Univerzitet Singidunum

DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE

MASTER STUDIJE

Master rad

PRAVNA SIGURNOST UČESNIKA ELEKTRONSKOG POSLOVANJA

Mentor:
Docent dr Gojko Grubor

Student:
Bojana Živković

Beograd, oktobar 2010.

Pregled slika

Sl. 1. Točak elektronskog poslovanja
Sl. 2. Obim elektronskog poslovanja u 2008.
Sl. 3. Očekivani razvoj modela B2B i B2C

Pregled tabela

Tabela 1. Matrica e-trgovine

SADRŽAJ

UVOD

1. METODOLOGIJA IZRADE RADA
1.1 Obrazloženje teme
1.2 Predmet istraživanja
1.3 Ciljevi i zadaci istraživanja
1.4. Istraživačke hipoteze
1.5. Metode istraživanja i tok istraživačkog procesa

2. **ELEKTRONSKO POSLOVANJE I ELEKTRONSKA TRGOVINA**
2.1. Definicija elektronskog poslovanja
2.2.Točak elektronskog poslovanja
2.3. Razvoj i oblici elektronskog poslovanja
2.4 . Elektronska trgovina (*e-commerce*)

3. PRAVNA REGULATIVA U OKVIRU ZEMALJA EVROPSKE UNIJE I SAD-A
3.1. Osnovni principi
3.2. Poverenje korisnika i potrošača
3.3. Pravni okvir OECD i UNCITRAL-a
3.4. Pravni okvir SAD –a i Evropske Unije
3.5. Zloupotrebe u elektronskom poslovanju
3.5.1. Sukob domeni – žigovi
3.5.2. Neželjene reklamne poruke
3.5.3. Ugrožavanje privatnosti
3.5.4. "Obaranje" sajtova

4. MEĐUNARODNE INSTITUCIJE I IZVORI
4.1. Pravni akti doneti u okviru UNCITRAL-a
4.1.1. Pravni vodič o elektronskom prenosu sredstava
4.1.2. Model zakon UNCITRAL-a o elektronskoj trgovini
4.1.3. UNCITRAL Model zakon o elektronskim potpisima
4.2. Pravni akti doneti u okviru Evropske Unije
4.2.1. Direktiva o elektronskom potpisu
4.2.2 Direktiva o elektronskoj trgovini
4.2.3. Direktiva o zaštiti privatnih podataka

5. **PRAVNA REGULATIVA ELEKTRONSKOG POSLOVANJA U SRBIJI**
5.1. Strategije razvoja informacionog društva u republici Srbiji
5.2. Strategije razvoja trgovine Republike Srbije
5.3. Elektronski potpis
5.4. Zakon o elektronskom potpisu
5.5. Zakon o elektronskoj trgovini
5.6. Zakon o elektronskom dokumentu

6.OSNOVE KOMPJUTERSKOG KRIMINALITETA

6.1.Pojam kompjuterskog kriminaliteta
6.2. Karakteristike kompjuterskog kriminaliteta
6.3. Karakteristike učinilaca krivičnih dela kompjuterskog kriminala
    6.3.1. Hakeri
    6.3.2. Zlonamerni učinioci kompjuterskih delikta
6.4.Koristoljubivi kompjuterski kriminalitet
6.5.Posledice kompjuterskog kriminaliteta

7.MEĐUNARODNO REGULISANJE KOMPJUTERSKOG KRIMINALITETA

7.1.Komjuterski kriminalitet u uporednom krivičnom pravu
7.2.Pravno regulisanje kompjuterskog kriminala na nivou Evropske Unije

8.**PROPISI REPUBLIKE SRBIJE U OBLASTI KOMPJUTERSKOG KRIMINALITETA**

8.1.Krivično materijalno pravo
8.2.Konvencija o visokotehnološkom kriminalu
    8.2.1. Nedozvoljeni pristup
    8.2.2. Nedozvoljeno presretanje
    8.2.3. Ometanje podataka
    8.2.4. Ometanje sistema
    8.2.5. Zloupotreba uređaja
    8.2.6. Falsifikovanje koje je u vezi sa kompjuterima
    8.2.7. Prevare koje su u vezi sa kompjuterima

9. ORGANIZACIJA I NADLEŽNOST DRŽAVNIH ORGANA U BORBI PROTIV KOMPJUTERSKOG KRIMINALA

9.1.Posebno tužilaštvo
9.2.Služba za borbu protiv visokotehnološkog kriminala
9.3.Nadležnost i organizacija sudova
9.4.Dosadašnja primena ovih zakona

10.PROBLEM KOMPJUTERSKOG KRIMINALITETA IZ UGLA PROCESNOG ZAKONODAVSTVA

10.1.Digitalni dokaz
10.2. Međunarodni aspekt digitalnog dokaza
    10.2.1. Priznavanje dokazne snage po nacionalnim pravima
    10.2.2. Priznavanje dokazne snage u Republici Srbiji

11. DISKUSIJA

12. ZAKLJUČAK

13. LITERATURA

UVOD

Elektronsko poslovanje predstavlja digitalno omogućene transakcije i procese u okviru jedne organizacije uz pomoć i pod kontrolom njenog informacionog sistema. Zahvaljujući ubrzanom razvoju informacionih i komunikacionih tehnologija, došlo je i do ubrzanog razvoja elektronskog poslovanja. Jedna od osnovnih pretpostavki za uspešno elektronsko poslovanje jesu ažurni i adekvatni pravni okviri koji treba u potpunosti da definišu potrebe poslovnih subjekata i potrošača. Svest o toj neophodnosti dovela je do ubrzanih reakcija na međunarodnom i nacionalnom planu. Naime, učesnici u elektronskom poslovanju zahtevaju pravnu sigurnost koja će im omogućiti kako zaštitu imovine i privatnosti, tako i zaštitu od sve brojnijih tzv. sajber kriminalaca.

Internet je danas jedna od najregulisanijih oblasti društvenog delovanja. U EU postoji najmanje 15 direktiva, predloga i preporuka koje pokušavaju da regulišu elektronsko poslovanje. Evropska Unija je nastojala da u toj oblasti nametne zakonsku kontrolu i postoji nada da će svaka zemlja inkorporirati različite delove evropske zakonske regulative u svoje lokalne zakone. Neki od njih su Direktiva o e-potpisu, Direktiva o prodaji na daljinu i ugovaranju na daljinu, Direktiva o zaštiti podataka, Direktiva o e-trgovini, Direktiva o autorskom pravu...

U našoj zemlji je prisutna i sve više se razvija svest o neophodnosti i velikoj koristi od primene elektronskog poslovanja. Taj novi model poslovanja obezbeđuje ekonomičnost poslovanja, lakše komuniciranje sa domaćim i inostranim partnerima i komercijalne prednosti na tržištu. U poslovnim krugovima Evropske Unije i SAD je sve više prisutno shvatanje da se elektronskim poslovanjem zadobija značajna komparativna prednost na tržištu. Upravo iz svih ovih razloga postoji velika potreba da se i u našoj zemlji pristupi donošenju zakona koji bi na pravi način regulisali ovu oblast, kao i da se izvrši usklađivanja pravnog okvira sa zemljama Evropske Unije.

U prvom delu rada opisan je način pravnog regulisanja elektronskog poslovanja u zemljama EU, način zaštite učesnika u građansko-pravnim odnosima, kao i stanje u kome se naša zemlja trenutno nalazi. Rad je baziran na pravnim propisima EU kao i naše zemlje koji su neophodni za stvaranje povoljnog okruženja za razvoj ove oblasti.

Drugi deo posvećen je najvećim zloupotrebama u ovoj oblasti, koje predstavljaju najozbiljniju pretnju razvoju ove oblasti i najveću nesigurnost za učesnike u elektronskom poslovanju, a koje su poznatije pod imenom „ kompjuterski kriminal". Naime, savremena informaciona i kompjuterska tehnologija unela je nove i drastične promene u sve sfere društvenog života. Te promene su pored pozitivnih i korisnih novina donele i niz problema vezanih za pojavu i širenje kompjuterskog kriminaliteta različitih oblika, formi i vidova ispoljavanja. Sve te promene se mogu svesti na sledeće: nove forme vrednosti, koncentracija podataka, novi ambijent delovanja, nove metode i tehnike delovanja, sužavanje vremenske skale delovanja, širenje geografskog prostora delovanja, pokretljivost, stabilnost rizika.

Kompjuterski kriminal je pojava novijeg vremena, koja predstavlja poseban vid kriminaliteta. Pod kompjuterskim kriminalom obično se podrazumeva kriminalitet koji angažuje kompjuter kao sredstvo ili kao cilj izvršenja krivičnih dela. Kriminal u vezi s kompjuterima nije samo još jedan oblik običnog kriminala, već je to opšti vid svih oblika kriminala, tako da će kako nenasilni, tako i nasilni kriminal biti vezan za kompjutere.

Ovaj vid kriminaliteta za razliku od drugih ne predstavlja još uvek zaokruženu fenomenološku kategoriju te ga je nemoguće definisati jedinstvenim i precizno pojmovnim određenjem. Kompjuterski kriminalitet je samo opšta forma kroz koju se ispoljavaju različiti oblici kriminalne delatnosti. To je kriminalitet koji je upravljen protiv bezbednosti informacionih (kompjuterskih, računarskih) sistema u celini ili u njenom pojedinim delu na različite načine i različitim sredstvima u nameri da se sebi ili drugom pribavi kakva korist ili da se drugome nanese kakva šteta

Borba protiv kompjuterskog kriminala zasniva se na preventivnim i represivnim merama. Represivne operativno-taktičke mere su iste kao i kod drugih vidova kriminaliteta. Preventivne mere su specifične, one su usmerene na preduzimanje aktivnosti u cilju otklanjanja izvora. uslova, okolnosti ili propusta koji pogoduju neovlašćenom korišćenju ili zloupotrebi kompjutera.

U ovom radu izložen je kratak pregled propisa organizacionog, materijalnog i procesnog karaktera koji su na pravnoj snazi u Republici Srbiji, a odnose se na suzbijanje visokotehnološkog kriminaliteta. Ukratko su izloženi osnovni problemi koji su uočeni prilikom primene navedenih pravnih propisa kao i preporuke za njihovu izmenu u cilju efikasnijeg obračuna sa kompjuterskim kriminalitetom.

U oblasti borbe protiv visokotehnološkog kriminala u Srbiji najznačajniji pomak učinjen je osnivanjem specijalizovanih organa na nivou policije, tužilaštva i suda. Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, koji je stupio na pravnu snagu 25. jula 2005. godine, osnovano je Posebno tužilaštvo u okviru Okružnog javnog tužilaštva o Beogradu, posebno sudsko odeljenje u Okružnom sudu u Beogradu i specijalizovana policijska jedinica pri Službi za borbu protiv organizovanog kriminala.

1. METODOLOGIJA IZRADE RADA

1.1 Obrazloženje teme

Osnovu razvoja savremenog poslovanja čini razvoj informacionih i komunikacionih tehnologija. Ove savremene (digitalne) tehnologije pokreću prelazak iz industrijski bazirane ekonomije ka informaciono baziranoj ekonomiji istovremeno stvarajući globalno tržište, međunarodni proizvodni sistem i informacionu ekonomiju sa globalnim marketingom. Tako dolazi do sve većeg razvoja elektronskog poslovanja i stvaranja potpuno novog tržišta.

Mnoge zemlje u razvoju i zemlje u tranziciji žele da učestvuju u globalnoj ekonomiji koja se bazira na informacijama. Ove zemlje shvataju da pravni okvir i politika vlade mogu da igraju važnu ulogu u kočenju ili pomaganju razvoja informacionih i komunikacionih tehnologija, razvoju *online* ekonomije, odnosno elektronskog poslovanja. Naša zemlja zaostaje u ovoj oblasti, tako da pravna regulativa elektronskog poslovanja gotovo i da ne postoji. Dakle, tema koju ćemo prikazati u ovom radu predstavlja aktuelni problem i to kako na međunarodnom tako i na nacionalnom nivou. Smatramo da je istraživanje u ovoj oblasti neophodno, i da će predstavljati dobru osnovu za stvaranje pravne regulative u ovoj oblasti. Istraživanje u ovoj oblasti doprinosi ne samo razvoju elektronskog poslovanja i usklađivanju pravnog okvira sa zemljama Evropske Unije, već i drugim naučnim disciplinama koje se direktno ili indirektno bave ovom materijom.

Obično se ističu ekonomski doprinosi informacionih tehnologija, ali se još uvek malo govori o socijalnim efektima koji su sve značajniji. Socijalni efekti se ogledaju u porastu kvaliteta ličnog života na bazi primene digitalnih uređaja, stvaranju infrastruktura za razvoj e-demokratije, doprinosu informacionih tehnologija u prilagođavanju javnih servisa potrebama građana, razvoju digitalne pismenosti kako bi se koristile blagodeti informacionih i komunikacionih tehnologija, pojavi kompjuterskog kriminala i sl.

Dakle, u ovom radu ćemo obraditi i jednu od negativnih pojava vezanih za razvoj informacionih tehnologija, pojavu novog oblika kriminaliteta , tzv. kompjuterskog kriminaliteta.

Kompjuterski kriminalitet predstavlja oblik kriminalnog ponašanja, kod koga se korišćenje kompjuterske tehnologije i informacionih sistema ispoljava kao način izvršenja krivičnog dela, ili se kompjuter upotrebljava kao sredstvo ili cilj izvršenja, čime se ostvaruje neka u krivično-pravnom smislu relevantna posledica. Kompjuterski kriminalitet je takodje protivpravna povreda imovine kod koje se računarski podaci s predumišljajem menjaju (manipulacija računara), razaraju (računarska sabotaža), ili se koriste zajedno sa hardverom (krađa vremena).

Naša zemlja se veoma kasno uključila u regulisanje ove oblasti, ali je poslednjih godina ta aktivnost pojačana, tako da je stvorena određena pravna regulativa i posebne institucije čiji je zadatak borba protiv kompjuterskog kriminala. Tema ovog rada je pre svega obrada do sada učinjenih koraka i analiza dosadašnjih rezultata, kao i problema sa kojima se institucije u ovoj oblasti sreću. U radu je napravljena i analiza zakonodavstva zemalja koje su se dosta ranije uključile u rešavanje ovog problema. Smatramo da je ovakav pristup ovom problemu neophodan, i da će predstavljati dobru osnovu za neophodne izmene pre svega procesnih zakona u krivičnoj materiji, ali istraživanje u ovoj oblasti doprinosi i drugim naučnim disciplinama koje se direktno ili indirektno bave ovom materijom.

1.2 Predmet istraživanja

Predmet istraživanja vezuje se za utvrđivanje i stvaranje adekvatne pravne regulative elektronskog poslovanja na nacionalnom nivou, koja treba da doprinese razvoju elektronskog poslovanja i da omogući pravnu sigurnost za učesnike u različitim oblicima elektronskog poslovanja.

Predmet istraživanja sastoji se u izučavanju određenih pravnih propisa u ovoj oblasti i to kako na međunarodnom planu u okviru relevantnih međunarodnih organizacija, tako i na nacionalnim nivoima, pre svega u tržišno razvijenim zemljama. Preduslov za razvoj i funkcionisanje svih oblika poslovanja, pa i elektronskog poslovanja predstavlja adekvatno pravno regulisanje ovih oblasti.

