SVEUČILIŠTE U SPLITU

EKONOMSKI FAKULTET

OPOREZIVANJE DIGITALNIH USLUGA U REPUBLICI HRVATSKOJ

ZAVRŠNI RAD

STUDENTICA
Ivana Ćurić

MENTOR
Prof.dr.sc.Nikša Nikolić

Split, kolovoz 2017.

SADRŽAJ

1.Uvod..... 3

1.1.Problem istraživanja rada..... 3

1.2.Cilj istraživanja..... 3

1.3.Metode istraživanja..... 3

1.4.Struktura završnog rada..... 3

2.Pojam digitalnih usluga..... 3

2.1.Strategija jedinstvenog digitalnog tržišta za Europu..... 4

2.2.Digitalne vještine i znanje..... 4

2.3.Digitalna agenda za Europu 2010.-2020..... 5

3. Sudionici internetskog poslovanja..... 6

3.1.Anonimnost sudionika internetskog poslovanja..... 6

3.1.1.Web preglednici..... 8

3.1.2.Skidanje torrenta anonimno..... 10

3.1.3.Nasilje preko interneta i načini internet prijevare..... 11

3.2.Primjeri anonimnosti internetskog poslovanja..... 15

4.Oporezivanje realnih,financijskih i digitalnih transakcija..... 18

4.1.Oporezivanje realnih transakcija..... 18

4.2.Oporezivanje financijskih transakcija..... 19

4.3.Oporezivanje digitalnih transakcija..... 21

4.4.Pravila za identifikaciju isporučitelja i primatelja usluga..... 24

4.5.Sustav MOSS – Mini One Stop Shop..... 26

4.6.Oporezivanje elektroničke trgovine PDV-om..... 32

5.Oporezivanje PDV-om digitalnih usluga u RH..... 35

5.1.Deep web u Hrvatskoj..... 37

5.2.Neprihvatljiv govor u komentarima na internetskih informativnim portalima..... 39

5.3.Ipsos Online klub..... 42

5.4. Anonimnost i kazne za uvrede na internetu..... 43

6.Zaključak.....45

7.Literatura.....46

1.Uvod

1.1.Problem istraživanja rada

Oporezivanje digitalnih usluga postaje jedno od najvažnijih tehnoloških problema u 20. stoljeću, te postavlja nova pravila za države članice EU. Predmet istraživanja rada je utvrditi specifičnosti oporezivanja digitalnih usluga u RH jer je ovaj sustav oporezivanja u RH na snazi tek od 01.01.2015. godine. Istraživanje je prikazalo kako se deep web razvio u RH. U radu će biti opisani različiti načini internet prijevare, te će biti prikazana anonimnost internetskog poslovanja u različitim zemljama svijeta. Vrlo važan dio rada se odnosi na oporezivanje digitalnih transakcija koje su bitne zbog toga što se današnja prodaja većinom odvija preko interneta.

1.2.Cilj istraživanja

Cilj ovog istraživanja je objasniti pojam digitalnih usluga, odrediti sve sudionike internetskog poslovanja, usporediti oporezivanje digitalnih usluga sa oporezivanjem realnih i financijskih transakcija, te odrediti specifičnosti oporezivanja digitalnih usluga.

1.3.Metode istraživanja

U izradu ovog rada korištena je povijesna metoda, statistička metoda, metoda komparacije, metoda deskripcije, analiza i sinteza.

1.4.Struktura završnog rada

Prvi dio rada sadržava problem istraživanja, ciljeve, metode istraživanja, te strukturu rada. U drugom dijelu rada su dane neke osnovne informacije o digitalnim uslugama. Treći dio rada se odnosi na sudionike internetskog poslovanja (prikazana je njihova anonimnost na internetu) i prikazani su neki od primjera internetske prijevare.

Četvrti dio se odnosi na oporezivanje realnih, financijskih i digitalnih usluga gdje su prikazane pojedine transakcije u različitim zemljama EU-e. Peti dio rada se odnosi na oporezivanje PDV-om digitalnih usluga u RH koje je na snazi od 01.01.2015. godine, opisan je deep web u RH (što sve možemo pronaći na njemu). Na kraju se prikazane i kazne za uvrede na internetu koje su na snazi od 01.01.2013.godine.

2.Pojam digitalnih usluga

Pojava i razvoj e-trgovine

Jedna od najvažnijih tehnoloških promjena koja je utjecala na korjenite promjene u društveno-ekonomskom okruženju krajem 20. stoljeća jest pojava interneta u svakodnevnim odnosima, uključujući i one poslovne, u kojima sudjeluju fizičke osobe, pravne osobe, pa i osobe javnog

prava. Jedna od mogućnosti koje pruža internet, a koja je dovela do revolucije u obavljanju čitavog niza poslovnih aktivnosti u posljednjih 20-ak godina jest elektronička trgovina.

Elektronička trgovina više nego bilo koji drugi oblik trgovine predstavlja izazov za porezne vlasti te zahtijeva njihovu najširu suradnju. Naime, njezine bitne karakteristike, npr. dezintermedijacija, tj. mogućnost kupnje proizvoda izravno od *online*-prodavatelja, smanjuje potrebu za posrednicima, koji su tradicionalno služili kao porezni platci. Stalno se stvaraju novi poslovni modeli i načini trgovanja, čak i prije nego što evoluiraju aktualni modeli, i to tako da se u pitanje dovodi i postojanje državnih granica kao takvih jer se one, u slučaju izravne elektroničke trgovine, više ne moraju ni prijeći.

2.1.Strategija jedinstvenog digitalnog tržišta za Europu

Na jedinstvenom digitalnom tržištu osigurano je slobodno kretanje robe, osoba, usluga i kapitala, a pojedinci i poduzeća mogu neometano pristupati aktivnostima na internetu i obavljati ih u uvjetima poštenog tržišnog natjecanja te uz visoku razinu zaštite potrošača i osobnih podataka, bez obzira na njihovo državljanstvo ili mjesto boravišta. Uspostavom jedinstvenog digitalnog tržišta osigurat će se da Europa zadrži vodeći položaj u svijetu u digitalnom gospodarstvu, što će pomoći europskim poduzećima da rastu na svjetskoj razini.

Strategija jedinstvenog digitalnog tržišta temeljit će se na trima stupovima[1]:

- Bolji pristup potrošača i poduzeća robi i uslugama na internetu u cijeloj Europi – to zahtijeva hitno uklanjanje ključnih razlika između okruženja na internetu i izvan njega kako bi se uklonile prepreke za prekogranične aktivnosti na internetu,
- Stvaranje odgovarajućih uvjeta za procvat digitalnih mreža i usluga – to zahtijeva brzu, sigurnu i pouzdanu infrastrukturu i usluge pružanja sadržaja, te odgovarajuće regulatorne uvjete za inovacije, ulaganja, pošteno tržišno natjecanje i ravnopravne uvjete,
- Iskorištavanje punog potencijala rasta europskog digitalnoga gospodarstva – to zahtijeva ulaganja u infrastrukturu i tehnologije IKT-a, npr. računalstvo u oblaku i veliki podaci te istraživanje i inovacije za poticanje industrijske konkurentnosti te bolje javne usluge, uključivost i vještine.

2.2.Digitalne vještine i znanje

Potražnja za digitalno osposobljenom radnom snagom svake se godine poveća za oko 4 %. Ako se ne poduzmu odlučne mjere, nedostatak stručnjaka za IKT u EU-u mogao bi se do 2020. očitovati u 825 000 upražnjenih radnih mjesta u tom području. EU bilježi određeno poboljšanje u stjecanju osnovnih digitalnih vještina među građanima (porast sa 55 % na 59 % stanovništva), ali pred nama je još dalek put. Potrebno je podići razinu digitalne

[1] www.digitalnahrvatska.org

osposobljenosti radne snage u svim gospodarskim sektorima i među tražiteljima zaposlenja kako bi se poboljšali njihovi izgledi na tržištu rada.

Promjene su nužne kako bi se sustav obrazovanja i osposobljavanja prilagodio tijeku digitalne revolucije. Pri uvođenju tih promjena mogu se iskoristiti iskustva inicijativa na razini EU-a poput „Velike koalicije za radna mjesta u digitalnom sektoru", „Europskog tjedna programiranja", i „Otvaranja obrazovanja".Odgovornost za obrazovne programe u rukama je država članica i one moraju hitno riješiti problem nedostatka ključnih digitalnih vještina. Komisija će poduprijeti njihove napore i, u skladu sa svojom ulogom, raditi na unapređivanju priznavanja digitalnih vještina i kvalifikacija te povećanju razine profesionalizma IKT-a u Europi.

2.3.Digitalna agenda za Europu 2010.-2020.

Prepreke za razvoj digitalnog tržišta

Jedinstveno tržište EU koje je nastalo prije pojave interneta, još uvijek nije potpuno jedinstveno za internet. Na temelju konzultacija s dionicima u sektoru, kao i uvida u Izjavu o Granadi i Rezoluciji Europskog parlamenta, Europske komisije identificirano je sedam glavnih prepreka: fragmentacija digitalnog tržišta, nedostatak interoperabilnost, povećanje cyber kriminala i rizik od niskog povjerenja u mreže, nedostatak investicija od strane mreže, nedovoljna istraživanja i inovacija, nedostatak digitalne pismenosti i vještina, te propuštene prilike u rješavanju društvenog izazova.

Europska Komisija pratit će pojavu novih prepreka i reagirati u skladu s tim. Činjenica je da 30% Europljana nikada nije koristilo internet. Također, EU troši na istraživanje ICT samo 40% od razine u SAD-u, tj. 37000000000 u odnosu na 88 milijardi eura u 2007. godini. Te prepreke pokazuju da je u tom području EU zaostaje svojim industrijskim partnerima poput SAD-a, Japana i Južne Koreje.

Stupovi Digitalne agende[2]:

- *Vitalno jedinstveno digitalno tržište* - Od deset transakcija elektronske trgovine manje od jedne su prekogranične, a Europljanima je često jednostavnije da obavljaju prekogranične transakcije sa poduzećem iz Sjedinjenih Američkih Država nego sa poduzećem iz druge europske zemlje.
- *Interoperabilnost i standardi* - Kako bi se potpuno iskoristila upotreba IKT, potrebno je poboljšati interoperabilnost između uređaja, aplikacija, spremišta podataka, usluga i mreža.
- *Povjerenje i sigurnost* - Pravo na privatnost i na zaštitu osobnih podataka su osnovna prava u EU, koja se moraju i na internetu efikasno provoditi upotrebom najšireg opsega sredstava: od širokih aplikacija principa „privatnost u dizajnu" u relevantnim informatičkim tehnologijama, do odgovarajućih sankcija gdje bude potrebno.

[2] Hodžić,A.(2014): Pregled strategije digitalna agenda za Europu 2010.-2020.

- *Brzi i ultra brzi pristup internetu* - Europi je potreban široko pristupačan i cijenovno konkurentan brzi i ultra brzi pristup internetu.U tu svrhu Europska komisija namjerava usvojiti Komunikaciju koja daje zajednički okvir unutar kojeg će se razvijati planovi EU i planovi zemalja članica kako bi se dostigli ciljevi Strategije Europe 2020.
- *Istraživanje i inovacije* - Akcije koje bi zemlje članice trebale poduzeti su da se do 2020. udvostruči ukupna javna potrošnja na IKT istraživanja i razvoj sa 5,5 milijardi EUR na 11 milijardi EUR (što uključuje i EU programe), u smislu da to utječe na ekvivalentan porast u privatnoj potrošnji sa 35 milijardi EUR na 70 milijardi EUR.
- *Poboljšanje digitalne pismenosti, vještina i inkluzije* - Jedna od ključnih akcija koje će Europska komisija poduzeti je predlaganje digitalne pismenosti i kompetencija kao prioritet za propise Europskog socijalnog fonda (2014-2020).
- *Koristi od informacijsko-telekomunikacijskih tehnologija za EU društvo* - Digitalno društvo treba osmisliti kao društvo sa boljim ishodom za sve.Suradnja između IKT industrije, ostalih sektora i vlasti je bitna za ubrzanje razvoja i rasprostranjenost rješenja zasnovanih na informacijsko-komunikacijskim tehnologijama (građevinarstvo, energija, transport).

3. Sudionici internetskog poslovanja

3.1.Anonimnost sudionika internetskog poslovanja

Opće je poznato da je Internet već davno izgubio svoju neutralnost. Više se nije moguće spojiti na „mrežu svih mreža“ i ostati anoniman kao što se moglo prije. Razlog tome je što vas svi pokušavaju nadzirati – vaš Internet poslužitelj koji bilježi sve što treba i što ne treba.

VPN ili „virtual private network“ je grupa računala umreženih preko javne mreže ili Interneta. To znači da više ne morate imati računala fizički na jednom mjestu, nego na bilo kojoj lokaciji u svijetu ali da možete imati sve povlastice lokalne mreže. Ovaj koncept se često koristi u raznim poduzećima jer dozvoljava korisnicima da se i od kuće spoje VPN-om u poslovnu mrežu i da mogu pristupiti računalnim resursima kompanije. Najčešće se radi o pristupanju serverima kompanije gdje se nalaze povjerljivi podaci koji se koriste u poslovanju. Međutim,VPN ima još jednu funkciju, a to je da zaštiti vašu konekciju od drugih sudionika na Internetu,odnosno, da zaštiti vaše podatke od neke treće osobe. Ta „treća osoba“ može biti ISP ili neka druga kompanija koja želi vidjeti vaš Internet promet.

