati ili prednjači u donošenju zakonskih regulativa koje prate razvoj informaciono komunikacionih tehnologija. Ljudi u domenu softverske industrije trebaju da rada na kreiranju bezbednijeg softvera koji će biti intuitivan za upotrebu kako bi korisnicima različitog nivo paznavanja računarske intustrije omogućili korišćenje istorg. Na kraju obrazovni sistem zemlja koje žele povećanje broja edukovanih korisnika elektronskih servisa i cyber prostora trebalo bi da se menja i priagođava upotrebi ovih servisa od domena osnovnog obrazovanja pa sve do visokog. Neprihvatljiva je činjenica završetka osnovne i srednje škole a posebno fakulteta bez adekvatnog stečenog znanja iz domena informaciono komunikacionih tehnologija.

9
Literatura

Acohido B. (2008). *Meet A-Z: The Computer Hacker behind a Cybercrime Wave.* Available on: http://usatoday30.usatoday.com/tech/news/computersecurity/2008-08-04-hacker-cybercrime-zeus-identity-theft_N.htm , date: 19.3.2017.

Agencija za informaciono društvo Republike Srpske, Dostupno na: https://www.aidrs.org/sr/aidrs/aidrsca/opste-informacije/, datum pregleda: 20.01.2018.

*Autorsko i srodna prav*a, Dostupno na: http://www.kombeg.org.rs/aktivnosti/c_privprav/Detaljnije.aspx?veza=13054, datum pregleda 05.12.2017.

Baker D. (2015). Tourism and Terrorism: Terrorists Threats to Commercial Aviation Safety & Security, *International Journal of Safety and Security in Tourism/Hospitality*, 1(2), pp. 1-19.

Baldor C.L. (2010). Computer Attack, Linked to Wealthy Group or Nation, Available at: http://www.sandiegouniontribune.com/sdut-computer-attacks-linked-to-wealthy-group-or-nation-2010sep26-story.html, date: 02.02.2018.

Banerjee K., Rana M., Mahfuz M. & Khan A. (2011). Mobile Banking and Payment System Using Bluetooth Media. *International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS*, 11(5), 1-8.

Banim J. (2018). *Cryptocurrency Trading Stopped After World's Largest Crypto Theft*. Available at: https://www.unilad.co.uk/news/cryptocurrency-trading-stopped-after-worlds-largest-crypto-theft/, date: 27.01.2018

Barton M, (2012). *The scram tether, How it works and how it doesn't"*, Available at: http://michigancriminalattorney.com/scram-tether-works/, date: 05.02.2018.

Basu S. (2010). *10 Package Tracking Websites for Alternative Ways to Track Your Shipments.* Available at: https://www.makeuseof.com/tag/10-package-tracking-websites-alternative-ways-track-shipments/, date: 26.12.2015.

BBC. (2012). *Acta: Controversial anti-piracy agreement rejected by EU*. Available at: http://www.bbc.com/news/technology-18704192, date: 10.12.2017

BBC, (2014). *Child abuse image investigation leads to 660 arrests*. BBC News, Available at: www.bbc.com/news/uk-28326128, date: 15.02.2018.

BBC. (2015). *50 arrests in NI online abuse images probe in past year, say police*. BBC News, Available at: www.bbc.com/news/uk-northern-ireland-31896685, date: 15.02.2018.

Beagle T. (2010). *Acta – The NZ Official Information Requests*. Available at: http://techliberty.org.nz/acta-the-nz-official-information-requests/, date: 12.12.2017.

Bellis M. (1998). *The History of Voting Machines*. Available on: http://theinventors.org/library/weekly/aa111300b.htm, date: 21.12.2018.

Bendon G. & Hundson S. (2010). *Our mobile future: how smartphones will transform visiting experiences*. London: Horizon Digital Economy Research.

Beta. (2017). *Vlada: Elektronska faktura validna bez pečata i pot*pisa. Dostupno na: http://rs.n1info.com/a349053/Vesti/Vesti/Vlada-Srbije-Elektronska-faktura-validna-bez-pecata-i-potpisa-stampanje-nije-obavezno.html, datum predlega: 22.12.2017.

Bettinger T. & Waddell A. (2005). *Domain Name Law and Practice- An International Handbook*. London: Oxford University Press.

Bisson D. (2016). *The 5 Most Significant DDoS Attacks of 2016.* The State Of Security, Available at: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/5-significant-ddos-attacks-2016, date: 18.02.2018.

Bodi A. (2015). *Monitoring for Life: Satellite Surveillance of Ex-Offender.* Available at: http://www.americancriminallawreview.com/aclr-online/monitoring-life-satellite-surveillance-ex-offenders/, date: 05.02.2018.

Boillat P. & Kjaerum M. (2014). *Handbook on European data protection law*. Belgium: European Union Agency for Fundamental Rights.

Bojović B. (2018) „Srpkinja doživela dramu. Poručila sam posteljinu preko interneta. Probudila sam se ofarbanog lica, ceo dan sam iskašljavala boju“, dostupno na: https://www.blic.rs/vesti/ekonomija/srpkinja-dozivela-dramu-porucila-sam-posteljinu-preko-interneta-probudila-sam-se/yn5dp77 datum pregleda: 22.01.2018.

Bonczar T. & Glaze L.E. (1999). *Correctional Populations in the United States 1998*. Washington DC: Bureau of Justice Statistics, US Department of Justice.

Bonnecaze A., Liardet P., Gabillon A. & Blibech K. (2002). Improving Time Stamping Schemes: A Distributed Point of View. *Satoshi Nakamoto Institute*. 1-13.

Bright Planet. (2014). *Clearing up confusion – deep web vs. dark web*. Available at: https://brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/, date: 10.02.2018.

Brock T. (2013). *Two brothers plead guilty to illegally shipping gun parts to Thailand*. Available at: http://q13fox.com/2013/10/22/brothers-plead-guilty-to-illegally-shipping-gun-parts-to-thailand/, date: 10.01.2018.

Bronskill J. (2013). *Criminals using Canada Post to transport illicit goods — including a rocket mlauncher — RCMP report says*. Available at: http://nationalpost.com/news/canada/criminals-using-canada-post-to-transport-illicit-goods-including-a-rocket-launcher-rcmp-report-says, date: 13.01.2018.

Brunazo F., *Computerization of voting in Brazil*. Available at: http://noleakybuckets.org/brasil-history.html, date:12.01.2017.

Brvar B. (1982). Pojavne oblike zlorabe računalnika. *Revija za kriminalistiko in kriminologijo,* 33(2), 92–104.

Bubert I. & Buening M. (2013). *Domain Name Issues - European Jurisdiction", Electronic Commerce Legal Issues Platform, ESPIRIT Project 27028.* Available at: www. qlinks.net/lab991216/trademarks.doc, date: 17.12.2017.

CARNet, (2007). Tor - mreža za anonimnost. *CarNet-Hrvatska akademija i istraživačka mreža*. 1-15.

Cekos in (2017). *Objašnjenje u vezi sa izdavanjem i knjiženjem računa (faktura) u papirnom i elektronskom obliku bez upotrebe pečata i potpisa.* Dostupno na: http://www.cekos.rs/obja%C5%A1njenje-u-vezi-sa-izdavanjem-i-knji%C5%BEenjem-ra%C4%8Duna-faktura-u-papirnom-i-elektronskom-obliku-bez, datum pregleda: 22.12.2017.

Coenen L.T. (2009). *Expert Fraud Investigation: A Step-by-Step Guide*. Hoboken, New Jersey: John Wiley & Sons, Inc.

