Sinteza
Međunarodna naučna konferencija Univerziteta Singidunum

Impact of Internet on Business Activities in Serbia and Worldwide
Uticaj Interneta na poslovanje u Srbiji i svetu

DOI: 10.15308/SINTEZA-2014-94-100

PRAVNI I ETIČKI ASPEKTI RIZIKA POSLOVANJA PUTEM INTERNETA

Vuk M. Raičević[1], Jelena D. Matijašević-Obradović[2], Maja S. Kovačević[1]
[1]Fakultet za ekonomiju i inženjerski menadžment u Novom Sadu
[2]Pravni fakultet za privredu i pravosuđe u Novom Sadu

Abstract:
Primena Interneta u poslovanju, dovela je do stvaranja potpuno novog poslovnog ambijenta. Prednosti ovakvog načina poslovanja su brojne. Sa druge strane, elektronsko poslovanje prate rizici, čija je osnovna karakteristika fenomenološka raznovrsnost koje je svakim danom sve obimnija. Predstavljanjem najčešće zastupljenih rizika postalo je jasno da ovim aktivnostima oblast elektronskog poslovanja može biti značajno ugrožena. Ovakav stav podržao je i širi zakonski obuhvat ove materije.

Key words:
elektronsko poslovanje,
Internet,
rizici poslovanja putem interneta,
pravna regulativa.

UVOD

Pod terminom informaciono društvo se zapravo podrazumeva fenomen koji pripada sferi socijalnog, psihološkog, ekonomskog, antropološkog i istorijskog, fenomen koji predstavlja interakciju čoveka i tehnologije [8, str. 1].

Internet je osnovna globalna komunikacijska kompjuterska mreža. Njegov razvoj doveo je do velikih promena u načinu života i rada savremenog društva. Omogućio je jednostavnu i brzu komunikaciju, prenošenje velikih količina podataka na velike udaljenosti gotovo trenutno, objavljivanje i ažuriranje elektronskih dokumenata i njihovu globalnu dostupnost, kao i niz virtuelnih aktivnosti koje su ili novina u svetu poslovanja i svakodnevnog života ili su izmesna modifikacija tradicionalnih aktivnosti koje se brže, lakše, komfornije obavljaju putem Internet konekcije.

O značaju Interneta, kao osnovne globalne komunikacijske kompjuterske mreže, govori podatak da je u 2012. godini broj korisnika Interneta na svetskom nivou bio 2,405,518,376, što čini 34,3% ukupne svetske populacije. Ako pogledamo evropski nivo, broj korisnika Interneta u istoj godini bio je 518,512,109, što čini 63,2% ukupne populacije u Evropi. Što se tiče broja korisnika Interneta u Srbiji, on za 2012. godinu iznosi 4,107,000, što čini 56,4% ukupne populacije u Srbiji [18].

Dakle, Intenet je od luksuza i apstraktnog eksperimenta, nepoznatog većini ljudi, postao neminovnost i sredstvo informisanja i komunikacije, zabave i edukacije koje svakodnevno koristi milijardu i po ljudi širom planete. Taj broj se svake godine uvećava novim korisnicima.

Problem koji postoji na Internetu, a koji veoma pogoduje vršenju različitih nedozvoljenih radnji jeste problem identiteta. Naime, teško je na Internetu utvrditi nečiji pravi identitet. [9, str. 744].

Ogromne mogućnosti koje ova globalna mreža svakodnevno pruža svim svojim korisnicima, konstantno su podložne različitim zloupotrebama.

Cilj ovog rada jeste analiza poslovanja putem Interneta sa aspekta rizika koji ovakav način odvijanja poslovnih procesa neminovno prate, kao i predstavljanje i analiza zakonske regulative u Srbiji u ovoj oblasti. Pre nego što pažnju posvetimo rizicima u poslovanju putem Interneta, celinu u radu koja sledi, namenićemo bližem pojašnjavanju pojmovnog određenja, karakteristika, kao i modela ovog vida poslovanja.

POJAM, KARAKTERISTIKE I MODELI POSLOVANJA PUTEM INTERNETA

Primena Interneta koji u organizaciju donosi i druge sadržaje dovela je do stvaranja potpuno novog poslovnog ambijenta. Ekspanzija u primeni Interneta afirmisala je i klasu informacionih tehnologija koje čine infrastrukturu elektronskog poslovanja. Ovakav trend promena u poslovanju ima za posledicu da se klasično poslovanje ubrzano seli na elektronsku infrastrukturu. Poslovanje putem interneta predstavlja generalni koncept pod kojim se podrazumeva svaka vrsta razmene poslovnih transakcija u kojoj strane učestvuju elektronskim putem, preko računarskih mreža, umesto razmene klasičnih dokumenata ili direktnih fizičkih kontakata [12, str. 1].