VPN je idealan i kada koristite vaš mobilni uređaj.Zbog toga što su mobiteli danas izuzetno ranjivi, pogotovo što se svi mi spajamo na javne Wi-Fi mreže kako bi uštedjeli koji megabajt, a zapravo tako riskiramo krađu svih naših podataka koje imamo na mobitelu. Mnoge „javne“

wi-fi mreže su pune sigurnosnih rupa i tko zna što se sve može dogoditi ako je taj wi-fi postavio netko tko zna što radi i tko se malo bolje razumije u računalne mreže. U ovom slučaju je jedino prihvatljivo rješenje – VPN.

Skupine VPN korisnika

Postoje 4 skupine VPN korisnika[3]:

- Studenti i osobe koji rade –VPN se koristi u poslovanju jer na taj način imate mnoge povlastice koje inače ne biste imali.Neke od povlastica su pristup resursima kompanije, sigurna konekcija bez straha od toga da vam netko ukrade podatke, možete raditi i od kuće, ne morate prenositi poslovne podatke USB stickom sa poslovnog na privatno računalo itd. Mnogi studenti također koriste VPN kako bi pristupili resursima fakulteta i kako bi se mogli spajati na Internet sa nesigurnih javnih mreža.
- Osobe koje skidaju puno sadržaja – Bez obzira da li sa Interneta skidate legalan ili ilegalan sadržaj, ne želite da netko vidi što vi radite u slobodno vrijeme. U tome slučaju VPN je idealan jer nitko ne vidi vaš Internet promet i možete danonoćno skidati materijale sa raznih torrent stranica. Svaka druga „zaštita“, osim VPN-a, je najčešće prijevara i ne možete biti sigurni da ste zaštićeni.
- Osobe koje se brinu za sigurnost – Ljudi u zadnje vrijeme sve više paze na sigurnost i postali su svjesni opasnosti koje vrebaju na Internetu. Bez obzira da li imaju što za skrivati ili ne, ljudi više ne žele dati podatke „na pladnju“ raznim kompanijama i na ovaj način se pokušavaju zaštititi.
- Osobe koji žive u zemljama kao što je Hrvatska – u Hrvatskoj su mnoge Internet usluge prilično ograničene, odnosno ne možete im pristupiti. Neke od njih su Hulu, Netflix, razne Internet televizije,… Kada koristite VPN, možete se spojiti „iz bilo koje zemlje na svijetu“ i tako zaobići filtriranje po IP adresi koje vas je zapravo i blokiralo u pristupanju spomenutim servisima.

Prednosti i mane VPN-a[4]:

- Sigurnost –VPN je sigurnosni tunel koji ima iznimno visok stupanj zaštite i velika većina VPN pružatelja usluge će učiniti sve da budete 100% zaštićeni i anonimni na

[3] http://pcchip.hr/internet/vpn-privatnost-i-sigurna-internet-veza/
[4] http://pcchip.hr/internet/vpn-privatnost-i-sigurna-internet-veza/

Internetu. Odnosno, učiniti će se da se vi više ne brinete o sigurnosti i da Internet koristite bez ikakvih sumnji, iako uvijek treba biti oprezan.

- Cijena –Cijena VPN-a za velike kompanije je prilično manja nego da se koristi neka druga vrsta zaštite, a daje sve ono što kompaniji treba. Kada se radi o privatnim korisnicima, cijene variraju. Cijene VPN usluge mogu koštati svega 3-4 dolara mjesečno, dok neke koštaju i do 14-15 dolara.
  Realno gledajući, to je mala cijena za anonimnost na Internetu, no i dalje prevelika cijena da bi se veći broj korisnika odlučio na godišnju pretplatu i uz pretplatu za Internet plaćao još i ovu uslugu.
- Fleksibilnost – VPN mreže su prilično fleksibilne, odnosno mogu se koristiti na svim uređajima koji se spajaju na Internet.Glavni uređaji su vaše računalo i mobilni uređaj, a važno je napomenuti da operativni sustav ne igra nikakvu ulogu u tome.

3.1.1.Web preglednici

Tijekom nekoliko godina preglednici su se mnogo razvili i prestali su biti samo aplikacija za otvaranje i pregledavanje web sadržaja. Danas su web preglednici postali prozor u magičan svijet Interneta uz pomoć kojeg dobivate zabavu, multimediju, rješavate stvari vezane uz posao, postajete produktivni i slično.

Dva najvažnija preglednika:

- Chrome
- Thor

- Chrome-Postoji nekoliko debata o tome koji je web preglednik najbolji, odnosno koji nudi najviše svojim korisnicima.Mogli bismo reći da je *Chrome* među 3 najbolja na svijetu. Chrome svoju popularnost može zahvaliti čistom i ulaštenom korisničkom sučelju i lakoći korištenja, te „skrivenim“ mogućnostima o kojima često niti ne razmišljamo, a ponekad ih koristimo.

  Neke od skrivenih mogućnosti[5]:

  - „Incognito mode“- dozvoljava nam „relativno“ anonimno surfanje, odnosno korištenje tog moda ne ostavlja trag na računalu da smo nešto posjetili. I dalje

[5] http://pcchip.hr/internet/skrivene-mogucnosti-google-chromea-kao-npr-skrivena-t-rex-igrica

će nam biti vidljiva IP adresa i sve ostalo, ali na računalu nećemo ostaviti nikakav trag da smo posjetili određene web stranice.

- Kreirajte sigurni profil za vaše dijete-ako imate djecu koja su već počela koristiti Internet, možete im napraviti profil za njihovo surfanje.Sve što trebate je klikniti na postavke – osobe – dodaj osobu (settings – people – add person), te kreirajte profil. Morate biti samo sigurni da ste označili opciju „Control and view the website this person visits from [vaš račun]“.Nakon 5-10 minuta će vam doći e-mail koji će vas odvesti na „administratorsku“ stranicu.Na njoj ćete moći blokirati određene stranice, ograničiti pristup određenim funkcijama, te vidjeti što je podređeni profil posjećivao na netu.
- Brzo brisanje historyja-ako ikada poželite obrisati history, to možete učiniti na dva način – brži i sporiji. Sporiji način je da otvorite settings, nađete opciju za brisanje historyja, odaberete što sve želite obrisati, označite i obrišete. Brži način je da stisnete kombinaciju tipki CTRL + SHIFT + DELETE.Otvara vam se prozor, odaberete samo od kada želite obrisati history.

- Thor- Mnogi korisnici koji traže osjećaj privatnosti se okreću Tor-u. Motivi za korištenje Tor-a, koji prilikom surafanja, distribuira vaš dolazni i odlazni promet kroz niz virtualnih tunela i na taj način štiti vašu privatnost. Koncept Tor-a, kao i konfiguriranje računala za slanje i primanje paketa u mreži postaje sve raširenije i prihvaćenije širom svijeta. Ako odaberete “Tor Browser Bundle” programski paket, dobit ćete najlakšu verziju instalacije, koja zahtjeva vaše minimalne intervencije prilikom instalacije.Da Tor misli ozbiljno, kada je u pitanju vaša anonimnosti, govori i podatak da prije same instalacije na vaše računalo možete provjeriti autentičnost skinute datoteke Tor Browsera. Kako biste bili sigurni da ste dobili željeni paket, možete verificirati digitalni potpis na preuzetom paketu prije nego što ga počnete koristiti.

3.1.2.Skidanje torrenta anonimno

U zadnje vrijeme događa se represija razno raznih agencija na ljude koji na bilo koji način sudjeluju u razmjeni podataka putem torrenta. To su svi oni koji skidaju torrente, postavljaju torrente online kako bi ih vi mogli skinuti i onih koji održavaju stranice za pretragu torrenta. Svi u tome lancu su krivi po određenim zakonima u svojim državama.

Mi u Hrvatskoj bi trebali odgovarati po hrvatskim zakonima, Austrijanci po austrijskim zakonima, a Amerikanci po američkim zakonima. Naravno, što se nalazite u „liberalnijoj zemlji" (op.a. kao što je Amerika), to ćete gore proći. Njihovi sudovi znaju pojedinca osuditi na kazne od 100-200 tisuća dolara za jedan skinuti glazbeni CD kao primjer drugima.

Vi kada skidate torrente (i dijelite ih drugima) ste ranjivi. Vaša IP adresa je vidljiva i lako vas mogu naći. Kompanija koja se bori protiv piratstva može, recimo, staviti glazbeni CD (koji je u njihovom vlasništvu) na torrente i gledati po IP adresama tko skida glazbu. Zatim vas sve po tim IP adresama naći.

Zato postoji način kako se zaštititi odnosno kako skidati torrente, a da vaša IP adresa ne bude javna i njima dostupna. Neke opcije su besplatne, neke nisu, no par dolara mjesečno je mala cijena naspram moguće velike kazne. U Hrvatskoj baš i nije bilo slučajeva da su ljudi zbog piratstva plaćali milijun kuna kazne, ali zasigurno ima pojedinaca koji su morali platiti softver koji su ilegalno skinuli.

Načini skidanja torrenta anonimno[6]:

- VPN- Zašto bi vaš Internet provider morao znati da ste cijeli dan na Internetu, da ste 15 puta u danu posjetili neki portal … ? VPN vam omogućuje sigurnost i anonimnost na internetu. Većina VPN providera vam ne ograničava skidanje torrenata, stoga možete bez problema uključiti VPN i staviti skidanje torrenta i „s druge strane" se neće vidjeti vaša IP adresa, nego IP adresa VPN servisa.
- BTGuard- je alat koji vam nudi da budete anonimni na Internetu. Zapravo BTGuard je firma koja ima u ponudi dva proizvoda, a oba vam nude sličnu mogućnost -da ostanete anonimni na Internetu. BTGuard nudi proxy uslugu i VPN uslugu. Proxy usluga je zapravo usluga namijenjena isključivo za skidanje torrenta.
- Torrentprivacy- proxy servis koji je namijenjen isključivo korisnicima BitTorrenta. Jedina loša strana svega toga je što ste ograničeni na Windowse, odnosno od ovoga mogu profitirati samo Windows korisnici.
- Anomos- je samostalni klijent za skidanje torrenata kojeg možete skinuti sa Interneta. Anomos je izrazito lako za koristiti, a koristite ga kao i sve druge torrente klijente.Ono što je „loše" kod Anomosa je nešto sporija brzina skidanja torrenata, nego sa klasičnim torrent klijentom.
- Seedbox- je udaljeni server koji vi možete iznajmiti i tada mu samo vi možete pristupiti. Na taj udaljeni server se stavlja torrent klijent.Pomoću njega skidate

[6] http://pcchip.hr/internet/torrent-5-nacina-kako-skidati-torrente-anonimno/

torrent datoteke, otvarate ih u klijentu za skidanje datoteka preko torrenta i podaci se pohranjuju na seedbox. Znači, ako netko i prati IP adrese, neće vidjeti vašu IP adresu, nego adresu seedboxa.

3.1.3.Nasilje preko interneta i načini internet prijevare

Nasilje preko interneta, koje je u svijetu poznato kao cyberbullying, opći je pojam za svaku komunikacijsku aktivnost cyber tehnologijom koja se može smatrati štetnom kako za pojedinca, tako i za opće dobro.Ovim oblikom nasilja među vršnjacima obuhvaćene su situacije kad je dijete ili tinejdžer izloženo napadu drugog djeteta, tinejdžera ili grupe djece, putem interneta ili mobilnog telefona. Odnosno i počinitelj(i) i žrtva(e) su maloljetnici.

Postoje dvije vrste nasilja preko interneta: izravan napad i napad preko posrednika.

Izravan napad događa se kad maloljetnik:

- šalje uznemirujuće poruke mobitelom, e-mailom ili na chatu,
- ukrade ili promijeni lozinku za e-mail ili nadimak na chatu,
- objavljuje privatne podatke ili neistine na chatu, blogu ili internetskoj stranici,
- šalje uznemirujuće slike putem e-maila ili MMS poruka na mobitelu,
- postavlja internetske ankete o žrtvi,
- šalje viruse na e-mail ili mobitel.

Nasilje preko posrednika događa se kad počinitelj napada žrtvu preko treće osobe, koja toga najčešće nije svjesna.

Primjerice, neko dijete dozna lozinku drugog djeteta za njegovu e-mail adresu ili nadimak na chatu. Tako s njegove e-mail adrese može slati uznemirujuće poruke njegovim prijateljima, ostavljati neprimjerene poruke na blogu, chatu ili forumu. Svima se tako čini da je žrtva zapravo ta koja čini loše stvari. Prijatelji će se posvađati s njime, administrator će isključiti njegov nadimak ili e-mail adresu, roditelji će se naljutiti na njega i bit će kažnjen. Oni su posrednici u zlostavljanju, a toga nisu ni svjesni.

Iako je provedeno malo istraživanja na temu međuvršnjačkog nasilja putem interneta, rezultati su vrlo zanimljivi. Naime, čak *18 %* djece u dobi od 12 do 14 godina bilo je žrtva nekog od oblika nasilja preko interneta, a *11 %* njih izjasnilo se kao "internet nasilnici". Od djece koja su bila izložena učestalom nasilju na internetu, njih *62 %* izjavilo je kako je nasilnik bio njima poznata osoba ili čak kolega iz razreda. Uz to, djevojčice su češće žrtve, ali i češći nasilnici na internetu od dječaka.

