Članak je objavljen u Zborniku
Symorg 2004

RAČUNARSKA PREVARA I INTERNET PREVARA

Miloš Babović
IV Opš.sud u Beogradu

Uvod

Svaka država je dužna da fizičkim i pravnim licima omogući nesmetano učestvovanje na tržištu, štiteći pri tome sva njihova lična i imovinska prava. Tržište koje se odvija na Internetu (e-commerce), kao i bankarske transakcije (e-banking) predstavljaju zalog za budućnost razvoja ljudskog društva i po Strategiji EU iz Tamperea, jedan je od temelja(e-health, e-education…) elektronskog društva (e-society) . Iznad njih i oko njih kao zaštitna opna stoji elektronska sigurnost (e-security) koja treba da ostvari zaštitnu funkciju jer je sadašnje stanje u oblasti Interneta takvo da je Internet kao Divlji zapad na kome se pljačkaši tuđeg novca pojavljuju niotkuda, otimaju tuđ novac i nestaju bez traga, a države, među kojima je i naša , teže da koriste nove tehnologije u razvoju tržišta. Neki autori govore o ranjivosti informatičkog društva i o potrebi da se ona otkloni, koliko je to moguće, efikasnom pravnom zaštitom. Time bi se sprečila situacija u kojoj bi Internet bio raj za kriminalce kada bi bio onemogućen adekvatan protok podataka koji su ključni za elektronsko bankarstvo ,elektronsku trgovinu i elektronsku upravu. Ovim problemom se danas ozbiljno bave Evropska Unija, Savet Evrope, G8, Interpol i UN. Zaštitna funkcija vrednosti se pre svega u državi ostvaruje putem krivično pravne zaštite kroz generalnu i specijalnu prevenciju.

Internet je proizvod novog veka a prevara je poznata u pravnom smislu kao takva i regulisana još u starom veku. *Fraus in auctorem recidit* govorili su još stari Rimljani .

Internet kao prostor u kome se odvijaju računarske i internet prevare

Internet je postojeća virtuelna mreža kreirana od drugih *internetworking* mreža koje su povezanie TCP/IP protokolom ili drugim vidovima otvorenog pristupa jer je on javna mreža svima dostupna. Internet nije entitet već komunikaciona infrastruktura. Internet je mreža „svih" mreža koje međusobno komuniciraju. Nastao je početkom 90.-tih spajanjem regionalnih mreža .Tu se javlja pravni problem nadležnosti obzirom na geografski raspored servera na Internetu koji se nalaze širom sveta. Pre nego što se uopšte postavi pitanje ko je nadležan za događaj koji se desio na Internetu, potrebno je odgovoriti na pitanje gde se događaj koji se odigrao u virtuelnom svetu Interneta odigrao u fizičkom realnom svetu. Problem koji postoji na Internetu a koji takođe pogoduje internet prevarama je problem identiteta. Naime teško je na Internetu utvrditi nečiji pravi identitet (*On the internet nobody knows you are a dog* , je tekst ispod čuvene karikature objavljene u 5.7.1993. u Newyorker-u na kojoj je naslikan pas koji surfuje Internetom). Pitanje identiteta se danas rešava elektronskim potpisom i raznim sistemima identifikacije (Smart karticama, biometrikom itd. koji su predmet bavljenja drugih disciplina), i to samo donekle za određene korisnike i određene potrebe , dok u ostalom delu ovaj problem i dalje ostaje nerešen. Takođe koristi se i

termin za elektronsku trgovinu *staro vino u novim flašama* jer se stari vidovi trgovine i drugih delatnosti nalaze u novim, još uvek nesigurnim i vrlo sofisticiranim elektronskim okvirima Interneta. Zaključivanje ugovora putem Interneta koje je sve češće praćeno je elementima identifikacije. Postoji i problem i teškoća privatnosti na internetu koji takođe pogoduju internet prevarama .