Commision Regulation (EC) No. 733/2002 of the European Parlament and of the Council of 22 April 2002 on the implementation of the .eu Top Level Domain (Official Journal of the European Communities L 113/1).

Commision Regulation (EC) No. 1654/2005 of 10 October 2005 amending Regulation (EC) No 874/2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration (Official Journal of the European Union L 266/35)

Commision Regulation (EC) No. 1255/2007 of 25 October 2007 amending Commission Regulation (EC) No 874/2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration (Official Journal of the European Union L 282/16)

Commision Regulation (EC) No. 560/2009 of 26 June 2009, amending Regulation (EC) No 874/2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration (Official Journal of the European Union L 166/03).

Corredera D. (2015). *Measuring postal e-services development.* Berne: Universal Postal Union.

Creative Commons. (2017). „O licencama", dostupno na: https://creativecommons.org/licenses/?lang=hr, datum pregleda: 05.12.2017.

Čekerevac Z., Dvorak D., & Čekerevac P. (2016). Da li je „tamni internet" dubok i taman? *FBIM Transactions*, 1-12.

Charles A. (2009). *SkyGrabber: the $26 software used by insurgents to hack into US drones*. Available at: http://www.guardian.co.uk/technology/2009/dec/17/skygrabber-software-drones-hacked, date: 08.02.2018.

Ciancaglini V., Balduzzi M., McArdle R., & Rosler M (2015). Below the Surface: Exploring the Deep Web. *Trend Labs - The Global Technical Support and R&D Center of Trend Micro*.

Clayton M. (2010). *Stuxnet malware is 'weapon' out to destroy…Iran'Bushehr nuclear plant?* Available at: https://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant, date: 03.02.2018

Consumers and Mobile Financial Services. (2016). Washington, DC: Board of Governors of the Federal Reserve System.

Cook J. (2014). *FBI Arrests Former SpaceX Employee, Alleging He Ran The 'Deep Web' Drug Marketplace Silk Road 2.0*. Available at: https://www.businessinsider.com.au/fbi-silk-road-seized-arrests-2014-11, date: 11.02.2018.

Counter, P. (2014). *The Biometric Upgrade: SRI International Introduces IOM PassPort SL*. Available at: http://findbiometrics.com/thebiometric-upgrade-sri-international-introducesiom-passport-sl/, date: 10.12.2017.

Court practice – online bulletins, Available at: http://www.sudskapraksa.com/sudske-odluke-presude-pravna-shvatanja.-najveca-baza-sudske-prakse-u-srbiji.html, date: 08.02.2018.

CryptoCurrencyFacts. (2017). *How Does Cryptocurrency work*. Available at: https://cryptocurrencyfacts.com/how-does-cryptocurrency-work-2/, date: 25.01.2018.

Dailey D., Cathey F. & Pumrin S. (2000). An algorithm to estimate mean traffic speed using uncalibrated cameras. *IEEE Transactions on Intelligent Transportation Systems*. 1(2), 97-108.

Daily Sabah Tech. (2017). *France sues e-commerce giant Amazon for abusing marketplace rules.* Available on: https://www.dailysabah.com/technology/2017/12/18/france-sues-e-commerce-giant-amazon-for-abusing-marketplace-rules, date: 22.01.2018.

Damnjanović I. (2009). Elektronska demokratija (E-Democracy) kao mogućnost demokratizacije. *Srpska politička misao.* 1. 85-98.

Defense Science Board Task Force. (2007). Report of the Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software, U.S. Department of Defense, pp. 19.

Department of Homeland Security. (2018). *Enhancing Security Through ‚Biometric Identification*. Available at: https://www.dhs.gov/xlibrary/assets/usvisit/usvisit_edu_biometrics_brochure_english.pdf , date: 12.02.2018.

Deutsch, K. W. (1966). The nerves of government: Models of political communication and control. *System Research and Behavioral Science*. 10(1), 81-83.

Digital Attacks Map. (2013). *What is a DDos attack*. Available at: http://www.digitalattackmap.com/understanding-ddos, date: 18.02.2018.

Directive 97/7/EZ, dostupno na: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31997L0007 datum pristupa: 15.01.2018

Direktiva 2000/31/EZ, dostupno na: http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:32000L0031, datum pristupa: 15.01.2018

Direktiva o elektronskoj trgovini, Directive, 2000/31/EC.

Djekić M.D. (2016). Sajber procedure za poslovno okruženje u Srbiji. *Tehnika*. 71(3). str. 471-474.

Diligenski A. (2014). *Ispitivanje IP-adresa i ugrožavanje privatnosti zbog kršenja autorskih prava gledanjem streaming-a-slučaj Redube*. Dostupno na: http://partners-serbia.org/privatnost/blog/ispitivanje-ip-adresa-i-ugrozavanje-privatnosti-zbog-krsenja-autorskih-prava-gledanjem-streaming-a-slucaj-redtube/, datum pregleda: 07.12.2017.

Доктрина информационной безопасности Российской Федерации, No. Pr-1895, Совет Безопасности Российской Федерации, Available at: http://www.scrf.gov.ru/documents/5.html, date: 03.03.2013.

Dragičević D. (2004). *Kompjuterski kriminalitet i informacijski sustavi*, Zagreb, IBS-Informatorov Biro Sustav.

Društvo za borbu protiv prevara (2008). *Ponzijeva šema (kako su Dafina i Jezda ojadili narod)*. Dustupno na: http://www.prevara.info/index.php?option=com_content&task=view&id=31 datum pregleda: 26.01.2018.

Dusollie S. (2010). *Scoping study on copyright and related rights and the public domain*. Belgium. WIPO.

Election Comission of India, FAQs – Electronic Voting Machine, Available at: http://eci.nic.in/eci/eci.html, date: 10.01.2018.

Embassy of the Bolivarian Republic of Venezuela to the U.S. (2012). *The Venezuelan VENEZUELA'S 2012 PRESIDENTIAL ELECTIONS - A model of transparency and democracy*. Available on: http://venezuela-us.org/live/wp-content/uploads/2009/08/08-31-12-FS-Elections-2012-Long.pdf, date: 12.01.2018.

Emmanuel G.B. (2014). *Europe Proposes New Laws and Regulations on Cybersecurity*. Available at: http://www.jonesday.com/europe-proposes-new-laws-and-regulations-on-cybersecurity-01-02-2014., date: 25.05.2017.

Enigmax. (2009). *The Pirate Bay Trial: Understanding Finreactor*. Available at: https://torrentfreak.com/the-pirate-bay-trial-understanding-finreactor-090223/, date: 05.12.2017.

Ernst & Young. (2013). *Cyber-crime is greatest global threat to organizations' survival today*. Available at: http://www.ey.com/lu/en/newsroom/news-releases/news_20131105_cyber-crime-is-greatest-global-threat-to-organizations-survival-today, date: 26.3.2017.

Esser M. (2011). *Industry Developed Temperature Tracking Device for Packages May Have Climate Metrology Applications*. Available at: https://www.nist.gov/news-events/news/2011/06/nistindustry-developed-temperature-tracking-device-packages-may-have, date: 15.02.2018.

Esteve J., Goldsmith B. & Turner J., (2012). *International Experience with E-Voting*. Washington, DC: International Foundation for Electoral Systems (IFES).

European Commission (2015). *eGovernment & Digital Public Services*. Available at: http://ec.europa.eu/information_society/activities/egovernment/ index_en.html, date: 27.10.2017.