Predmet istraživanja obuhvata i temu vezanu za proučavanje opasnosti koje sa sobom nosi razvoj novih tehnologija bez odgovarajućih pravnih akata i razvijenih kontrolnih mehanizama. Istraživanje se vezuje za mnogobrojne zloupotrebe, povrede prava na privatnost, nedostatak poverenje i ostale probleme koji se javljaju u oblastima koje nisu pravno regulisane.

Dakle,predmet istraživanja sastoji se i u izučavanju određenih krivično-pravnih propisa u ovoj oblasti, izučavanje pojma „ kompjuterski kriminalitet”, krivičnih dela iz ove oblasti, kao i novih institucija koje su uključene u borbu protiv kompjuterskog kriminala.

1.3 Ciljevi i zadaci istraživanja

Imajući u vidu važan nacionalni interes Srbije za pridruživanje Evropskoj Uniji, neminovno je da se moramo pridržavati Direktiva EU u cilju usklađivanja našeg zakonodavstva sa zakonodavstvom EU, te u skladu s tim i kompletnu zakonsku e-regulativu moramo u što kraćem roku uskladiti sa Direktivama EU iz te oblasti. U ovom radu koji se bavi pravnom regulativom elektronskog poslovanja na nivou Evropske Unije,

proučavane su i prevedene brojne Direktive EU, koje treba da posluže kao primer za izgradnju nacionalnog pravnog sistema.

U radu su proučeni kako građansko-pravni, tako i krivično-pravni aspekti pravne sigurnosti učesnika u elektronskom poslovanju, a napravljen je i uporedo-pravni pristup sadašnjem stanju u ovoj oblasti.

Dakle, cilj ovog istraživanja je stvaranje osnove za izradu pravnih propisa koji bi regulisali ovu oblast. Navedeni propisi trebaju biti u skladu s potrebama praktične primene u poslovanju i da budu usklađeni sa Direktivama EU.

1.4. Istraživačke hipoteze

Glavna hipoteza u istraživanju je pravno regulisanje elektronskog poslovanja koje treba da doprinese njegovom razvoju. Polazimo od pretpostavke da je za ubrzani razvoj elektronskog poslovanja u Srbiji neophodno doneti adekvatne pravne propise koji bi pravno uredili ovu oblast.

Takođe, polazi se od pretpostavke da brojne zloupotrebe koje su opisane u ovom radu, mogu da se otklone adekvatnim zakonskim propisima, kao i da navedene zloupotrebe utiču na proces razvoja elektronskog poslovanja, tako što se učesnici poslovnih procesa teže odlučuju da stupe u navedene poslovne procese. Ukoliko uporedimo proces razvoja elektronskog poslovanja u Evropskoj Uniji sa procesom pravnog regulisanja ovog oblika poslovanja, možemo videti da su se ta dva procesa razvijala gotovo uporedo, na način što je potpuno pravno uređivana svaka oblast elektronskog poslovanja.

U ovom radu su obrađene i najteže zloupotrebe informacionih tehnologija koje su zakonom predviđena kao krivična dela, a za čije je otkrivanje i procesuiranje nadležno posebno tužilaštvo i posebno odeljenje Okružnog suda u Beogradu. Izdvajanjem ovih institucija priznata je specifičnost ove vrste kriminaliteta, ali i velik značaj informacionih tehnologija.

1.5. Metode istraživanja i tok istraživačkog procesa

Dakle, kao što smo pomenuli svrha istraživanja je proučavanje pravnih akata koji regulišu oblast elektronskog poslovanja u tržišno razvijenim zemljama, međunarodnim organizacijama, a pre svega onih koje su donete na nivou Evropske Unije, kako bi se došlo do određenih saznanja koja su neophodna za definisanje pravnog okvira elektronskog poslovanja i izrade neophodnih zakonskih akata na nacionalnom nivou. Radi toga u

istraživanju su primenjene određene metode, i to metod teorijske analize koji obuhvata proučavanje literature i drugih izvora teorije i prakse pravne oblasti.

Pored navedenog u ovom radu smo koristili i metod analize, i to tako što smo najpre izvršili podelu pravne regulative u ovoj oblasti na pravne akte koji se donose na nacionalnim nivoima i na pravne akte koje donose međunarodne organizacije i koji imaju nadnacionalno dejstvo.

Zatim smo sve pravne akte podelili u grupu koja reguliše oblast elektronskog poslovanja, koja propisuje način poslovanja, definiše neophodne pojmove za elektronsko poslovanje i uvodi pravila koja moraju poštovati učesnici elektronskog poslovanja. Druga grupa propisa obrađuje najčešće zloupotrebe informacionih tehnologija i pokazuje koji su najčešći problemi sa kojima se sreću učesnici u elektronskom poslovanju.

U radu smo koristili i metod komparativne analize kako bi uočili određene sličnosti i razlike pravnih akata koji se donose u zemljama Evropske Unije i SAD, kao i postupak usklađivanja propisa zemalja Evropske Unije sa propisima koje donosi Evropska Unija. Izučavajući postojeće pravne propise u navedenim oblastima, njihovim detaljnim analiziranjem, a zatim i poređenjem došli smo i do određenih zaključaka koji se trebaju primeniti u procesu stvaranja pravne regulative elektronskog poslovanja kod nas.

S obzirom da je kompjuterski kriminalitet najveća pretnja razvoju elektronskog poslovanja i svakako najveći problem učesnika ovog poslovanja, u radu su proučeni I pravni akti koji regulišu oblast kompjuterskog kriminaliteta u tržišno razvijenim zemljama, međunarodnim organizacijama, a pre svega onih koje su donete na nivou Evropske Unije, kako bi se došlo do određenih saznanja koja su neophodna za rešavanje ovih problema u našoj zemlji.

2. ELEKTRONSKO POSLOVANJE I ELEKTRONSKA TRGOVINA

2.1. Definicija elektronskog poslovanja

Tradicionalno poslovanje

Tradicionalno poslovanje zasnovano je na korišćenju strukturiranih papirnih dokumenata u prethodno definisanoj i opšteprihvaćenoj komunikaciji između učesnika u procesu poslovanja.

Elektronsko poslovanje (e-busines):

Elektronsko poslovanje predstavlja digitalno omogućene transakcije i procese u okviru jedne organizacije uz pomoć i pod kontrolom njenog informacionog sistema

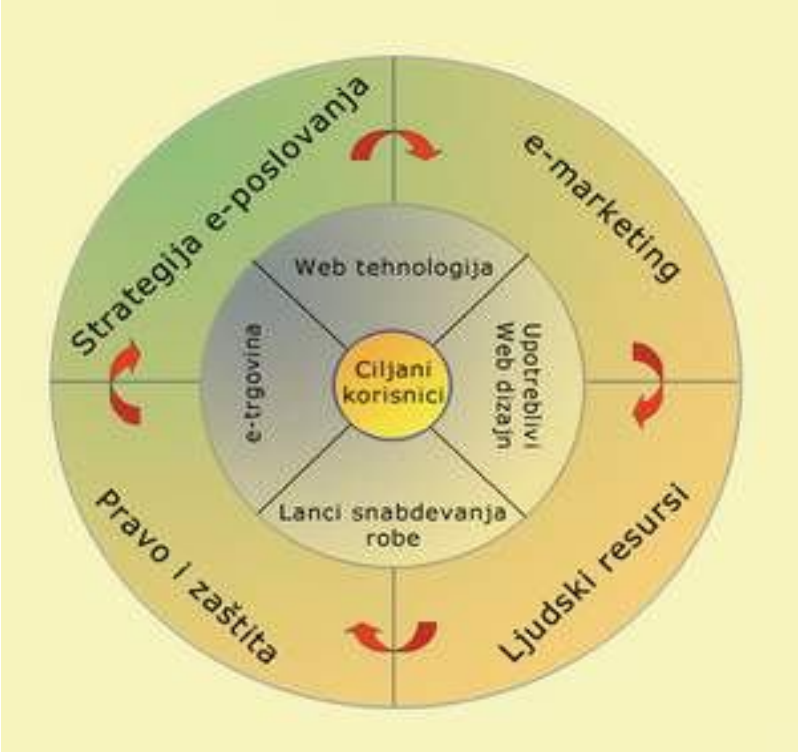
E-biznis ne obuhvata komercijalne transakcije izvan granica organizacije gde se vrši razmena vrednosti.

2.2. Točak elektronskog poslovanja

Poznavanje upotrebe elektronskog poslovanja podrazumeva poznavanje poslovnih procesa elektronskog poslovanja. Konceptualni model *"eBusiness Wheel" (točak elektronskog poslovanja)*, opisuje najbitnije procese e-poslovanja.

On se sastoji od sedam delova koji okružuju klijenta kao polaznu osnovu svih savremenih poslovnih procesa. Osnovni cilj svih savremenih poslovnih koncepcija jeste zadovoljenje potreba klijenata i formiranje takvog poslovnog okruženja u firmi da svi poslovni procesi budu u funkciji klijentovih potreba, a da se kao rezultat kvalitetnih odnosa s klijentima pojavi profit.

Točak elektronskog poslovanja se sastoji iz dva glavna dela: strategije elektronskog poslovanja i primene elektronskog poslovanja (operativni procesi) (Sl. 1). Strategijama elektronskog poslovanja definišu se svi poslovni procesi koji imaju za krajnji cilj zadovoljstvo klijenta i profit firme. Međutim, da bi se ostvario cilj elektronskog poslovanja, potrebno je kreirati i voditi operativne procese koji u biti čine elektronsko poslovanje.



Sl. 1. Točak elektronskog poslovanja [11]

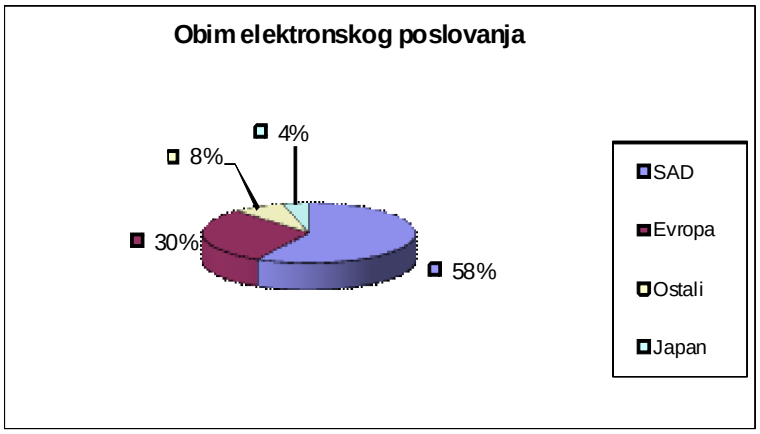
2.3. Razvoj i oblici elektronskog poslovanja

Elektronsko poslovanje se pojavilo početkom 80-tih godina prošlog veka, ali je ubrzan razvoj doživelo poslednjih godina, pre svega zahvaljujući Internetu.

Elektronsko poslovanje (*electronic business*) predstavlja razmenu standardizovanih elektronskih poruka u obavljanju raznih poslova u kompanijama, bankama, upravi, aktivnostima građana i u svim drugim poslovnim transakcijama.

Elektronsko poslovanje podrazumeva obavljanje poslovnih procesa uz primenu elektronske tehnologije. Ova vrsta tehnologije omogućava slanje velikog broja informacija, na velike daljine u kratkom vremenskom periodu. To omogućava kompanijama koje u svom poslovanju koriste elektronsku tehnologiju da ostvare značajne uštede u troškovima poslovanja, efikasnije obave svoje zadatke i budu konkurentnije na tržištu. Obim elektronskog poslovanja razlikuje se od države do države (Sl. 2).

[1] *Informacije preuzete sa sajta* *www.lugram.net/e_**poslovanje***



Sl. 2. Obim elektronskog poslovanja u 2008
Izvor: *"The Real Numbers behind 'Net Profits 2008"*

Elektronsko poslovanje ima vrlo široko područje uticaja i primene, pa bi tako osnovi oblici bili :

e-Trgovina - predstavlja poslovnu komunikaciju i prenos dobara i usluga (kupovina i prodaja) – razmena vrednosti.

e-Bankarstvo - predstavlja poslovanje na relaciji banka-klijent

e-Uprava - elektronsko poslovanje u upravi ili administraciji (države, preduzeća,kompanije ...)

Jedna od tačaka eEurope operativnog plana Evropske komisije iz 2002. godine naglašava značaj razvoja savremenih javnih servisa i u oblasti *e-Zdravlja* i *e-Obrazovanja* i *sl.*

Elektronsko poslovanje ima sledeće prednosti:

- smanjenje troškova poslovanja, i to prevashodno vezane za izradu papirnih dokumenata,
- smanjenje grešaka, pogotovo gde je tačnost informacija od značaja,
- ušteda vremena, posebno u prenosu informacija,
- smanjenje obima ljudskoga rada,
- pristupačnost i razmenjivost informacija.

2.4 . Elektronska trgovina (*e-commerce*)

Predstavlja razmenu poslovnih informacija, održavanje poslovnih veza i vođenje poslovnih transakcija između različitih organizacija putem telekomunikacionih mreža.

Pored toga, možemo reći da je kupovina i prodaja informacija, proizvoda i usluga putem računarske mreže i podrška za bilo koju vrstu poslovnih transakcija putem digitalne infrastrukture - digitalno omogućene komercijalne transakcije između organizcija (B2B), organizacija i pojedinaca (B2C), pojedinaca (C2C), organizacija i vladinih agencija (B2G),vladinih agencija (G2G) itd.

Klasifikacija e-trgovine prema tipovima učesnika uobičajeno se prikazuje matricom e-trgovine (Tabela 1).

Tabela 1. Matrica e-trgovine

	Business	*Consumer*	*Government*
Business (poslovni sistemi)	B2B	B2C	B2G
Consumer (potrošači)	C2B	C2C	C2G
Government (vlade zemalja)	G2B	G2C	G2G

B2B (*Business-to-business***)**

Interorganizacioni informacioni sistem u kojem kompanija upravlja transakcijama unutar njenog sopstvenog vrednosnog lanca ili sa drugim kompanijama i organizacijama. B2B se ponekad naziva *business-to-employee* (**B2E**) kada je fokusiran na upravljanje aktivnostima unutar organizacije.