Izazovi pred kojima se pravo nalazi

Sve ovo pravo postavlja pred velike izazove koji se ogledaju u tome da se u virtuelnom svetu javljaju neke situacije koje su nepoznate u fizičkom svetu i da ne postoje izgrađena pravna rešenja za te situacije. Zatim javljaju se problemi u smislu da je virtuelni svet digitalan i da su njemu neke akcije koje su fizičkom svetu zavisne od volje ovde automatske i da je u toj situaciji vrlo često teško otkriti ko je odgovoran i da li je odgovoran - što je primarno kod utvrđivanja građanske ili krivične odgovornosti. Izazov je u tome i da se benigne i uobičajene Internet transakcije obavljaju preko teritorija više zemalja i njihovih pravnih sistema. To dovodi do situacija mnogostrukih sukoba nadležnosti što za predmet ima u građanskopravnoj materiji posebna i složena disciplinamеđunarodnog privatnog prava. Lek za ovaj problem mogu biti međunarodne konvencije gde se opet postavlja problem unifikacije ili harmonizacije vrlo različitih pravnih sistema, sukoba interesa država koji obuhvataju i različite nacionalne standarde i tradicije, i mnogo veće sukobe interesa moćnih interesnih grupa koje pre svega obrazuju velike multinacionalne kompanije.

Terminološka pitanja

Postojeća literatura na stranim jezicima i na našem jeziku koristi termin *Internet Fraud* tj . internet prevara ili *Computer Fraud* ili kompjuterska prevara. Termin Internet Fraud je koristan i uobičajen pre svega na Internetu što nije za zanemarivanje. Ostaje kao primaran u Konvenciji o kibernetskom kriminalu Saveta Evrope iz 2001.godine i u legislativnim aktima unutrašnjih pravnih sistema država (koji su u Evropi uglavnom usklađeni sa Konvencijom o kibernetskom kriminalu Saveta Evrope iz 2001 iako ne uvek i u popunosti) termin računarska prevara iako se termin odnosi pre svega na internet prevaru jer kao što će biti prikazano u zakonskoj definiciji ona je dublje definisana samo kroz definisanje krivičnog dela prevare korišćenjem računara. Termin računarska prevara je širok i obuhvata definisanje i drugih vidova prevare putem računara. Oba ova termina su korektna i odgovarajuća za različite pojmove koje definišu. Za sud i za pravnike po vokaciji prednost ima termin iz konvencija i zakona a za laike kolokvijalni termin. U ovom radu je pažljivo pravljena ova terminološka razlika zavisno od pojma na koji se termin odnosio jer je i običaj sekundarni izvor prava pa se ona može koristiti za prevaru koja je nastala u određenoj vezi sa Internetom.

Definisanje pojma računarske prevare i internet prevare

Definisanje nekog pojma po Aristotelu , a koji i se i danas koristi u teoriji je *per genus et differentiam*, odnosno definisanje prvo rodnog pojma ili najbližeg pojma *genus proximum* a zatim i osobene razlike *differentia specifica*, pojma koji se definiše i ostalih pojmova koji se podvode po dati rodni pojam.

Ko u nameri da sebi ili drugom pribavi kakvu protivpravnu imovinsku korist, dovede koga lažnim prikazivanjem ili prikrivanjem činjenica u zabludu ili ga održava u zabludi i time ga navede da ovaj na štetu svoje ili tuđe imovine nešto učini ili ne učini izvršava krivično delo prevare u osnovom obliku iz člana 171 stav 1 Krivičnog zakona Republike Srbije .

Ko unese netačan podatak ili ne unese kakav važan podatak ili na drugi način prikrije ili lažno prikaže podatak i time utiče na rezultat elektronske obrade i prenosa podataka u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist i time drugom prouzrokuje imovinsku štetu izvršava krivično delo računarske prevare u osnovnom obliku iz člana 186g stav 1 Krivičnog zakona Republike Srbije.

Računarska prevara predstavlja bilo kakvu radnju izvršenja, u nameri pribavljanja protivpravne imovinske koristi sebi ili drugome koja se odnosi na rad računara i elektronsku obradu na njemu putem brisanja, unosa, izmene ili oštećenja podataka kao mogući načini da se prikrije ili lažno prikaže podatak.