European Council. (2017). VAT on electronic commerce: New rules adopted, Available on: http://www.consilium.europa.eu/en/press/press-releases/2017/12/05/vat-on-electronic-commerce-new-rules-adopted/, date: 20.01.2018.

Europol. (2014). *Operation Rescue*. Available at: www.europol.europa.eu/content/operation-rescue, date: 18.12.2017.

Falconer J. (2012). *Mail-order drugs, hitmen & child porn: A journey into the dark corners of the deep web*. Available at: http://thenextweb.com/insider/2012/10/08/mail-order-drugs-hitmen-child-porn-a-journey-into-the-dark-corners-of-the-deep-web/, date: 15.02.2018.

Federal Election Commision, Punch Card Voting Device, Available on: http://www.fec.gov/pages/punchrd.htm, date: 12.01.2017.

Finkle J. (2014). *Pony botnet steals bitcoins, digital currencies: Trustwave.* Available at: https://www.reuters.com/article/us-bitcoin-security/pony-botnet-steals-bitcoins-digital-currencies-trustwave-idUSBREA1N1JO20140224, date: 26.01.2018.

Frangoul A. (2017), *UK businesses were hit 230,000 times each by cyber-attacks in 2016, says internet service provider*. Available at: http://www.cnbc.com/2017/01/11/uk-businesses-were-hit-230000-times-each-by-cyber-attacks-in-2016-says-internet-service-provider.html, date: 25.05.2017.

Gallagher S. (2012). *The Fast, Fabulous, Allegedly Fraudulent Life of Megaupload's Kim Dotcom.* Available at: https://www.wired.com/2012/01/kim-dotcom/, date: 07.12.2017.

Gavrilović B. (nn). *Osnovni modeli elektronskog poslovanja*. Dostupno na: http://vesti.kombib.rs/osnovni_modeli_elektronskog_poslovanja.html, datum pregleda: 22.12.2017.

Goudie C. & Marcoff B. (2015). *Mailing marijuana: Officials report spike in pot-laden packages*. Available at: http://abc7chicago.com/news/mailing-marijuana-officials-report-spike-in-pot-laden-packages-/1076486/, date: 09.12.2017.

Gorman S., Barnes J. (2011). *Cyber Combat: Act of War*. Available at: http://www.rootsaction.org/news-a-views/108-cyber-combat-act-of-war- , date: 15.02.2018.

Grady v. North Carolina. (n.d.). Oyez. Retrieved 15.01.2018, from https://www.oyez.org/cases/2014/14-593.

Graham J. S. (2002). *Interent Law and Regulation 4th*edt.. London: Sweet & Maxwell.

Grannan C. (unknown). *What's the Difference Between the Deep Web and the Dark Web?*. Available at: https://www.britannica.com/demystified/whats-the-difference-between-the-deep-web-and-the-dark-web. date: 15.02.2018..

Harris H., Perlroth N. & Propper N. (2014). *Neiman Marcus Data Breach Worse Than First Said*. Available: https://www.nytimes.com/2014/01/24/business/neiman-marcus-breach-affected-1-1-million-cards.html?_r=0, date: 22.01.2018.

Helme S. (2014). *Hotel Hipo Insecure, so I've herd*. Available at: https:// scotthelme.co.uk/hotel-hippo-insecure/, date: 15.06.2017.

IDTA. (2002). Illegal Drugs and Trafficking. Annual Report of Investigations, *United States Postal Inspection Service*.

Ilić M. & Spalević Ž. (2016). *Primena elektronskih servisa u turizmu*. International Thematic Monograph - Thematic Proceedings: Modern Management Tools and Economy of Tourism Sector in Present Era, Beograd: Association of Economists and Managers of the Balkans in cooperation with the Faculty of Tourism and Hospitality, Ohrid, Macedonia.

Ilić M., Spalević Ž., Spalević P. & Veinović M. (2016). Mobilno bankartsvo-primena i sigurnost. U: *Zbornik radova 22. naučne i biznis konferencije – YUINFO*. (str. 252-255). Kopaonik, Društvo za informacione sisteme i računarske mreže.

Ilić M., Spalević Ž. & Veinović M. (2015). Elektronsko Bankarstvo – Primena i Sigurnost. In: Procedings of Sinergija University International Scientific Conference, (pp. 113-117). Bijeljina: Sinergija University.

Ilić M., Spalević Ž., Veinović M. & Spalević, Ž. (2016). Electronic services for tourist destination reservations. U: *Zbornik radova 15. Međunarodno naučno-stručnog Simpozijuma INFOTEH*. (str. 621-626). Jahorina: Univerzitet u Istočnom Sarajevu, Elektrotehnički fakultet.

Intellectual Property Code (Legislative Part), Law No 92-597 of 1 July 1992 as last amended by Law No 96- 1106 of 18 December 1996. Available at: http://oami.europa.eu/ genhtm/mark/nl_fr_1_en.htm, date: 15.12.2017.

Johnson T. (1999). Monitoring device trial hailed a success. *Corrective Services Bulletin*, 1(466), 1-6.

Jovičić K. (2014). *Pravna pitanja elektronskih ugovora, s osvrtom na ugovor o prodaji robe*. U: *Međunarodni tematski zbornik radova – Internet i društvo*. (str. 353-363), Niš: Srpsko sociološko društvo Univerzitet u Nišu, Beograd: Filozofski fakultet Institut za uporedno pravo.

Juniper Research. (2015). *Cybercrime Will Cost Businesses Over $2 Trillion by 2019, Finds Juniper Research*. Available at: *www.prnewswire.com/news-releases/cybercrime-will-cost-businesses-over-2-trillion-by-2019-finds-juniper-research-503449791.html*, date: 19.3.2017.

Kalinić Z. & Ranković V. (2014). Razvoj e-uprave na lokalnom nivou – Ocena sadašnjeg stanja i mogućnosti unapređenja. U: *Tematski zbornik: Stanje i perspektive ekonomskog razvoja grada Kragujevca*. (str. 365-383). Kragujevac: Univerzitet u Kragujevcu-Ekonomski fakultet.

Knibbs K. (2014). *Silk Road 3 Is Already Up, But It's Not the Future of Darknet Drugs*. Available at: http://gizmodo.com/silk-road-3-is-already-up-butits-not-the-future-of-da-1655512490, date: 11.02.2018.

Kovach E. (2012), *Site of nato croatia hacked and defaced by teamp0ison*, Softpedia News, Available at: http://news.softpedia.com/news/Site-of-NATO-Croatia-Hacked-and-Defaced-by-TeaMp0isoN-262429.shtml, date: 18.02.2018.

Krebs B. (2012). *Double Cashing With Mobile Banking*. Available at: https://krebsonsecurity.com/2013/06/double-cashing-with-mobile-banking/, date: 15.12. 2017.

Kreca M. & Vaskovic J. (2013). Analysis of the current state of E-government services in Serbia. In: *Proceedings of ITC Conference and Exhibition Infotech*. (str. 1-6). Aranđelovac: Asocijacija za računarstvo, informatiku, telekomunikacije i nove medije Srbije.

Krivični zakonik Republike Francuske.

Krivični zakonik, "Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 i 94/2016.

Крылов В.В. (1997). Информационные компьютерные преступления: Учебное и практическое пособие. – М.: Инфра-М – Норма, 285.

Laronde P. (2012). *Technologies in the Voting process: An Overview of Emerging Trends and Initiatives (Research Note)*. Available at: http://www.elections.ca/content.aspx?section=res&dir=rec/tech/note&document=index&lang=e, date: 18.01.2018.

Laurent M.A. (2004). *Understanding Open Source and Free Software Licensing.* Sebastopol, CA: O'Reilly Media.