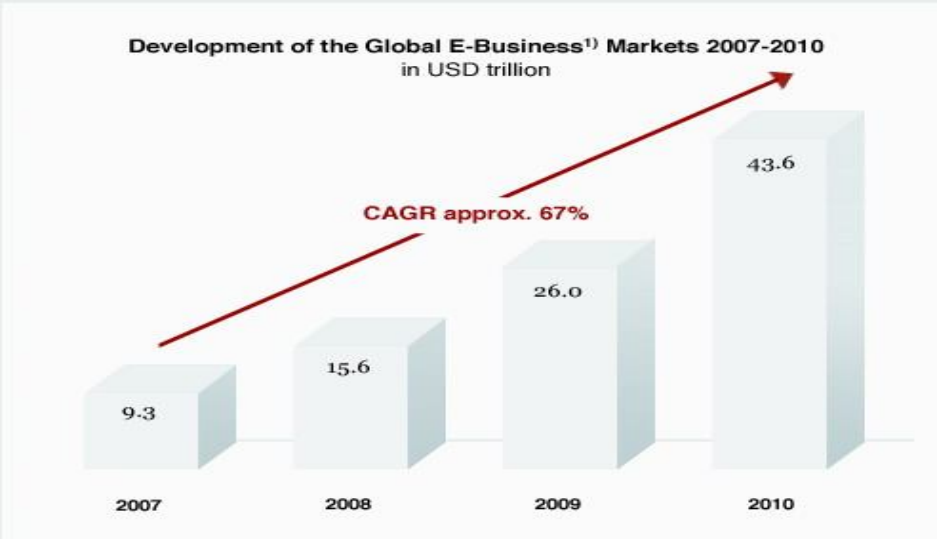
Učesnici u ovom tipu e-trgovine su organizacije i poslovni sistemi. Početak B2B poslovanja vezuje se za pojavu prvih EDI (*electronic data interchange*) sistema. Eliminišu se brojni nedostaci komunikacije klasičnim sredstvima (gubljenje dokumenata, oštećenje u prenosu, greške u prekucavanju teksta itd.).

Predstavlja najvažniji oblik e-trgovine, transakcijama na ovom tržištu ostvaruje se između 80-85% ukupnih prihoda od e-trgovine na Internetu

B2C (*Business-to-consumer*)

Prodavci su organizacije, a kupci su pojedinci. Uglavnom se odnosi na maloprodajne transakcije između kompanija i individualnih potrošača. Jedan od uspešnih primera je *Amazon.com***,** osnovan 1994. godine, i on predstavlja tipičan primer kompanije koja se bavi ovim poslovanjem. Neverovatan uspon Amazona - 20 miliona korisnika u više od 160 zemalja kupilo je 2000. g. robu u vrednosti od 2,8 milijardi $.

Ovaj poslovni model oslanja se na sposobnost Interneta da prenosi ogromnu količinu informacija brzo i efikasno. B2C je najjasniji aspekt e-trgovine iz korisničke perspektive. Očekivani razvoj globalnog tržišta e-poslovanja 2007-2008 u SAD prikazan je na slici 3.



Sl. 3. Očekivani razvoj modela B2B i B2C [2]

C2C (*Consumer-to-consumer***)**

Potrošači direktno prodaju robu ili usluge drugim potrošačima on-line putem, uključuje i prodaju nekretnina, automobila i dr. u *on-line* oglasima. Najpoznatiji primer C2C je web sajt ***eBay.com*** Neki aukcijski sajtovi nude mogućnost C-C elektronske trgovine- omogućavaju korisnicima da ponude robu na *on-line* aukcijama. Ovaj oblik transakcija podrazumeva učešće i treće strane u *online* trgovini.

Treća strana može biti neki aukcijski sajt: eBay, *Gnutella* (prodaja muzike), Monsters (*online* poslovi), Owners.com (klasifikovane reklame), itd.

Poseban oblik C-C transakcija predstavljaju transakcije u *peer-to-peer* komunikaciji bez posrednika (*KazaA, Tornet* programi).

[2] Izvor : *Internet Advertising, B2B-E-Commerce, B2C E-Commerce*
Sources: International Data Corporation (IDC), Standard & Poor`s, 2007;
Global Industry Analysts, 2007, WilkofskyGruenAssociates 2007

3. PRAVNA REGULATIVA U OKVIRU ZEMALJA EVROPSKE UNIJE I SAD-A

Uspešan razvoj elektronskog poslovanja zahteva ispunjenje određenih preduslova i to :

- postojanje odgovarajućih pravnih okvira.
- razvoj informacione strukture,
- korišćenje odgovarajuće informacione tehnologije i usluga koje treba da obezbede pouzdan i neometan pristup globalnom tržištu,
- obezbedjenje pogodnih poslovnih uslova i okruženja i sl.

U ovom radu pažnju smo usmerili na prvi preduslov razvoja elektronskog poslovanja, te smo želeli da pokažemo koji su to aktuelni problemi sa kojima se učesnici u ovom prometu najčešće sreću, kao i način regulisanja ove oblasti sa stanovišta međunarodnih institucija i međunarodnog prava.

3.1. Osnovni principi

Evropska unija ceo svoj pravni okvir bazira na dva komplementarna principa

- Izgradnji poverenja i
- obezbeđivanje punog pristupa jedinstvenom tržištu.[3]

SAD u okviru Globalne informacione infrastrukture ide dalje bazirajući se na principima :

- vodeće uloge privatnog sektora u poslovanju na internetu,
- vladine intervencije samo kao podrške u jačanju budućeg jedinstvenog pravnog okruženja,
- nužnom olakšavanju ovog poslovanja na globalnim osnovama,
- zaštitom intelektualne svojine.[4]

OECD je kao osnovne principe istakao :

- Izgradnju poverenja za korisnike i potrošače ;
- Uspostavljanje osnovnih pravila digitalnog tržišta,
- Razvijanje informacione infrastrukture za e-poslovanje i sl.[5]

3.2. Poverenje korisnika i potrošača

Doktrina *fer poslovanja i trgovine* potekla je iz *Common Law* sistema, a punu afirmaciju stiče u elektronskom poslovanju i trgovini. Ovaj vid trgovine i poslovanja nužno počiva na poverenju svih strana, a naročito trećih lica. U klasičnom poslovanju stranke svoje međusobne odnose uspostavljaju u pravnim okvirima vezanim za ugovore, prava, obaveze i odgovornosti. Postojeća pravna pravila nisu pogodovali Internet

[3] Izvor : *Communication to the European Parliament, the Council, The Economic and Social Commitee and the Committee of the Regions, A European Initiative in Electronic Commerce, COM*
[4] Izvor *U.S Goverment Working Group on Electronic Commerce* www.ecommerce.gov
[5] Izvor *Directorate for Science, Tehnology and Indastry OECD, A global plan for Electronic Commerce*

ekonomiji, poslovanju i elektronskoj trgovini. Tako nastaje pravna praznina koju su pokušali da popune organi i tela G-8, OECD, Svetske trgovinske organizacije, izgrađujući pravnu i regulativnu infrastrukturu. Međutim, to nije bili dovoljno, te su morala stupiti na snagu nova pravila. Jedan od njih je princip poverenja i fer trgovine.[6] Ovaj modifikovani princip počiva na poverenju korisnika i potrošača.

Postizanje poverenja zasniva se na obezbeđenju njihove zaštite, odnosno na sigurnosti njihovih transakcija i omogućava verifikaciju bitnih informacija koje se tiču njihove aktivnosti, odnosa i partnera. Korisnici i potrošači žele da imaju kontrolu nad korišćenjem svojih podataka o ličnosti i da su sigurni da su primenjeni odgovarajući sistemi zaštite.

Dakle, zaštita korisnika odnosi se na obezbeđenje njihove privatnosti i anonimnosti, kao i kontrolu sadržaja njihovih poruka i ostalih bitnih elemenata od kojih zavisi njihovo poverenje u sistem i mehanizme ovog tipa poslovanja.

Zaštita potrošača treba da pruži odgovore na pitanja vezana za tačnost podataka i informacija, forme ugovora, zadovoljenje potreba, izgradnju mehanizama zaštite od potencijalnih zloupotreba i prevara, osiguranje privatnosti, zaštitu elektronskog okruženja za elektronsko poslovanje. Izgradnja poverenja potrošača pretpostavlja eliminaciju nelojalnih i obmanjivačkih radnji i prakse i uspostavljanje ravnoteže u odnosima između prodavca i potrošača u komercijalnim transakcijama. Ovakva zaštita je veoma otežana na elektronskom tržištu, naročito što nema direktnog odnosa " licem u lice " kao što je to slučaj u klasičnom poslovanju. Zato je poverenje jedna od osnovnih pretpostavki funkcionisanja ovog tržišta i elektronskog poslovanja. Zato je sve prisutnija regulacija zaštite potrošača i stvaranje uslova za obezbeđivanje njihovog poverenja. Međunarodne institucije, asocijacije i organizacije preduzimaju brojne aktivnosti i donose posebne akte kojima bi se to i realizovalo. Tako je npr. OECD doneo Ministarsku deklaraciju o zaštiti potrošača u kontekstu elektronske trgovine, slično je učinjeno i u okviru Evropske Unije , tj, doneto je Uputstvo za zaštitu potrošača u kontekstu elektronske trgovine. Svemu treba dodati i probleme koje donose udaljene lokacije potrošača i prodavca, ekstenzivnost i fluktuiranost elektronskog tržišta.[7]

3.3. Pravni okvir OECD i UNCITRAL-a

Kako elektronsko poslovanje omogućava izvršavanje klasičnih poslovnih zloupotreba kao što su prevare, finansijske malverzacije ili izbegavanje plaćanja poreza na nov način potrebno ga je posebno regulisati jer se pravila i kontrolni mehanizmi klasičnog poslovanja ne mogu primeniti.

Međutim, to nije tako jednostavno, prvenstveno zato što je ova nova oblast poslovanja u stalnim i brzim promenama. Pored toga, tehnologija koja se primenjuje nije

---

[6] Izvor *Directorate for Science, Tehnology and Indastry OECD, A global plan for Ele Electronic Commerce. www.oecd.org*

[7] Izvor *Drakulić M., Osnovi Poslovnog prava, Beograd, FON, 2001*

ograničena samo na jedan region ili zemlju, što sa svoje strane dovodi do problema na koji postojeći pravni sistemi ne daju zadovoljavajuće odgovore pošto je njihovo važnije ograničeno teritorijom države u kojoj se primenjuje.

Izlaz je pokušan da se nađe u međunarodnim organizacijama i telima Ujedinjenih nacija, Svetske trgovinske organizacije ili u okviru regionalnih ekonomskih blokova, kao što je Evropska Unija. Sporost u dogovaranju koja je posledica usaglašavanja stavova između zainteresovanih država prouzrokuje relativnu neefikasnost ovih tela.

Pored toga, njihove odluke su obavezne samo za one države koje su se izjasnile da ih prihvataju. Međutim, potrebe za smanjenjem troškova poslovanja i želja za povećanjem tržišta koja je sublimirana u elektronskom poslovanju dovela je do toga da mnoge razvijene zemlje ubrzano pristupaju njegovom regulisanju.

Ulogu međunarodnih organizacija vezanu za elektronsko poslovanje, možda, najbolje ilustruje OECD koji je 1996. godine doneo izveštaj pod nazivom "Globalna informaciona infrastruktura - globalno informaciono društvo" prvenstveno namenjen vladama država članica. U Izveštaju se ističe globalni karakter elektronskog poslovanja i sugeriše vladama, uvažavajući sve političke i pravne razlike između država, da podstiču digitalno poslovanje stvarajući uslove uz što manje povećanje regulative. Kako nacionalna zakonodavstva nisu i neće biti direktno primenjiva u svim oblastima kiber prostora (*cyberspace*) poslovanja, potrebno je regulativi ovog područja pristupiti putem samoregulacije.

Naročitu pažnju treba obratiti na sigurnosti i autentičnosti elektronski dokumenata koja se razmenjuju između subjekata iz različitih država kako bi ona bila pravno valjana. OECD predlaže da se što pre dođe do zajedničkih stavova vezanih za legalnost elektronskih dokumenata putem elektronskog potpisa.

Bez obzira što je u mnogim zemljama obavljanje poslovnih transakcija telefonom i/ili faksom uobičajena stvar, izgleda da postoji psihološka barijera za njihovo izvršavanje putem Interneta. To je najverovatnije posledica dileme koja se javlja kod poslovnih subjekata i vezana je za nadležnosti pravnih sistema na globalnoj računarskoj mreži. Naime, postavlja se pitanje koji pravni sistem će se koristiti u slučaju spora u prekograničnom prometu roba i usluga putem mreže?

Rešavanje ovog problema sigurno će pozitivno uticati na uspeh elektronskog poslovanja. Jedno od rešenja bi moglo biti da je za pravne posledice proizašle iz ugovora koji se odnose na elektronsko poslovanje nadležan pravni sistem sa teritorije gde se nalazi prodavac. Problem postaje složeniji kada se posao vodi u nekoliko zemalja. Takođe se postavlja pitanje da li je sedište prodavca u elektronskom poslovanju tamo gde je lociran server sa koga on nudi svoju robu i usluge ili na nekom drugom mestu. U globalnom elektronskom poslovanju uobičajeno je da organizacija u nekoj zemlji ima server i ništa više, to je naročito izraženo kod "virtualnih organizacija" koje sigurno ne potpadaju ni pod jedan geografski ograničen pravni sistem.

Komisija Ujedinjenih nacija za međunarodno trgovačko pravo (UNCITRAL)[8] sačinila je model zakona kojim se reguliše elektronsko poslovanje. Bez obzira što se ovaj model bazira na zakonu o trgovini SAD, njegova namena nije da pojedinačnim zemljama preporuči prilagođavanje američkog modela njihovom pravnom sistemu već da ukaže na pravce mogućih rešenja koja će zavisiti od pravne tradicije i interesa svake zemlje da se uključi u elektronsko poslovanje.[9]

3.4. Pravni okvir SAD –a i Evropske Unije

Evropska Unija je svoju politiku u oblasti elektronskog poslovanja deklarisala 1997. godine kao "Evropsku inicijativu u oblasti elektronskog poslovanja". Na osnovu ove inicijative bliska su rešenja koje su zemlje članice pojedinačno donele u regulisanju digitalnog potpisa, sistema šifriranja i potvrde autentičnosti. U EU postoji najmanje 15 direktiva, predloga i preporuka koje pokušavaju da regulišu e-trgovinu. Taj udar je značajan, iako izgleda da su te direktive donete deo po deo. EU je nastojala da u toj oblasti nametne zakonsku kontrolu i postoji nada da će svaka zemlja inkorporirati različite delove evropske zakonske regulative u svoje lokalne zakone. Neki od njih su Direktiva o e-potpisu, Direktiva o prodaji na daljinu i ugovaranju na daljinu, Direktiva o zaštiti podataka, Direktiva o e-trgovini, Direktiva o autorskom pravu...

Iako su mnoge evropske *online* organizacije svesne brojnih EU Direktiva koje se odnose na e-trgovinu, one još uvek nisu donele plan o poslovanju u skladu sa njima. Razlog za to je da su organizacije u svom poslovanju uglavnom zabrinute zbog nesigurnosti i agresivnog nastupanja zakona u B2C e-trgovini, sa akcentom na razlici između principa “zemlja porekla” i ”zemlja odredišta”. Neke države i regionalne organizacije su usvojile princip ”zemlja odredišta”, čije je značenje da se primenjuje zakon one države na kojoj sedište ima potrošač, kada je u pitanju B2C model e-poslovanja. Postoji mišljenje da je primena principa “zemlja porekla” ipak poželjnije i funkcionalnije rešenje.

Podaci pokazuju da mnoge kompanije danas jednostavno nisu voljne da snose troškove istraživanja i usaglašavanja sa mnoštvom pravila u svakoj od zemalja, ili da rizikuju mogućnost sankcija, neprimenjivih ugovora, ili nepovoljnog publiciteta u stotinama zemalja. Shodno tome, kompanije se ograničavaju na upotrebu svojih veb-sajtova na poznate partnere, odnosno zatvorene sisteme. Negativan rezultat zakonske dvosmislenosti u e-trgovini, ili agresivno insistiranje na usaglašavanju sa detaljnim lokalnim zakonima je dvostruk: sužena ponuda roba i usluga i nedostatak konkurencije na globalnom e-tržištu.