Elektronsko poslovanje je poslovni proces koji se obavlja korišćenjem internet tehnologija i ostalih informaciono- komunikacionih tehnologija i sistema. Obuhvata sve oblike poslovnih transakcija koje se ostvaruju elektronskim putem između organizacija i njihovih kupaca ili između organizacija i javne administracije [10, str. 3].

Poslovanje putem Interneta sastoji se iz nekoliko oblasti: elektronska trgovina, elektronska plaćanja, elektronske komunikacije, elektronska proizvodnja i elektronska distribucija.

Elektronska trgovinu (posmatrano u širem smislu) obuhvata razmenu poslovnih informacija, održavanje poslovnih odnosa i vođenje poslovnih transakcija putem informaciono- komunikacione tehnologije. Ovo je najbrži, ali često i najjeftiniji način kupovine nekog proizvoda. Jednom rečju, smatra se najprofitabilnijim oblikom trgovine.

Elektronska plaćanja predstavljaju transfer novca i izvršenje plaćanja primenom informaciono-komunikacione tehnologije.

Elektronske komunikacije jesu oblast elektronskog poslovanja u kojoj se sama komunikacija (razmena poruka, poslovnih dokumenata i drugog materijala) između poslovnih subjekata odvija primenom informaciono-komunikacione tehnologije.

Elektronska proizvodnja, kao i elektronska distribucija obuhvataju stvaranje i distribuciju proizvoda i izvršenje usloga primenom informaciono-komunikacione tehnologije. Ove dve oblasti poslovanja primenom informaciono-komunikacione tehnologije zasnovane su na stvaranju i cirkulisanju elektronskih proizvoda, čija je bazična osobenost digitalni oblik postojanja (elektronski se proizvode, elektronski se koriste i na isti način distribuiraju).

Poslovanje na Internetu je uslovljeno razvojem informaciono-komunikacionih tehnologija i pripadajućih standarda, koji su omogućili unificirano povezivanje i komunikaciju između poslovnih partnera [13]. Drugim rečima, primena elektronskog poslovanja moguća je ukoliko su za to stvoreni preduslovi: primena internet tehnologija i ostalih informaciono-komunikacionih tehnologija i sistema, usvajanje propisa o elektronskom poslovanju i elektrnskom potpisu, kao i prihvatanje elektronskog poslovanja od strane rukovodstva preduzeća [10, str. 5].

Elektronsko poslovanje je globalna privredna aktivnost. Ono je nastalo na procesima globalizacije svetske privrede i ne poznaje granice nacionalnih privreda. Elektronsko poslovanje, a pogotovo Internet kao poslovni kanal, omogućilo je da preduzeća mogu poslovati u bilo kom delu sveta, pod istim uslovima. Zato sve više preduzeća danas usvaja koncept globalne firme, što znači da na svetsko tržište gledaju kao na jedinstveni privredni ambijent [6].

Prednosti poslovanja putem interneta su brojne. Neke od njih su: smanjenje troškova poslovanja, ušteda vremena, redukcija papirne dokumentacije, smanjenje obima ljudskog rada, istovremena komunikacija sa više stotina klijenata, pristupačnost i razmenljivost informacija, rast prihoda i proizvodnje, ušteda u troškovima distribucije, unapređenje poslovnih procesa [10, str.

Teorija elektronskog poslovanja poznaje nekoliko osnovnih modela poslovanja: elektronsko poslovanje između preduzeća (B2B - Business to Business), elektronsko poslovanje između preduzeća i klijenta (B2C - Business to Consumer), elektronsko poslovanje između klijenata (C2C - Consumer to Consumer), elektronsko poslovanje između preduzeća i zaposlenog (B2E - Business to Employee), elektronski servis organa državne uprave (E-Government). B2B2C je noviji model koji predstavlja kombinaciju korišćenja modela B2B koji podržava poslovanje preduzaća po modelu B2C. C2B2C uključuje sprovođenje transakcija između potrošača koristeći online preduzeće kao posrednika [2].

Sa ekspanzijom korišćenja Interneta i primene i razvoja elektronskog poslovanja može doći do mnogih neželjenih pratećih pojava, odnosno rizika i opasnosti. Pored zaista mnogo pozitivnih prednosti istovremeno su se javili i ogromni problemi zloupotrebe tuđih računara i informacionih tehnologija uopšte. Pitanje rizika, odnosno pretnji bezbednosti u elektronskom poslovanju neminovno se postavlja.

RIZICI POSLOVANJA PUTEM INTERNETA

Implementacija informacionih tehnologija u skoro svim sferama života i rada savremenog čoveka uključuje, pored brojnih prednosti, i izvesne rizike.

Osnovna njihova karakteristika jeste fenomenološka raznovrsnost. Brojni su pojavni oblici zloupotreba informaciono- komunikacionih tehnologija [17, str. 214].