Lawrence J. & Tar U. (2010). Barriers to ecommerce in developing countries. *Information, Society and Justice*, 3(1), 23-25.

Lee M, Hornby L. (2010). *Google attack puts spotlight on China's "red" hackers*. Dostupno na: https://www.justice.gov/archive/criminal/_cybercrime/press-releases/2002/_melissaSent.htm, datum pregleda: 15.11.2017.

Leyde J. (2014). *The Guide to E-Commerce Fraud*. Available at: https://www.2checkout.com/upload/documents/ebook_Guide_to_Ecommerce_Fraud.pdf, date: 15.01.2018.

Liang L. (2005). *Guide to Open Content Licenses*. Rotterdam: Piet Zwart Institute e for postgraduate studies and research Willem de Kooning Academy Hogeschool.

Lista prihvaćenih verodajnica Republike Hrvatske, Dostupno na: https://gov.hr/e-gradjani/lista-prihvacenih-vjerodajnica/1667, datum pregleda: 20.01.2018.

Luković M. (2014). *Deep internet - Droga, ubistva, pornografija - šta se sve krije u crnoj web rupi?* Available at: http://www.beforeafter.rs/tehnologija/deep-internet/, date:12.02.2018.

Mali A. (2015). *Electronic Evidence/Digital Evidence & Cyber Law in India*. Available at: https://www.linkedin.com/pulse/electronic-evidence-digital-cyber-law-india-adv-prashant-mali- date: 08.02.2018.

Marković M. (2007). Opšti uvod u pravo intelektualne svojine. *Seminar IS i privreda u Srbiji*.

Matić T. (2008). Formularni ugovori u elektroničkom obliku (Sklapanje ugovora klikom miša - elektroničkim očitovanjem volje putem Interneta na web stranici – click wrap i browse wrap ugovori). U: *Zbornik Pravnog fakulteta u Zagrebu (ur. M. Petrak)*.(str. 779-803). Zagreb: Pravni fakultet Sveučilišta u Zagrebu.

Maunsbach U. (2004). Some Reflexions Concerning Jurisdiction in Cases on Cross-border Trademark Infringements Through the Internet. *Stockholm Institute for Scandianvian Law*, 47, 494-512.

McAfee, Inc. (2014). *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II*. Santa Clara USA: Center for Strategic and International Studies.

McCormick R. (2015). *Megaupload founder Kim Dotcom can be extradited to the US to face copyright charges*. Available at: https://www.theverge.com/2015/12/22/10655646/megaupload-founder-kim-dotcom-can-be-extradited-to-the-us-to-face, date: 05.12.2017.

McMillan R. (2010). *Former Contractor Says FBI Put Back Door in OpenBSD*, Available at: https://www.pcworld.com/article/213751/former_contractor_says_fbi_put_back_door_in_openbsd.html , date: 15.02.2018.

McNub C. (2007). *Network Security Assessement.* Gravenstein Highway North, Sebastopol: O'Reilly Media, Inc.

Mergen L. (2015). *On anonymous networking in Haskell: announcig Tor and I2P for Haskell*. Available at: https://leonmergen.com/on-anonymous-networking-in-haskell-announcing-tor-and-i2p-for-haskell-f1e30f52294f, date: 15.02.2018.

Mihajlović P. (2014). *Bitcoin – Vesnik monetarne revolucije*. Dostupno na: https://startit.rs/bitcoin-vesnik-monetarnerevolucije/?utm_source=google&utm_medium=cpc&utm_content=bitcoin&utm_campaign=blog, datum pregleda: 24.01.2018.

Milatović I. (2015). *Serbia's efforts to respond to cyber security threats.* OSCE, Available at: http://www.osce.org/serbia/170361, date: 18.02.2018.

Milić D. (2017). *Creative commons licenses – licence kreativne zajednice – pojam i vrste*, dostupno na: http://www.milic.rs/blog/autorsko-pravo/164-creative-commons-licenses-licence-kreativne-zajednice-pojam-i-vrste, datum pregleda: 05.12.2017.

Milošević N. (2014). *Case of the cyber war: kosovo conflict.* Inspiration,org, Available at: http://inspiratron.org/blog/2014/07/01/case-cyber-war-kosovo-conflict/, date: 18.02.2018.

Minić S. & Spalević Ž. (2014). Abuse of Cpmputer Networks in Cyber Space: The Role of Family in the Modern Information Age. *Teme*, 38(1), 417 – 431.

Minić S., Spalević Ž. & Gadžić A. (2011). Edukativne igre kao savremeno sredstvo za učenje. *Teme*, 35(4), 1677 – 1689.

Mirković A. (2017). *Bitcoin menjačnica bankrotirala posle hakerske pljačke*. Dostupno na: https://pcpress.rs/bitcoin-menjacnica-bankrotirala-posle-hakerske-pljacke/, datum pregleda: 20.01.2018.

Mirković A. (2018). *Kriptovalute i varanje – novi unosni posao prevaranata*. Dostupno na: https://pcpress.rs/kriptovalute-i-varanje-novi-unosni-posao-prevaranata/, datum pregleda: 23.01.2018.

Mitrović M. (2016). *Mračne tajne globalne mreže*. Dostupno na: http://www.novaenergija.net/mracne-tajne-globalne-mreze/, datum: 10.02.2018.

Mudrinić M. (2016). Od prevare na Limundu do zatvorske kazne, Dostupno na: http://www.netokracija.rs/limundo-prevara-zatvor-124958, datum pregleda: 12.01.2018.

Munson L. (2015). *Trump Hotel chain investigates potential payment card breach*. Available at: https://nakedsecurity.sophos.com/2015/07/03/trump-hotel-chain-investigates-potential-payment-card-breach/ date: 12.12.2017.

Muscovitch Z. (2013). *A Short History of Cybersquatting Law*. Available at: http://domain-name-lawyer.blogspot.com/2013/04/a-short-history-of-cybersquatting-law.html, datum pregleda: 12.12.2017.

N1 Zagreb. (2015). *Darknet - mračna strana surfovanja interneto.* Dostupno na: http://rs.n1info.com/a50647/Sci-Tech/Sve-o-Deep-Web-ili Darknetu. html, date: 10.02.2018.

Nacrt zakona o elektronskoj upravi – Teks propisa, Dostupno na: http://www.paragraf.rs/dnevne-vesti/210917/210917-vest19.html, datum pregleda: 02.02.2018

Nagesh S. (2013). Roll of Data Mining in Cyber Security. *Journal of Exclusive Management Science*, 2(5), 1-5.

Naumovski G. & Popović D. (2011). *Information Technology Law*. Skoplje, Macedonia: Iustinianus Primus Law Faculty, SS.Cyril and Methodius University of Skopje.

Net security training. (nn). *What is a Public Key Infrastructure*. Dostupno na: https://web.archive.org/web/20161009124244/http://www.net-security-training.co.uk/what-is-a-public-key-infrastructure, datum pregleda: 29.12.2017

Nissan U. (nn). *Nissan vs Nissan, Nissan Motor Sued Nissan Computer For Trademark Infringement, Trademark Dilution And Cyber-Squatting*. Available at: http://www.digest.com/Big_Story.php, datum pregleda: 13.12.2017.

Oakley K, (2002). *What is e-governance?* Available at: https://www.coe.int/t/dgap/democracy/Activities/GGIS/E-governance/Work_of_egovernance_Committee/Kate_Oakley_eGovernance_en.asp, date: 10.11.2017.