Internetski bullying uključuje populaciju koja je većim dijelom srednja klasa, djecu najčešće poznatu kao "dobru " ili "one od kojih bismo najmanje očekivali" zlostavljanje ili ponižavanje drugih. Internet izaziva neobuzdano ponašanje dijelom i zbog činjenice da je riječ o "sivom području" društvene interakcije.

Nasilje na chatu-Chat je vrlo popularan kod mladih, pa je stoga i privlačan osobama koje ga žele zloporabiti. Zloporaba vršnjaka najčešće uključuje prijeteće ili ucjenjujuće poruke koje jedno dijete ili više njih upućuje drugom djetetu. U takvim situacijama treba biti oprezan jer nasilnik može biti doista opasna osoba.

Nasilje na forumu-Od svih oblika komunikacije na internetu, forumi su najčešće najbolje organizirani. Na njima se nalaze administrator (jedan ili više njih) i moderatori, zaduženi za posebne dijelove foruma. Oni čitaju sve teme i diskusije te paze da ne bude vrijeđanja, prijetnji, objavljivanja privatnih podataka i kršenja prava.

Nasilje putem bloga-Nasilje putem blogova odnosi se ponajprije na "otimanje" blogova drugim ljudima (žrtvama) te nadopunjavanje osobnim uvredama i/ili seksualnim sadržajima. Takvim se oblikom nasilja narušava ugled i ugrožava privatnost druge osobe. Toj vrsti međuvršnjačkog nasilja posebno su podložna djeca koja šalju fotografije i osobne podatke s ciljem da pronađu prijatelje na internetu.

Najčešći načini internet prijevare

Internet sam po sebi nije opasan, no kada se spoje neiskustvo i naivnost pojedinih korisnika onda smo na prilično skliskom terenu. Nažalost, ima pojedinaca koji nasjednu na razne Internet prijevare i sretni su ako prođu samo sa par stotina izgubljenih kuna.

Najčešći načini prijevara[7]:

- Nigerijska prijevara-Godinama na Internetu kruži nekoliko varijanti Nigerijskog pisma (poznatog i kao prijevara "419"- broj 419 označava nigerijski zakon koji ova poruka krši – zakon o online prijevari). Osoba je jedva došla do vaše e-mail adrese i treba uslugu. Ponekad je ta osoba ženska osoba koja je naslijedila milijune (pa čak i milijarde) dolara od pokojnog supruga i treba vas da joj pomognete prebaciti novce iz

[7] http://www.binaryoptions.com.hr/5-najcescih-prijevara-na-internetu/

Nigerije u Europu ili Ameriku. Ako joj pomognete da to napravi, dobiti ćete dio "kolača". U svakoj varijanti vam obećavaju drugu svotu, no uvijek se spominje određeni postotak, a kako se radi o velikoj sumi novca, zvuči lijepo da za pola sata ili sat posla dobijete na desetke tisuća dolara.

Ovdje se igra na emocije ljudi koji žele brzu zaradu i na one ljude koji nemaju puno iskustva sa Internetom ili prijevarama na Internetu.Ima jako puno ljudi koji će nasjesti na ovo i odgovoriti na e-mail poruku. Naravno, ponekad to nisu ženske osobe nego bogati naftaši iz Nigerije. Kada odgovorite na ovaj e-mail, dobiti ćete detaljne upute o tome da toj određenoj osobi trebaju detalji o vašem bankovnom računu – ime, prezime, ime banke, broj banke, broj vašeg računa, informacija koliko točno imate novaca na računu i slično.

Kada im to uplatite, ako uplatite, tražiti će vas još novca… i tako dok vi ne posumnjate da je to prijevara. Na ovaj način izvučeno je jako puno novaca, sudeći po podacima koje je dao FBI. Prosječna žrtva izgubila je oko 3000 dolara, a mnogi su i ubijeni kada su malo dublje zakopali u ovaj slučaj i išli u "potragu" za osobom kojoj su uplatili novac.

- Dobili ste ogroman dobitak na lutriji-Druga Internet prijevara koja se često događa – otvarate svoj e-mail pretinac i vidite poruku u kojoj ste dobili milijune dolara na nekoj stranoj loto igri. Postoji nekoliko varijanti ove e-mail prijevare, no prilično su slične. Vaša email adresa je ubačena u "nagradni bazen" i vi ste izvučeni za veliki dobitak. Niste se morali prijaviti, oni su sami vas prijavili i žele vam dati novce. To je već prva stvar koja bi vam trebala biti sumnjiva – od kuda su oni uzeli te adrese? Da li je Google ili Microsoft prodao vaše adrese? Ako to i zanemarimo – u drugom e-mailu će vas tražiti vaše podatke. Kao i kod Nigerijske prijevare – vaše ime, prezime, banku, račun itd.

  Nakon toga ćete morati uplatiti par tisuća dolara za naknadu nakon koje će vam novci doći na račun. Neki će pomisliti, osvojio sam milijune, što je par tisuća dolara i uplatiti će na nepoznati račun te novce. Naravno, nakon toga vam se više neće javiti, nego će pokupiti vaše novce.Po čemu možete znati da je riječ zasigurno o prijevari? Osim što niste odigrali lutriju i što je vaša adresa baš "slučajno" izvučena. Pošiljatelj je osoba, a ne loto agencija. Nadalje, vaše ime nije u "To" polju, ako proguglate lutriju vidjeti ćete da takva lutrija ne postoji,te ako zatražite bilo kakve dodatne informacije nećete ih dobiti. Uostalom, držite se jednostavnog savjeta – lutriju koju ne igrate ne možete

dobiti i to je to. Možete uostalom igrati samo hrvatsku lutriju i europsku lutriju. Ne možete sudjelovati u nekim drugim stranim lutrijama, a pogotovo ne bez vlastitog znanja.

- Anketa-Najčešće se radi o nekim "socijalnim" pitanjima kao što su globalno zatopljenje ili rat na bliskom istoku, no kada ih otvorite shvatite da je nešto drugo u igri. Zapravo, postoje dva scenarija.

  Prvi je normalna anketa koja u pravilu ima oko 5-15 kratkih pitanja, ali vas na kraju dočeka obrazac koji morate popuniti. I tu se traži ogromna količina vaših podataka. Često je taj obrazac opširniji nego anketa. Traže se vaši podaci, na kojim društvenim mrežama imate profil, da li posjedujete PayPal i slične račune… ne traže vas nigdje šifru, no ako znaju gdje imate profil i ako znaju vašu e-mail adresu (koju traže u tom obrascu) mogu vam pokušati ukrasti identitet, te provaliti u e-mail pretinac i slično.

  Drugi način prijevare je da kad kliknete na anketu, zapravo povučete i spyware na računalo koji prikupla vaše podatke, šifre i ostale osjetljive podatke i na taj način vam opet ukradu identitet. Većina tih anketa je zapravo krađa identiteta i vaših podataka. Možda na taj način neki pojedinci skupljaju puno podataka koje kasnije prodaju raznim agencijama. Ne oštete vas direktno, zarade pristojnu svotu novca, a vi imate hrpu reklama u svom inboxu, te ste postali predmet automatizirane obrade ljudi. U svakom slučaju nije dobro.

- "PayPal" prijevara-u Hrvatskoj postoji veliki broj ljudi koji se boje kupovati na Internetu, ali i postoji značajan broj ljudi koji se ipak upustio u to i koristi sve blagodati Interneta. Kada imate PayPal račun, otvara vam se mogućnost kupovine mnogih predmeta preko Interneta i cijelu kupnju možete obaviti iz svoje sobe. Dovoljno vam je samo sjesti za računalo, odabrati što želite kupiti i platiti taj isti predmet preko svoje kartice ili PayPala. I to je dobro dok kupujete sa provjerenih web stranica kao što su eBay i slične.
  No što kada vam počnu dolaziti e-mail poruke od "PayPala" sa naslovima poput "Vaš račun će biti izbrisan ", mnogi korisnici se odmah uspaniče. Piše da je pošiljatelj PayPal i ne gledaju jesu li stvarno to oni. U pravilu nisu! Naravno, odmah stisnu na link koji im je došao u poruci i upisuju podatke od svog PayPal računa jer stranica

izgleda kao da je stvarno naslovna stranica PayPala. I samim time što ste upisali podatke na lažnoj web stranici, poslali ste cyber kriminalcima svoje podatke.

- Radite od kuće i zaradite novce-zadnji vrlo popularan način prijevare je ljudima ponuditi posao koji će raditi od kuće i na taj način zaraditi.Možete raditi kad hoćete, sve što vam treba je računalo, ne morate izlaziti iz kuće i k tome ćete još zaraditi više nego neki ljudi koji se ubijaju od posla svaki dan. Zvuči predobro da bi bilo istinito.Nažalost, mnogi misle da je tako nešto moguće i odluče prihvatiti "posao".

  Također, postoji i scenarij u kojem vi morate platiti 100-ak dolara za neku naknadu da vas oni mogu prijaviti da radite za njih, ali će vam se to brzo isplatiti jer možete zarađivati toliko novca dnevno. Ukratko – nitko vam neće dati 100 dolara dnevno da sjedite doma, surfate po Internetu i javljate im o popustima koje ste našli na Internetu, da stišćete određene reklame ili da sudjelujete u raspravama na forumu. Nadalje, neki oglasi ovog tipa zahtijevaju da kupite komad hardvera ili softvera kako biste mogli obavljati posao. Kada ga kupite, više se neće javiti niti postoji kakav posao.

3.2.Primjeri anonimnosti internetskog poslovanja

Engleska-Da bi uveli kontrolu i pokušali smanjiti broj online prijestupnika, Londonska policija se odlučila na stvaranje posebnog odjela koji će biti zadužen samo za suzbijanje online nasilja.Osnovni cilj ovog odreda biti će pomaganje žrtvama nasilja i sprečavanje prijestupnika u njihovim naumima. Iako Londonska policija ne želi javnosti prezentirati detalje, jasno je kako se radi o velikom izdatku, ali koji bi vrlo skoro trebao donijeti nekakav napredak u smanjenju broja online prijestupnika.Sva ta anonimnost uskoro bi mogla postati samo stvar prošlosti jer je velika vjerojatnost da će odjel imati sredstva i znanja kojima će moći raskrinkati zlostavljače.

Estonija- Delfi je jedan od najvećih web-portala u Estoniji, koji daje mogućnost svima da slobodno komentiraju objavljene članke. U siječnju 2006. godine, na portalu je objavljen članak o odluci jedne estonske trajektne kompanije da promijeni rutu putovanja prema određenim otocima što je dovelo do razbijanja leda na površini mora. Mnogi čitatelji su ispod članka napisali uvredljive i prijeteće komentare o trajektnoj kompaniji koja je poslala dopis Delfiju tražeći uklanjanje tih komentara.

Delfi je po prijemu dopisa uklonio sporne komentare, međutim, trajektna kompanija ih je ipak tužila i dobila presudu kojom je utvrđeno da su komentari bili klevetnički, i da je Delfi odgovoran za njih. Trajektnoj kompaniji su dodijeljena simbolička sredstva kao naknada štete na što je Delfi podnio žalbu tvrdeći da se prema zakonima EU ne može smatrati odgovornim za komentare, jer ih ne kontrolira. Vrhovni sud Estonije se nije složio i ustanovio da je Delfi imao kontrolu nad objavljivanjem komentara. Sud je na ovaj način pružio zaštitu svim građanima čija prava krše anonimni komentatori.

Njemačka- Liječnik je tužio jednog korisnika portala jer je "širio lažne informacije o njegovom radu i ordinaciji i spor je dobio, no nakon što je portal sanogo.de uložio žalbu, Vrhovni sud je presudio da se anonimni korisnik može otkriti samo u rijetkim slučajevima i da internetski portal nije dužan otkriti identitet osobe koja je na tom mjestu anonimno komentirala medicinske usluge u Njemačkoj. Korisnik je na portalu napisao da je u ordinaciji na pregled čekao tri sata i da je "gledao kako se bolesnički kartoni i dokumentacija nose u košarama za rublje".Liječnik je sudskim putem zatražio da portal sanogo.de otkrije ime i prezime i adresu čovjeka koji je to napisao.

Portal je odbio otkriti identitet svoga korisnika nakon čega je sud u Stuttgartu presudio u korist liječnika, uz obrazloženje da su ugrožena njegova osobna prava, jer da "nije dopustivo da netko optužuje nekoga, a da pritom ne otkriva svoj identitet". Sanogo.de odbio je otkriti identitet svoga korisnika pozivajući se na Zakon o medijima i uložio je žalbu na presudu. Na kraju je u korist internetskog portala presudio Vrhovni sud.

Rusija- ruske vlasti su odlučile novčano nagraditi svaku osobu koja će detaljno istražiti TOR. Od potencijalnih primaoca nagrade očekuje se da otkriju način kojim će se ukloniti anonimnost korisnika TOR mreže, kao i tehničke pojedinosti o korisnicima i njihovoj opremi koju koriste pri pristupu toj mreži.Prijaviti se smiju isključivo građani s ruskim državljanstvom. Sretnici koji uspiju ostvariti traženo moći će uživati u 111 tisuća američkih dolara za probijanje mreže Tor.Mreža koju stvara softver postala je vrlo popularna među novinarima, različitim aktivistima, ali i korisnicima koji jednostavno žele biti anonimni. Ipak, anonimnost je i kriminalcima osigurala mjesto boravka. Samo u Rusiji ovu platformu koristi više od 200 tisuća korisnika, a tamošnje vlasti navodno nisu prve koje opako žele ući u sustav.