Gore navedene definicije su zakonske i pošto se radi o imperativnim normama mi ih kao takve prihvatamo i koristimo. Definisanje Internet prevare ostaje zadatak primenom metoda *per genus et differentiam*. Time ćemo, po profesoru Kosti Čavoškom, dobiti deskriptivnu definiciju Internet prevare.

Genus proximum u navedenom slučaju je prevara, a mi tražimo osobenu razliku (*differentia specifica*) između računarske prevare i Internet prevare.

Internet prevara uošte se odnosi na bilo koju prevaru pri čijem izvršenju se lice koje u nameri pribavljanja protvpravne imovinske koristi za sebe ili drugoga iskoristi jednu ili više komponenti Interneta kao što su chat rooms (sobe za ćaskanje) , veb stranice (Web sites) , elektronska pošta (e-mail) da bi se stvorili uslovi za lažno prikazivanje ili prikrivanje činjenica kojim bi se neko lice dovelo u zabludu ili u njoj održavalo, da bi to lice učinilo nešto na štetu svoje ili tuđe imovine tako što bi na primer sprovelo neko finansijsku transakciju ili prenelo neke podatke nekoj finansijskoj instituciji koja je meta napada. Intenet prevarom se obmanjuje lice.

Računarska prevara može biti ostvarena na samo jednom računaru ili na intranetu (mreži koja nije na internetu i kontrolisana je od strane jednog ili više računara servera) i ne mora se odnositi na korišćenje resursa Interneta.Internet prevara nije uvek i obavezno računarska prevara , jer neke internet prevare odgovaraju klasičnim prevarama koje za sredstvo izvršenja imaju Internet bez nekog posebnog uticaja na elektronsku obradu ili rad računara (koristi se ljudski faktor koji je u elektronskoj sigurnosti obično slaba karika tj . obmanjuju se ljudi). Računarskom prevarom se „obmanjuje" računar i elektronska obrada navodi na pogrešan rezultat koji je usmeren na sticanje protivpravne imovinske koristi i to je *differentia specifica* ova dva pojma.

Bitni elementi prevare i računarske prevare

Bitan element kod prevare je subjektivni element zablude ili održavanja u zabludi(uopšteno rečeno – obmanjivanje), i uzročno posledična veza između obmane i radnje lica koje je pod obmanom izvršilo nešto na štetu svoje ili tuđe imovine (činjenje i nečinjenje).

Stvaranje odluke kod nekog lica putem dovođenja u zabludu je subjektivni element prevare i odnosi se na stvaranje odluke da lice preduzme neku delatnost ili je ne preuzme. To se pre svega odnosi na lažno prikazivanje ili prikrivanje činjenica kod krivičnog dela prevare a kod računarske prevare je to preciznije definisano na način kako se vrši izmena elektronskih podataka radi lažnog prikazivanja ili prikrivanja činjenica.Kod računarske prevare se ne vara neko lice već se računar uticajem na podatke navodi da izvrši određenu operaciju što je bio *ratio legis* uvođenja ovog instituta u odnosu na postojeće delo prevare a pod koji uglavnom podvodimo i Internet prevaru.

Dakle treba postojati veza između radnje lica koja ima nameru ostvarivanja protivpravne korisiti i zablude u kojoj se prevareno lice nalazi da bi se u krivičnom sudskom postupku mogla ostvariti krivično pravna zaštita i došlo do osuđujuće presude.

Objekat zaštite se ovde odnosi na imovinu u celini .

Kao oblik vinosti potreban je umišljaj.

Kod dela prevare i kod dela računarske prevare postoji kvalifikovani oblik kada vrednost prelazi određeni iznos i privilegovani oblici kada se delo vrši u nameri da se drugi samo ošteti ili ako šteta ne prelazi zakonom propisan iznos za krivično delo prevare a kad je umišljaj učinioca bio upravljen na ostvarivanje male imovinske koristi (sitno delo prevare).

Propisane kazne

Prevara -Član 171 stav 1 KZ RS

(1) Ko u nameri da sebi ili drugom pribavi kakvu protivpravnu imovinsku korist dovede koga lažnim prikazivanjem ili prikrivanjem činjenica u zabludu ili ga održava u zabludi i time ga navede da ovaj na štetu svoje ili tuđe imovine nešto učini ili ne učini, kazniće se zatvorom od tri meseca do pet godina.