Verodostojnost elektronskih poruka i autentičnost strana su samo od nekih problema koji se pojavljuju u e-trgovini. Ali, ovi problemi postoje, kako u elektronskoj,

---

[8] *Izvor* [www.**uncitral**.org/](http://www.uncitral.org/)

[9] Više o aktima UNCITRAL-a u odeljku *"Pravni akti doneti u okviru UNCITRAL-a"*

tako i u tradicionalnoj, na koju smo navikli. Najbolji primer je e-ugovor koji okuplja sve navedene probleme. Svaki ugovor obavezuje strane na uslove koji su predviđeni ugovorom.

Pošto ne postoji međunarodni zakon koji se primenjuje na uslove i važnost međunarodnih ugovora, postavlja se pitanje pod čijom je jurisdikcijom takav ugovor. Ipak, postoji međunarodni zakon koji uređuje slučajeve nesporazuma i rešava konflikte kada se više zakona primenjuje simultano i proizvode kontradiktorne efekte. Kada su međunarodni ugovori u pitanju to je *the United Nations Commission on International Trade Law* (UNCITRAL) i *Convention on Contracts for the International Sale of Goods.*

Najveća manifestacija želje Evropske Unije da očuva individualnu kontrolu ličnih informacija je Direktiva o zaštiti privatnih podataka EU. Prema ovoj Direktivi, između ostalog, svaka organizacija koja poseduje podatke o vama, mora da vam, na vaš zahtev, te podatke da na uvid.

Prema ovoj Direktivi pojedinci u Evropi imaju znatno više kontrole nad svojim ličnim podacima od onih u SAD. Iako ove razlike u suštini imaju korena u kulturnim razlikama, posledice ovih različitih stavova u pogledu zaštite informacija o ličnosti više ne otežavaju u tolikoj meri e-trgovinu između EU i SAD. Rešenje je formulisano u vidu "*safe harbor*" principa.

SAD imaju najviše interesa da razvijaju elektronsko poslovanje, međutim, daleko je od toga da se to i desilo. "Okviri globalne elektronske trgovine" iz 1997. godine predstavlja plan Vlade SAD u kome privatni sektor treba da preuzme inicijativu. Preduzete su akcije i na prilagođavanju Jednoobraznog trgovačkog zakona SAD. Po njemu ukoliko je omogućena on-line trgovina preko web site-a, prodavac je u onoj državi u kojoj je obavljena kupovina.

Potreba za rešenjem u oblasti privatnosti, koje može da obuhvati i pomiri nadzor Vlade, sile tržišne dinamike i pritisak javnosti, u SAD se pojavilo u vidu *Self Governance*, koja uravnotežuje sve ove kritične tačke. Za razliku od samoregulacije, *Self Governance* pretpostavlja da industrija ne deluje samostalno, već u saglasnosti sa postojećim zakonima i u cilju razvoja što boljeg delovanja. *Self Governance* se zasniva na informisanom tržištu koje zahteva otkrivanje informacija, ali i mogućnost izbora kako se te informacije koriste. *Self Governance* je postala izražena karakteristika Internet industrije. Vizija *Self Governance* je posledica demokratskog kvaliteta Interneta, gde je zakon definisan kao učešće i udeo svakog pojedinca u društvu. Možda najjasniji znak da *Self Governance* funkcioniše je uspeh mnogih *Privacy Seal* programa.[10]

To su mahom neprofitne, globalne i nezavisne inicijative, koje su lansirane da bi obezbedile mehanizam kojim veb-sajtovi mogu da smanje brigu potrošača kada je privatnost u pitanju. Suština je u tome da se vizuelni simbol - *Privacy Seal* nalazi na svakom sajtu koji zadovoljava zahteve programa vezane za privatnost: sakupljanje

[10] Izvor www.selfgov.net/

podataka i njihova distribucija. Veb-sajtovi koji nose *Privacy Seal* su prošle evaluaciju i zadovoljavaju zahteve ovih programa u oblasti privatnosti.

Sporazum između dva najveća trgovačka bloka, EU i SAD, vezan za elektronsko poslovanje trebao bi da reši glavninu problema koji ovaj tip poslovanja nameće. On će zahvaljujući veličini ovih tržišta predstavljati i osnovu pravnog okruženja na globalnom nivou jer ukoliko će neka zemalja hteti da posluje sa EU ili SAD moraće da donese sličan propis ili da mu pristupi. Mnogo je lakše podsticati različite zemlje da ovakav sporazum podrže uključujući se u njegov razvoj od početka nego težiti naknadnoj harmonizaciji velikog broja pojedinačnih prava.

Usled nedostatka regulacije elektronskog poslovanja na globalnom nivou nameće se zaključak da je i za subjekte ovog poslovanja najbolje da sklope ugovor u kome će se precizirati pravna nadležnost u slučaju bilo kog nesporazuma.[11]

3.5. Zloupotrebe u elektronskom poslovanju

Privredni kriminal pojavljuje se još od davnina, a danas on dobija nove konotacije i novo okruženje. Sa kompjuterskom tehnologijom ovaj kriminal postaje transnacionalan, brišući razlike između zemalja, područja, kontinenata. Razvoj i ekspanzija kompjuterskih mreža otvorili su "brešu" za nove oblike zloupotreba, čemu posebno pogoduje elektronsko poslovanje, kao način obavljanja poslovnih transakcija koje se preduzimaju i realizuju elektronski, pogotovo preko otvorenih mreža, kakav je Internet.

Takvo poslovanje zahteva i nameće, istovremeno, izgradnju novih principa i pravila čije kršenje može predstavljati svojevrsne oblike zloupotreba. Problem postaje mnogo kompleksniji sa činjenicom da se pravila i principi kojima se definiše i reguliše elektronsko poslovanje više ne nalaze u domenu država, niti uobičajenih međunarodnih organizacija i asocijacija.

Pored navedenog, postoje i drugi veoma ozbiljni problemi koji remete funkcionisanje virtuelnog sveta i otežavaju elektronsko poslovanje kao njegovog značajnog dela. No, nisu sve aktivnosti istog značaja i težine, kao što nisu ni iste učestalosti njihovog preduzimanja.

Najčešći napadi su vezani za: zloupotrebu domena, slanje *spam* poruka, ugrožavanje privatnosti, razne malverzacije sa podacima, *online* krađe i prevare, nelojalnu konkurencija, povrede intelektualne svojine, narušavanje autentičnosti učesnika u e-poslovanju, kao i manipulacije sa elektronskim novcem. Tome svakako treba dodati i brojne aktivnosti koje postoje i u tradicionalnim oblicima poslovanja, ali dobijaju nove

[11] *Preuzeto Drakulić M., Osnovi Poslovnog prava, Beograd, FON, 2001*

sadržaje i modalitete u elektronskom okruženju, kao što je pranje novca, odavanje tajni (poslovnih, trgovačkih), pronevere, prevare.

3.5.1. Sukob domeni – žigovi

Nakon prvog nesnalaženja pravnika oko *domain name*-a, kao tekstualne adrese pozicije neke organizacije, institucije, države ili pojedinca na Internetu i njegovog značaja i udela u elektronskom poslovanju, počelo je njegovo prihvatanje, ali ne i brzo rešavanje.

Naime, u početku se pravo domena potpuno ignorisalo i tek nakon prvih zbunjujućih sudskih sporova (npr. spor poveden u SAD od strane poznatog proizvođača dečijih igračaka koji je propustio da registruje domen pod svojim žigom, a taj propust brzo je iskoristila druga firma postavljajući na sajt sa tim domenom porno materijal) počela je ubrzana aktivnost rešavanja ovog sukoba.

Danas, WIPO[12], OECD[13] ali i brojne druge međunarodne organizacije preduzimaju ozbiljne korake ne bi li ovo komplikovano pravno klupko razmotale. Tim više što su se u "igru" oko domena počele uključivati i države, između ostalog i zbog svojih grešaka. Jedan od najupečatljivijih bio je slučaj sa domenima http://www.nasa.gov/ i http://www.nasa.com/ koji su obuhvatali ne samo različite, već i međusobno suprotstavljene sadržaje.

To se desilo i sa brojnim organizacijama, pogotovo onim koje su nosile čuvene žigove i poznata trgovačka imena. Njihova inertnost naterala ih je kasnije da otkupljuju domene sa svojim nazivima od veštih i brzih trgovaca domena. Pojavile su se čak i profesionalne grupe snalažljivih pojedinaca i organizacija koje se bave registrovanjem poznatih žigova i trgovačkih imena kao domena i nudjenjem njihovog "otkupa" za veliki novac.

Od ove pojave nije bio pošteđen ni jugoslovenski poslovni *cyberspace* (npr. čovek koji je registrovao www.vrnjackabanja.com u jednom momentu tražio je od turističkog saveza i opštine Vrnjačka Banja preko 2000 DIN mesečno za njegovo iznajmljivanje).

Druge, poput *McDonalds*-a (koji je registrovao i uobičajene greške) ili *Mercedes-Benz* (od 19 registrovanih domena na "temu" *Mercedes - Benz* samo dva nisu bila njihova - *Mercedes Club of Cyberspace*, Mercedes Benz Car Club of America) nisu gotovo ništa prepustile slučaju. Iako je jasno da se zloupotrebom domena i žigova olakšava nelojalna utakmica, povreda prava intelektualne svojine, ucena, ili druge nedozvoljene aktivnosti ipak ovaj problem još uvek nije na adekvatan način rešen.

---

[12] *WIPO - World Intellectual Property Organization www.wipo.int/*

[13] *OECD je još 1997. godine u okviru posebnog Izveštaja o domenima istakao neophodnost rešavanja problema i kroz iznete slučajeve ukazala na njihove razmere*

Zbog sve većeg broja i raznolikosti zloupotreba domena WIPO ne samo da pokušava da donese odgovarajuće akte kojima bi se obezbedio osnov za njihovo rešavanje, već arbitražno rešava i konkretne slučajeve. Pominje se broj od podnetih 817 tužbi, od kojih je 316 rešeno. Od okončanih slučajeva 81% je rešeno protiv optuženih " otimača" imena domena[14]. Jedan od najzanimljivijih bio je i spor između novinske agencije *Reuters* i iranske kompanije *Global Net* 2000 koja je registrovala 5 imena vezanih za *Reuters.* Gubitak spora značio je i povratak svih 5 imena novinskoj agenciji Reuters.

3.5.2. Neželjene reklamne poruke

Jedan od velikih problema, a istovremeno i oblika zloupotreba je i slanje neželjenih "*spam*" *(junk e-mail, unsolicited e-mail, bulk messages*) poruka.

Naime, u želji da se odvoje od ostalih konkurenata i da "nateraju" potencijalne potrošače da obrate pažnju na njih, pojedine organizacije počele se da "bombarduju" reklamnim porukama elektronske adrese pojedinaca.

To je izazvalo zagušenja pošte pojedinaca ali i saobraćaja na mreži zbog čega su sve glasniji protesti i razlog da se provajderi i drugi akteri u e- poslovanju počinju baviti ovim problemom. Razmere ove pojave primorale su i neke države da reaguju donošenjem odgovarajućih akata ne bi li sankcionisale sve one koji se bave slanjem ogromnog broja ovakvih poruka.

Tako je u SAD donet *Zakon o privatnosti elektronskih komunikacija*, a potom je federalna država Juta donela i svoj poseban zakon. Pokrenuto je više sudskih slučajeva od koji je jedan od najslikovitijih bio protiv dvojice australijanaca koji su poslali ekonomske poruke na preko milion adresa u SAD. To je mobilisalo policije obe zemlje i rezultat je bio hvatanje počinioca i pokretanje sudskog postupka.

Borba protiv ovakvih napasti nastavila se i u oblasti softvera, ali i različitih inicijativa pojedinih grupacija (npr. YASA - *Yugoslav Anti Spam Association*). Počele su se stvarati "crne liste" i postavljati na odgovarajuće sajtove. Na njih se stavljaju pojedinci i organizacije koji čine razne oblike zloupotreba, pa i šalju *spam* poruke, bilo da je u pitanju elektronska pošta ili *newsgroup*-e.

Postoji više određenja šta je *spam*, mada većina se kreće u razmerama da je u pitanju svaki neželjeni e mail koji dobija korisnik. U smislu američkog Zakona o privatnosti komunikacija, to su komercijalne elektronske poruke :

- Poslate bez saglasnosti primarnog primaoca

[14] *među kompanijama koje su uspele da povrate svoja imena su Christian Dior, Microsoft i Nike.*

- Poslate nekome ko sa pošiljaocem nema nikakve prethodne poslovne niti lične veze.
- Poslate više zbog ispunjenja nečijih ciljeva nego radi ispunjenja postojećih obaveza.

Te poruke se šalju kao pravi *spam*, latentni, kamuflažni i kao težnja za brzom zaradom.

U prvom slučaju " bombarduje " se elektronska pošta neželjenim porukama, koje mogu biti u reklamne svrhe, ali i u druge. Među te druge spadaju i poruke političke prirode i poseban oblik informacionog rata.

Postoje posebne alijanse koje se bave protiv spamiranja. Jedan od njih je i američki *Spam Recycling Center*[15] na čijem sajtu se mogu pronaći ne samo određenja šta je to *spam*, već i uputstva kako se protiv njega boriti i koja je pozitivna pravna regulativa. Sajt takođe sadrži tekstove zakona i drugih akata, prvenstveno američkih, kao što je Zakon o zaštiti pojedinaca, porodica i internet servis provajdera od nenaručenih i neželjenih elektronskih poruka. Ovaj zakon se dopunjuje i Zakonom o nenaručenim elektronskim porukama iz 2001 godine

3.5.3. Ugrožavanje privatnosti

Gotovo da nema ni jednog dokumenta u kome se posebna pažnja ne posvećuje problemu privatnosti i njene zaštite. Među mnogobrojnim podacima koji su u fokusu elektronskog poslovanja su i podaci o ličnosti čije objavljivanje ili *online* dostupnost ugrožavaju privatnost pojedinaca. Čuvene baze: *Database America, Four 11, Internet White Pages, Map Blast, KnowX* postaju predmet stalne kontrole zbog permanentne sumnje o ugrožavanju privatnosti.

Sve one sadrže uobičajene podatke: ime i datum rođenja, adresu, broj telefona, identifikacioni broj (matični broj ili broj socijalnog osiguranja), kao i druge brojne podatke (imena ljudi koji žive na istoj adresi, podatke o procenama primanja, vlasništvu automobila ili drugih prevoznih sredstava, kreditne informacije, kriminalne podatke). Tu su i podaci o "potencijalnim potrošačima" koji se skupljaju za različite "snabdevače". Veoma često takvi podaci su na samoj granici dozvoljenosti. Sve su učestaliji zahtevi da se delikatni podaci o ličnostima izbrišu iz baza.

Privatnost je ugrožena i intenzivnim razvojem industrije informacija koja najčešće obuhvata agencije za izveštavanje o kreditima, interaktivnim *online* servisima, proizvođačima baza i finansijskim uslugama.