Kina-Svi koji žele pristup fiksnoj telefonskoj liniji i mobilnom internetu u Kini ubuduće će se morati registrirati. Povjerenstvo parlamenta zemlje s najviše korisnika interneta na svijetu razmatra zakon koji će obvezati registraciju svih korisnika imenom i prezimenom. Ako zakon bude prihvaćen, bit će to drugi koji je Kina usvojila od 2000. godine, a da se bavi regulacijom interneta. Tada je usvojen zakon o održavanju sigurnosti na webu.
Cenzura interneta u Kini već je sad jedna od najstrožih na svijetu. Vlasti blokiraju pristup pornografiji, kockanju i sadržaju kojim se kritizira vladajuća Komunistička partija. Početkom 2015. godine uveli su obvezu registriranja pravim imenom i prezimenom za mikroblogere. Uhitili su šest mikroblogera pod optužbom za širenje glasina o državnom udaru u Pekingu.

Iran- Iranska vlada namjerava (ponovo) pokrenuti nacionalni intranet kojega nazivaju i „čistim Internetom“ koji bi za većinu korisnika bio odsječen od Interneta. Ukoliko se, pak, to provede u djelo, mnogi bi uobičajeni internetski sadržaji ostali posve blokirani, a bilo kakva anonimnost u komunikaciji bi vjerojatno nestala.
Na taj način bi Google,Hotmail i druge poznate globalne stranice bile nedostupne korisnicima u Iranu, a njih bi zamijenilo državni servis kao što je Iran Mail. Korisnici e-pošte bi se, pak, trebali registrirati punim imenom i adresom u vladinoj agenciji da bi dobili svoju e-mail adresu kod Iran Maila. Veliki povlašteni korisnici kao što su vladine agencije, burza, velike tvrtke i banke imali bi pristup Internetu, dok bi za obične građane bio dostupan samo „Nacionalni Internet“.Zbog toga mnogi Iranci koriste VPN mreže i proxy servere kako bi zaobišli ovakva ograničenja.

Južna Koreja- je 2007. godine usvojila zakon prema kojem su internet-portali koji imaju visoku posjećenost bili obavezni prikupljati brojeve osobnih karti korisnika kao način praćenja što se postavlja online, a kako bi se smanjio rizik od klevete, lažnih glasina i uvredljivih komentara. Međutim, pet godina nakon toga, i nakon brojnih hakerskih napada i curenja osobnih podataka koji su prikupljani kod internet-portala, Ustavni sud ove zemlje proglasio je ovakvu praksu neustavnom, navodeći da nema dokaza da je ovaj zakon ispunio postavljena očekivanja, te da praksa obaveznog korištenja stvarnog imena smanjiva slobodu govora i obeshrabruje ljude da iskazuju mišljenja zbog straha od kazne. Može se uočiti, dakle, da u online sferi ne postoje jednostavna rješenja, te da rješavanje jednog problema može prouzročiti pojavu nekolicine drugih.

Kanada-tragičan kraj sa ubojstvom 13-godišnje djevojčice u prvi plan je stavio kanadsku aplikaciju Kik koji je poslužio kao kanal između djevojčice i dvoje studenata na sveučilištu Virginia,koji su iskovali i proveli plan njezina ubojstva.Kanadska aplikacija za razmjenu poruka potom je postala sredstvom za međusobni kontakt,a anonimnost koju pruža postavila je ozbiljne prepreke u istrazi slučaja.Prilikom registracije za Kik,dovoljno je unijeti ime,prezime i e-mail adresu koji mogu biti i izmišljeni.Do razotkrivanja počinitelja došlo je nakon što je Kik surađivao s istražiteljima i pritom otkrio sve što zna.

4.Oporezivanje realnih,financijskih i digitalnih transakcija

4.1.Oporezivanje realnih transakcija

Svaka članica EU-a imala je do sedamdesetih godina vlastiti sustav oporezivanja proizvodnje, potrošnje dobara i usluga, što je uvelike otežavalo prekogranično poslovanje te izazivalo narušavanje tržišnog natjecanja. Europska komisija, u suradnji s državama EU-a, radi na kreiranju sustava PDV-a utemeljenoga na odredištu za ukupna dobra i usluge.

Hrvatska je rekorder EU po porezima na potrošnju.U ukupnim poreznim prihodima Hrvatske oporezivanje potrošnje čini 49,1 % .Oporezivanje potrošnje u Hrvatskoj veliko je zbog vrlo visoke stope PDV-a od 25 %, što je nakon Mađarske druga najveća stopa PDV-a u EU.Implicitna porezna stopa na potrošnju u Hrvatskoj iznosila je 29,1 % i bila je druga najveća u Uniji nakon Danske. Ta je vrijednost znatno iznad prosjeka EU od 19,9 %.

Jedno od međunarodno prihvaćenih načela oporezivanja potrošnje jest oporezivanje u zemlji u kojoj nastaje krajnja potrošnja, tj. načelo zemlje odredišta.Načelo oporezivanja prema zemlji odredišta međunarodna je norma, koju podupiru i OECD, EU te Svjetska trgovinska organizacija (WTO).U Europskoj Uniji načelo odredišta robe u međunarodnoj razmjeni uvedeno je 1967 godine. U skladu s načelom oporezivanja prema zemlji odredišta, izvoz je izuzet od oporezivanja, a porez se plaća prema stopi zemlje uvoznice, što znači da se oporezivanje obavlja prema mjestu potrošnje i da porezni prihodi pripadaju zemlji u kojoj nastaje krajnja potrošnja. Smatra se da načelo zemlje odredišta pravednije raspoređuje porezni teret jer krajnja potrošnja bolje odražava korist od javnih dobara nego druge porezne osnovice, kao što je proizvodnja.

4.2.Oporezivanje financijskih transakcija

Svjetsko se financijsko tržište snažno razvijalo u protekla dva desetljeća prije izbijanja ekonomske krize. Četrdeset država primjenjivalo je u 2011 godine neki oblik poreza na financijske transakcije i to najčešće na unilateralnoj osnovi uz mnogo specifičnosti u obliku i načinu oporezivanja. Usprkos toj činjenici relativni prihod od tog poreza je vrlo nizak te jedva dostiže 0,5% BDP-a pojedine zemlje. U posljednjih dvadesetak godina prije gospodarske krize značaj tog oblika oporezivanja se smanjivao jer su države nastojale smanjiti trošak kapitala kako bi poboljšale konkurentnost domaćeg financijskog tržišta.

Predviđa se oporezivanje svih financijskih institucija koje trguju osnovnim ili derivatnim financijskim instrumentima, čak i izvan organiziranih tržišta. Transakcije izvornim instrumentima oporezivale bi se po minimalnoj stopi od 0,1% na iznos transakcije, a transakcije derivatnim instrumentima po minimalnoj stopi od 0,01% na nominalnu vrijednost derivatnog ugovora. Osnovicom oporezivanja smatra se nominalni iznos sklopljenog posla.

Porez na financijske transakcije je primarno usmjeren na oporezivanje financijskih transakcija koje provode financijske institucije, bilo za svoj račun ili za račun neke druge osobe.

Primjena poreza na financijske transakcije ne bi bila ograničena na trgovanja na organiziranim tržištima, već bi obuhvaćala izvanburzovna tržišta što dovodi do povećanja porezne osnovice. Naime, transakcije većih iznosa zbog blažih regulatornih zahtjeva i nižih troškova obično se obavljaju izvan organiziranog tržišta. Oporezivi bi također bili repo poslovi i obrnuti repo poslovi no samo u okviru prve razmjene instrumenta. Povratna transakcija ne bi bila predmetom oporezivanja.

Tablica 1.Prihodi od oporezivanja financijskih transakcija u odabranim članicama EU-a, 2011.

Država	**Prihodi od oporezivanja(u mil.EUR)**	**Udio prihoda u BDP-u(u%)**
Belgija	132,0	0,04
Cipar	1,4	0,01
Finska	249,0	0,13
Francuska	1100,0	0,06
Grčka	92,0	0,04
Irska	322,4	0,21
Luksemburg	605,0	1,41
Malta	2,1	0,03
Ujedinjeno Kraljevstvo	3987,6	0,23

Podaci iz tablice 1. pokazuju na niski iznos prikupljenog poreza,te kako su 2011 godine različiti oblici oporezivanja financijskih transakcija uključujući financijske instrumente postojali u 11 zemalja članica. Premda je Italija već 2011 godine imala određene naznake oporezivanja financijskih transakcija, novi sustav oporezivanja uveden je u ožujku 2013 godine za izvorne vrijednosnice odnosno srpnju iste godine za derivate.

Mogućnosti oporezivanja financijskih transakcija u RH

Hrvatska porezna politika zbog povijesnih razloga, ali i nastojanja povećanja konkurentnosti domaćeg tržišta kapitala izbjegava financijske transakcije. Uzimajući u obzir stabilnost financijskih institucija uz provedene određene regulatorne mjere Hrvatske narodne banke (HNB) državne intervencije u financijski sektor nisu bile potrebne, već je on i u kriznim vremenima izdašno doprinosio javnim financijama.

U 2013 godini nije bilo značajnijih promjena u ukupnoj vrijednosti prometa no može se istaknuti 42 puta veći promet komercijalnih zapisa, te dvostruko veći promet strukturiranim proizvodima u odnosu na 2012 godinu. U 2014 godini nije došlo do značajnog rasta redovnog prometa u ukupnom iznosu. Promet dionica, koji čini gotovo 80% ukupnog prometa, ostao je

na razini iz 2013 godine, promet obveznicama povećan je za 65%, dok je promet strukturiranim proizvodima smanjen za 44%.U 2015 godini je redovni promet smanjen za 9,3%, a OTC trgovanja za 17,8% što ukazuje da je tržište kapitala ulagačima postalo manje atraktivno.

Ukoliko domaće financijske institucije obavljaju oporezive financijske transakcije s financijskim institucijama u zemljama EU ili trguju financijskim instrumentima izdanim u tim zemljama bile bi obvezne platiti FTT u zemlji rezidentnosti suprotne strane odnosno zemlji izvora vrijednosnog papira, što bi dovelo do odljeva prihoda od oporezivanja izvan granica Hrvatske. Stoga bi bila opravdana pojačana suradnja Hrvatske oko pitanja oporezivanja financijskih transakcija kako bi se osiguralo da rezidenti Hrvatske plaćaju porez u svojoj zemlji.

4.3.Oporezivanje digitalnih transakcija

Osim određenih specifičnosti vezano uz uvjete za obavljanje internetske prodaje, internetska prodaja i razni oblici internetske prodaje posebno je zanimljiva s poreznog stajališta, odnosno sa stajališta poreza na dodanu vrijednost.

Internetska prodaja (tzv. prodaja na daljinu) je oporeziva PDV-om jednako kao i prodaja u klasičnim prodavaonicama. Specifičnosti o kojima treba voditi računa najčešće se javljaju kada je kupac iz druge članice EU ili treće zemlje. Tako internetski prodavatelj iz RH koji prodaje i isporučuje robu kupcu - poreznom obvezniku u drugu državu članicu EU, neće se zaračunati hrvatski PDV, već će se primijeniti prijenos porezne obveze pri čemu će PDV svoje zemlje obračunati kupac. Ukoliko prodavatelj iz RH isporučuje dobra kupcu u trećoj zemlji, takve (izvozne) isporuke su oslobođene PDV-a.

Kod prodaje robe fizičkim osobama, odnosno osobama koje nisu registrirane za PDV u drugim državama članica EU, takva isporuka se oporezuje hrvatskim PDV-om. Međutim, takvo oporezivanje primjenjuje se samo do prelaska tzv. praga vrijednosti isporuke u dotičnoj zemlji. Prag isporuke predstavlja određenu vrijednost robe koju prodavatelj kod prodaje na daljinu isporuči kroz tekuću ili prošlu godinu u drugu državu članicu EU.

Tablica 2.Prag isporuke po pojedinim zemljama

Zemlja	**Prag isporuke**
Hrvatska	270 000 HRK
Austrija	35 000 EUR
Belgija	35 000 EUR
Italija	35 000 EUR
Mađarska	35 000 EUR
Nizozemska	100 000 EUR
Njemačka	100 000 EUR
Slovenija	35 000 EUR

Što se tiče oporezivanja transakcija između poduzetnika (eng. *business to business*– elektronička trgovina B2B), Europska Unija (EU) i Organizacija za ekonomsku suradnju i razvoj (OECD) slažu se da je model samooporezivanja najprihvatljiviji u te svrhe. Za prikupljanje poreza od krajnjeg potrošača u EU-u se primjenjuje model registracije stranog isporučitelja kad obavlja prodaju unutar EU-a. Taj je model preporučila i Organizacija za ekonomsku suradnju i razvoj (OECD), ali samo kao kratkoročno rješenje. Naime, stvarni je problem sadašnjeg modela nemogućnost nametanja obveze plaćanja poreza stranim dobavljačima jer ih je teško identificirati, jednako kao što je teško identificirati kupce, tj. odrediti njihovu lokaciju.