Obradović S., Spalević Ž., Knežević M., Tešić D., Marković V. & Žorić A. (2012). Causes Delays in the Development of Card Business. *TTEM - Technics Technologies Education Management*, 7(4), 1796 – 1808.

OCCRP. (2016). *Bosnia and Herzegovina: crackdown on 'cyber blackmail' group*. Organized crime and corruption reporting project, Available at: https://www.occrp.org/en/daily/4793-bosnia-and-herzegovina-crackdown-on-cyber-blackmail-group, date: 18.02.2018.

Odluka o elektronskom načinu obavljanja platnog prometa, Službeni glasnik RS, br. 57/2004

Odluka o elektronskom potpisivanju dokumenata s podacima koje banke dostavljaju Narodnoj banci Srbije, Službeni glasnik RS, br. 28/2009, 47/2009

Odluka o minimalnim standardima upravljanja informacionim sistemom finansijske institucije, Službeni glasnik RS, br. 23/2013 i 113/2013.

Otair M. & Tarawneh H. (2011). Mobile Banking Based on Stand-alone Mobile Aplcation Clients. *Journal of Information & System Management*, 1(2), 47-59.

Page L. (2009). *MoD networks still malware-plagued after two weeks*. Available at: http://www.theregister.co.uk/2009/01/20/mod_malware_still_going_strong/, date: 15.02.2018.

Palević P. & Spalević Z. (2014). Zloupotreba moći u Cyber prostoru. U: *Zbornik radova "Zloupotreba moći" sa istoimene međunarodne konferencije*. (str. 326-344). Tara: Udruženje za međunarodno krivično pravo, Intermex.

Paro, D. (2001). *Wireless application protocol (WAP): What is it all about....How does it work*. SANS Institute.

Paunović S. (2013). Biometrijski sistemi za utvrđivanje identiteta. U: *Zbornik radova Međunarodne konferencije i izložbe Infotech 2013*. (str. 1-6). Aranđelovac – Srbija: Asocijacija za računarstvo, informatiku, telekomunikacije i nove medije Srbije.

Petrić S. (2005). Zakon o elektronskoj trgovini i zaštita potrošača. U: *zborniku Zaštita potrošača i ulagatelja u europskom i hrvatskom pravu, (ur. Tomljenović, V., Čulinović-Herc, E.)*. (str. 123-153). Rijeka: Pravni fakultet Sveučilišta u Rijeci.

Petrova K. (2002). Mobile banking: backgroung, services and adoption. In *Delener, N. & Chao, C.-N. (eds), "Beyond Boundaries". Proceedings of the 2002 GBATA International Conference*,(pp.928-939).

Pilipović D. (2015). Odnos e-demokratije i e-glasanja. U: *Zbornik 7. Naučni skup Mreža 2015*. (str. 280-287). Valjevo: Univerzitet Singidunum, Poslovni Fakultet.

Pilipović D. (2014). Razvoj, trenutno stanje i perspektive e-glasanja. U: *Zborniku medjunarodnog simpozijuma - Infoteh 2014*. (str. 1225 - 1228). Jahorina: Elektrotehnički fakultet Istočno Sarajevo.

Pilipović D. & Starčević D. (2014). Pregled šema za elektronsko glasanje. *Info M*. 51, 19-25.

Ponemon Institute. (2015). *2015 Cost of Cybercrime Study: Global*. Traverse City, Michigan: Ponemon Institute LLC.

Popović D. (2005). *Imena internet domena i pravo intelektualne svojine*. Beograd: Institut za uporedno pravo, Monografija Beograd.

Popović D. (2015). Kritički osvrt na srodnopravnu zaštitu izdavača: zaštita privrednog ili kulturnog poduhvata. *Anali Pravnog fakulteta u Beogradu - Časopis za pravne i društvene nauke*, 63(1), 116-132.

Pravilnik o bližim uslovima za izdavanje kvalifikovanih elektronskih sertifikata, Službeni glasnik RS, br. 26/2008.

Pravilnik o izdavanju vremenskog žiga, Sližbeni glasnik RS, br. 112/2009

Pravilnik o načinu podnošenja poreske prijave elektronskim putem, Službeni glasnik RS, br. 8/12, 113/13

Pravilnik o načinu postupanja sa elektronskim ponudama i načinu sprovođenja elektronske licitacije u postupcima javnih nabavki, Službeni glasnik RS, br. 50/2009.

Pravilnik o Registru sertifikacionih tela za izdavanje kvalifikovanih elektronskih sertifikata u Republici Srbiji, Službeni glasnik RS, br. 26/2008

Pravilnik o tehničkotehnološkim postupcima za formiranje kvalifikovanog elektronskog potpisa i kriterijume koje treba da ispune sredstva za formiranje kvalifikovanog elektronskog potpisa, Službeni glasnik RS, br. 26/2008, 13/2010.

Prlja D., Reljanović M. & Ivanović Z. (2012). *Internet pravo.* Beograd: Institut za uporedno pravo.

Proof space. (2007). System Technical Overview. Available at: http://fios.com/proofmarksystemtech.pdf, date: 02.01.2018.

PwC (PricewaterhouseCoopers). (2016). *Russian Economic Crime Survey 2016.* Available at: https://www.pwc.ru/en/publications/resc-2016.html, date: 20.02.2018.

Rakić Vodinelić V. (2012). *Opasne pravne posledice ACTA*. Dostupno na: http://pescanik.net/opasne-pravne-posledice-acta/, datum pristupa: 15.12.2017.

Ranisavljević M. (2013). *Halcom e-fakture*. Dostupno na: https://poslovnisoftver.net/halcom-e-fakture/, datum pregleda: 22.12.2017.

Rathmell A., Valeri L., Robinson N., Servida A. (2003). *Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries*, Brussels –Luxembourg, European Commission-Rand Europe.

Rauscher K, Korotkov A. (2011). *Russia-u.s. bilateral on critical infrastructure protection Working Towards Rules for GoverningCyber Conflict - Rendering the Geneva and Hague Conventions in Cyberspace*.

Reavis J. (2004). *Microsoft, the National Security Agency and backdoors.* Available at: http://www.networkworld.com/newsletters/sec/0927sec2.html, date: 12.03.2013.

Republika Srbija Republičko javno tužilaštvo. (2013). *Rad javnih tužilaštava na suzbijanju kriminaliteta i zaštiti ustavnosti i zakonitosti u 2012. godini.* Dostupno na: http://www.rjt.gov.rs/ci/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%98%D0%B5-%D0%BE-%D1%80%D0%B0%D0%B4%D1%83, datum pregleda: 15.12.2017.

Republika Srbija Republičko javno tužilaštvo (2017). *Rad javnih tužilaštava na suzbijanju kriminaliteta i zaštiti ustavnosti i zakonitosti u 2016. Godini*. Dostupno na: http://www.rjt.gov.rs/ci/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%98%D0%B5-%D0%BE-%D1%80%D0%B0%D0%B4%D1%83, datum pregleda: 15.12.2017.

Rezaee Z. & Riley R. (2014). *Prijevara u finansijskim izvještajima, sprečavanje i otkrivanje*. Zagreb: Mate d.o.o.

Ribeiro J. (2010). *Google faces privacy investigation in Canada*. Available at: https://www.cio.com/article/2417788/legislation/google-faces-privacy-investigation-in-canada.html, date: 18.02.2018.

Rowland D. & MacDonald E. (2005). *Information Technology Law*. 3rd ed. London: Cavendish Publishing Limited.

Sanader D. (2014). Mobilno bankarstvo: Novi trend u savremenom bankarskom sektoru. *Bankarstvo,* 5, 86-109.