Naime, inventivnost informatički edukovanih osoba rešenih da ugroze sistem elektronskog poslovanja u bilo kom segmentu ili situaciji, nema granica. Otuda možemo

izvesti još jedan veliki problem korišćenja Interneta kao svojevrsnog posrednika u poslovanju i radu uopšte. To je problem sigurnosti. Ovaj problem proističe iz karakteristika svih računarskih mreža, putem kojih se obavlja komunikacija. Upravo je problem sigurnosti ključan u ovom domenu, s obzirom da svi rizici sa kojima se možemo susresti u elektronskom poslovanju i proističu iz situacije da niko nije apsolutno siguran u komunikaciji koja se odvija putem Interneta. Dakle, nema aspolutno bezbedne komunikacije (bilo poslovne, bilo privatne). Preduzimaju se različite metode koje imaju za cilj da obezbede što veći stepen garancije da će sigurnost komunikacije na računarskim mrežama biti što kvalitetnija, no, suštinski, sve je pitanje konkretne situacije i raspoloživih mogućnosti. U komunikaciji koja se odvija putem računarskih mreža (naročito putem Interneta kao najzastupljenije računarske mreže) svako može biti meta napada, i to u bilo kom trenutku, na bilo kojoj udaljenosti. Otuda proističu i rizici koji mogu ugroziti elektronsko poslovanje. Oni su vrlo izmesni, vrlo realni i svakodnevni. Ne postoje jedinstvena mišljenja o broju i vrsti svih rizika sa kojima se savremeni vidovi poslovanja suočavaju, odnosno, mogu suočiti. Domaća literatura se ovim domenom bavila u proteklih nekoliko godina. Tako, Pavlović i Tomić ističu da u rizike poslovanja putem Interneta spadaju maliciozni programi i aktivnost zaposlenih u samoj kompaniji. Pri tome se pod malicioznim programima podrazumeva svaki program koji izvršava namerne, nedokumentovane akcije, bez znanja i često na štetu korisnika. Ovakvim aktivnostima se bave hakeri, a njihova aktivnost (hakerisanje) predstavlja neovlašćen pristup tuđim računarima povezanim na Internet sa namerom da ih pretražuju, onesposobe ili u potpunosti unište. Sa druge strane, aktivnosti zaposlenih u samoj kompaniji mogu biti namerne (smišljene štetne aktivnosti od strane zaposlenih ili bivših zaposlenih) i nenamerne (aktivnosti učinjene zbog neznanja ili omaške) [12, str. 2-3].

Oslanjajući se na sve prethodno rečeno, u nastavku su prikazani rizici poslovanja putem Interneta, česti u praksi, koji ovaj sistem poslovanja čine podložnim različitim načinima manipulisanja i zloupotrebe.

Računarska sabotaža i računarska špijunaža - Računarske sabotaže se sastoje u uništenju ili oštećenju kompjutera i drugih uređaja za obradu podataka u okviru kompjuterskih sistema, ili brisanju, menjanju, odnosno sprečavanju korišćenja informacija sadržanih u memoriji informatičkih uređaja. Najčešći vidovi računarske sabotaže su oni koji deluju destruktivno na operativno-informativne mehanizme i korisničke programe, pre svega one koji imaju funkciju čuvanja podataka [7].

Računarska špijunaža predstavlja protivpravno sticanje ili otkrivanje, prenos ili korišćenje poslovne i komercijalne tajne bez zakonskog prava ili bilo kojeg drugog zakonskog opravdanja, bilo sa namerom uzrokovanja ekonomskog gubitka osobi nosiocu tajne, bilo sa namerom ostvarenja protivpravne ekonomske prednosti za sebe ili za treću osobu. Počinioci računarske špijunaže koriste različite maliciozne programe i tehnike u cilju infiltriranja u računarsku mrežu koja za njih predstavlja metu.

Upotreba malicioznih programa - Upotreba programa sa štetnim sadržajem je jedan od najpoznatijih oblika iz širokog spektra računarskog kriminala. Najpoznatiji maliciozni programi predstavljeni su u nastavku.

Računarski virusi su mali programi, koji imaju sposobnost samoumnožavanja i isključivi cilj da naprave štetu na zaraženom računaru.

Računarski crv je deo softvera koji se kreće kroz samo jedan računarski sistem ili kroz mrežu računarskih sistema, manipulišući ili uništavajući podatke i/ili programske kodove gde god dobije pristup. Ovo je specifičan računarski program koji ima sposobnost samoumnožavanja, bez intervencije od strane korisnika, ali nema sposobnost da zarazi druge programe ili fajlove.

Trojanski konj je program koji je na prvi pogled potpuno bezazlen, a u stvari krije potpuno drugu agendu. Najčešće se koristi da omogući napadaču kontrolu nad zaraženim računarom. Ovo je maliciozni program koji kada se ubaci u nečiji računar šalje sve šifre na e-mail onoga koji ga je i ubacio i time omogućuje toj osobi da pristupi zaraženom disku ili čak može da dobije pun pristup celokupnoj memoriji zaraženog računara.