MasterCard pokreće rast sigurnih digitalnih transakcija

MasterCard usluga za digitalna plaćanja pokreće rast sigurnih digitalnih transakcija diljem Europe uz više od 60 projekata u tijeku.

Usvajanje digitalnog plaćanja nastavlja rasti diljem svijeta, a MasterCard predviđa da će do 2020. godine 38 % plaćanja u Europi biti digitalno. MasterCard usluga za digitalna plaćanja omogućava potrošačima sigurna digitalna plaćanja.
Još od 2014 godine kada je Apple Pay uveden u SAD-u, izdavatelji kartica i pružatelji usluga digitalnih novčanika provode MDES projekte u 18 zemalja diljem Europe – u Ujedinjenom Kraljevstvu, MDES povezuje banke koje predstavljaju više od 70% korisnika računa s uslugom Apple Pay. Među pružateljima usluga digitalnog novčanika koji se povezuju s MDES-om, Google je nedavno najavio da će lansirati Android Pay u Ujedinjenom Kraljevstvu.

MDES je temelj postignutog napretka u omogućavanju sigurnih digitalnih transakcija uz koje korisnici mogu plaćati gdje i kako žele te biti sigurni da njihova transakcija ili informacije o plaćanju nisu u opasnosti.Korisnici će imati sve veći izbor pri korištenju kartica u digitaliziranom obliku kako pružatelji usluga digitalnih novčanika budu donosili svoja rješenja na tržište.

Hrvatski Bitcoin Portal

Bitcon je prva decentralizirana digitalna valuta ili način plaćanja.Funkcionira kao sustav kroz koji korisnici transakcije provode direktno, bez treće strane, odnosno posrednika. S obzirom na to da je bitcoin zamišljen kao virtualno zlato, može ga se "iskopavati" po internetu.Bitcoin novčanik sadrži tajni dio podataka koji se zove privatni ključ ili *sjeme,* a njime se potpisuju transakcije pružajući matematički dokaz da je taj ključ došao od vlasnika novčanika. Taj potpis isto tako osigurava da se transakcija ne može promijeniti jednom kad je izdana. Da bi se izvršila transakcija nekog određenog iznosa bitcoinova sa jednog digitalnog novčanika na drugi, potrebne su vam tri stvari[8]:

- Adresa- možete je smatrati kao svoj privatni bankovni račun, ali da biste došli do nje, ne treba vam brdo papirologije i odobrenja, već odete na za to predviđene pružatelje te je postavite u nekoliko sekundi. Adrese su generirane određenim postupkom te izgledaju kao nasumična kombinacija slova i brojeva, jedinstvene su i povezane na taj račun.
- Privatni ključ- je tajni dio podataka koji dokazuje vaše pravo da možete prenositi bitcoinove s određenog novčanika pomoću kriptografskog potpisa. Ti privatni ključevi spremaju se na vašem računalu, ako koristite softwerski novčanik, ili na serveru, ako koristite web novčanik.
- Kriptografski potpis- je matematički mehanizam koji omogućuje osobi da dokaže da je jedinstveni vlasnik te adrese, odnosno novčanika. Kada Bitcoin software potpiše transakciju odgovarajućim privatnim ključem, cijela Bitcoin mreža može vidjeti da taj potpis odgovara transakciji koja se izvršava, ali je zato nemoguće vidjeti privatni ključ koji zaštićuje vaš račun.

[8] http://crobitcoin.com/bitcoin/transakcije/

Ukupna vrijednost transakcija putem interneta u 2015 godini iznosila je 1.5 milijardi kuna, a u 2014 godini približno 1 milijardu kuna. Pokazali su to najnoviji podaci Hrvatske narodne banke koji potvrđuju rast e-trgovine, i to ne računajući online narudžbe kod kojih se plaća pouzećem ili virmanom. Svaka dva od tri hrvatska potrošača na internetu traži informacije o proizvodima i uslugama, što je isti omjer kao i u EU.

Pokazatelji digitalnog bankarstva

58 % zapadnih Europljana preferira digitalne kanale pred odlaskom u poslovnicu, stanovnici Sjeverne Europe čak 85 %, a samo 52 % Amerikanaca prihvaća digitalni način bankovnih transakcija.2014 godine u svijetu je zabilježeno 390 milijardi bezgotovinskih platežnih transakcija.Time je njihov broj poskočio 9% u odnosu na 2013 godinu kada je uvećan 7,6%.Među pojedinim regijama najviše je prema procjenama poskočio broj bezgotovinskih transakcija u azijskim gospodarstvima u nastajanju, za čak 27 %, prvenstveno zahvaljujući širenju Interneta i mobilnog plaćanja u Kini i Indiji.

Tablica 3. Države koje najviše upotrebljavaju digitalni način plaćanja

Države	**Udio ukupnog plaćanja potrošača**	**Plaćanje debitnom karticom**
Belgija	93%	86%
Francuska	92%	69%
Kanada	90%	88%
Ujedinjeno Kraljevstvo	89%	88%
Švedska	89%	96%
Australija	86%	79%
Nizozemska	85%	98%
SAD	80%	72%
Njemačka	76%	88%
Južna Koreja	70%	58%

4.4.Pravila za identifikaciju isporučitelja i primatelja usluga

Identifikacija isporučitelja usluga

Pravilo oporezivanja usluga nalaže nam da je za usluge koje se pružaju krajnjim kupcima obveznik PDV-a isporučitelj usluge.Zbog specifičnosti digitalnih usluga, vrlo je teško utvrditi sa sigurnošću isporučitelja usluga,naročito u mnogobrojnim situacijama kada se usluge pružaju preko posrednika.Radi se o uslugama pristupa ili preuzimanja glazbe ili igrica na

mobilnim telefonima,upitima na razne direktorije,za vremensku prognozu i različite aplikacije.Način pružanja ovih usluga se razlikuje npr.na osnovu posebnog pristupa,preko SMS i sl.Razlikuju se i načini plaćanja ovih usluga.Usluge se obično plaćaju putem naknade za korištenje,preko posebnog računa na određenoj platformi,kreditnom karticom i sl.

Specifičnost ovih usluga je i mogućnost pojave više osoba koje sudjeluju u distribuciji usluge kao posrednici.Primjerice, za distribuciju tonova/melodija za mobilne telefone vlasnik melodije mora ući u sporazum sa osobom koja sakuplja melodije i koja stupa u ugovorene odnose sa operaterom mobilne telefonije,kako bi operater prodavao melodije svojim klijentima.U ovakvim situacijama potrebno je odrediti tko je isporučitelj usluge i tko će ujedno obračunati i plaćati PDV.

Pravila za primatelja usluge[9]:

- Mjesto primatelja usluga-Mjesto oporezivanja usluga ima svoj pravni,porezni i teritorijski aspekt.Pravni status odnosi se na činjenicu da li se radi o pravnoj ili fizičkoj osobi.

  Porezni status određen je osnovnim pravilima oporezivanja PDV-om.Digitalne usluge se mogu isporučivati poreznim obveznicima i u krajnjoj potrošnji.Kao krajnja potrošnja ove usluge se mogu pružati fizičkim i pravnim osobama,koje nisu porezni obveznici.Kada se radi o pravnim osobama,riječ je o osobama koje nemaju status PDV obveznika,kao što su npr.javne ustanove i drugi pravni subjekti koji su oslobođeni PDV-a.Mjesto oporezivanja za pravnu osobu je mjerodavno mjesto uspostavljanja poslovanja,a za fizičku osobu prebivalište ili boravište.

  Teritorijski aspekt mjesta oporezivanja podrazumijeva da se ono odnosi na državu članicu u kojoj će se obračunati i platiti PDV,ukoliko se radi o prometu usluga unutar EU-a,odnosno na treću zemlju ili EU,ukoliko se radi o transakcijij prometa usluga između EU-a i ostalih država.

- Mjesto primatelja u transakcijama sa krajnjim potošačima-Fizička osoba,kao primatelj usluge,može biti obveznik PDV-a.Ukoliko nije obveznik PDV-a primanje usluge predstavlja krajnju potrošnju.Stalna adresa fizičke osobe predstavlja adresu koja je unesena u bazu podataka i kreirana prilikom popisa stanovništva.Stalna adresa može

[9] Slavulj Pavletić,A.(2013):Posebni postupci oporezivanja PDV-om elektroničkih i telekomunikacijskih te usluga radijskog i televizijskog emitiranja,Porezni vijesnik

biti adresa koju je osoba naznačila kod porezne administracije,ukoliko nema drugog dokaza.Mjesto gdje je pravna osoba koja nije porezni obveznik uspostavljena može se smatrati mjesto obavljanja funkcije središnje administracije ili mjesto operativnog upravljanja.

- Utvrđivanje lokacije primatelja usluga-Novo pravilo za oporezivanje digitalnih usluga PDV-om podrazumijeva oporezivanje prema mjestu primatelja usluge (kupca),u svim slučajevima,bez obzira na porezni status primatelja usluge i bez obzira na to da li je isporučitelj usluge (prodavatelj) iz EU-a ili izvan EU-a.

Osnovne pretpostavke kojima bi se trebali voditi isporučitelji digitalnih usluga mogu se svrstati u dvije kategorije:

- identifikacija lokacije kupca na indirektan način,
- identifikacija lokacije kupca na direktan način.

Kod *indirektnog utvrđivanja lokacije* pravila se podjednako odnose i na oporezivne i neoporezive primatelje usluga.Digitalne usluge koriste se na određenoj fizičkoj lokaciji. Za isporučitelja usluge lako je odrediti lokaciju kupca prema fizičkoj lokaciji koja je statična.Problem nastaje kada je lokacija sa koje se pruža usluga mobilna.

Kod *direktnog oporezivanja* propisuje se utvrđivanje lokacije na bazi različitih tehničkih načina pružanja digitalnih usluga osobama koje nisu porezni obveznici.Pretpostavlja se da je osoba koja koristi fiksnu telefonsku liniju za primanje digitalnih usluga ujedno i vlasnik,koji stanuje u tom objektu ili je pravna osoba koja koristi liniju za vlastite aktivnosti.Ako se radi o ljetnoj kući za iznajmljivanje,potrebno je uzeti u obzir i ostale dokaze prisustva osobe na lokaciji,npr.adresu na računu,bankovni račun ili druge podatke koji ukazuju na to da osoba pripada tom mjestu gdje se usluga isporučuje.

4.5.Sustav MOSS – Mini One Stop Shop

MOSS aplikacija će omogućiti obveznicima koji isporučuju telekomunikacijske usluge, usluge radio i TV emitiranja te elektronički obavljene usluge krajnjim korisnicima u drugim državama članicama ,a u kojima nemaju stalnu poslovnu jedinicu, jednostavnije poslovanje i izvršenje obveza tako da svoje obveze po PDV-u prijavljuju i podmiruju u državi članici identifikacije. Bez MOSS sustava, isporučitelj bi se trebao registrirati u svakoj državi članici u kojoj isporučuje usluge svojim klijentima.

U praksi, u sklopu novog postupka oporezivanja, porezni obveznik koji se registrira kao korisnik MOSS sustava u državi članici identifikacije:

- Podnosi putem aplikacije prijavu PDV-a
    - u kojoj iskazuje isporuke telekomunikacijskih usluga, usluga radio i TV emitiranja te elektronički obavljenih usluga krajnjim korisnicima u drugim državama članicama, kao i iznos obračunatog PDV-a,
    - prijava se podnosi kvartalno,
    - ukoliko u navedenom kvartalu nije bilo isporuka, podnosi se prazna prijava.
- MOSS sustav obvezniku prosljeđuje podatke za plaćanje temeljem podnesene prijave.
- Porezni obveznik uplaćuje sredstva temeljem zaprimljenih podataka.

Obveznici sa sjedištem unutar EU, ukoliko se žele registrirati za korištenje MOSS sustava:

- Obvezni su se registrirati u državi članici u kojoj imaju sjedište,
- Ukoliko obveznik unutar EU nema sjedište, već samo stalnu poslovnu jedinicu, obvezan je registrirati se u državi članici stalne poslovne jedinice,
- Ukoliko obveznik ima više stalnih poslovnih jedinica unutar EU, može slobodno odabrati državu članicu identifikacije između država članica u kojima ima stalne poslovne jedinice,
- Za potrebe registracije koristi se PDV ID broj obveznika.

Izbor države članice identifikacije veže obveznika na period kalendarske godine u kojoj je napravio odabir, te dvije naredne godine.

Obveznici sa sjedištem izvan EU:

- Državu članicu identifikacije mogu birati slobodno, uz uvjet da nemaju stalnu poslovnu jedinicu na teritoriju EU, kao i da nisu identificirani za potrebe PDV-a nigdje na teritoriju EU,
- Država članica identifikacije će obvezniku dodijeliti novi PDV ID broj (formata EUxxxyyyyyz).

Izbor države članice identifikacije veže obveznika na period kalendarske godine u kojoj je napravio odabir, te dvije naredne godine.

Registracija korisnika koji imaju sjedište na području EU-EU shema

„EU shema“ se odnosi na korisnike/porezne obveznike koji imaju sjedište, stalnu poslovnu jedinicu, prebivalište ili uobičajeno boravište na području Europske unije, ali nemaju sjedište, stalnu poslovnu jedinicu, prebivalište ili uobičajeno boravište na području države članice potrošnje.