(2) Ako je delom iz stava 1 ovog člana pribavljena imovinska korist u iznosu koji prelazi trista hiljada dinara, učinilac će se kazniti zatvorom od jedne do deset godina.

(3) Ako je delom iz stava 1 ovog člana pribavljena imovinska korist u iznosu preko osamstopedeset hiljada dinara, učinilac će se kazniti zatvorom najmanje tri godine.

(4) Ko delo iz stava 1 ovog člana učini samo u nameri da drugog ošteti,kazniće se novčanom kaznom ili zatvorom do jedne

Računarska prevara - Član 186g stav 1 KZ RS

(1) Ko unese netačan podatak ili ne unese kakav važan podatak ili na drugi način prikrije ili lažno prikaže podatak i time utiče na rezultat elektronske obrade i prenosa podataka u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist i time drugom prouzrokuje imovinsku štetu, kazniće se zatvorom od šest meseci do pet godina.

(2) Ako je delom iz stava 1 ovog člana pribavljena imovinska korist u iznosu preko sto hiljada dinara, učinilac će se kazniti zatvorom od dve do deset godina.

(3) Ako je delom iz stava 1 ovog člana pribavljena imovinska korist u iznosu preko šesto hiljada dinara, učinilac će se kazniti zatvorom od dve do dvanaest godina.

(4) Ko delo iz stava 1 ovog člana učini samo u nameri da drugom nanese štetu, kazniće se novčanom kaznom ili zatvorom do dve godine.

Iz navedenog zaključujemo da je pored postojećeg krivičnog dela prevare obzirom na stepen društvene opasnosti zakonodavac inkriminisao uskladu sa Konvencijom o kibernetskom kriminalu Saveta Evrope iz 2001. i računarsku prevaru i da je propisao u nekim slučajevima istu kaznu (član 171 stav 1 i član 186g stav 1) , u nekim oštriju kod prevare (član 171 stavovi 2 i 3 i član 186g stavovi 2 i 3) a u trećim oštriju kod računarske prevare (član 171 stav 4 i član 186g stav 4). Očigledno je primenjena slična nomotehnika (zakonodavna tehnika) .

Vođenje krivičnih postupaka i stanje u svetu i kod nas u borbi protiv računarskih i internet prevara

U oba slučaja, i kod prevare i računarske prevare, postupak pokreće javni tužilac po krivičnoj prijavi oštećenog ili policije. Od javnog tužioca i činjeničnog opisa dela zavisi pravna kvalifikacija dela , tj. da li će sepostupak voditi za računarsku prevaru ili će možda neku internet prevaru podvesti pod krivično delo prevare.

Iako se broj računarskih prevara masovno povećava u svetu samo mali broj kompanija koje su česte žrtve napada formiraju odgovarajuću politiku sigurnosti . Bez obzira što se gube milioni dolara , a inače godišnje u svetu elektroska trgovina ostvari zaradu od 10 milijardi dolara , mali broj kompanija uopšte objavljuje gubitke nastale na ovaj način a još ređe se vode sudski postupci protiv počinilaca računarskih i internet prevara. Borba se svodi na hardversku i softversku zaštitu što je kod prevare manje bitna nego kod drugih dela kompjuterskog kriminala jer je kod internet prevara vrlo često meta ljudski faktor. Sa razvojem tehnologije

računarska prevara postaje kompleksnija, sofisticiranija i njen međunarodni karakter je sve veći.

II opštinsko javno tužilaštvo je prošle godine pokrenulo postupak protiv grupe lica koja su se bavila internet prevarama sa elektronskim gitarama. U Srbiji obzirom na dugogodišnju izolaciju se pojavio veliki i dosta razgranat sistem hakerskih grupa kao što su Crna ruka , Srpska vojska inteneta i Srpski anđeli koji su vrlo često hvaljeni u javnosti zbog svojih ilegalnih pothvata , jer su uzimali učešće u različitim propagandnim ratovima . Postoji tendencija da se poveća broj korisnika Interneta u zemlji i samim tim poveća broj krivičnih dela u ovoj oblasti među kojima je i krivično delo računarske prevare.