Logička, odnosno tempirana bomba je program ili procedura koji se metodom „Trojanskog konja" ili na drugi način unosi u sistem i pričinjava štetu kada nastupi određeni uslov ili skup uslova. Uslov, odnosno uslovi se mogu odnositi na datum, vreme ili vršenje određenih funkcija od strane ovlašćenih korisnika u sistemu.

Računarska prevara - Računarske prevare predstavljaju najrašireniji vid računarskog kriminaliteta, koji često prouzrokuje enormne štetne posledice. Najbrojnije su u oblasti finansijskog poslovanja, osiguranja, poreskih obaveza, socijalnog osiguranja, u vezi sa proglašavanjem stečaja, pranjem novca, itd. Računarski prevaranti zloupotrebljavaju upravo one karakteristike cyber prostora koje doprinose rastu elektronskog poslovanja: anonimnost, distanca između strana i trenutna priroda transakcija. Uz to, oni koriste prednost činjenice da prevara preko Interneta ne zahteva pristup do nekog sistema za isplatu, kao što to zahteva svaka druga vrsta prevare, i što je digitalno tržište još uvek nedovoljno uređeno i kao takvo konfuzno za potrošače, što za njih predstavlja skoro idealne uslove za prevaru Težina računarske prevare je utoliko veća što one daleko dopiru zbog veličine Interneta, zatim, prilično se teško otkrivaju i dokazuju, a zbog male upadljivosti, vrlo često se ova dela vrše veoma dugo i u kontinuitetu.

Podvrsta računarskih prevara su Internet prevare. Internet prevara se odnosi na bilo koju prevaru pri čijem izvršenju se lice koje u nameri pribavljanja protivpravne imovinske koristi za sebe i drugoga iskoristi jednu ili više komponenti Interneta. Specifična vrsta Internet prevara jeste i svojevrsna grupacija prevara pod nazivom Nigerijske prevare.

Nigerijska prevara je metoda vršenja krivičnog dela prevare uz pomoć računara i najčešće počinje pismom ili elektronskom porukom koja je tako osmišljena da izgleda kao da je namerno poslata primaocu poruke. Radi se o prevarama koje se vrše pomoću lažnih poruka o dobicima na igrama na sreću, lažnih poruka vezanih za dobrotvorne priloge, poruke u vezi sa ljubavnim i poslovnim ponuda-

ma, humanitarnim akcijama, nasleđa imovine preminulih osoba - najčešće daljih rođaka. [11].

Ukoliko žrtva prevare odgovori na prvu poruku, ona se metodom socijalnog inženjeringa navodi da pomisli da je njena pomoć neophodna da bi se određena radnja izvršila. Nakon što oštećeni uplati određeni novčani iznos prema instrukcijama izvršilaca krivičnih dela sledi odlaganje novčanih transakcija vezanih za isplatu obećane sume novca. Stalno se pojavljuju novi troškovi za oštećenog na ime realizacije posla i traže nova odlaganja, stalno se obećava ekspresna isplata novca, uz ubeđivanje žrtve prevare da će joj se ulaganje u dogovoreni posao višestruko isplatiti [14, str. 148].

Zloupotrebe računarske mreže - Nesumnjivo je da računarska mreža može biti predmet različitih zloupotreba i sledstveno tome, može se naći u nekoliko različitih uloga.

Kriminal vezan za ovaj segment je oblik kriminalnog ponašanja kod koga je specifičnost okruženja razlog toga što se računarske mreže pojavljuju u trostrukoj ulozi:

kao sredstvo ili alat (npr. u vidu uznemiravanja, koje se, pre svega, odvija putem beskonačnog slanja elektronskih poruka licu koje ne želi ili nema razloga da komunicira sa pošiljaocem poruka),

kao cilj ili objekt napada (npr. napad na servise, funkcije i sadržaje koji se na mreži nalaze. Kradu se usluge i podaci, oštećuju se ili uništavaju delovi ili cela mreža i računarski sistemi, ili se ometaju funkcije njihovog rada) ili

kao okruženje izvršenja krivičnog dela (npr. okruženje služi za vrlo efikasno prikrivanje kriminalnih radnji).

Krađa identiteta - Krađa identiteta znači preuzimanje uloge nekog lica na Internetu, u cilju sticanja materijalne ili druge koristi. Ovo je najdrastičniji način narušavanja privatnosti nekog lica, jer se učinilac ove forme računarskog kriminaliteta, nakon što je došao do vitalnih podataka za preuzimanje nečijeg identiteta, predstavlja u njegovo ime vršeći različit broj aktivnosti, ostavljajući najčešće vrlo teške posledice za sobom, kako materijalne, tako i nematerijalne koje pogađaju žrtvu ovakve vrste zloupotrebe.