Procedura registracije počinje pristupom na javni portal:*https://www.eusustavi.porezna-uprava.hr/wps/myportal.*Korisnik na ekranu odabire vezu „imate sjedište u Republici Hrvatskoj ili nemate sjedište u Europskoj uniji ali imate poslovnu jedinicu u Republici Hrvatskoj (union shema)?“

Slika 1. Union shema

Slika 2. Nova union registracija

Tablica 4.Forma koju je potrebno popuniti za union registraciju podacima

Informacije o tvrtki:
PDV ID broj: PDV identifikacijski broj
Naziv tvrtke: ime tvrtke poslovanja uvedeno pri trgovačkom sudu
Alternativni naziv tvrtke (neobavezno):

Država poslovanja, ako nije EU: odabrati sa padajućeg izbornika
Web stranica (neobavezno): URL-ovi web stranica poreznog obveznika koji zahtjeva registraciju
Adresa tvrtke
Ulica: naziv ulice u adresi tvrtke poslovanja
Broj: kućni broj u adresi tvrtke poslovanja
Poštanski broj: broj koji označava područje na koje jedna pošta isporučuje poštanske pošiljke
Grad: grad tvrtke poslovanja
Država: država u adresi tvrtke poslovanja
Kontakt podaci predstavnika
Ime: Ime kontakt osobe
Prezime: Prezime kontakt osobe
e-mail: adresa e-pošte kontakt osobe preko koje će se odvijati komunikacija
Broj telefona: broj telefona kontakt osobe
Bankovni račun tvrtke
IBAN: International Bank Account Number ili međunarodni broj bankovnog trans.računa
BIC: Bank Identifier Code ili SWIFT adresa banke primatelja naloga
Vlasnik računa: osoba koja je vlasnik bankovnog računa
Stalna poslovna jedinica u Drugim članicama EU- MSEST
PDV identifikacija u ostalim članicama EU
Prethodne registracije u članicama EU
Detalji registracije (Datum prve isporuke ako je prije datuma registracije)

Prije samog podnošenja registracijskog zahtjeva porezni obveznik dužan je potvrditi izjavu da u svrhe oporezivanja telekomunikacijskih usluga, usluga radijskog i televizijskog emitiranja i elektronički obavljenih usluge, nije registriran u nekoj drugoj državi članici.

Korisnik odabire opciju *"Pošalji registraciju"*

Ako je validacija zahtjeva uspješna, korisnik se obavještava da će primiti obavijest o zaprimljenom zahtjevu na adresu svoje e-pošte. Zahtjev se sprema u bazu i čeka na odobrenje službenika Porezne uprave.

Registarcija korisnika koji nemaju sjedište na području EU-NON EU shema

„NON EU shema“ se odnosi na korisnike/porezne obveznike koji nemaju sjedište, stalnu poslovnu jedinicu, prebivalište ili uobičajeno boravište na području Europske unije i koji ne moraju biti registrirani za potrebe PDV-a. Procedura registracije počinje pristupom na javni portal: https://www.eusustavi.porezna-uprava.hr/wps/myportal.Korisnik na ekranu odabire vezu „nemate sjedište ni poslovne jedinice u Europskoj uniji i ne morate biti registrirani za potrebe PDV-a (non-union shema)?“

Slika 3. Non-union shema

Slika 4. Nova non union registracija

Tablica 5.Forma koju je potrebno popuniti za union registraciju podacima

Informacije o tvrtki:
Nacionalni porezni broj (Izdan od države)
Naziv tvrtke: ime tvrtke pod kojim je registrirana

Alternativni naziv tvrtke (neobavezno):
Država poslovanja: odabrati sa padajućeg izbornika
Web stranica (neobavezno): URL-ovi web stranica poreznog obveznika koji zahtjeva registraciju
Adresa tvrtke
Ulica: naziv ulice u adresi tvrtke poslovanja
Broj: kućni broj u adresi tvrtke poslovanja
Poštanski broj: broj koji označava područje na koje jedna pošta isporučuje poštanske pošiljke
Grad: grad tvrtke poslovanja
Država: država u adresi tvrtke poslovanja
Kontakt podaci predstavnika
Ime: Ime kontakt osobe
Prezime: Prezime kontakt osobe
e-mail: adresa e-pošte kontakt osobe preko koje će se odvijati komunikacija
Broj telefona: broj telefona kontakt osobe
Bankovni račun tvrtke
IBAN: International Bank Account Number ili međunarodni broj bankovnog trans.računa
BIC: Bank Identifier Code ili SWIFT adresa banke primatelja naloga
Vlasnik računa: osoba koja je vlasnik bankovnog računa
Bankovni račun tvrtke ukoliko ne posjeduje IBAN:
OBAN
BIC: Bank Identifier Code ili SWIFT adresa banke primatelja naloga
Vlasnik računa: osoba koja je vlasnik bankovnog računa
Stalna poslovna jedinica u Drugim članicama EU- MSEST
PDV identifikacija u ostalim članicama EU

Prethodne registracije u članicama EU
Detalji registracije (Datum prve isporuke ako je prije datuma registracije)

Prije samog podnošenja registracijskog zahtjeva porezni obveznik dužan je potvrditi izjavu da u svrhe oporezivanja telekomunikacijskih usluga, usluga radijskog i televizijskog emitiranja i elektronički obavljenih usluge, nije registriran u nekoj drugoj državi članici.

Korisnik odabire opciju "Pošalji registraciju".Ako je validacija zahtjeva uspješna, korisnik se obavještava da će primiti obavijest o zaprimljenom zahtjevu na adresu svoje e-pošte. Zahtjev se sprema u bazu i čeka na odobrenje službenika Porezne uprave. Brisanje/ mijenjanje podataka iz forme je moguće korištenjem opcije "Uredi registraciju".

4.6.Oporezivanje elektroničke trgovine PDV-om

Vrste e-trgovine i njihova osnovna obilježja

E-trgovina znači da se poslovanje obavlja elektroničkim putem. Temelji se na elektroničkoj obradi i prijenosu podataka, uključujući tekst, zvuk i video sadržaj. Obuhvaća razne aktivnosti:

- elektroničko trgovanje dobrima i uslugama,
- mrežnu (*online*) isporuku digitalnog sadržaja,
- elektroničke transfere sredstava,
- elektroničko trgovanje dionicama,
- elektroničke teretnice,
- komercijalne aukcije,
- zajednički dizajn i inženjering,
- elektroničku javnu nabavu,
- izravni potrošački marketing i usluge nakon prodaje.

Suvremeni značaj e-trgovine u EU i u svijetu najlakše je ilustrirati pomoću nekoliko statističkih podataka. Prema procjenama danas se oko dvije milijarde ljudi (gotovo trećina ukupnog svjetskog stanovništva) svakodnevno služi internetom. EU danas predstavlja najveće svjetsko tržište širokopojasnog interneta sa preko 124 milijuna linija,ali po opsegu e-trgovine i

dalje zaostaje za SAD-om, s time da treba imati na umu postojanje velikih razlika između pojedinih država članica.

Poduzetnici koji žele nuditi dobra i usluge putem interneta izrađuju stranicu koja prikazuje podatke o društvu i njegovim proizvodima. Nakon što se stranica putem računala stavi na internet, ona postaje dostupna svim kupcima koji imaju računalo s pristupom internetu. Nakon ispitivanja podataka i ponuda sa internetske stranice, kupac može naručiti dobra i usluge od poduzetnika.Tu nastaje i razlika između dvije osnovne vrste e-trgovine. Ovisno o tomu uključuje li transakcija isporuku kakvog dobra u materijalnom obliku ili ne, razlikujemo direktnu i indirektnu e-trgovinu. Razlikovanje pojedinih vrsta e-trgovine značajno je stoga što oporezivanje PDV-om ima različite implikacije ovisno o kojoj je vrsti e-trgovine riječ.

Indirektna e-trgovina obuhvaća „elektroničke narudžbe materijalnih dobara, koja ipak moraju biti fizički dostavljena tradicionalnim putem,npr. poštom ili preko komercijalnih dostavljača.“ Iako je danas vrlo raširena, indirektna e-trgovina ne predstavlja veliki problem sa stajališta oporezivanja PDV-om. Naime, takve transakcije, usporedive s različitim oblicima prodaje na daljinu (npr. kataloška prodaja, telefonska prodaja i sl.), u biti predstavljaju klasične prekogranične isporuke dobara, koje bi se trebale oporezovati prilikom uvoza, u skladu s načelom odredišta.

S druge strane, puno veći izazov za porezne vlasti diljem svijeta predstavlja oporezivanje PDV-om *direktne e-trgovine* koja u potpunosti iskorištava mogućnosti interneta te obuhvaća internetsku (*online*) narudžbu, plaćanje i dostavljanje nematerijalnih dobara i usluga, kao što su računalni softver, zabavni sadržaji ili informacijske usluge na globalnoj razini.Ovaj fenomen predstavlja temeljnu promjenu u odvijanju komercijalnih aktivnosti s kojom se načela i pretpostavke tradicionalnih sustava PDV-a nisu spremni nositi.

Pet osnovnih kategorija e-usluga:

- isporuka web sjedišta, udomljavanje web sjedišta, daljinsko održavanje programa i opreme,
- isporuka računalnih programa i njihovo ažuriranje,
- isporuka slika, tekstova i informacija te osiguravanje pristupa bazama podataka,
- isporuka glazbe, filmova i igara, uključujući igre na sreću i kockarske igre te političkih, kulturnih, umjetničkih, sportskih, znanstvenih i zabavnih emisija i priredbi,

- obavljanje usluga učenja na daljinu.

Proces globalizacije donio je internet kao jednu od najznačajnijih tehnoloških pojava u novijem dobu, a trenutno u svijetu internet koristi više od dvije milijarde ljudi. Razina penetracije interneta u društvu često je povezan sa društvenim i ekonomskim razvojem neke zemlje. Novinari *agencije Anadolija* istražili su razinu pristupa internetu u zemljama jugoistočne Europe, ali i u ostatku svijeta, i saznali da je ova regija u gornjem dijelu svjetske liste. Hrvatska i Kosovo su regionalni lideri prema broju domaćinstava priključenih na internet, a Srbija, Bosna i Hercegovina i Albanija su na začelju regionalne liste.

Tablica 6. Postotak domaćinstava koja imaju direktan pristup internetu među zemljama regije

Država	**Postotak**
Hrvatska	64%
Kosovo	64%
Makedonija	58%
Crna Gora	55%
Srbija	50%
BiH	49%
Albanija	31%

Važno je napomenuti da je u svim zemljama regije postotak domova koji su spojeni na internet, iz godine u godinu u porastu. Podaci govore da su internet, prije svega, prihvatile mlađe generacije, posebno oni u dobi od 15 do 24 godine, među kojima se njih gotovo tri četvrtine služi internetom. Studenti i učenici su grupa koja se najviše od svih služi internetom **(84%),** a slijede ih stalno zaposleni **(50%),** dok se među umirovljenicima nalazi samo oko **4%** korisnika.

Tablica 7. Postotak domaćinstava koja imaju direktan pristup internetu od zemalja šire regije

Država	**Postotak**
Švedska	93%
Slovenija	83%
Irska	67%

Mađarska	66%
Slovačka	65%
Bugarska	51%
Rumunjska	49%
Grčka	44%
Turska	40%
Gruzija	33%
Armenija	33%

5.Oporezivanje PDV-om digitalnih usluga u RH

Hrvatska je postala punopravna članica Europske unije 01.srpnja 2013. Sa svim pravima i obvezama koje iz tog članstva proizlaze,propisano je da se od 1. siječnja 2015. telekomunikacijske usluge (fiksne i mobilne telefonske usluge, telefaks i teleks, pristup internetu) i usluge radijskog i televizijskog emitiranja (radio i televizijski programi preko radijske ili televizijske mreže te prijenosi uživo preko interneta), što ih obavlja isporučitelj u EU osobama neobveznicima sa sjedištem, prebivalištem ili uobičajenim boravištem, oporezuje PDV-om u državi članici potrošača, odnosno kupca. U tu svrhu, poduzeća u i izvan EU-a rabit će webportal u državi članici identifikacije, odnosno prijave.

Elektronički obavljenim uslugama smatra se i sljedeće usluge[10]:

- isporuka web-sjedišta,udomljavanje web-sjedišta(webhosting),daljinsko održavanje programa i opreme - smještaj mrežnih mjesta (websitehosting) i mrežnih stranica(webpagehosting) na poslužitelju; automatizirano, u mreži i održavanje programa na daljinu; daljinska administracija sustava; skladištenje podataka u mreži, pri čemu se odredene podatke pohranjuje i dohvaća elektronički; mrežna isporuka diskovnog prostora na zahtjev,
- isporuka računalnih programa i njihovo ažuriranje - software za pristupanje ili preuzimanje (pa i programe za nabavu/računovodstvo i software za antivirusnu zaštitu) uz ažurirane inačice; software za blokadu prikaza oglasa poznat pod nazivom Bannerblokers; pogonski sklop za preuzimanje,poput softwarea što spaja računala s perifernom opremom(pisači); mrežna automatska instalacija filtera na mrežnim mjestima; mrežna automatska instalacija vatrozidova,

[10] Slavulj Pavletić,A.(2015):Oporezivanje PDV-om digitalnih usluga od 1.1.2015.