U našoj zemlji što se policije tiče ovim problemima se bavi Uprava za informatiku MUP-a Srbije. Suzbijanje ove vrste kriminala je jako teško i u ovoj igri žandarma i lopova žandarmi svuda u svetu su u zaostatku pa i kod nas zbog visokog stepena obučenosti učinilaca dela i tehnologije koju poseduju. Nešto bolje rezultate ostvaruje NHTCU - National High Tech Crime Unit (specijalizovana britanska jedinica, najstarija te vrste u svetu) i FBI.

U Velikoj Britaniji je šestoro lica osuđeno na ukupno 15 i po godina zatvora za prevare tri britanske banke u iznosu od 350.000 funti a u SAD je u 2003. protiv 125 lica pokrenut postupak zbog internet prevara što su vodeći
rezultati u borbi protiv ove vrste krivičnih dela u svetu i odnose se samo na lica koja se nalaze pod jurisdikcijom i nadležnošću navedenih država, dok ostali ostju uglavnom nedostupni. Naša praksa ima jednocifren broj ovakvih postupaka.

Američki kongres je formirao posebnu komisiju koja se bavi kompjuterskim kriminalom a ona radnu grupu za kompjuterske prevare. Rezultat rada grupe su izveštaji a značajniji zaključci su sledeći:

1. da je veliki broj postupaka pored postojećeg krivičnog dela kompjuterske prevare vođena za prevaru,
2. da je prosečna kazna osuđenih za ovo delo 7 meseci zatvora ,
3. da postojeća pravna rešenja u velikom broju nisu odgovarajuća obzirom da je pojavni oblik u fizičkom svetu kod mnogih dela magnetni impuls, kako je to navedeno u izveštaju radne grupe za kompjutersku prevaru, a koji nije moguće podvesti pod postojeće pravne norme.

Postoje predviđanja po kojima , a među kojima je i II OJT u Beogradu, da će broj internet i računarskih prevara u budućnosti veoma rasti od strane širokog kruga korisnika interneta i elektronske trgovine kojaupravo pruža mogućnosti za internet i računarske prevare , i da će meta biti pre svega nedovoljno oprezni investitori i vlasnici kapitala željni brze i lake zarade.

Broj danas postojećih internet prevara je zaista veliki. Prema U.S. National Center for Computer Crime prevare čine 44% ukupnog kompjuterskog kriminala. One se odnose kako na privatni tako i na javni sektor. Većina njih je u stvari poznata od ranije , te je dobila svoj novi oblik i na Internetu mada su neke od njih nastale tek sa pojavom Interneta. Među njima postoje i određene klasifikacije po grupama (prevare sa plaćanjem unapred, aerodromske prevare, prevare sa popravkama automobila, bankarske i finansijske operacije prevara, prevare bankrota, kompjuterske lutrije, prevare sa kompjuterskom opremom, prevare sa kuponima za popuste, prevare sa razmenom valuta, prevare kreditnim karticama, prevare u

advertajzingu, prevare sa distribucionim centrima, prevare sa donacijama, elektronske prevare ,prevare imigranata ,prevare sa falsifikovanjima, prevare sa isporukama hrane, prevare vidovnjaka, prevarne internet kupovine, prevare u industriji zabave i igara, prevare sa dragim kamenjem, prevare sa američkom zelenom kartom, prevare u vezi sa građevinarstvom, prevare u vezi sa pružanjem medicinske nege, prevare sa ukradenim identitetom, prevare u vezi sa osiguranjem, prevare u vezi sa automobilima, jamajkanske prevare razmene, prevare u vezi sa nepokretnostima, prevare u vezi sa lutrijama , prevare u vezi sa investicijama u industriju, prevare sa medicinskim osiguranjem, internet onlajn aukcije, prevare sa ponudama posla, piramidalni sistemi prevare,prevare sa iznajmljivanjem, prevare starijih građana, prevare i krijumčarenje, spam , prevare sa telemarketima, zapadnofričke investicione prevare i mnoge druge jer se nova polja prevare stalno otkrivaju .