[15]Izvor : *www.spamrecycling*

Ova industrija beleži ogroman porast meren u milijardama dolara, a prodaja podataka postaje seriozan posao i izvor prihoda.

Privatnost biva ugrožena i "pabirčenjem" podataka o učestalosti i pravcima slanja elektronskih poruka, korišćenju Interneta i posetama WWW sajtovima ili obavljanju *online* trgovine i na osnovu koga se mogu stvoriti moćne baze o navikama, potrebama, željama, poslovima, motivima pojedinaca i korišćenjem takvih podataka olakšati elektronsko poslovanje.

Takođe, evidentna je ekspanzija elektronske pošte (u 1994. godini bilo je oko 776 biliona elektronskih poruka samo u SAD, u 1997. taj broj se popeo na 2.6 triliona, a do kraja 2000. računa se da će ih biti preko 6.6 triliona). Mnoge od ovih poruka šalju se iz organizacija u radnom vremenu. Njih u velikom procentu pregledaju i kontrolišu rukovodioci sa opravdanjem da ne žele oticanje podataka koji su poslovne tajne, kršenja autorskih i drugih prava, ili zbog praćenja novozaposlenih (1996. godine 36% menadžera je priznalo da stalno pregleda e-poštu zaposlenih). Tome doprinosi i razvoj softvera koji omogućuje takvu kontrolu i prismotru.

Provajderi su sledeći na listi onih koji kontrolišu e-poštu. Ali ne samo nju, već i komercijalne elektronske poruke, naročito stare, odbačene. Te svoje "aktivnosti" oni preduzimaju manje u cilju zaštite od kriminala, a više zbog radoznalost, koristi ili kontrole po nalogu.

Posebno se privatnost ugrožava od strane WWW sajt operatora koji skupljaju tzv. "kolačiće"[16]. Ove informacije obuhvataju i podatke o Internet servis provajderu posetioca, tipu kompjutera i softvera koji se koriste, linkove, kao i na kojim delovima sajta je i koliko bio. Na osnovu ovih podataka može se saznavati šta posetioci na određenom sajtu vole, a šta ne. Mada su oni često anonimni i teško se mogu identifikovati to ipak nije nemoguće na osnovu rekonstrukcije dobijenih podataka ukoliko nije u pitanju sajt čije pregledavanje zahteva identifikaciju. Nekad upravo na ovakvim sajtovima postoji "zamka" za posetioce koji kroz identifikaciju odgovaraju na pitanja vezana za njih ali i porodicu. Ovi se podaci potom koriste za marketing.

Apsurd koji se javlja je u praćenju puteva kojim surferi prolaze u traženju relevantnih podataka. On se postavlja kao dvostruk: surferi ugrožavaju privatnost drugih, a provajderi usluga i drugi surferi njihovu.

Kupovina ili bankarske usluge, takođe, zahtevaju otkrivanje podataka o onome ko se pojavljuje kao stranka ili komitent. Podaci o imenu i adresi nisu dovoljni nego su nužni još i podaci o broju kreditne kartice, kupovnoj sposobnosti i mnogi drugi. Zbog osetljivosti i značaja ovih podataka pribegava se njihovoj posebnoj zaštiti, a što predstavlja izazov za znatiželjne ili zlonamerne.

---

[16] *kolačići su informacije o posetama Web sajtovima koje brozer prima sa Web sajta i skladišti na posetiočev hard disk. Web sajt "čita" informaciju svaki put kada ga korisnik poseti.*

3.5.4. "Obaranje" sajtova

Zloupotrebe često imaju i spektakularne oblike. Jadan od takvih je aktivnost hakera i krakera koji, za sopstvene ili potrebe naručioca, vrše raznovrsne mrežne napade. Ti napadi se mogu sastojati u promeni izgleda sajta, promeni sadržine, odbijanju usluga ili pretrpavanju raznovrsnim *spam* porukama.

Ne retko hakeri i krakeri to rade po nečijem nalogu (npr. nekog od konkurenata). Postojala je sumnja da se to upravo desilo sa dvodnevnim februarskim zahvatima na velikim sajtovima kao što je: *Amazon.com, Buy.com, eBuy, CNN.cim, Zdnet, ETrade ili Derek.*

Njima svakako treba dodati i pad *Yahoo.com*. Njihov rad je bio obustavljen na po 2 do 5 sati, a gubici koje s pretrpeli bili su ogromni. Motivi, su naravno, raznovrsni, mada nikako n treba zanemariti koristi koje konkurencija može postići, odnosno štete koje napadnuta strana pretrpi, a koje su ne samo materijalne, već i u ugledu, pouzdanosti, "imidžu".

O ostalim zloupotrebama, načinu otkrivanja učinioca, kao i ostalim aspektima ove pojave detaljno se govori u drugom delu rada koji se bavi izučavanjem kompjuterskog kriminala.

4. MEĐUNARODNE INSTITUCIJE I IZVORI

Od međunarodnih organizacija koje deluju u ovom domenu najznačajnije su :

-Komisija UN za međunarodno trgovinsko pravo (UNCITRAL)[17]
-Međunarodna trgovinska komora (ICC)
-Evropska komisija UN-a za Evropu (CEFACT)
-Evropska unija

Najznačajniji izvori prava su

- Model zakon UNCITRAL-a o elektronskoj trgovini
- Model zakon UNCITRAL-a o elektronskim potpisima
- Direktiva o elektronskom potpisu
- Direktiva o elektronskoj trgovini
- Direktiva o zaštiti privatnih podataka

4.1. Pravni akti doneti u okviru UNCITRAL-a

Komisija UN-a za međunarodno trgovinsko pravo (UNCITRAL)

Osnovana je Rezolucijom 2205 Generalne skupštine 1966. godine. Glavne oblasti rada su međunarodna prodaja robe, međunarodni instrumenti plaćanja, međunarodni prevoz i međunarodna arbitraža. Pored ovih, Komisija je usmerila aktivnosti i na druge oblasti, odnosno na oblast unifikacije pravnih pravila u oblasti elektronske trgovine. Pa su tako doneti: Pravni vodič o elektronskom prenosu sredstava,Model zakon UNCITRAL-a o elektronskoj trgovini i Model zakon o elektronskom potpisu.

4.1.1. Pravni vodič o elektronskom prenosu sredstava

Pravni vodič je objavljen 1987. godine kao posebna publikacija UNCITRAL-a. Sadrži pet poglavlja koja se odnose na opšta pitanja elektronskog prenosa sredstava. To su sporazum o prenosu sredstava i uputstvo o prenosu, prevara, greške, nepravilno rukovanje i postupanje po uputstvima o prenosu kao i odgovornost u vezi navedenih pitanja.

[17]Izvor www.uncitral.org/ *Model Law on Electronic Commerce prevod Bojana Živković*

4.1.2. Model zakon UNCITRAL-a o elektronskoj trgovini

Komisija UN-a za međunarodno trgovinsko pravo (UNCITRAL) je 12 juna 1996. godine usvojila Model zakon UNCITRAL-a o elektronskoj trgovini sa ciljem da se olakša korišćenje savremenih sredstava komunikacija i skladištenje podataka. Zakon propisuje određena međunarodno prihvatljiva pravila koja treba da uklone pravnu nesigurnost i stvore povoljno okruženje za razvoj elektronske trgovine.

Pravila trebaju biti prihvatljiva za države sa različitim pravnim, socijalnim i ekonomskim sistemima, a u cilju razvoja međunarodnih ekonomskih odnosa. Model zakon otklanja nedostatke koje stvara neadekvatno zakonodavstvo na nacionalnom nivou.

Dakle, ovaj zakon treba da posluži nacionalnim zakonodavcima prilikom izrade propisa kojima se reguliše materija zaključivanja ugovora korišćenjem elektronske tehnologije. U čl.1 Model zakona istaknuto je da se ovaj zakon primenjuje na sve informacije u obliku poruke, koja se koristi u kontekstu trgovačkih aktivnosti. Pravno priznanje poruka uređeno je čl. 5 ovog akta, pa je predviđeno da se informaciji neće oduzeti pravna valjanost ili izvršnost, samo iz razloga što je data u obliku poruke.

Pored toga, čl. 9 zabranjuje da se u bilo kojim pravnim postupcima predvide rešenja koja bi značila negiranje dopuštenosti poruke kao dokaza, te da će se informaciji u obliku poruke dati odgovarajuća dokazna snaga. Pismeni oblik informacije, potpisa i originala informacija Model zakon je rešio članovima 6, 7 i 8 . Kada se zakonom zahteva da informacija bude u pismenom obliku, poruka ispunjava taj uslov ako je informacija koja je u njoj sadržana pristupačna i iskoristiva u kasnijim referencama.

Pitanja vezana za slanje poruka, zaključenje i valjanost ugovora, Model zakon je rešio u čl 11-15. Ako se poruka koristi prilikom zaključenja ugovora , takvom ugovoru se neće oduzeti valjanost ili izvršnost isključivo na osnovu činjenice što je za tu svrhu korišćena poruka. Vreme i mesto slanja i prijema poruke Model zakona je rešio članom 15. Ukoliko nije drugačije dogovoreno između nalogodavca i adresata, smatra se da je poruka poslana u trenutku kada je ušla u informacioni sistem koji je van kontrole nalogodavca ili lica koje poruku šalje u ime nalogodavca.

Režim prevoznih isprava regulisan je članovima 16 i 17 Model zakona, ukoliko se zakonom zahteva pismena forma bilo koje radnje ili korišćenja papirne isprave, taj zahtev je ispunjen ako je radnja obavljena korišćenjem jedne ili više poruka.

4.1.3. UNCITRAL Model zakon o elektronskim potpisima[18]

Model zakon o elektronskim potpisima je usvojen 2001 godine. Model zakon ima za cilj da doprinese pravnoj sigurnosti pri upotrebi elektronskog potpisa. On sadrži 12 članova. Ovaj zakon se primenjuje kad se elektronski potpisi koriste u kontekstu trgovinskih aktivnosti.

U članu 2 elektronski potpis je definisan *kao poruka u elektronskom obliku koja je priložena ili se logički povezuje sa drugim elektronskim porukama i služi da identifikuje potpisnika poruke i njegovu saglasnost sa sadržajem poruke.* Pored definicije elektronskog potpisa, istim članom su date definicije i drugih relevantnih pojmova kakvi su sertifikat, elektronska poruka, potpisnik, sertifikovani servis provajder.

Pravno delovanje elektronskog potpisa uređeno je članom 6. Model zakona. Ako se zakonom zahteva potpis jednog lica, taj uslov se smatra ispunjenim u odnosu na datu poruku, ukoliko je korišćen metod kojim se identifikuje potpisnik i ukoliko je tražena njegova saglasnost sa informacijom koju poruka sadrži. Istovremeno se traži da taj metod bude pouzdan.

Obaveze potpisnika su sadržane u članu 8 , a dužnosti sertifikovanog servis operatera su sadržane u članu 9. Ukratko, one se sastoje u delovanju po pravilima struke i svojih propisa, obezbeđivanju sigurnosti elektronskog potpisa i ažurnom unošenju u sistem svih relevantnih promena. U cilju razvijanja poverenja sertifikovani servis operator mora raspolagati određenim finansijskim i ljudskim resursima, određenim kvalitetnim hardverskim i softverskim sistemima. Obaveza priznanja stranih sertifikata i elektronskog potpisa, bez obzira na lokaciju izdavanja uređena je članom 12. S obzirom na globalni karakter elektronske trgovine, ova odredba je od izuzetnog značaja.

4.2. Pravni akti doneti u okviru Evropske Unije

4.2.1. Direktiva o elektronskom potpisu[19]

Direktiva 1999/93/EC Evropskog Parlamenta i Saveta od 13. decembra 1999. godine o zajedničkom okviru za elektronski potpis

[18]Izvor www.**uncitral**.org/ *Model Law on Electronic Signatures* - prevod Bojana Živković

[19]Izvor eur-lex.europa.eu prevod Bojana Živković

Sve veći razvoj elektronske trgovine može se smatrati pozitivnim trendom koga treba podsticati. Ipak, autentičnost potpisa kod mnogobrojnih transakcija predstavlja određene prepreke koje otežavaju razvoj elektronske trgovine, kao i elektronskog poslovanja uopšte. U Evropskoj Uniji nekoliko država članica imaju nacrt zakona ili pak donete zakone o elektronskom potpisu. Problem dalje predstavlja različit pristup regulisanja ovog problema. U skladu s tim, Evropska Komisija je 1999 godine usvojila Direktivu koja treba da obezbedi zajednički pravni okvir za definisanje elektronskog potpisa, odnosno ona treba da obezbedi definisanje pravne valjanosti elektronskog potpisa.

Direktiva ima za cilj da olakša primenu elektronskog potpisa i da propiše kriterijume koji će služiti kao osnova za pravno priznavanje elektronskog potpisa u državama članicama.

Glavne odredbe odnose se na činjenicu da elektronski potpis treba da zadovolji iste pravne zahteve kao i rukopisni, kao i da bude prihvatljiv kao dokaz u pravnim postupcima.

Direktiva je izgrađena pod velikim uticajem američkog udruženja pravnika vezanog za digitalne potpise. Prema ovoj direktivi elektronski potpis označava poruke u elektronskom obliku koje su priložene ili se logički povezuju sa drugim elektronskim porukama i služe kao metod za svrhe utvrđivanja verodostojnosti.

Sertifikaciono telo u direktivi se naziva operaterom sertifikacione usluge. On predstavlja entitet, pravno ili fizičko lice koje izdaje sertifikate i obezebeđuje druge usluge koje se odnose na elektronske potpise. Sertifikaciono telo izdavanjem sertifikata postaje odgovorno za štetu koju bi imalo bilo koje pravno ili fizičko lice koje se oslonilo na sertifikat.

4.2.2. Direktiva o elektronskoj trgovini[20]

Direktiva o elektronskoj trgovini je usvojena 2000 godine sa ciljem da uspostavi pravne okvire elektronskog poslovanja na domaćem tržištu.

U skladu sa razvojem elektronske trgovine u okviru informacionog društva dolazi do značajnog povećanja zapošljavanja u Evropskoj Uniji, a posebno u malim i srednjim preduzećima, što dalje dovodi do povećanja privrednog rasta i investicija u kompanijama Evropske Unije.

U skladu sa tim, u Evropskoj Uniji zauzet je stav da se mora obezbediti pravna sigurnost i poverenje potrošača u elektronskom poslovanju, te je jedan od preduzetih koraka na tom planu bilo usvajanje Direktive o elektronskoj trgovini, koja je utvrdila jasne i opšte okvire za pokrivanje određenih pravnih aspekata elektronske trgovine na unutrašnjem tržištu. Ona nastoji da doprinese pravilno funkcionisanje unutrašnjeg tržišta obezbeđivanjem slobodnog kretanja usluga informacionog društva između država članica.

[20] Izvor eur-lex.europa.eu prevod Bojana Živković

Cilj je stvaranje pravnog okvira kako bi se obezbedilo slobodno kretanje usluga, a ne da se uskladi sa područja krivičnog prava.

Države članice treba da obezbede da informatičko društvo pruža usluge servis provajdera u skladu sa nacionalnim zakonodavstvom te države članice. Države članice ne mogu ograničiti slobodu pružanja usluga servis provajdera koji potiče iz druge države članice.