- isporuka slika, tekstova i informacija te osiguravanje pristupa bazama podataka - pristup ili preuzimanje prikaza za zaslon; pristup i preuzimanje fotografija, slikovnih prikaza ili zaštita za zaslon; digitalizirani sadržaj knjiga i drugih elektroničkih izdanja;pretplata na mrežna izdanja novina i časopisa; statistički podaci o blogovima i mrežnima mjestima; vijesti, podaci o prometu i vremenskim prilikama u mreži; informacije u mreži što ih software automatski generira od posebnih ulaznih podataka korisnika, npr. pravni i financijski podaci (stalno ažurirani podaci o tržištu kapitala, u stvarnom vremenu; oglasni prostor uključivši oglase u obliku bannera na mrežnome mjestu/mrežnoj stranici; uporaba pretraživača i internetskih direktorija,
- isporuka glazbe, filmova i igara, pa i igara na sreću i kockarskih te emitiranje političkih, kulturnih, umjetničkih, sportskih, znanstvenih i zabavnih programa i priredba - pristup ili preuzimanje glazbe na računala i mobilne telefone;pristupanje ili preuzimanje jinglova, glazbenih isječaka, zvukova zvona i drugih zvukova; pristupanje ili preuzimanje filmova; preuzimanje igrica na računala i mobilne telefone;pristupanje automatskim igrama na mreži što ovise o internetu i sličnim elektroničkima mrežama, pri čemu su igrači geografski udaljeni;
- učenje na daljinu - automatizirano podučavanje na daljinu, ovisno o internetu ili sličnoj elektroničkoj mreži, čije funkcioniranje i isporuka zahtijeva ograničenu ili nikakvu ljudsku intervenciju, uključivši virtualne učionice, osim kada se internet ili slična elektronička mreža uporabljuje kao alat samo za komunikaciju učitelja i učenika; radne bilježnice što ih učenici ispunjavaju u mreži i automatski označuju, bez ljudske intervencije.

Potrebno je razlikovati dva postupka oporezivanja PDV-om digitalnih usluga od 2015:

- posebni postupak oporezivanja za digitalne usluge koje obavljaju porezni obveznici koji nemaju sjedište u EU(taj postupak predstavlja proširenje usluga na koje se odnosi postupak propisan Zakonom o PDV-u koji je na snazi),
- posebni postupak oporezivanja digitalnih usluga koje obavljaju porezni obveznici sa sjedištem u EU,al bez sjedišta u državi članici potrošnje(novi postupak).

Od 01.01.2015. stupaju na snagu izmjene i dopune koju propisuju da se telekomunikacijskim uslugama smatraju:

- fiksne i mobilne telefonske usluge za prijenos i komutaciju tonskog prijenosa,podatkovnog prijenosa i videoprijenosa,uključujući telefonske usluge s videosastavnicom,

- telefonske usluge pružene putem interneta,uključujući govor preko IP mreže,
- govornu poštu,poziv na čekanju,prošljeđivanje poziva,identifikaciju pozivatelja,trosmjerno pozivanje i ostale usluge upravljanja pozivima,
- usluge osobnog poziva,
- audiotekstualne usluge,
- telefaks,telegraf i teleks,
- pristup internetu,
- privatne mrežne veze koje pružaju telekomunikacijske poveznice za isključivu uporabu korisnika usluga.

Usluge radijskog i televizijskog emitiranja,uključuju usluge koje se sastoje od audio sadržaja i audiovizualnog sadržaja poput radijskih i televizijskih programa koje isporučitelji medijskih usluga pružaju široj javnosti putem komunikacijskih mreža i u okviru uredničkih odgovornosti,za istodobno slušanje ili gledanje,na osnovi programskog rasporeda.

5.1.Deep web u Hrvatskoj

Općepoznati internet ili tzv. 'otvoreni internet' kojim se ljudi većinom služe u svakodnevnom radu ili slobodnom vremenu za primjerice čitanje portala i korištenje društvenih mreža, predstavlja samo jedan maleni dio interneta, odnosno vrh ledenog brijega, dok sve ostalo, nekih 80 % predstavlja 'deep web', neindeksirani dio interneta na kojem je skriven i 'dark web'.

Deep web je platforma koju zbog legitimnih razloga koriste brojne grupacije od tvrtki do aktivista za ljudska prava, a uključuje neindeksirane internetske stranice do kojih se ne može doći putem pretraživača već točno određenom putanjom i izravnim unošenjem adrese.Uključuje i skrivene servise, poznate kao 'darknet' ili 'dark web' koji su dostupni samo putem posebnog softwarea, poput TOR-a. Priliku za unosan posao preko interneta prepoznali su i kriminalci, koji skrivajući identitet, proizvode i usluge prodaju ili kupuju preko crnih tržišta na 'dark webu', iako je pogrešno misliti da ih je nemoguće uhvatiti u nezakonitoj zoni.

Sadržaji na 'deep webu' sve su popularniji jer ljudi otkrivaju stvari koje su im dostupne na crnim tržištima pa unatrag nekoliko godina i u Hrvatskoj predstavljaju problem.Postoji dosta darkmarketa na kojima se nudi apsolutno sve - od droge, oružja i ukradenih osobnih podataka do dječje pornografije, podataka o kreditnim karticama i nedozvoljenih lijekova.

Danas su internetska crna tržišta sve popularnija jer su zabranjene stvari ljudima dostupne u dnevnoj sobi i više se ne moraju izlagati dodatnom riziku.Ako netko želi nabaviti drogu više ne treba tražiti dilera po mračnim uličicama kad može naručiti drogu koja će na kućnu adresu stići zapakirana u kutiji od CD-a ili bombonjere.

U Hrvatskoj je popularna kupovina droge koja je najčešći predmet interesa, a ima i korištenja crnih tržišta za dječju pornografiju koju se naručitelju dostavlja kriptirano na neki digitalni način. Preko crnih tržišta može se primjerice kupovati ukradene umjetnine ili čak naručiti ubojstvo, no u Hrvatskoj zasad nije zabilježen takav slučaj.Naručitelj odabire najzgodniji način dostave, poput kurirskih službа koje nisu upoznate sa stvarnim sadržajem paketa, primjerice bombonjere, koji ni na koji način neće odavati stvarni sadržaj.

Facebook primjerice ima skriveni servis za pristupanje u zemljama s restrikcijama na slobodu govora i informacija te koje filtriraju i cenzuriraju internet, a brojne medijske kuće koriste te servise za komunikaciju i razmjenu dokumenata.

Plaćanje na darknetu se odvija virtualnom valutom od kojih je trenutno najpopularniji 'bitcoin', čija se prednost u odnosu na kreditne kartice očituje u težem praćenju traga novca.

Internet ne poznaje granice pa ni Hrvatska nije izolirana od takvog oblika kriminala zbog čega policija često surađuje i razmjenjuje podatke s drugim policijskim organizacijama, prvenstveno Europolom, Interpolom i FBI-om, sudjeluje u međunarodnim akcijama, ali i prati trendove.

Jednom online, uvijek online

Problem koji se javlja je što nešto što je bilo online uvijek ostaje online. To je prva stvar o kojoj ljudi trebaju razmišljati kad bilo kakav sadržaj stavljaju na internet.

Neoprezno objavljivanje osobnih podataka može završiti neugodnim posljedicama i zbog krađe identiteta tako da počinitelji izrade dokumente na njihovo ime i počnu se kao oni predstavljati.

Korisnici interneta mogu u jednom trenutku svjesno postati anonimni, ali ne može postati anonimno ono što su ostavili kao digitalni trag za sobom na facebooku i googleu.

Neke subkulture žele koristiti TOR, imaju blogove na darknetu jer su svjesne problema i žele zadržati svoju privatnost i anonimnost.Jedno objašnjenje je da će biti sve više zadiranja u privatnost zbog profiliranja korisnika, no zbog takvog prikupljanja podataka ljudi moraju biti svjesni problema. Korporacije su prepoznale rizike koje donosi moderna tehnologija pa u sigurnu komunikaciju, nadzor mreže i sigurnosne aplikacije ulažu milijarde dolara.

Crna internetska tržišta samo su dio cyber kriminaliteta koji uz terorizam i ilegalne migracije spada među "top prijetnje" u EU. U Hrvatskoj je zabilježenio oko 1200 nedjela cyber kriminala godišnje, što je osjetan porast u odnosu na 300 do 400 takvih slučajeva 2008. i 2009.

Sve se više kriminaliteta seli na internet jer je tako jednostavnije i jeftinije. Taj trend se pojavio unatrag nekoliko godina jer više ne morate prodavati krivotvorene tenisice na štandu kad ih možete prodavati preko facebooka.

5.2.Neprihvatljiv govor u komentarima na internetskih informativnim portalima

Portal Net.hr 2013. godine odlučio je ukinuti mogućnost postavljanja komentara na članke od strane čitatelja.Tada su mnogi mediji prenijeli vijest o tome potezu, s obzirom da je to bila prva takva inicijativa čitanijeg portala u Hrvatskoj. Razlozi za to su, kako su u Net.hr-u objasnili u članku pod vrlo direktnim naslovom „Dosta je gadosti“, to da je „postalo gotovo pravilo da komentari služe za izražavanje poremećenih, bolesnih i zadrtih stavova čitatelja koji su iskazivali frustracije ne štedeći pritom nikoga i ništa.Njima je portal služio kao mjesto ispucavanja mržnje i agresije doslovno prema svemu i svima koje su smatrali drugačijima.“

Kako bi provjerili kakvu praksu u ovom području imaju internetski portali u Hrvatskoj, analizom su obuhvaćeni deset najčitanijih portala u Hrvatskoj u razdoblju od 1. siječnja 2016. do 31. svibnja 2016. To su:

- 24sata.hr,
- jutarnji.hr,
- net.hr,
- dnevnik.hr,
- vecernji.hr,
- rtl.hr,
- tportal.hr,
- telegram.hr,

- poslovni.hr
- express.hr.

Od svih analizom uključenih internetskih portala, svi imaju određenim pravilnikom, uvjetima korištenja ili kriterijima za komentiranje uređeno što se na specifičnom portalu u komentiranju smije, a što ne.

Indikativno je istaknuti da nemaju svi uređene sankcije za čitatelje koji ta pravila, odnosno uvjete krše.

Vecernji.hr, jutarnji.hr, 24sata.hr, express.hr i tportal.hr imaju sankcije u obliku suspendiranja korisničkog računa čitatelja na određeno vrijeme ukoliko čitatelj krši određena pravila komentiranja – najčešće se to odnosi na kršenje pravila koje zabranjuje govor mržnje i vrijeđanje te diskriminiranje po različitim osnovama.

Eksplicitno zabranjen govor mržnje u komentarima čitatelja imaju vecernji.hr, jutarnji.hr, 24sata.hr, express.hr, poslovni.hr te tportal.hr. Rtl.hr ima najmanje uređenu politiku prema govoru mržnje i drugom neprihvatljivom sadržaju u komentarima svojih čitatelja. Oni ističu kako je dozvoljeno „komentiranje članaka u dobroj namjeri“, bez dodatnih pojašnjenja što se smije, a što ne smije objavljivati i koje su potencijalne kazne za čitatelje koji komentarima krše zakonska pravila.

Telegram.hr, net.hr i dnevnik.hr nemaju direktno zabranjen govor mržnje, no uvjeti korištenja i komentiranja uključuju zabranu komentara koji krše hrvatske i/ili međunarodne zakone te koji sadrže uvredljive, vulgarne, prijeteće, rasističke ili šovinističke elemente. Svi analizirani portali imaju određenu vrstu sustava prijave – što kroz društvenu mrežu Facebook, što ostavljanjem korisničkih podataka poput imena i prezimena te mail adrese.

Vukovarac.net-njegov vlasnik Fintić vjerojatno će u zatvor zbog toga što je na njegovom portalu netko anoniman vrijeđao gradonačelnika Vukovara, a on je odbio otkriti identitet, odnosno IP adresu tog nekog. Fintić možda nije jedini bloger na svijetu koji će završiti u zatvoru zbog radikalnog stava o slobodi govora na internetu.

Stranice na kojima 'djeca ubijaju djecu'

Dječje zlostavljanje na internetu poprimilo je strašne razmjere i postalo smrtonosno.

Bujice uvreda, prijetnji, ponižavajućih poruka tinejdžerice sipaju jedna drugoj, a ubace se tu i dečki. Zbog takvih se riječi, ubila jedna curica u Hrvatskoj prije dvije godine, nije mogla podnijeti uvrede i ponižavanja.

Na Facebooku su pak istodobno bolesni i ljubomorni anonimci objavljivali fotografije cura iz Vinkovaca i Županje i proglasili ih "droljama" i "kurvama". Hrvatska policija nije u tome vidjela nikakvo kazneno djelo, a od bilo kakve odgovornosti pošteđeni su bili i ostali i kreatori Facebooka, pa i mreže Ask. fm.

U prvih šest mjeseci 2013. godine, kad je Ask.fm bio nov i izrazito popularan, od Irske i SAD-a do Hrvatske i Latvije, zabilježeni su bili deseci samoubojstava dječaka i djevojčica koji nisu mogli podnijeti vrijeđanje na stranicama Ask. fm. Kad su se, nakon strašnih ponižavanja na toj stranici prije skoro tri godine u Irskoj ubile 15-godišnjakinja i 13-godišnjakinja , njihovi mediji su prozvali autora i vlasnika te društvene mreže, Latvijca *Marka Terebina*, zaključivši kako je i nezreloj djeci dao poligon za najokrutnija iživljavanja, anonimna i oslobođena bilo kakve odgovornosti.