Sandoval G. (2017). *An interview with alleged KickassTorrents founder in his jail cell in Poland*. Available at: https://www.theverge.com/2017/5/23/15681160/kickasstorrents-founder-artem-vaulin-interview-bittorrent, date: 06.12.2017

Sanford C. & Rose J. (2007). Characterizing eParticipation. *International Journal of Information Management*. 27(6), 406-421.

Saravanan D. & Srininvasan S. (2012). Video Image Retrieval Using Data Mining Techniques. *Journal of Computer applications*, 5(1), 39-42.

Savage C. (2010). *U.S. Tries to Make It Easier to Wiretrap the Internet*. Available at: http://www.nytimes.com/2010/09/27/us/27wiretap.html?pagewanted=1&_r=1&hp, date: 08.02.2018.

Schmölzer G. (1997). Internet i kazneno pravo, *prevod u Hrvatskom ljetopisu za kazneno pravo*, vol. 4 2/97, str. 891-897.

Shalom S.A.A., Dash M., Tue M. (2008) Efficient K-Means Clustering Using Accelerated Graphics Processors. In: *Song IY., Eder J., Nguyen T.M. (eds) Data Warehousing and Knowledge Discovery. DaWaK 2008*. Lecture Notes in Computer Science, vol 5182. Springer, Berlin, Heidelberg.

Sheppard, S. (2015). *Notifies Customers Of Malware Activity*. Available at: http://newsroom.hyatt.com/news-releases?item=123450, date: 20.06.2017.

Sieber U. (1999). Responsibility of internet providers—A comparative legal study with recommendations for future legal policy. *Computer Law & Security Review*, 15(5), 291-310.

Singh S. & Karaulia S, (2011). E-governance: information security issues. In *Proceedings of the International Conference on Computer Science and Information Technology*. (pp.120-124). Pattaya.

Sklaver L.S. (2010). The pros and cons of using electronic monitoring programs in juvenile cases. *Juvenile Justice Committee Newsletter*, 5, 1-5.

Skrlec B., Grecke M. (2007). Usklađenost KZ i ZKP Republike Srbije sa zahtevima Konvencije Saveta Evrope o visokotehnološkom kriminalu*, Expert report,* Council of Europe.

Slovakova Z. (2006). Protection of trademarks and the Internet with respect to the Czech law. *Journal of International Commercial Law and Technology*, 1(2), 72-79.

Službeni list SFRJ, br. 29/78, 39/85, 57/89, Službeni list SRJ, br. 31/93; u daljem tekstu ZOO

Spalević Ž. (2012). *Krivična odgovornost pravnih i fizičkih lica na polju elektronskih komunikacija i elektronske uprave prouzrokovana cyber kriminalom*. Doktorski rad. Novi Sad: Pravni fakultet za privredu i pravosuđe, Univerzitet privredna akademija.

Spalević Ž., (2017). Elektronska demoktatija i elektronsko glasanje, Zbornik radova „Usluge i odgovornost" sa istoimene međunarodne konferencije, XIII majsko savetovanje, (str. 771-784), Pravni fakultet Univerziteta u Kragujevcu-Institut za pravne i društvene nauke, Kragujevac, Srbija.

Spalević Ž., Banović B. & Vrhovšek M. (2013). Cyber Crime in the States of Western Balcan. *TTEM - Technics Technologies Education Management,* 8(2), 886 – 895.

Spalević Ž., Ilić M. (2017). The use of dark web for the purpose of illegal activity spreading, Ekonomika, 63 (1), 73-82.

Spalević Ž., Ilić M. & Arsić N. (2016). Legal aspects of data mining algorithms for stream processing in traffic surveillance. *Journal of criminalistics and law, Academy of criminalistic and police studies Belgrade – The Republic of Serbia*, 1, 57-79.

Spalević Ž., Ilić M., Jerotijević D. (2016). Electronic monitoring devices and data processing, Ekonomika, 62(4), 155-166.

Spalević Ž., Ilić M. & Palević M. (2016). Electronic tracking of postal services. in *Proceedings of 3rd the International Scientific Conference on ICT and e-Business Related Research - Sinteza 2016.* (pp.479-485). Belgrade: Singidunum University.

Spalević Ž., Ilić M. & Spalević P. (2015). Electronic monitoring devices and data processing. In: *Proceedings of 2nd International scientific conference of IT and Business Related Research – Synthesis*. (pp. 242-247). Belgrade: Singidunum University.

Spalević Ž., Ilić M. & Spalević Ž. (2016). Electronic government in the fight against terrorism". in *Proceedings of 3rd the International Scientific Conference on ICT and e-Business Related Research - Sinteza 2016*. (pp. 518-525). Belgrade: Singidunum University.

Spalević Ž., Ilic M., & Spalevic Ž. (2017). Cyber terrorism as a threat to tourism development, in *International scientific conference on economics and management Eman 2017: Globalization challenges*. (pp.862-868). Ljubljana, Slovenia. Udekom Balkan.

Spalević Ž., Knežević M. & Bjelajac Z. (2012). Foreign Investments in Banking Systems of Serbia and Western Balkan Countries. *TTEM - Technics Technologies Education Management*, 7(2) 747 – 757

Spalević Z., Milisavljević B. & Ilić M. (2017). Pravni aspekti razvoja Elektronske uprave u Republici Srbiji. U: *Zbornik radova Međunarodni naučni skup Sinergija*. (str. 93-98). Bijeljina: Univerzitet Sinergija.

Spalević Ž., Počuča M. & Bjelajac Ž. (2013). Terrorist Activities and Internet Government with Focus on Importance of Prevention within a Family. *TTEM - Technics Technologies Education Management*, 8(1),195 – 203.

Spalević Ž. & Spalević Ž. (2017). Stanje servisa elektronske uprave baziranih na računarstvu u oblaku, Kulturna polisa, 14(1), 171 – 183.

Spalević Ž. & Spalević Ž. (2016). Terorizam kao prijetnja hotelijerstvu. *International Thematic Monograph – Thematic Proceedings: Modern Management Tools and Economy of Tourism Sector in Present Era*, 520 – 528.

Spalević Ž., Trajcevski Z., Bjelajac Z., Pocuca M. & Dimitrijević D. (2013) Regulatory Framework Distribution of HDTV in the Western Balkan Countries. *TTEM - Technics Technologies Education Management*, 8(3), 1173 – 1183.

Spalević Ž. & Vićentijević K. (2017). Forenzičko računovodstvo i revizija u digitalnom okruženju. *Kultura polisa*. XIV(33), 203-216.

Spalević Ž. & Vićentijević K. (2017). Challenges of forenic accounting in tourist industry. *Second international thematic monograph – thematic proceedings –modern management tools and economy of tourism sector in present era*, 230-239.

Spasić D. (2010). Vremenski žigovi sertifikacionog tela pošte. U: *Zbornik radova XXVIII Simpozijuma novim tehnologijama u poštanskim ulugama i telekomunikacionom saobraćaju –PosTel 2010*. (str. 175-184). Beograd: Univerzitet u Beogradu - saobraćajni fakultet odsek za poštanski i telekomunikacioni saobraćaj.

Spasic V. & Stevanovic B. (2015). Dokazivanje digitalnih povreda prava intelektualne svojine – osvrt na anglosaksonski pravni sistem. U: *Zbornik radova Pravnog fakulteta u Nišu*. (str. 203-226), Niš: Pravni fakultet.

Spindler G. & Borner F. (2007). E-Commerce Law in Europe and the USA. Germany: Springer.