Vrši se na mnogo načina, od tradicionalne krađe i lažnog predstavljanja radi prikupljanja ličnih podataka, pa do skimming-a i phishing-a, sa kojima se danas u velikom broju slučajeva izjednačava sama pojava krađe identiteta. U svom osnovnom značenju, skimming predstavlja preuzimanje podataka sa magnetne trake ili čipa kreditne kartice uz pomoć posebnog elektronskog uređaja, tzv. skimera, što je podrobno objašnjeno u delu o zloupotrebama platnih kartica, dok phishing označava lažno predstavljanje u elektronskoj pošti kao postojeće kompanije, kojim se primalac navodi da prosledi svoje podatke na lažne adrese elektronske pošte.

Zloupotrebe platnih kartica, tzv. kartičarstvo- Poslednjih godina, zloupotrebe i prevare platnim karticama, kao i u sferi elektronskog bankarstva, postaju svakodnevna pojava.

Elektronski novac i elektronsko plaćanje je jeftinije od plaćanja u konvencionalnom bankarstvu, što doprinosi snižavanju troškova transfera novca. Prilikom elektronskog plaćanja troškovi transfera u zemlji su izjednačeni sa troškovima transfera u inostranstvu, čime ubrzavamo i pojeftinjujemo proces u međunarodnom prometu. Posebna prednost elektronskog plaćanja je njegova dostupnost svim korisnicima Internetu i za razliku od plaćanja kreditnim karticama kod elektronskog plaćanja postoji mogućnost plaćanja između dva fizička lica. Upravo snižavanje troškova i mogućnost plaćanja fizičkim licima otvara nove poslovne mogućnosti i doprinosi ekspanziji Internet aktivnosti [15, str. 108].

Izvršioci ovih kriminalnih delatnosti i bankama i njihovim klijentima nanose ogromnu štetu. Načini njihovog delovanja u cilju protivpravnog pribavljanja imovinske koristi za sebe ili drugog, putem zloupotrebe ili prevare platnim karticama, mogu biti različiti. Ovakve kartice se uglavnom ne koriste u zemljama u kojima su podaci ukradeni. Falsifikovane kartice se najčešće koriste na bankomatima.

PRAVNI OKVIR KOJI UREĐUJE OBLAST INFORMACIONOG DRUŠTVA I ELEKTRONSKOG POSLOVANJA U SRBIJI

U okviru Evropske unije informaciono-komunikacione tehnologije su prepoznate kao glavni faktor uticaja na ekonomski rast i inovativnost [5]., a među sedam vodećih inicijativa ekonomske strategije Evropa 2020 [3]. nalazi se "Digitalna agenda za Evropu", što pokazuje značaj koji informaciono-komunikacione tehnologije imaju u razvoju moderne ekonomije (Strategija razvoja informacionog društva u Republici Srbiji do 2020. godine, "Sl. glasnik RS", br. 51/2010 (u daljem tekstu: Strategija), deo I).

Razvoj informacionog društva treba usmeriti ka iskorišćenju potencijala informaciono-komunikacionih tehnologija za povećanje efikasnosti rada, ekonomski rast, veću zaposlenost i podizanje kvaliteta života svih građana Republike Srbije, pri čemu motor razvoja informacionog društva čine: otvoren, svima dostupan i kvalitetan pristup Internetu, kao i razvijeno e- poslovanje, uključujući: e-upravu, e-trgovinu, e-pravosuđe, e- zdravlje i e- obrazovanje (Strategija, deo I).

Potpisivanjem eSEE Agende+ [4]. za razvoj informacionog društva u Jugoistočnoj Evropi, Vlada je prihvatila i2010 inicijativu kao opšti okvir za razvoj Informacionog društva. Nakon toga Vlada je usvojila Akcioni plan za sprovođenje prioriteta iz "eSEE Agenda+ za razvoj informacionog društva u Jugoistočnoj Evropi za period 2007-2012. godine" ("Službeni glasnik RS", broj 29/09). Jedna od aktivnosti predviđena tim akcionim planom je i izrada Strategije (Strategija, deo II, str. 3).

Strategija razvoja informacionog društva u Republici Srbiji do 2020. godine jeste akt Vlade kojim se na celovit način definišu osnovni ciljevi, načela i prioriteti razvoja informacionog društva i utvrđuju aktivnosti koje treba preduzeti u periodu koji obuhvata ova strategija (Strategija, deo I). U skladu sa rečenim, Strategija ima prioritete i oblasti koje uređuje.

Aktivnosti koje se preduzimaju u cilju razvoja Informacionog društva treba da budu usmerene ka prioritetima u okviru sledećih oblasti (Strategija, deo III): elektronske komunikacije, e-uprava, e-zdravstvo i e-pravosuđe, IKT

u obrazovanju, nauci i kulturi, elektronska trgovina (e-trgovina), poslovni sektor IKT, informaciona bezbednost.