On im je, pak, odgovorio: "Naravno da postoji problem zlostavljanja na mrežama. Ali, čini se da je ovaj problem zasad samo specifičnost Irske i Britanije. Nema primjedbi iz drugih zemalja. Čini se da su djeca okrutnija u Irskoj i Britaniji..."

No brzo se ispostavilo da je već tada Terebin bio posve u krivu. Pošast dječjeg zlostavljanja, ali i samoubojstva zbog uvreda na njegovoj mreži, širila se Europom i SAD-om. U prosincu 2012. godine na Floridi se ubila 16-godišnjakinja, a onda su uslijedili i deseci drugih slučajeva, od Kanade do Italije, u kojima je bilo zajedničko čak i nagovaranje vršnjaka da počine samoubojstvo.

5.3.Ipsos Online klub

Kao član Ipsos Online kluba možete sudjelovati u online istraživanjima i izražavati svoje mišljenje o proizvodima i uslugama. Sudjelovanjem u istraživanjima sakupljamo bodove koje ćemo moći mijenjati za poklon bonove.

Uvjeti članstva u Ipsos Online klubu:

- Članstvo u klubu je besplatno,
- Svaki član može imati samo jedan korisnički račun. A unutar kućanstava samo jedan član kućanstva može biti član kluba,
- Članovi kluba povremeno se pozivaju na sudjelovanje u Online istraživanjima putem elektroničke pošte i za svaki ispunjeni upitnik dobiva bodove na svoj račun u Ipsos Online klubu. Broj bodova za pojedino istraživanja varira od 5 do 20 bodova i ovisi o duljini upitnika,
- Nakon što broj bodova dosegne 80, član ih ima pravo zamijeniti za bon u protuvrijednosti 80 kuna za kupnju u nekom od hrvatskih maloprodajnih lanaca.

Zaštita podataka

- Ipsos Online klub pridaje veliku važnost privatnosti svakog člana te ophođenju s osobnim i osjetljivim podacima svojih članova. Prikupljanje, obrada i korištenje osobnih podataka svakog člana odvija se u skladu s hrvatskim Zakonom o zaštiti osobnih podataka,
- Ipsos Online klub se obvezuje da osobne podatke svojih članova neće prosljeđivati trećim osobama ili prodavati njihove podatke o adresama. Ipsos Online klub će obrađivati podatke koje je član prikupio i koristiti isključivo u svrhu provođenja Online istraživanja, ugovorenih ovim uvjetima poslovanja,
- Svi, pa i osobni podaci, koje klub zaprimi od svojih članova koristit će se isključivo radi ostvarenja predmetne poslovne svrhe i dostupni su isključivo zaposlenicima Ipsos Online kluba i ne prosljeđuju se ni u kojem slučaju trećim osobama,

- Sve informacije, koje je član dao prilikom registracije, odnosno naknadnog ažuriranja vlastitog profila u okviru Online istraživanja, strogo se povjerljivo obrađuju i ostaju anonimne,

- U slučaju prekida članstva, Ipsos Online klub će sve osobne podatke tog člana neopozivo izbrisati u roku od 60 dana,
- Svaki član snosi odgovornost o povjerljivosti svog korisničkog imena i lozinke. Član je odgovoran za korištenje svog korisničkog imena i lozinke, kako prema klubu, tako i prema trećim osobama. U slučaju da treća osoba neovlašteno koristi korisničko ime i lozinku člana, taj će član o tome odmah obavijestiti Ipsos Online klub i odmah sam promijeniti lozinku.

Kako bi mogao sudjelovati u Online ispitivanjima Ipsos Online kluba, član mora sljedeće:

- Prihvatiti priložene uvjete poslovanja,
- Biti fizička osoba, starija od 14 godina, koja ponuđenu uslugu kluba ne koristi u poslovne svrhe,
- Ne smije navoditi netočne podatke o sebi, koji su potrebni za registraciju te za dobrovoljno sudjelovanje u Online istraživanjima,
- U članstvu kluba smije biti registriran samo jedanput,
- Mora biti jedini član u svojemu kućanstvu koji je registriran u članstvo Ipsos Online kluba,
- Ne smije članstvo koje je stekao potpunom registracijom u klubu prenositi na treće osobe. Izuzetak je kada klub od člana zatraži sudjelovanje ukućana članova kluba.

5.4. Anonimnost i kazne za uvrede na internetu

Anonimnost na internetu:za i protiv

Poštivanje ljudskih prava u digitalnom svijetu postaje sve veći izazov. Nove tehnologije snažno su integrirane u naš svakodnevni život, pružajući nam mnogo više mogućnosti za izražavanje. To svakako povlači i veću odgovornost, koja pripada kako korisnicima, tako i onima koji omogućuju razmjenu informacija – portali, forumi, blogovi, tražilice.Uklanjanje ili neobjavljivanje komentara anonimnih korisnika mijenja koncept slobode izražavanja koji je u određenom trenutku poprimio velike razmjere. Stoga se postavlja pitanje da li treba inzistirati na podršci online anonimnosti ili se pridružiti onima koji je žestoko kritiziraju? Razloga ima i za i protiv.

Anonimnost je bitna jer dozvoljava potpunu slobodu izražavanja za one koji se boje govoriti. Specijalno je bitna za nedemokratske režime, gdje riječ koja ne odgovara vladajućem aparatu može značiti kaznu za onoga ko je izgovori. Isto tako, anonimnost je značajna u svim društvima za ugrožene skupine i pojedince kojima daje komfor i sigurnost u smislu nepostojanja bojazni za psihički ili fizički integritet.Neke od pravnih doktrina najvišim propisima štite anonimnost. Prema Ustavu SAD-a, anonimni govor figurira kao neraskidiva kategorija slobode govora i kao takav zaslužuje supstancijalnu zaštitu.Bitno je primijetiti da američki koncept podrazumijeva da sloboda izražavanja, a time i anonimnost, predstavlja temeljni princip, a ograničenja se mogu nametnuti samo ako se dokaže da vodi ka ugrožavanju ili kršenju nečijeg prava.

S druge strane, protivnici anonimnosti inzistiraju da anonimnost uključuje neodgovornost za izrečeno. Na primjer,ako neki sadržaj anonimnog autora krši nečije pravo, onda onaj kome pripada legitimno pravo na određenu vrstu kompenzacije nema kome da se obrati. Zbog anonimnih online nasilnika, mnogi podliježu psihičkom pritisku.

Kazne za uvrede na internetu: Anonimnost više nije zaštita

Novi *Kazneni zakon* koji je stupio na snagu 1.1.2013. donosi i nova pravila ponašanja na internetu. Tako su po njemu uvreda, kleveta i sramoćenje kazneno djelo i na računalnim sustavima ili mrežama, a tko bude osuđen kaznit će se novčanom kaznom, ovisno o primanjima.

Najviša kazna može biti do 360 dnevnih dohodaka. Dnevni iznos ne može biti manji od 20 kuna ni veći od 10 000 kuna.

Sud počinitelja može osloboditi kazne ako je bio izazvan nedoličnim ponašanjem oštećenika, ili je ovaj prihvatio ispriku, a nema uvrede ni ako iz načina izražavanja i drugih okolnosti proizlazi da je omalovažavanje počinjeno radi zaštite drugih opravdanih interesa. Nema kaznenog djela sramoćenja ni ako počinitelj dokaže istinitost činjeničnih tvrdnji.

Novim zakonom određuju se kazne za hakiranje, ometanje rada sustava, oštećenje ili krađu podataka, online prijevaru, a posebno će kažnjavati svi ovi napadi protiv tijela državnih vlasti te lokalnih samouprava, javnih ustanova ili trgovačkih društava od posebnog javnog interesa.

Tako za neovlašteni pristup sustavu ili podacima kazna može biti do godine dana zatvora, a tri godine za tijela državne vlasti, lokalne ili područne samouprave.

Do tri godine zatvora možete dobiti za ometanje rada računalnog sustava, oštećenje računalnih podataka, neovlašteno presretanje računalnih podataka i računalno krivotvorenje.

Što se tiče prijevare, odnosno tko s ciljem da sebi ili drugome pribavi protupravnu imovinsku korist unese, izmijeni, izbriše, ošteti, učini neuporabljivim ili nedostupnim računalne podatke ili ometa rad računalnog sustava i tako prouzroči štetu drugome, može dobiti od šest mjeseci do pet godina zatvora.

Do tri godine mogli bi dobiti oni koji izrade, nabave, prodaju, posjeduju ili omoguće drugima dostupnim programe ili hardver stvoren za počinjenje gore navedenih kaznenih djela.

6.Zaključak

U budućnosti se očekiva sve veća uporaba informatičke tehnologije u svijetu koja će se širi iz dana u dan, sa sve većim brojem novih tehnoloških izuma, koji imaju mogućnost brzog i jednostavnog pristupa internetu, te širokom ponudom novih, u pravilu digitalnih, sadržaja namijenjenih uglavnom krajnjim potrošačima. Posljedica je snažan rast e-trgovine, a posebno B2C isporuka e-usluga. S druge strane, porezni trendovi u EU i drugim svjetskim državama u posljednjim godinama ukazuju da raste značaj potrošnih poreza,kao što je PDV, a posljednja je ekonomska kriza to samo potvrdila. Time se samo dodatno naglašava važnost svake nove pojave značajne za sustav PDV-a i drugih potrošnih poreza, a to e-trgovina svakako jest.

Provedba od 1. siječnja 2015. mini *One Stop Shop* postupka za davatelje telekomunikacijskih usluga na području EU-a, usluga radijskog i televizijskog emitiranja te ostalih elektroničkih usluga potrošačima bit će važan korak naprijed kad je u pitanju pojednostavnjenje pravila o usklđivanju PDV-a u EU. *One Stop Shop* postupak omogućit će poduzećima prijavu i plaćanje PDV-a u državi članici u kojoj imaju sjedište, a ne u državi članici svoga kupca. *One Stop Shop* postupak što ga se sada primjenjuje ograničen je na davatelje elektronički obavljenih usluga sa sjedištem izvan EU-a, proširit će se i na poduzeća sa sjedištem u EU te na usluge radijskog i televizijskog emitiranja i telekomunikacijske usluge.

6.Conclusion

In the future, the increasing use of IT technology in the world is expected to expand day by day, with the increasing number of new technological innovations, with the ability to quickly and easily access the Internet, and a wide range of new, mostly digital content intended mainly for end consumers. The result is strong growth of e-commerce, especially B2C e-service delivery. On the other hand, tax trends in the EU and other world countries in recent years indicate that consumption tax revenue is increasing, such as VAT, and the last economic crisis has only confirmed this. This only adds to the importance of every new phenomenon that is significant for the VAT and other taxation system, and that's certainly the e-commerce.

Implementation of 1 January 2015 mini One Stop Shop procedure for EU telecommunications service providers, radio and television broadcasting services and others electronic consumer services will be an important step forward when it comes to simplifying the EU harmonization policy. One Stop Shop procedure will allow companies to apply for and pay VAT in the Member State where they are based and not in the State member of its buyer. The One Stop Shop procedure being applied now is limited to providers of electronic services that are headquartered outside the EU will also be extended to companies headquartered in the EU and to the services of radio and television broadcasting and telecommunication services.

7.Literatura

Hodžić,A.(2014): Pregled strategije digitalna agenda za Europu 2010.-2020.

Slavulj Pavletić,A.(2013):Posebni postupci oporezivanja PDV-om elektroničkih i telekomunikacijskih te usluga radijskog i televizijskog emitiranja,Porezni vijesnik,11, str.70-82

Slavulj Pavletić,A.(2015):Oporezivanje PDV-om digitalnih usluga od 1.1.2015.

Ministarstvo financija Porezna uprava (2014) MOSS – priručnik za registraciju korisnika

Milevoj,M.(2016.):Porez na financijske transakcije u Europskoj uniji i Republici Hrvatskoj

Lalić,S.,Senta,C. i Žagan,D.(2016.):Neprihvatljiv govor u komentarima na internetskim i informativnim kanalima

http://pcchip.hr/internet/vpn-privatnost-i-sigurna-internet-veza/

http://pcchip.hr/internet/skrivene-mogucnosti-google-chromea-kao-npr-skrivena-t-rex-igrica

http://pcchip.hr/internet/torrent-5-nacina-kako-skidati-torrente-anonimno/

http://www.binaryoptions.com.hr/5-najcescih-prijevara-na-internetu/

http://pcchip.hr/internet/vpn-kompanije-koje-anonimnost shvaćaju ozbiljno

https://onilne.ipsosadria.com

htpps://www.tportal.hr/vijesti

http://crobitcoin.com/bitcoin/transakcije/

www.digitalnahrvatska.org

www.poliklinika-djeca.hr/publikacije

www.monitor.hr

www.24sata.hr/rech

www.vijesti.me/vijesti/odgovornost-za-komentare-korisnika

www.jutarnji.hr/life/tehnologija/dark web

m.bug.hr/komentari/europa-poslovno-digitaliziranija-nego SAD