Direktiva sadrži odredbe koje se odnose na :

- usluge informatičkog društva koje se odnose na unutrašnje tržište.
- Servis provajdere
- Komercijalnu komunikaciju
- Elektronske ugovore
- Kodeks ponašanja
- Sudske i vansudske postupke
-

U njoj je obrađeno 5 osnovnih problema

* osnivanje informatičkog društva
* utvrđivanje pojma trgovačke komunikacije
* zaključivanje on-line poslovnih transakcija
* odgovornost posrednika

Najvažnija novina ove Direktive je osnivanje Informatičkog društva servis operatera. Njegova dužnost bi bila da otkloni postojeću pravnu nesigurnost u pogledu određivanja mesta osnivanja servis operatera. Cilj je usaglasiti ovu oblast sa principima Osnivačkog sporazuma i nadležnosti Evropskog suda pravde.

4.2.3. Direktiva o zaštiti privatnih podataka[21]

Ova Direktiva zasniva se na poštovanju osnovnih prava i načela proklamovanih Poveljom o osnovnim pravima Evropske unije. Poverljivost informacija zagarantovana je Evropskom konvencijom o zaštiti ljudskih prava i osnovnih sloboda kao i Ustavima država članica.

Osnov za usvajanje ove Direktive predstavlja činjenica da razvoj informacionog društva karakteriše uvođenje novih elektronskih komunikacionih usluga, da je pristup

[21]Izvor eur-lex.europa.eu prevod Bojana Živković

digitalnim mobilnim mrežama postao dostupan i pristupačan velikom broju ljudi, te da postoje specifični zahtevi u vezi zaštite ličnih podataka i privatnosti korisnika.

Pravne, regulatorne i tehničke odredbe koje su usvojene od strane država članica u vezi sa zaštitom ličnih podataka, privatnosti i legitimnih interesa pravnih lica u sektoru elektronskih komunikacija treba da budu usklađeni kako bi se izbegle prepreke za funkcionisanje unutrašnjeg tržišta elektronskih komunikacija.

U članu 1. navodi se da Direktiva zahteva od država članica da se usklade odredbe koje treba da obezbede odgovarajući nivo zaštitite osnovnih prava i sloboda, a posebno pravo na privatnost, s obzirom na obradu ličnih podataka u elektronskim komunikacijama i da obezbedi slobodno kretanje takvih podataka, komunikacione opreme i usluga u zajednici.

Dakle, predmet Direktive je pravo na privatnost u sektoru elektronskih komunikacija i slobodno kretanje podataka, komunikacione opreme i usluga.

Prva opšta obaveza u Direktivi je pružanje bezbednosti usluga. To se odnosi na provajdere usluga elektronskih komunikacija. Ova obaveza uključuje i obavezu obaveštavanja pretplatnika kad god postoji određeni rizik, kao što su napadi virusa i slično.
Druga opšta obaveza odnosi se na održavanje poverljivosti informacija. Države članice bi trebalo da zabrane bilo koji oblik prisluškivanja, presretanja, skladištenja ili nadgledanja komunikacija.

Zabranjuje se korišćenje e-mail adrese u marketinške svrhe. Direktiva uspostavlja režim gde neželjeni e-mail može biti poslat samo uz prethodnu saglasnost primaoca.

Direktiva takođe prepoznaje važnost i korisnost *cookies* za funkcionisanje modernog interneta , ali takođe upozorava na opasnost koje takvi instrumenti mogu da predstavljaju.

5. **PRAVNA REGULATIVA ELEKTRONSKOG POSLOVANJA U SRBIJI**

5.1. Strategije razvoja informacionog društva u republici Srbiji[22]

Stvaranje pravne regulative u oblasti elektronskog poslovanja započelo je donošenjem *Zakona o elektronskom potpisu*. Vlada Republike Srbije postupak daljeg razvoja, unapređenja i pravnog regulisanja elektronskog poslovanja nastavila je kroz donošenje " *Strategije razvoja informacionog društva u republici Srbiji* " i " *Strategije razvoja trgovine Republike Srbije* ".[23]

[22] Izvor *www.srbija.gov.rs*
[23] Izvor www.nauka.gov.rs

U "*Strategiji razvoja informacionog društva u republici Srbiji* " navodi se da elektronsko poslovanje u osnovi znači automatizaciju poslovnih procesa primenom informacionih i komunikacionih tehnologija i predstavlja efikasno sredstvo za obavljanje poslovnih aktivnosti na nacionalnom i međunarodnom nivou. Prema Akcionom planu e-Evropa 2005, e-poslovanje obuhvata e-trgovinu (kupovinu i prodaju putem interneta) i restrukturisanje poslovnih procesa sa ciljem realizacije najbolje upotrebe digitalnih tehnologija.

Prednosti primene e-poslovanja mogu biti definisane na sledeći način: smanjenje troškova poslovanja, povećanje efektivnosti u smislu širenja tržišnog potencijala i boljeg zadovoljavanja potreba potrošača, unapređivanje inovacija proizvoda i usluga putem interaktivnog odnosa na relaciji potrošač-snabdevač, povećanje konkurentnosti i mogućnosti zaposlenja.

Strategija za izradu okvira za e-poslovanje treba da se bavi sledećim pitanjima: analizom i prestrukturiranjem procesa poslovanja; prilagođavanjem nacionalne telekomunikacione mreže i obrazovnog sistema potrebama razvoja e-poslovanja; stvaranjem zakonske osnove za e-poslovanje, u skladu sa acquis communautaire; i usklađivanjem (harmonizacijom) dokumenata i podataka sa međunarodnim standardima i zahtevima. U tom smislu, nacionalne institucije zadužene za standardizaciju trebalo bi da budu uključene u izgradnju informacionog društva i da u tom društvu budu nadležne za primenu međunarodnih standarda za IKT i e-poslovanje. Relevantni stručnjaci iz institucija za standardizaciju treba da učestvuju u radu Odseka za informaciono društvo.

Odgovornost je Vlade da prati razvoj novog zakonodavstva i uputstava u EU, i da na njima bazira praksu koju će primenjivati u domaćoj privredi. Informacije o aktuelnim evropskim zakonima i standardima su važan element poslovnog okruženja i njihova raspoloživost će znatno olakšati donošenje odluka na nivou kompanija i u različitim administrativnim organima.

Važna briga mnogih zemalja je da postojeći pravni okvir ne može adekvatno da se prilagodi e-trgovini/poslovanju i da postojeći zakoni koji su usmereni na sistem zasnovan na papirnim dokumentima mogu da predstavljaju prepreku rastu globalne e-trgovine. Postojanje predvidljivog pravnog okvira je često isticano kao osnovno sredstvo za podizanje nivoa poverenja poslovnog sektora i potrošača u komercijalne transakcije. Pošto su pravna sigurnost i poverenje glavna pitanja u bilo kojoj trgovinskoj transakciji, kredibilitet e-poslovanja će u celini zavisiti od kapaciteta domaćih zakonodavaca da definišu i stvore čvrsto i sveobuhvatno pravno okruženje za e-poslovanje koje bi izgradilo poverenje.

Pravne aktivnosti na domaćem nivou treba sprovoditi u tesnoj koordinaciji s međunarodnim razvojem i inicijativama da bi se obezbedila usklađenost domaćeg zakonodavstva s međunarodnim normama kao što je acquis communautaire, čije se odrednice glavne smernice za zemlju koja želi da se pridruži Evropskoj uniji. Okosnica rada realizovana u Evropskoj uniji, odnosno evropska uputstva koje se odnose na e-trgovinu i e-potpis imaće jak uticaj na stvaranje pravnog okvira za e-poslovanje u Republici

Srbiji. Ipak, Republika Srbija prilikom izrade okvira za e-poslovanje mora uvažiti svoje razvojne prioritete i svoju tradicionalnu pravnu kulturu.

Jednako je važan i Model zakona o elektronskoj trgovini koji je izradio UNCITRAL 1996. godine. Ovaj zakon nudi set međunarodno priznatih pravila namenjenih kao pomoć državama da uklone pravne prepreke u primeni e-poslovanja, i smanje razlike koje mogu postojati između nacionalnih zakonodavstava u ovom području. Štaviše, nedavno usvojen UNCITRAL-ov model zakona o elektronskom potpisu (jul 2002) i uputstva za njegovu primenu trenutno razmatraju brojne zemlje koje žele da donesu svoje zakone o elektronskom potpisu. Prilikom izrade pravne osnove za e-poslovanje u zemlji, model zakona koji je izradio UNCITRAL može da bude logična polazna tačka, ali se mnogo šira pravna problematika mora takođe razmotriti i uzeti u obzir.

Zemlje koje žele da obezbede da su elektronske transakcije pravno važeće, obavezujuće i sprovodive, moraju da daju odgovore na sledeća tri osnovna pitanja:

- Da li je transakcija primenljiva (ima li pravnu moć) u elektronskom obliku?
- Da li partneri u transakciji veruju poruci?
- Koja pravila važe za transakciju realizovanu elektronskim putem?

Polazeći od navedenog, ključne oblasti koje treba da budu razmotrene prilikom izgradnje pravnog okvira za e-poslovanje obuhvataju:

- zaštitu podataka;
- sigurnu formu ugovora u pravnom i komercijalnom smislu;
- regulisanje interent okruženja;
- punovažnost elektronskog potpisa;
- zaštitu potrošača - prodaja na daljinu;
- e-privatnost;
- pitanja vezana za rešavanje sporova, uključujući rešavanje sporova preko mreže (ODR);
- zaštitu od terorizma (anti-terorističke mere, mere za sprečavanje pranja novca, pitanja neželjenih poruka);
- prava intelektualne svojine;
- propise o regulisanju sadržaja na internetu;
- zakon o elektronskom dokumentu;
- zakon o elektronskom arhiviranju;
- zakon o slobodnom pristupu informacijama;
- zakon o zaštiti ličnih podataka.

5.2. Strategije razvoja trgovine Republike Srbije[24]

Strategija razvoja trgovine Republike Srbije u četvrtom delu bavi se trgovinskom politikom i pravnom regulativom. U ovom delu dat je predlog neophodnih promena pravne regulative u domenu tržišta i trgovine. Osnovna opredeljenja u domenu trgovinske politike u Republici Srbiji nalaze se na stanovištu da državna intervencija na tržištu, naročito u sektoru trgovine, uvek treba biti opravdana i u širem društvenom interesu. Osnovno polazište treba biti da država interveniše samo u slučajevima kada su javni interesi u pitanju.

Tržišni mehanizam skoro u celini obezbeđuje alokaciju sredstava u čitavom trgovinskom sektoru. U fokusu se nalaze potrošači koji su konačni arbitar tržišne efikasnosti subjekata u okviru trgovinskog sektora. Efikasno upravljanje tokovima u trgovini u najvećoj meri se treba poveri tržištu.

Pored navedenog, ovaj dokument sadrži i strategiju razvoja elektronske trgovine. Kao jedno od značajnih prepreka za razvoj elektronske trgovine navode se problemi s kojim se susreće naša zemlja a koji su vezani za nerazvijenost zaštite autorskih prava, korišćenje piratskih softvera i veliku nestabilnost sistema u kojem se posluje i druge probleme pravne nesigurnosti (zaštita poverilaca, brzina postupka u pravosuđu i sl.).

Većina tržišno razvijenih zemalja nema posebno definisane zakone koji se odnose na zaštitu potrošača prilikom kupovine na Internetu. Ovde se, posebno, misli na pitanja zaštite potrošača u elektronskoj trgovini u pogledu definisanja ugovornih uslova i termina vezanih za obaveze po navedenim ugovorima. Osnovna zamisao odnosi se na standard s kojim se može najbolje uskladiti privatnost nekog Web sajta sa preferencijama koje iskazuju korisnici, što će omogućiti automatski prenos informacija uz uzajamnu saglasnost oba partnera kroz P3P sporazum (*Platform for Privacy Preferences*). P3P je standard koji je prihvatio *World Wide Web Consortium* putem kojeg se podržava uzajamna preferencija ponuđača sadržaja i korisnika u komunikaciji putem web-a.

5.3. Elektronski potpis

Jedan od najvažnijih "tehničkih" rešenja vezanih za elektronsko poslovanje je elektronski potpis. Elektronski potpis je tehnika šifriranja koja je "rešila" glavni problem elektronskog poslovanja: strah od nedovoljne sigurnosti transakcija. Njime se obezbeđuje integritet podatka, odnosno omogućuje da podaci ostanu nepromenjeni tokom transakcije, i omogućuje utvrđivanje pošiljaoca.

Digitalnim šifriranjem se elektronski dokument, koji će se nalaziti u transakcijama na Internetu, čini nečitljivim svima koji nemaju ključ za dešifriranje. Samim tim, povećava se sigurnost transfera poverljivih podataka. Identifikacija pošiljaoca se obavlja potvrdom

[24]Izvor www.mtu.sr.gov.yu

autentičnosti kod "poverljive treće strane". Poverljiva treća strana (TTP - *Trusted Third Party*) je neko kome je dozvoljeno da proizvodi digitalne sertifikate autentičnost digitalnog potpisa i u koju imaju poverenje obe zainteresovane strane za transakciju. Potvrda autentičnosti predstavlja dokaz da je vlasnik digitalnog potpisa upravo onaj koji tvrdi da jeste. Najrasprostranjenija metoda je metoda šifriranja javnim ključem koja pošiljaocu i primaocu elektronske poruke dodeljuje dva ključa - jedan javni i jedan privatni. Javni ključ se deponuje kod TTP.

Pristup korišćenju elektronskog potpisa u svetu nije jednoobrazan. Međunarodna tela kao što su, na primer, IETF (*Internet Engineering Task Force*) ili ISO (*International Organization for Standardisation*) rade na njegovoj standardizaciji, a OECD i UNCITRAL daju uputstva državama kako pravno regulisati elektronsko poslovanje i/ili neke njegove delove. Prava samo nekih zemalja su podržala upotrebu elektronskog potpisa bilo u obliku zakona bilo preporuka. U SAD je svega devetnaest država članica pravno regulisalo ovu problematiku, Evropa je u blagom zaostatku.

Prva zemlja u Evropi koja je pravno definisala korišćenje elektronskog potpisa je Velika Britanija 1997 godine, a za njom 1998 godine slede Francuska i Nemačka, koja, čak, donosi poseban Zakon o elektronskom potpisu. Još neke evropske zemlje (Švedska, Italija i Belgija) su najavile zakonsku regulaciju. Te iste godine Evropska komisija je iznela predlog Direktive o digitalnom potpisu, donete 1999. (usvojena 13. decembra 1999, a formalno stupila na snagu 19. januara 2000. godine) koji sadrži minimum zahteva za potvrdu elektronskog potpisa naročito u prekograničnim transakcijama. Direktiva predviđa i saradnju sa trećim zemljama čak do nivoa da se organizacije za izdavanje sertifikata autentičnosti nalaze na njihovoj teritoriji.

Direktiva EU 1999/93/EC o elektronskim potpisima predstavlja pravno utemeljenje elektronskog potpisa i na osnovu nje su doneti Zakoni o elektronskom potpisu u svim zemljama EU, kao i u većini ostalih zemalja Evrope.