Pored Strategije, najznačajniji zakoni koji uređuju oblast informacionog društva su: Zakon o elektronskom potpisu ("Službeni glasnik RS", broj 135/04), Zakon o elektronskom dokumentu ("Službeni glasnik RS", broj 51/09), Zakon o telekomunikacijama ("Službeni glasnik RS", br. 44/2003, 36/2006, 50/2009 - odluka US i 44/2010 - dr. zakon), Zakon o elektronskoj trgovini ("Službeni glasnik RS", br. 41/2009 i 95/2013), Zakon o zaštiti podataka o ličnosti ("Službeni glasnik RS", br. 97/2008, 104/2009 - dr. zakon, 68/2012 - odluka US i 107/2012), Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu i Zakon o potvrđivanju Dodatnog protokola uz Konvenciju o visokotehnološkom kriminalu koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih preko računarskih sistema ("Službeni glasnik RS", broj 19/09).

Zakoni koji su takođe značajni, a uređuju materiju koja može biti značajna za pojedine aspekte elektronskog poslovanja su: Zakon o autorskom i srodnim pravima ("Službeni glasnik RS", br. 104/2009, 99/2011 i 119/2012), Zakon o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine (" Službeni glasnik RS", br. 46/2006 i 104/2009 - dr. zakoni) i Odredbe Krivičnog zakonika ("Službeni glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012 i 104/2013), glava XXVII - Krivična dela protiv bezbednosti računarskih podataka.

Zakonom o elektronskom potpisu uređuje se upotreba elektronskog potpisa u pravnim poslovima i drugim pravnim radnjama, poslovanju, kao i prava, obaveze i odgovornosti u vezi sa elektronskim sertifikatima, ako posebnim zakonima nije drugačije određeno.

Zakonom o elektronskom dokumentu uređuju se uslovi i način postupanja sa elektronskim dokumentom u pravnom prometu, upravnim, sudskim i drugim postupcima, kao i prava, obaveze i odgovornosti privrednih društava i drugih pravnih lica, preduzetnika i fizičkih lica, državnih organa, organa teritorijalne autonomije i organa jedinica lokalne samouprave i organa, preduzeća, ustanova, organizacija i pojedinaca kojima je povereno vršenje poslova državne uprave, odnosno javnih ovlašćenja u vezi sa ovim dokumentom.

Zakonom o telekomunikacijama se uređuju pitanja ovlašćenja za odlučivanje o broju i rokovima, odnosno periodu na koji se izdaje licenca za javne telekomunikacione mreže, odnosno usluge za koje se, u skladu sa ovim zakonom, može izdati ograničeni broj dozvola, kao i o minimalnim uslovima za izdavanje ovih dozvola, uključujući i najmanji iznos jednokratne naknade koja se plaća prilikom dobijanja dozvole, zatim pitanja o izdavanju licence, posebnim pravilima za izdavanje licence, kao i sadržaju licence i odobrenja.

Zakonom o elektronskoj trgovini uređuju se uslovi i način pružanja usluga informacionog društva, obaveze informisanja korisnika usluga, komercijalna poruka, pravila u vezi sa zaključenjem ugovora u elektronskom obliku, odgovornost pružaoca usluga informacionog društva, nadzor i prekršaji.

Zakonom o zaštiti podataka o ličnosti uređuju se uslovi za prikupljanje i obradu podataka o ličnosti, prava lica i zaštita prava lica čiji se podaci prikupljaju i obrađuju, ograničenja zaštite podataka o ličnosti, postupak pred nadležnim organom za zaštitu podataka o ličnosti, obezbeđenje podataka, evidencija, iznošenje podataka iz Republike Srbije i nadzor nad izvršavanjem ovog zakona (član 1. Zakona).

Zakonom o potvrđivanju Konvencije o visokotehnološkom kriminalu potvrđuje se Konvencija o visokotehnološkom kriminalu, sačinjena 23. novembra 2001. godine u Budimpešti, u originalu na engleskom i francuskom jeziku.

Zakonom o potvrđivanju Dodatnog protokola uz Konvenciju o visokotehnološkom kriminalu koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih preko računarskih sistema potvrđuje se Dodatni protokol uz Konvenciju o visokotehnološkom kriminalu koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih preko računarskih sistema, sačinjen 28. januara 2003. godine u Strazburu, u originalu na engleskom i francuskom jeziku.

Zakonom o autorskom i srodnim pravima uređuju se prava autora književnih, naučnih, stručnih i umetničkih dela (autorsko pravo), kao i pravo interpretatora, pravo prvog izdavača slobodnog dela, prava proizvođača fonograma, videograma, emisija, baza podataka i pravo izdavača štampanih izdanja kao prava srodna autorskom pravu (srodna prava), način ostvarivanja ovih prava i njihova sudska zaštita (član 1. Zakona). Kao što se vidi iz određenja predmeta Zakona, odredbe koje se odnose na regulisanje prava proizvođača baze podataka (kao kategorije dostupne najčešće elektronskim putem), nalaze se u delu koji uređuje prava srodna autorskom pravu.