Jedna od najčešćih vrsta internet prevare je poznata koa nigerijska ili 491 prevara . ICC (International Chamber of Commerce- Međunarodna trgovinska komora) je 12.7.2002. godine našla za shodno da objavi i upozorenje na ovu temu. Njen biro za borbu protiv kriminala je objavio upozorenje korisnicima Interneta da se čuvaju mejlova u kojim se traži pomoć za tajne transfere desetina miliona dolara van Afrike čak i kada su pošiljaoci tvrdili da su zvaničnici vlada ili bivši šefovi država .Ovakveporuke slate uglavnom iz Lagosa mada je bilo i onih koji su ovakva delačinili iz Kanade i Velike Britanije. Dešavalo se da neki oštećeni otputuju čak i u Nigeriju vođeni lakovernošću, pohlepom i željom za brzom zaradom a neki su skončali i tragično. U mejlu bi se navodilo da je potrebno da primalac mejla dostavi podatke o bankovnom računu kako bi novac bio prenet na račun uz proviziju od 25% i naravno potpunu tajnost. Ono što bi sledilo je da bi sa tim dobijenim podacima vrlo lako mogao skinuti novac sa računa lica koje je poveravalo navodima iz ovakvog mejla.

Internet prevare u vezi sa akcijama su takođe veoma izražene. Naime, koriste se za mahinacije sa akcijama, jer sa internetu lako proturaju lažne informacije i na taj način utiče da akcije naglo padaju ili rastu i čime se pravovremenim kupoprodajama akcija ostvaruje protivpravna imovinska korist. Ovo je takođe stari način koji je sa Internetom kriminalce učinio efikasnijim .Posebno za borbu protiv ovakvihprevara u SAD je formiran SEC (Security and Exchange Comission) koji koordinirano deluje sa FBI - om.

Po podacima za 2001. godinu u SAD šteta nastala internet prevaramaiznosi od 6 miliona dolara po jednima do 700 milona dolara do drugim izveštajima(ova velika razlika u prcoeni zavisi od izvora i krriterijuma mada je tamna brojka sigurno velika). U samoj internet prevari kao pojavi je različit stepen zastupljenosti raznih vidova prevare. 70% internet prevara se odnosi prema nekim podacima na onlajn aukcije gde kupci plaćenu robu ili nikad ne dobiju ili obrnuto pošalju robu a novac im nikad ne stigne. Od oko 31% Amerikanaca koji koriste internet koristi usluge onlajn aukcija, od toga broja 41% je imao navedene probleme. Prosečan izgubljen iznos novca per capita je 326$. Smatra se da je u 2001. godini na ovaj način izgubljeno oko 700 miliona dolara , a postoje slučajevi gde su pojedinci gubili i više od 100 000 dolara. Naravno uglavnom su oštećeni svojim neodgovornim ponašanjem doveli sebe u navedenu situaciju. 9% internet prevara se odnose generalno na trgovinu, 9% na Nigerijske transfere novca, 2% na industriju seksa i porno industriju, 2% na nabavke računarske opreme, 2% na ponude za rad kod kuće, 2% na prevare za pristup internetu, 1% na pozajmice, 0,5 % na poslovne ponude i 0,5 % na prevare sa kreditnim karticama. Onima koji čine prevare Internet i računari pružaju velike mogućnosti. Pre svega u pogledu brzine, nedostupnosti organima gonjenja jedne zemlje ako se nalaze na teritoriji druge, i nedostatak javno objavljenih podataka o načinima vršenja ovih prevara. Desila se situacija ukojoj su već postojeće prevare do tada poznate dobile svoj Internet oblik(koliko je trgovina uznapredovala do elektronske trgovine prevare su možda i ostvarile još i veći napredak). Jednostavno razvoj