5.4. Zakon o elektronskom potpisu

Proces stvaranja pravnog okvira za regulisanje oblasti elektronskog poslovanja započeo je donošenjem *Zakona o elektronskom potpisu.*[25]

Zakon o elektronskom potpisu u Srbiji, u potpunosti je usklađen sa EU Direktivom 1999/93/EC, izglasan je u Narodnoj skupštini Republike Srbije dana 14. decembra 2004. i publikovan u Službenom glasniku Republike Srbije br. 135 od 21. decembra 2004. godine. Osnovna uloga Zakona o elektronskom potpisu svodi se na dve najvažnije stvari:

Da propiše uslove pod kojima je elektronski potpis pravno ekvivalentan svojeručnom potpisu.

Da propiše uslove koje moraju da ispune sertifikaciona tela koja izdaju kvalifikovane sertifikate za verifikaciju kvalifikovanih elektronskih potpisa.

[25] Izvor *www.**parlament**.sr.gov.yu/*

U Zakonu o elektronskom potpisu navedene su sledeće definicije:

Elektronski potpis - skup podataka u elektronskom obliku, koji su pridruženi ili su logički povezani sa elektronskim dokumentom i koji služe za identifikaciju potpisnika.

Kvalifikovani elektronski potpis - elektronski potpis kojim se pouzdano garantuje identitet potpisnika, integritet elektronskih dokumenata i onemogućava naknadno poricanje odgovornosti za njihov sadržaj, i koji ispunjava uslove utvrđene Zakonom o elektronskom potpisu.

Takođe, prema tekstu Zakona, kvalifikovani elektronski potpis mora da zadovolji sledeće uslove:

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

Kvalifikovani elektronski potpis, koji zadovoljava prethodno navedene uslove, u odnosu na podatke u elektronskom obliku ima isto pravno dejstvo i dokaznu snagu kao i svojeručni potpis, odnosno svojeručni potpis i pečat, u odnosu na podatke u papirnom obliku**.**

Dakle, ovim zakonom 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**.**

Odredbe ovog zakona primenjuju se na opštenje organa, opštenje organa i stranaka, dostavljanje i izradu odluke organa u elektronskom obliku u upravnom, sudskom i drugom postupku pred državnim organom - ako je zakonom kojim se uređuje taj postupak propisana upotreba elektronskog potpisa.

U zakonu se određuju :

- Upotreba elektronskog potpisa, prava, obaveze i odgovornosti u vezi sa elektronskim sertifikatima.
- Definiše se značenje ključnih izraza koji se koriste za potrebe ovog zakona.
- Definiše se punovažnost elektronskog dokumenta u dokaznom postupku, kao i određeni izuzeci.
- Mogućnost čuvanja određenih dokumenata u elektronskom obliku
- Definiše elektronski potpis i kvalifikovani elektronski potpis

- Definiše elektronske sertifikate i sertifikaciona tela
- Određuje prava, obaveze i odgovornosti korisnika i sertifikacionih tela
- Uređuje nadzor nad primenom ovog zakona.
- Propisuje novčane kazne za prekršaje u skladu sa Zakonom o prekršajima.

Jedan od preuzetih članova iz Direktive o elektronskom potpisu je i čl. 3 u kome se navodi da " *Elektronskom dokumentu se ne može osporiti punovažnost ili dokazna snaga samo zbog toga što je u elektronskom obliku* ."

Elektronski potpis može imati pravno dejstvo i može se koristiti kao dokazno sredstvo u zakonom uređenom postupku, osim kada se, u skladu sa posebnim zakonom, zahteva da samo svojeručni potpis ima pravno dejstvo i dokaznu snagu.

Ministarstvo nadležno za informaciono društvo (u daljem tekstu: nadležni organ) propisuje tehničko-tehnološke postupke za formiranje kvalifikovanog elektronskog potpisa i kriterijume koje treba da ispune sredstva za formiranje kvalifikovanog elektronskog potpisa.

Elektronski sertifikat, u smislu ovog zakona, je elektronska potvrda kojom se potvrđuje veza između podataka za proveru elektronskog potpisa i identiteta potpisnika.
Elektronske sertifikate izdaje sertifikaciono telo.

Sertifikaciono telo u smislu ovog zakona jeste pravno lice koje drugim pravnim i fizičkim licima pruža usluge izdavanja elektronskih sertifikata, kao i druge usluge povezane sa ovom delatnošću. Sertifikacionim telima nije potrebna posebna dozvola za izdavanje elektronskih sertifikata. Nadležni organ vodi evidenciju sertifikacionih tela.

Elektronski sertifikati koje izdaje strano sertifikaciono telo ravnopravni su sa domaćim elektronskim sertifikatima.Kvalifikovani elektronski sertifikati izdati od strane inostranih sertifikacionih tela ravnopravni su sa domaćim:

1) ako je inostrano sertifikaciono telo dobilo rešenje od nadležnog organa, u skladu sa odredbama ovog zakona; ili
2) ako potiču iz zemlje sa kojom postoji bilateralni sporazum o međusobnom priznavanju kvalifikovanih elektronskih sertifikata.

Nadležni organ vrši inspekcijski nadzor nad primenom ovog zakona i radom sertifikacionih tela.

Nadzor nad radom sertifikacionih tela na poslovima prikupljanja, upotrebe i zaštite ličnih podataka korisnika vrše organi određeni zakonom i drugim propisima kojima se uređuje zaštita ličnih podataka.
Podzakonski akti koji regulišu ovu oblast su :

- Pravilnik o evidenciji sertifikacionih tela

- Pravilnik o Registru sertifikacionih tela za izdavanje kvalifikovanih elektronskih sertifikata u Republici Srbiji

- Pravilnik o tehničko-tehnološkim postupcima za formiranje kvalifikovanog elektronskog potpisa i kriterijumima koje treba da ispune sredstva za formiranje kvalifikovanog elektronskog potpisa

- Pravilnik o bližim uslovima za izdavanje kvalifikovanih elektronskih sertifikata

5.5. **Zakon o elektronskoj trgovini**[26]

Ustavni osnov za donošenje zakona

Ustavni osnov za donošenje Zakona o elektronskoj trgovini sadržan je u članu 97. tač. 6. Ustava Republike Srbije, kojima se utvrđuje da Republika Srbija uređuje i obezbeđuje, pored ostalog, jedinstveno tržište, pravni položaj privrednih subjekata, sistem obavljanja pojedinih privrednih i drugih delatnosti.

Razlozi za donošenje zakona

Proces deregulacije različitih tržišta, globalizacija, razvoj novih tehnologija koje omogućavaju brzu razmenu informacija širom sveta, uticali su na stvaranje novih uslova poslovanja i kod nas. Razvoj informacione tehnologije sa sobom nosi čitav niz promena i za korisnike znači nov način rada i života, posebno u pogledu prikupljanja informacija.

U takvom okruženju, koje na ubrzani tehnološki razvoj gleda kao na uslov bez kojeg se ne može, industrijski i privredni rast i razvoj može opstati samo stalnim prisustvom u središtu globalnih informatičkih zbivanja. Informaciona tehnologija je postala glavni pokretač promena i rešavanja privrednih, socijalnih i svih drugih problema i sredstvo povezivanja sa međunarodnom zajednicom.

Elektronsko poslovanje, koje je posebno preko Interneta dobilo zamah, danas otvara mogućnost novom vidu komuniciranja sa potrošačima i konkurencijom. Ignorisanje i nespremnost za uključivanje u to novo tržište, značajno umanjuje konkurentske prednosti svakog poslovanja. Takva situacija zahteva prilagođavanje novim informacionim i tehnološkim trendovima, kao i stvaranje zakonske osnove za kreiranje dugoročnog plana razvoja tog područja. Nesumnjivo, elektronska trgovina danas predstavlja jedan od najsavremenijih načina vršenja poslovnih aktivnosti i obuhvata sve segmente društvenog života, od privrede, bankarstva, zdravstva, državne uprave, pravosuđa i sl.

Elektronsko poslovanje, kao jedan vid poslovnih aktivnosti, obuhvata lepezu komercijalnih transakcija koje se u celini ili delimično vrše elektronskim putem, uključujući oglašavanje i promociju, odnose između trgovaca i prodajne aktivnosti,

[26] Izvor *www.mtu.sr.gov.yu*

elektronsku nabavku i podršku poslovnim procesima, a delimično i isporuku putem interneta kao otvorenog sistema čijom komercijalizacijom dolazi do procvata elektronske trgovine. Napredak elektronske trgovine zavisi od automatizacije internih poslovnih procesa, transakcija između poslovnih organizacija i potrošača, kao i između privrednih subjekata i administracije ili drugih privrednih subjekata.

Razvoj elektronske trgovine unutar informacionog društva, stvara mogućnosti za zapošljavanje, posebno u malim i srednjim preduzećima, stimuliše ekonomski rast i ulaganje u inovacije i doprinosi jačanju konkurentnosti industrije, pod uslovom da je svima omogućen pristup Internetu.

Republika Srbija je donošenjem Zakona o elektronskom potpisu, započela proces stvaranja pravnog okvira, neophodnog za uspešno uspostavljanje, funkcionisanje i razvoj informacionog društva. Punom implementacijom tog zakona stvaraju se uslovi za primenu elektronskog potpisa i razmena elektronskih dokumenata uz poverenje najšire javnosti u delovanje i upotrebu elektronskog potpisa, čime se stvara prostor za intenzivnije delovanje sistema elektronske trgovine, koja sve više postaje imperativ konkurentnosti na svetskom tržištu.

Donošenjem Zakona o elektronskoj trgovini stvorili su se pravni osnovi za izjednačavanje elektronskih oblika poslovanja sa klasičnim neposrednim oblikom, što će privredi i organima državne uprave stvoriti značajnu konkurentsku prednost. To područje do sada nije bilo zakonski regulisano, što je predstavljalo značajnu prepreku u razvoju elektronske trgovine, odnosno opšteg privrednog razvoja Republike.

Donošenjem ovog zakona želi se podstaći brz tehnološki razvoj elektronske trgovine, sa posebnim naglaskom na izjednačavanje sigurnih elektronskih oblika poslovanja sa klasičnim papirnim oblikom i izjednačavanju sigurnog (naprednog) elektronskog potpisa sa svojeručnim potpisom.

Sadržaj zakona

Zakon se sastoji iz sedam delova, koji obuhvataju 23. člana.

Prvi deo sadrži opšte odredbe (član 1. do 5.)

- predmet zakona i sadržina
- objašnjenje značenja određenih pojmova koji se koriste u zakonu;
- područje primene (u teritorijalnom smislu);
- lica na koja se zakon primenjuje;
- princip slobode pružanja usluga informacionog društva, što podrazumeva da za vršenje tih usluga nije potrebno pribavljanje posebne dozvole ili odobrenja kao i minimalni uslovi koje svaki pružaoc usluga mora da zadovolji.

Drugi deo (član 6. do 8.) sadrži odredbe kojima se:

- određuju obavezne informacije koje je pružaoc usluga informacionog društva dužan da pruži korisnicima;
- definišu uslovi koje mora da zadovoljava komercijalna poruka, koja je predmet usluge koju pruža informaciono društvo;
- određuje pojam netražene komercijalne poruke.

Treći deo (član 9. do 16.) sadrži propise koji se odnose na ugovor u elektronskom obliku:

- forma i punovažnost ugovora; ugovori na koje se ovaj zakon ne primenjuje;
- obavezni podaci i obaveštenja koja je pružaoc usluga dužan da pruži primaocu usluge pre zaključenja ugovora;
- dostupnost ugovora;
- regulisanje potvrde prijema, odnosno prihvata ponude;
- momenat zaključenja ugovora.
- uređuje pitanje elektronskog potpisa

Četvrti deo (član 17. do 21.) uređuje

- odgovornost pružaoca usluga informacionog društva,
- uslovi za isključenje odgovornosti povodom sadržaja poslate poruke;
- privremeno skladištenje podataka (*caching*);
- trajnije skladištenje podataka (*hosting*).

Peti deo (član 22.) uređuje nadzor nad sprovođenjem ovog zakona

- tržišna inspekcija,
- inspekcija poštanskog saobraćaja i
- inspekcija nadležna za poslove telekomunikacija i informatike.

Šesti deo (član 23.) prekršaji

- utvrđene su radnje koje predstavljaju prekršaje, u smislu ovog zakona, kao i
- visina novčanih kazni.

Možemo da primetimo da je osnov za izradu ovog predloga Direktiva EU o elektronskoj trgovini, te da su u skladu s ovim aktom uređeni mnogi članovi, pa tako i član 5 koji se odnosi na slobodu pružanja usluga.

Za pružanje usluga informacionog društva nije potrebna posebna dozvola ili odobrenje.

Pružaoc usluga mora, pre nego što otpočne da obavlja delatnost pružanja tih usluga, da bude registrovan u Registar privrednih subjekata u skladu sa zakonom kojim se uređuje registracija privrednih subjekata.

Zatim član 8 *Netražena komercijalna poruka (spam)*

Korišćenje elektronske pošte u svrhu slanja netražene komercijalne poruke, dozvoljeno je samo uz prethodni pristanak lica kome je takva vrsta poruke namenjena, u skladu sa zakonom.

Pored navedenog, ovim zakonom su regulisani i Ugovori u elektronskom obliku.

Što se forme i punovažnosti ugovora tiče, Zakon propisuje da ugovor može biti zaključen elektronskim putem, odnosno u elektronskoj formi, da ponuda i prihvat ponude mogu se dati elektronskim putem, odnosno u elektronskoj formi. Kada se elektronska poruka, odnosno elektronska forma koristi prilikom zaključenja ugovora, takvom ugovoru se ne može osporiti punovažnost samo zbog toga što je sačinjen u elektronskoj formi.

Međutim, zbog izuzetne važnosti pojedinih ugovora Zakon predviđa odstupanja, pa se tako ne primenjuje na sledeće kategorije ugovora:

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

Zakon propisuje i sam postupak zaključenja ugovora, te govori da je pružalac usluga dužan da potencijalnom korisniku usluga, pre zaključenja ugovora o pružanju usluga, obezbedi na jasan, razumljiv i nedvosmislen način podatke i obaveštenja o:

- postupku koji se primenjuje kod zaključivanja ugovora;
- ugovornim odredbama;
- opštim uslovima poslovanja, ako su sastavni deo ugovora;
- jezicima na kojima ugovor može biti zaključen;
- kodeksima ponašanja u skladu sa kojima postupaju pružaoci usluga i kako se ti kodeksi mogu pregledati elektronskim putem.

Pružalac usluga dužan je da obezbedi da tekst ugovora i odredbe opštih uslova poslovanja koje su sastavni deo ugovora zaključenih u elektronskoj formi budu dostupni korisnicima usluga na način koji omogućava njihovo skladištenje, ponovno korišćenje i reprodukovanje.Pružalac usluga dužan je da, bez odlaganja, elektronskim putem, posebnom

elektronskom porukom, potvrdi prijem elektronske poruke koja sadrži ponudu ili prihvat ponude za zaključenje ugovora.

Ugovor u elektronskoj formi smatra se zaključenim onog časa kada ponuđač primi elektronsku poruku koja sadrži izjavu ponuđenog da prihvata ponudu. Ponuda i prihvat ponude, kao i druge izjave volje učinjene elektronskim putem, smatraju se primljenim kada im lice kome su upućene može pristupiti.