Spisak zakona RS, Agencija za informaciono društvo Republike Srpske, Dostupno na: https://www.aidrs.org/sr/legislativa-i-standardizacija/zakoni/, datum pristupa: 05.10.2017.

Središnji državni portal – O sistemu e-Građani, Dostupno na: https://gov.hr/e-gradjani/o-sustavu-e-gradjani/1584, datum pregleda: 27.01.2018.

Staff N. (2008). *EU Council refuses to release secret ACTA documents*. Available at: https://www.neowin.net/news/eu-council-refuses-to-release-secret-acta-documents, date: 09.12.2017.

Stanivuković B. & Marković D. (2014). RFID u funkciji poštanske marke–čipovanje poštanskih pošiljaka. In: *XXXII Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – PosTel*. (str. 3-14). Beograd: Univerzitet u Beogradu – Saobraćajni fakultet.

Stefanoski Lj. (2015). *Upravni postupak registracije internet domen imena i pravna zaštita*. Doktorski rad. Niš: Prani fakultet.

Steve. (2016). *Surface web, deep web, dark web -- What's the difference?*. Available at: https://www.cambiaresearch.com/articles/85/surface-web-deep-web-dark-web----whats-the-difference, date: 10.02.2018.

Stojanović D. (nn). Normativno uređenje oblasti elektronskog potpisa. *Pravo i privreda*. 5(8/05). 471-482

Stojković M. (2015). *Fejsbuk i praćenje korisnika putem dodataka za društvene mreže*. Dostupno na: http://pravoikt.org/fejsbuk-i-pracenje-korisnika-putem-dodataka-za-drustvene-mreze/, datum: 10.02.2018.

StrafGesetzbuch, StGB, Član 126 i 148. StGB.

Sunbye P., Butkovic M. & Rapic I. (2016). *Globalno istraživanje gospodarskog kriminala iz 2016. – Hrvatska Naoružani i spremni za bitku (Vaši protivnici jesu!)*. Available at: http://www.pwc.hr/hr/forenzicke-usluge/Globalno-istrazivanje-gospodarskog-kriminala-iz-2016-za-Hrvatsku.pdf, datum: 20.02.2018.

Šušak O. (2010). *Elektronsko bankarstvo i elektronski novac*. Master rad. Beograd: Univerzitet Singidunum.

Tella R, & Schargrodsky E. (2013) „Criminal recidivism after prison and electronic monitoring“, journal of Political Economy, 121(1), 28-73.

The White House. (2011). *International Strategy For Cyberspace.* Available at: https://obamawhitehouse.archives.gov/sites/default/files/rssviewer/international_strategy_for_cyberspace.pdf, date: 19.02.2018.

The EastWest Institute, pp.36-37, Available at: https://www.eastwest.ngo/sites/default/files/ideas-files/US-Russia.pdf, date: 18.02.2018.

Timothy L.T. (2003). Al Qaeda and the Internet: The danger of cyberplanning. *Parameters*. 33(1), 112–123.

Tittel E. & Lindros K. (2017). *Best Digital Forensics Certifications 2018*. Available at: http://www.tomsitpro.com/articles/computer-forensics-certifications,2-650.html, date: 29.01.2018.

Tomović D. (2017). *Montenegro on alert over new cyber attacks.* BalkanInsight, Available at: http://www.balkaninsight.com/en/article/montenegro-govt-on-alert-over-new-cyber-attacks-02-21-2017, date: 18.02.2018.

Trnavci G. (2009). Zaključenje, punovažnost i dokazivanje elektronskih ugovora: komparativna analiza. *Zbornik Pravnog fakulteta* Sveučilište u Rijeci. 30(1), 449-472.

UK Legislation. (1971). *Criminal Damage Act 1971*. Available at: http://www.legislation.gov.uk/ukpga/1971/48/contents, date 25.03.2017

Uredba o posebnim merama zaštite tajnih podataka u informaciono-telekomunikacionim sistemima, Sl. glasnik RS", br. 53 od 20/2011.

U.S. Department of Justice. (2002). Creator of Melissa Computer Virus Pleads Guilty to State and Federal Charges, *Press Release*.

Vaas L. (2015). *Mandarin Oriental hotel chain confirms credit card breach*. Available at: https://nakedsecurity.sophos.com/2015/03/06/mandarin-oriental-hotel-chain-confirms-credit-card-breach/, date: 12.12.2017.

Van der Sar E. (2014). *Judge Understands BitTorrent, Kills Mass Piracy Lawsuits*. Available at: https://torrentfreak.com/judge-understands-bittorrent-kills-mass-piracy-lawsuits-140130/, date: 06.12.2017.

Vasić D. (2008). Zakonska zaštita elektronskih informacija i komunikacija u Srbiji - kritički osvrt na stepen normativne uređenosti, *Srpska politička misao*, 57(5-6), 135-146.

Vault. (2017). *2018 Best Accounting Firms for Forensic Accounting*. Available at: http://www.vault.com/company-rankings/accounting/best-firms-in-each-practice-area?sRankID=418; date: 26.3.2017.

Veinović M. & Jevremović A. (2011). *Računarske mreže*. Beograd: Fakultet za informatiku i računarsvo, Univerzitet Singidunum.

Vigneau V. (2010). Commerce électronique et protection du consommateur, Paris. pp. 297.

Vijesti online. (2015). *Tamni internet: Tu su hakeri, prodavci ljudskih organa, oružja*. Preuzeto 10.02.2018., sa

http://www.vijesti.me/techno/tamni-internet-tu-su-hakeri-prodavci-ljudskih-organa-oruzja-828308.

Vlada Republike Srbije. (2015). *Strategija razvoja elektronske uprave u Republici Srbiji za period od 2015-2018. godine i akcioni plan za spovođenje Strategije za period od 2015-2016. godine*, Dostupno na: http://www.mduls.gov.rs/doc/Strategija%20razvoja%20eUprave%20sa%20AP%202015-2018.pdf

Vona L.W. (2016). *Fraud Data Analytics Methodology: The Fraud Scenario Approach to Uncovering Fraud in Core Business Systems*. Hoboken, New Jersey: John Wiley & Sons, Inc.

Vučković V. & Rajković P. (2010). *Zaštita informacija.* Niš: Elektronski fakultet.

Vujović S. (2005). Elektronsko poslovanje i elektronska inteligencija. Beograd: Beogradska poslovna škola

Vukic U. (2016). *Elektronsko glasanje krupan zalogaj za BiH*. Dostupno na: https://www.rtvbn.com/377696/Elektronsko-glasanje-krupan-zalogaj-za-BiH, datum pregleda: 1.02.2018.

Wayne O. & Genelle B. (2011). *Major Principles of Media Law*. Boston: Stamford: Cengage Learning.

Weimann G. (2004). Cyberterrirism? How real is the threat, Special Report 119, *United States Institute of peace*, 1-12.

Weimann G. (2016). Terrorist Migration to the Dark Web. *Perspectives on terrorism*. 10(3), 40-40.

Wenninger J. (2000). The Emerging Role of Banks in E-Commerce. *Federal Reserve Bank of New York Current Issues in Economics and Finance*. 6(3), 1–6.

West Virginia University (2012). *Education and Training in Fraud and Forensic Accounting: A Guide for Educational Institutions, Stakeholder Organizations, Faculty, and Students*. Virginia: West Virginia University - Forensic Science Initiative, 2012.

Willsher K. (2009). *French fighters planes grounded by computer virus*, Available at: http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html, date: 02.02.2018.