Zakonom o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine regulisana je jedna od oblasti koja spada u visokotehnološki kriminal - zaštita intelektualne svojine. Ovim zakonom se uređuju posebna ovlašćenja nadležnih organa radi efikasne zaštite prava intelektualne svojine u skladu sa propisima kojima se uređuje pravo intelektualne svojine (član 1. Zakona). Odredbe Zakona primenjuju se na proizvodnju, promet, upotrebu i držanje robe i na pružanje usluga kojima se povređuju prava intelektualne svojine (član 2., stav 1. Zakona).

U skladu sa potrebom prilagođavanja našeg društva promenama koje se dešavaju u savremenom svetu, razvoju računarskih tehnologija i uopšte informacionih sistema, kao i zaštiti od opasnosti koje mogu nastati njihovom zloupotrebom, nacionalno krivično zakonodavstvo je upotpunjeno propisima kojima su sankcionisana krivična dela iz oblasti računarskog kriminala. Konkretna krivična dela, propisana krivičnim zakonodavstvom, jesu pre svega ona koja se odnose na bezbednost računarskih podataka. U Krivičnom zakoniku propisana su u Glavi XXVII (članovi 298-304a).

Iz predstavljenog pravnog aspekta može se zaključiti da je oblast informacionog društva uređena sa većim bro-

jem zakona, uključujući i Strategiju, odnosno akt koji na celovit način definiše i uređuje sva bitna pitanja razvoja informacionog društva. Zakonski okvir potpunjen je i sa zakonskim tekstovima koji uređuju oblasti veoma značajne za pojedine sfere elektronskog poslovanja, a koje su svakodnevno ugrožene preduzetim (konkretna opasnost) ili potencijalnim (apstraktna opasnost) rizicima.

ZAKLJUČAK

U radu je istaknuto da je ekspanzija Interneta na globalnom nivou dovela do mnogobrojnih promena koje su se reflektovale u brzom protoku informacija, prevazilaženju vremenskih i jezičkih barijera, brisanju lokalnih i regionalnih granica, napuštanju tradicionalnih i uvođenju novih oblika poslovanja i komunikacija.

Tehnološke mogućnosti koje je pružila globalna računarska mreža su potpuno otvorile vrata konceptu elektronskog poslovanja, time što su omogućile potpuno drugačije pristupe, u odnosu na tradicionalne načine, sferama prodaje, kupovine i internom kreiranju poslovnih procesa. Uvođenje novih tehnologija u oblast poslovanja uticao je na korenitu reorganizaciju ne samo u komunikaciji sa okruženjem, već istovremeno i u internim odnosima.

Ovakve promene svakako su meta različitih rizika. Drugim rečima, s obzirom da ne postoji ni jedno tehničko, niti tehnološko dostignuće koje do danas nije postalo predmet različitih zloupotreba, tako ni oblast elektronskog poslovanja nije odolela različitim mogućnostima manipulacija ili zloupotreba.

Kao prateća pojava različitim mogućnostima manipulativnog delovanja, svakako je usvajanje i primena zakonskih tekstova, upodobljenih evropskim standardima i zahtevima prakse. Pravna regulativa u oblasti uređenja informacionog društva, kao i zaštite određenih vrednosti u oblasti elektronskog poslovanja, veoma je sadržajna. Oslanjajući se na principe Strategije razvoja informacionog društva u Republici Srbiji do 2020. godine, u radu su predstavljeni svi relevantni zakoni iz ove oblasti.

Širi analitički pristup je neophodan zato što je oblast rizika u poslovanju putem Interneta veoma kompleksna i obuhvata veliki broj mogućnosti. Predstavljanjem najčešće zastupljenih rizika postalo je jasno da ovim aktivnostima oblast elektronskog poslovanja može biti značajno ugrožena, i da su posledice nesagledive ne samo sa moralnog aspekta, već i sa ekonomskog. Ovakav stav podržao je i širi zakonski obuhvat ove materije. Naime, tržišna utakmica obiluje različitim načinima tržišnog nadmetanja i isticanja komparativnih prednosti i konkurentnosti. Zloupotrebom informacionih tehnologija ovakva vrsta nadmetanja može poprimiti sasvim drugačije obime i oblike, sasvim suprotne tradicionalnim pristupima i principima konkurentnog poslovanja.

S obzirom da se oblast konkurencije i komparativnih prednosti procesa i sektora poslovanja smatra sistemom u kome svi privrednopravni subjekti nastupaju svojom privrednom inicijativom, jasno je da među njima nastaje svojevrsno privredno takmičenje koje je neophodno u svakom slučaju posmatrati dihotomno, odnosno uz ekonomski aspekat uključiti i adekvatne principe pravnog stanovišta [16, str. 225].

LITERATURA

[1] Akcioni plan za sprovođenje prioriteta iz "eSEE Agenda+ za razvoj informacionog društva u Jugoistočnoj Evropi za period 2007-2012. Godine, "Službeni glasnik RS", broj 29/09

[2] B. Gavrilović, „Osnovni modeli elektronskog poslovanja", Kompjuter biblioteka, 2006, Dostupno na: http://vesti.kombib.rs/Osnovni_modeli_elektronskog_poslovanja.html (23.01.2014.)