elektronske trgovine dovodi do cvetanja internet i računarskih prevara. Potrebne sunovestrategije za borbu i međunarodna saradnja. Elementi borbe su transparentnost u pogledu otkrivenih načina prevare, prijavljivanje prevara koje su se dogodile od strane oštećenih i kritika postojećih sistema borbe. Za efikasniju borbu u Americi je formiran IFCC (Internet Fraud Compliant Centre) kao zajednički projekat FBI-a i Nacionalnog centra zaborbu protiv kriminala belog okovratnika (National White Colar Crime Center) koji ima jedini zadatak da prikuplja prijave, analizira razne vrste internet prevara na osnovu kojih se pokreću postupci protiv učinilaca. Institut za nacionalnu bezbednost je objavio da je 85% organizacija objavilo narušavanje svojih računarskih sistema. Kompanije koje izdvoje 2%-5% svog budžeta se mogu izboriti sa ovom pretnjom i to ili primenom firewall ili encryption , međutim u oko 80% slučajeva su zaposleni iz firmi svesno ili nesvesno pomogli izvršenju ovih dela . Posebno o slabostima ljudskog faktora govori knjiga Kevina Mitnika ,, Umetnost obmane " koja sadrži veliki broj konkretnih primera iz prakse.

Uporedno pravo

Konvencija o kibernetskom kriminalu Saveta Evrope propisuje obaveze potpisnica konvencije da u unutrašnjem pravu regulišu dela iz oblasti kompjuterskog kriminala. Ova oblast traži pravna rešenja na globalnom nivou i harmonizaciju prava kao i učešće UN-a, EU , SAD, G8. Tako da danas Velika Britanija , Francuska , Nemačka ,Švedska,Finska, Luksemburg, Norveška, Austrija, Poljska , Češka , Danska , Španija , Turska , Hrvatska , Slovenija , Srbija i Crna gora , Estonija, Grčka regulišu delimično ili u potpunosti ovu oblast. Razlike postoje i one nisu velike. Delo ima svoj osnovni oblik koji je naveden i u Zakonskoj definiciji u KZ RS, a razlike postoje zavisno od različitih pravnih sistema i propisane kazne, a naša kaznena politika u ovoj oblasti spada u Evropi među strožije.Od vanevropskih zemalja regulativu u ovoj oblasti imaju pre svega SAD , Kanada , Australija , Japan , Kina , Indija itd.. Uporedno pravna analiza u ovoj oblasti bi mogla biti predmet jednog zasebnog i izuzetno značajnog rada za ovu oblast.

Krivična dela kompjuterskog kriminala su dokaz da postoji potreba za novim inkriminacijama u krivičnom pravu, i da postojeća regulativa koja u navedenim zemljama postoji treba da se unapređuje. Krivično delo računarske prevare je uglavnom regulisano svim navedenim pravnim sistemima. Neverovatan je podatak da pored postojećih krivičnih dela (nedostaje nam samo regulisanje kompjuterskog falsifikovanja) krivičnopravna zaštita u ovoj oblasti skoro da uopšte ne funkcioniše.Od zakonodavne regulative treba razlikovati uporednu sudsku praksu koju Nemci npr. kao i Britanci i Amerikanci imaju po oko30 godina, a koji imaju i veoma razvijene policijske jedinice za suzbijanje kopjuterskog kriminala i koja u stvari pokazuje kako i koliko se ove norme primenjuju. Veliki problem sudova je da prihvate stavove da su krivična dela kompjuterskog kriminala dela iste ili možda čak i veće društvene opasnostiod dela „klasičnog" kriminala i da u skladu sa tim sude počiniocima.

Z a k l j u č a k

Iz svega do sada navedenog slede dva osnovna zaključka:

1. da država ima zadatak da pojedincima obezbedi adekvatnu sudsku zaštitu kao preduslov za kvalitetno elektronsko tržište,

1. da pojedinac u svom ponašanju ima obavezu da se ponaša u skladu sa kulturom sigurnosti jer time štiti i privatni i javni interes.Ova oblast je u svetu a pogotovu kod nas nova . Ona zahteva konstantno praćenje jer je veoma dinamična. Sa rapidnim razvojem elektronske trgovine i bankarstva računarska i internet prevara postaju sve zastupljeniji oblici kompjuterskog kriminala i u interesu je društva da počinioce krivično goni jer time stvara preduslove za razvoj ovih grana važnih za razvoj države i društva.Počinioci su za sada u prednosti i elektronsko tržište je veoma ranjivo, ipak postoje realni planovi da se ovaj sistem uredi i na taj način trgovina i ekonomija znatno unaprede.