Yeager R. (2006). Criminal computer forensics management. In: *Proceedings of the 3rd annual conference on Information security curriculum development - InfoSecCD'06*. (pp.168-174). Kennesaw, Georgia: ACM.

Yoskowitz A. (2008). *Elite Torrents admin gets 18 months in jail.* Available at:http://www.afterdawn.com/news/article.cfm/2008/09/10/elitetorrents_admin_gets_18_months_in_jail, date: 05.12.2017.

Zakon o autorskim i srodnim pravima, Službeni glasnik RS, br. 104/2009, 99/2011, 119/2012 I 29/2016 – odluka US

Zakon o bezbednosti saobraćaja, „Službeni glasnik", br. 41/2009, 53/2010, 101/2011, 32/2013 - odluka US, 55/2014, 96/2015 - dr. zakon i 9/2016 - odluka US, član 296.

Zakon o elektronskim komunikacijama, „Sl. glasnik RS", br. 44/2010, 60/2013 - odluka US i 62/2014.

Zakon o elektronskim komunikacijama Crne Gore, Službeni list Crne Gore, broj 32/2014.

Zakon o elektronskoj trgovini, Službeni glasnik RS, br. 41/2009 i 95/2013.

Zakon o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju, Službeni glasnik RS, br. 94/2017.

Zakon o elektroničkom potpisu, Republika Hrvatska

Zakon o elektronskom potpisu, Službeni glasnik RS, br. 135/2004.

Zakon o izvršenju vanzavodskih sankcija i mera, Službeni glasnik RS, br. 55/2014.

Zakon o monetarnoj politici i finansijama Republike Francuske.

Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, „Službeni glasnik RS“, br. 61/2005 i 104/2009.

Zakon o platnim uslugama, Službeni glasnik RS, br. 139/2014.

Zakon o posebnim ovlašćenjima radi zaštite prava intelektualne svojine, *Službeni glasnik RS,* broj 46/06, 104/2009.

Zakon o sprečavanju pranja novca i finansiranja terorizma, „Službeni glasnik RS“, br. 20/2009, 72/2009, 91/2010 i 139/2014.

Zakon o zaštiti intelektualne svojine Republike Francuske

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

Zakonik o krivičnom postupku, „Službeni glasnik RS“, br. 72/2011, 101/2011, 32/2013, 45/2013 i 55/2014.

Zakon o poštanskim uslugama, Službeni glasnik RS, br. 18/2005, 30/2010 i 62/2014

Zakon o zaštiti potrošača, Službeni glasnik RS, br. 62/2014, 6/2016-dr

Zetter K. (2013). *How the Feds Took Down the Silk Road Drug Wonderland*. Available at: www.wired.com/2013/11/silk-road/, date: 10.02.2018.

Zorić N. (2017). *Elektronsko glasanje u Srbiji, realnost ili fantastika*, Dostupno na: https://rs.sputniknews.com/komentari/201704071110672860-sve-o-elektronskom-glasanju1/, datum pregleda: 01.02.2018.

Zweites Gesetz zur Bekampfung der Wirtschaftskriminalitat*,* 2.WiKG.

10
Indeks pojmova

CCL-Creative Commons Licenses
GPL - General Public License
LGPL - Lesser General Public License
BSD - Berkeley Source Distribution
ACTA - Anti - Counterfeiting Trade Agreement
DNS - Domain Name System
UDRP Policy - Uniform Domain Name Dispute Resolution Policy
UDRP Rules - Rules for Uniform Domain Name Dispute Resolution Policy
FTP – File Transfer Protocol
G2G - Goverment to Government
G2B - Goverment to Business
G2C - Goverment to Consumer
B2G - Business to Government
B2B - Business to Business
B2C - Business to Consumer
C2G - Consumer to Government
C2B - Consumer to Business
C2C - Consumer to Consumer
B2E - Business to Employee
B2B2C – Business to Business to Consumer
C2B2C – Consumer to Business to Consumer
EDI- Electronic Data Interchange
CA-Certification Authority
PKI - Public key infrastructure
TSA - Time-Stamping Authority
UTC - Universal Time Coordinate
MAC - Message Authentication Code
CBC-MAC - Cipher Block Chaining Message Authentication Code
PMAC - Parallelizable MAC
OMAC - One-key MAC
TSA - Time-Stamp Authority
ICT - Information and communications technology
SSL - Secure Sockets Layer
IVR - Interactive Voice Response
WAP - Wireless Access Protocol
AUC - Authentication Centers
SRES - Signed RESponse

WTLS - Wireless Transport Layer Security
SSL - Secure Sockets Layer
mTAN - mobile transaction authentication
AKA -nAuthentication and Key Agreement
GIAC - Global Information Assurance Certification
IIA - The Institute of Internal Auditors
AICPA - The American Institute of Certified Public Accountants
ACFE - Association of Certified Fraud Examiners
IC3 - Internet Crime Complaint Center
PwC – Price water house Coopers
FRR - false rejection rate
FAR - false acceptance rate
TAM -Technology Acceptance Model
TOE -Technology Organization Environment
EKD - Enterprise Knowledge Development
ANT - Actor Network Theory
EVM - Electronic Voting Machine
DRE - Direct Recording Electronic
AIDRS - Agenciji za informaciono društvo Republike Srpske
UNPACS - United Nations Public Administration Country Studies
RIK – Republička Izborna Komisija
GPS – Global Position System
LCD - Liquid-crystal display
UPU - Universal Postal Union
RFID - Radio Frequency Identification
PoS - Point-of-Sale
GIS - Geographic Information System
EEG – Electroencephalogram
TSDB - Terrorist Screening Database
Tor - The Onion Router
I2P - Invisible Internet Project
DoS - Denial of service
DDoS – Distributed Denial of service
BSA - Business Software Alliance

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

347.77/.78:004.738.5
004.738.5.072.5
004.7:339

СПАЛЕВИЋ, Жаклина, 1977-
Pravni aspekti sajber prostora / Žaklina Spalević. - 2. izd. - Beograd : Univerzitet Singidunum, 2020 (Beograd : Caligraph). - 230 str. : tabele ; 24 cm

Tiraž 900. - Napomene i bibliografske reference uz tekst. - Bibliografija: str. 211-226. - Registar.

ISBN 978-86-7912-676-4

а) Интелектуална својина -- Интернет б) Електорнско пословање -- Правна заштита

COBISS.SR-ID 282647052

© 2020.
Sva prava zadržana. Nijedan deo ove publikacije ne može biti reprodukovan u bilo kom vidu i putem bilo kog medija, u delovima ili celini bez prethodne pismene saglasnosti izdavača.

www.singidunum.ac.rs

9 788679 126764



Žaklina Spalević

PRAVNI ASPEKTI SAJBER PROSTORA

Pravni aspekti sajber prostora predstavljaju monografsko izdanje koje sagledava institute prava u novom sajber okruženju, u kome se analizira i daje predlog za unapređenje postojeće legislative sa ciljem definisanja ugovornih i deliktnih odnosa, prava na privatnost, slobode govora, zaštite od zlostavljanja, intelektualne svojine, autorskog prava na kodovima računarskih programa i baza podataka, internet bezbednosti, krivičnih dela proizašlih iz radnji na internetu i na polju elektronskih komunikacija, prava svojine digitalnih podataka i poreskog akpekta razmene roba, usluga i kapitala u sajber prostoru. Takođe, sagledani su pravni aspekti izgradnje sistema elektronske uprave kao novog modela javne uprave i lokalne samouprave i načini borbe protiv organizovanog kriminala i međunarodnog terorizma u sajber okruženju.

Univerzitet Singidunum