[3] Evropska strategija za pametan, održiv i sveobuhvatni razvoj - Europe 2020 - A strategy for smart, sustainable and inclusive growth - Communication from the Commission, COM (2010) 2020, Brisel 3. mart 2010. godine.

[4] "eSEE Agenda+ za razvoj informacionog društva u Jugoistočnoj Evropi 2007-2012" - Pakt za stabilnost, Inicijativa za elektronsku jugoistočnu evropu "eSEE" ("eSEE Agenda+ for The Development of Information Society in SEE 2007-2012" - Stability Pact, Electronic South Eastern Europe Initiative "eSEE"), Sarajevo, 29. oktobra 2007.

[5] "i2010 - Godišnji izveštaj o informacionom društvu 2007" - Saopštenje Evropske komisije Evropskom parlamentu, Savetu, Evropskom ekonomskom i socijalnom komitetu i Komitetu regiona ("i2010 - Annual Information Society Report 2007" - Communication from the Commission to the European parlament, the Council, the European Economic and Social Committee and the Committee of the regions), SEC(2007) 395, Brisel, 30. mart 2007. godine.

[6] J. Končar, „Elektronska trgovina", Ekonomski fakultet, Subotica, 2003

[7] Kompjuterski kriminalitet, APIS Security Consulting, APIS Group; http://www.apisgroup.org/sec.html/Knjige/UMOB/sec.html?id=29 (05.09.2010.)

[8] M. Gomilanović i M. Ivković, „Internet u Srbiji i segmentacija tržišta", Zbornik sa XII konferencije „YU INFO 2006", održane 6-10. marta na Kopaoniku, Društvo za informacione sisteme i računarske mreže, Beograd, 2006

[9] M. Babović, „Hakerska subkultura i kompjuterski kriminal", Pravni život, br. 9/2004, Godina LIII, Knjiga 485, 1-1356, Udruženje pravnika Srbije, Beograd

[10] M. Najdanović i S. Rajković, „Internet i elektronsko poslovanje", Poslovno komuniciranje, Departman za Multimedijalne tehnologije, Univerzitet u Nišu, 2012; Dostupno na: http://www.slideshare.net/MiB018/internet-i- elektronsko-poslovanje (23.01.2014.)

[11] MUP: "Nigerijska prevara" odnela Srbima stotine hiljada evra, Dostupno na adresa: http://www.vesti-online.com/Vesti/Hronika/48828/MUP-Nigerijska- prevara-odnela-Srbima-stotine-hiljada-evra (08.01.2011.)

[12] N. Pavlović i D. Tomić, „Osnovni rizici elektronskog poslovanja", Zbornik sa XII konferencije „YU INFO 2006", održane 6-10. marta na Kopaoniku, Društvo za informacione sisteme i računarske mreže, Beograd, 2006

[13] Strategije za elektronsko poslovanje, Dostupno na: www.ekof.bg.ac.rs/upload/1119SEP-2013-CAS02.pptx (22.01.2014.)

[14] V. Urošević, „Nigerijska prevara u Republici Srbiji", Bezbednost, Br. 3/2009, Godina LI, Beograd

[15] V. Raičević, J. Matijašević i S. Ignjatijević, „Ekonomski efekti i pravni aspekti elektronskog novca i elektronskog plaćanja", Economy and Market Communication Review (Emc Review), Fakultet poslovne ekonomije, Panevropski Univerzitet Apeiron, God./Vol. II, Br./No. I, Banja Luka, 2012, str. 105-118

[16] V. Raičević, S. Ignjatijević i J. Matijašević, "Economic and legal determinants of export competitiveness of the food industry of Serbia", Industrija, Journal of Economics Institute, Belgrade, Serbia Vol. 40, No. 1/2012, pp. 201-226

[17] V. Raičević, R. Glomazić i J. Matijašević, „Upravljanje projektima kroz IT komunikacije", Zbornik radova sa I Međunarodnog naučnog skupa „Moć komunikacije 2012" - održane 1-2. juna 2012. God. u Beogradu; Panevropski Univerzitet „Apeiron", Banja Luka; str. 206-217

[18] World Internet Usage and Population Statistics - for June 30, 2012, Copyright © 2001 - 2013, Miniwatts Marketing Group, http://www.internetworldstats.com/ (25.01. 2014.)

LEGAL AND ETHICAL ASPECTS OF THE RISKS OF E-BUSINESS

Abstract:
The use of the Internet in business has led to the creation of an entirely new business environment. The advantages of this type of business are many. On the other hand, e-business monitor risks, with the main feature of phenomenological variety that was growing more extensive. With the introduction of the most frequently represented risks, became clear that the area of e- business may be significantly compromised. This opinion is supported by the broader legal coverage of this matter.

Key words:
E-business,
Internet,
Risks of e-Business,
Legal legislation.