Zakonom je uređeno pitanje odgovornosti pružaoca usluga informacionog društva. propisano je da pružalac usluga informacionog društva nije odgovoran za sadržaj poslate poruke, ali je dužan da spreči bilo kakvu zloupotrebu svojih resursa, za koju nije odgovoran, osim u slučaju učestvovanja u takvoj zloupotrebi. U tom smislu propisano je isključenje odgovornosti, privremeno čuvanje podataka, trajnije čuvanje podataka, linkovi i obavezna obaveštenja. Pod privremenim čuvanjem podataka podrazumeva se čuvanje u svrhu uštede komunikacionih resursa. Takav oblik čuvanja podataka je privremen iz razloga što se podaci kojima nije niko pristupio u određenom vremenskom intervalu automatski brišu. Trajnije čuvanje podataka podrazumeva čuvanje u svrhu njihove reprodukcije, kao što su npr. Internet serveri posredstvom kojih se prodaje usluga *hosting*-a,Internet stranica.

Još jedan od članova koji je preuzet iz navedene Direktive odnosi se na odgovornost pružaoca usluga. Zakon predviđa isključenje odgovornosti na sledeći način:

" *Pružalac usluga koji prenosi elektronske poruke koje mu je predao korisnik usluga, nije odgovoran za sadržaj poslate poruke i njeno upućivanje, ako nije*:

- ✓ *inicirao prenos;*
- ✓ *izvršio odabir podataka ili dokumenata koji se prenose;*
- ✓ *izuzeo ili izmenio podatke u sadržaju poruke ili dokumenata;*
- ✓ *odabrao primaoca prenosa.*

Prenos poruka i pružanje pristupa porukama iz stava 1. ovog člana moraju biti obavljeni na način koji omogućava automatsko, posredničko i privremeno skladištenje prenetih poruka i u njima sadržanih podataka i moraju biti privremeno skladištene samo u vremenskom periodu koji je neophodan za prenos poruka."

Zakon još uređuje i oblast privremenog skladištenja podataka i trajnog skladištenja podataka.

Na oblast elektronske trgovine primenjuju se i odredbe drugih zakona, kao što su:

Zakon o obligacionim odnosima, koji reguliše obavljanje trgovinske delatnosti na daljinu;
*Zakon o elektronskom potpisu***,** čije odredbe su veoma značajne za punovažnost stavljanja u promet dokumenata u elektronskoj formi;
Zakon o zaštiti potrošača;
Krivični zakonik.

5.6. Zakon o elektronskom dokumentu

Predmet ovog zakona predstavlja uređenje uslova i načina 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 u vezi sa ovim dokumentom.

Prema zakonu, elektronski dokument jeste skup podataka sastavljen od slova, brojeva, simbola, grafičkih, zvučnih i video zapisa sadržanih u podnesku, pismenu, rešenju, ispravi ili bilo kom drugom aktu koji sačine pravna i fizička lica ili organi vlasti radi korišćenja u pravnom prometu ili u upravnom, sudskom ili drugom postupku pred organima vlasti, ako je elektronski izrađen, digitalizovan, poslat, primljen, sačuvan ili arhiviran na elektronskom, magnetnom, optičkom ili drugom mediju.

Zakon predviđa da se elektronskom dokumentu ne može se osporiti punovažnost ili dokazna snaga samo zato što je u elektronskom obliku.

Ako je propisom utvrđen pismeni oblik kao uslov punovažnosti pravnog akta, pravnog posla ili druge pravne radnje, odgovarajući elektronski dokument potpisuje se kvalifikovanim elektronskim potpisom, u skladu sa zakonom kojim se uređuje elektronski potpis.

Ovaj zakon stvara pravni okvir za potpuno izjednačavanje klasičnog oblika poslovanja, pomoću papira, sa elektronskim oblicima poslovanje, a treba da omogući i dosledno sprovođenje Zakona o elektronskom potpisu koji je donet 2004. godine.

Zakon definiše proceduru postupanja sa elektronskim dokumentom, prijem takvog dokumenta, način čuvanja duplikata i izdavanje potvrde o prijemu. Takođe, zakon omogućava da sva dokumenta u elektronskom obliku budu, pod zakonom određenim uslovima, pravno relevantna, da elektronski dokument bude punovažan i da ima dokaznu snagu. Osnovi cilj zakona je da se podstakne šira upotreba elektronskih dokumenata, jer bi to doprinelo ukupnoj efikasnosti rada i materijalnoj uštedi.

6. OSNOVE KOMPJUTERSKOG KRIMINALITETA

Iako je u svetu uobičajeno da se krivična dela protiv bezbednosti podataka u savremenim informatičkim sistemima nazivaju kompjuterska krivična dela (kompjuterski kriminalitet) naš je zakonodavac za ova dela upotrebio termin računarski kriminalitet, takođe u upotrebi je i termin visokotehnološki kriminalitet. Inače radi se o sinonimima, pa ćemo ukazati na osnovne teorijske definicije pojma kompjuterskog kriminaliteta

6.1. Pojam kompjuterskog kriminaliteta

Kompjuter (računar) u svakom slučaju predstavlja jednu od najznačajnijih i najrevolucionarnijih tekovina razvoja tehničko - tehnološke civilizacije. No, pored svih prednosti koje sobom nosi i ogromne koristi čovečanstvu, kompjuter je brzo postao i sredstvo zloupotrebe nesvesnih pojedinaca, grupa čak i organizacija. Tako nastaje kompjuterski kriminalitet kao poseban i specifičan oblik savremenog kriminaliteta po strukturi, obimu i osobenostima. Sve to zaslužuje pažnju države i njenih organa pa i cele međunarodne zajednice.

Uporedo sa ubrzanom informatizacijom društva i ulaskom Interneta u sve oblasti društvenog i privatnog života ljudi, kompjuterski kriminal postaje dominantan oblik zloupotreba, kršenja zakona i drugih normi ponašanja. Novi oblici napada na računare i računarske mreže javljaju se velikom brzinom, a novi tipovi kompjuterskog kriminala praktično zavise samo od mašte malicioznih napadača. Osnovne elemente krivičnog dela kompjuterskog kriminala čine:

- događaj, odnosno, šta se dogodilo u ispitivanom slučaju,
- okolnosti, ili kako se dogodilo i
- mentalno stanje počinioca kriminala, što je potrebno za klasifikaciju kriminala i profilisanje kompjuterskih kriminalaca.

Glavne kategorije kompjuterskog kriminala mogu se grupisati na bazi uloge računara u izvršavanju krivičnog dela kompjuterskog kriminala, gde računar može biti:

- cilj napada (upad u računar, krađa podataka),
- sredstvo za napad (prevare sa kreditnim karticama, slanje *spama* i sl.),
- povezan sa klasičnim kriminalom (trgovina drogom i ljudima, dečija pornografija i dr.) i
- repozitorijum (skladište) digitalnih dokaza kompjuterskog kriminala.

Takođe, u porastu je i klasičan kriminal povezan sa računarom, kao što su povreda intelektualne svojine (neovlašćeno kopiranje i krađa autorskih prava) i piraterija softvera.

Tipovi kompjuterskog kriminala su brojni, a najčešći su:

- krađa računarskih servisa,
- neovlašćeni pristup,

- piraterija softvera,
- otkrivanje, krađa i izmena računarskih podataka i informacija,
- iznuđivanje pomoću računara,
- neovlašćeni pristup bazama podataka,
- zloupotreba ukradenog pasvorda,
- prenos destruktivnih virusa i
- industrijska i politička špijunaža[27].

Zahvaljujući ogromnoj moći kompjutera u memorisanju i brzoj obradi velikog broja podataka, automatizovani informacioni sistemi postaju sve brojniji i gotovo nezamenjivi deo celokupnog društvenog života svih subjekata (fizičkih, ali i pravnih lica) na svim nivoima. Tako kompjuter postaje svakodnevni i nezaobilazni deo, segment svih sfera društvenog života od proizvodnje, prometa, vršenja usluga pa do nacionalne odbrane i bezbednosti u najširem smislu.

No sve ove raznolike forme neposredne primene kompjutera u svim oblastima života nisu ostale nezapažene od strane nesavesnih i neodgovornih pojedinaca i grupa koji ne birajući sredstva i način protivpravnim ponašanjem pokušavaju da sebi ili drugom pribave protivpravnu imovinsku korist.

Kompjuter postaje sredstvo vršenja različitih oblika nedozvoljenih, protivpravnih i društveno opasnih delatnosti. Naravno, kompjuterski kriminalitet pod čijim zbirnim nazivom su obuhvaćeni svi ovi raznoliki oblici i forme ponašanja vezani za zloupotrebu kompjutera i informacionih sistema uopšte iako štetna i opasna negativna društvena pojava modernog doba nema opšte usvojenu definiciju.

Tako se u krivičnopravnoj literaturi za ove raznolike oblike kompjuterskog kriminaliteta upotrebljavaju različiti termini kao što su:

1) zloupotreba kompjutera (*computer abuse*),

2) kompjuterska prevara (*computer fraud*),

3) delikti uz pomoć kompjutera (*crime by computer*),

4) informatički kriminalitet,

5) računarski kriminaliteti i

6) tehno kriminalitet.

[27] *Izvor M. Milosavljević, G. Grubor „ Digitalna forenzička istraga kompjuterskog kriminala“, Univerzitet Singidunum, 2009*

Ovaj vid kriminaliteta za razliku od drugih ne predstavlja još uvek zaokruženu fenomenološku kategoriju te ga je nemoguće definisati jedinstvenim i precizno pojmovnim određenjem. Kompjuterski kriminalitet je samo opšta forma kroz koju se ispoljavaju različiti oblici kriminalne delatnosti.

Naime, to je kriminalitet koji je upravljen protiv bezbednosti informacionih (kompjuterskih, računarskih) sistema u celini ili u njenom pojedinim delu na različite načine i različitim sredstvima u nameri da se sebi ili drugom pribavi kakva korist ili da se drugome nanese kakva šteta[28].

No, u teoriji krivičnog prava se mogu naći različita pojmovna određenja kompjuterskog kriminaliteta. Tako Don Parker određuje kompjuterski kriminalitet kao zloupotrebu kompjutera u smislu svakog događaja koji je u vezi sa upotrebom kompjuterske tehnologije u kome žrtva trpi ili bi mogla da trpi gubitak, a učinilac deluje u nameri da sebi pribavi ili bi mogao da pribavi korist[29] *August Bequai* definiše kompjuterski kriminalitet kao vršenje krivičnih dela kod kojih se računar pojavljuje kao oruđe ili objekt zaštite odnosno kao upotreba kompjutera pri vršenju prevare, utaje ili zloupotrebe čiji je cilj prisvajanje novca ili usluge ili vršenje političke ili poslovne manipulacije uključujući i radnje uperene protiv samog računara[30]. *Bogo Brvar* daje sledeću definiciju kompjuterskog kriminaliteta. To su krivična dela kod kojih se kompjuter pojavljuje kao sredstvo (oruđe), predmet ili objekt napada za čije je vršenje ili pokušaj neophodno izvesno znanje iz računarstva ili informatike Konačno Đorđe Ignjatović pod kompjuterskim kriminalitetom pak smatra poseban vid inkriminisanih ponašanja kod kojih se računarski sistem (shvaćen kao jedinstvo hardvera i softvera) pojavljuje ili kao sredstvo izvršenja ili kao objekt krivičnog dela ukoliko se delo na drugi način ili prema drugom objektu uopšte ne bi moglo izvršiti ili bi ono imalo drugačije karakteristike[31].

Iz navedenih definicija nesumnjivo se mogu izvući osnovne karakteristike ili obeležja pojma kompjuterskog kriminaliteta. To su sledeća obeležja:

- društveno opasna, protivpravna ponašanja za koja zakon propisuje krivične sankcije,

- specifičan način i sredstvo vršenja krivičnih dela, uz pomoć ili posredstvom kompjutera,

- poseban objekt zaštite, bezbednost računarskih podataka ili informacionog sistema u celini ili pojedinog segmenta (dela),

---

[28] *Izvor : Dragan Jovašević, Leksikon krivičnog prava, JP Službeni list SRJ, Beograd, 2002. godine*

[29] *Izvor :Don Parker, Computer abuse, Springfild, 1973. godine, str. 70*

[30] *Izvor :August Bequai, Computer crime, Lexington, 1978. godine, str. 4*

[31] *Izvor: Đorđe Ignjatović, Pojmovno određivanje kompjuterskog kriminaliteta, Anali Pravnog fakulteta u Beogradu, Beograd, broj 1-3/1991. godine, str. 14*

- namera učinioca da sebi ili drugom na ovaj način pribavi kakvu korist (imovinsku ili neimovinsku) ili da drugome nanese kakvu štetu.

U teoriji krivičnog prava se u oblast kompjuterskog kriminaliteta svrstavaju različiti oblici protivpravnog, nedozvoljenog ponašanja kao što su :

1. kompjuterska prevara,

2. finansijske krađe, prevare i zloupotrebe,

3. krađa dobara,

4. falsifikovanje podataka i dokumenata,

5. vandalizam,

6. sabotaža,

7. hakerisanje,

8. kompjuterska špijunaža i

9. krađa vremena.

Velike praktične mogućnosti koje pruža savremena visoko sofisticirana kompjuterska i informatička tehnologija sa sobom nose i opasnosti od širenja i masovne upotrebe elektronskog prisluškivanja, krađe poslovnih i drugih tajni kao i različitih oblika intelektualne svojine, zatim ozbiljnog narušavanja privatnosti i drugih ljudskih sloboda i prava kao i ličnog integriteta, a u poslednje vreme prisutna je i realna opasnost od talasa terorističkih akata raznih vrsta (tzv. tehno ili *kiber* terorizam).

Jedna novija američka studija iz ove oblasti ukazuje na činjenicu da se informatički kriminalitet dešava čak 40 puta češće od klasičnog, opšteg, tradicionalnog kriminaliteta, a da 90% informatičkih zločina ostaje praktično neotkriveno (dakle u zoni tamne brojke kriminaliteta). Ta vrsta kriminaliteta se razvija takvom brzinom da praktično nema presedana u praksi[32].

[32] *Izvor :Slobodan Petrović, Kompjuterski kriminal, Beograd, 2002. godine*

6.2. Karakteristike kompjuterskog kriminaliteta

Kompjuterski (računarski) kriminalitet se pre svega karakteriše velikom dinamikom i izuzetnim bogatstvom svojih pojavnih formi i vidova ispoljavanja. To je i razumljivo jer se radi o novoj tehnologiji sa velikih mogućnosti i primene u skoro svim oblastima društvenog, privrednog pa i ličnog života te su i mogućnosti za zloupotrebu kompjutera svakim danom sve veće.

Pored novih pojavnih oblika ranije već poznatog kriminaliteta, koje pod uticajem kompjutera menja svoj tradicionalni način i modus ispoljavanja, sada se javljaju i novi, znatno opasniji oblici kriminalnog ponašanja, koji do sada nisu bili poznati u kriminalističkoj praksi, a koji ne poznaju granice između država pa ni između kontinenata.

Štetne posledice kompjuterskog kriminaliteta su izuzetno velike. One se mogu ispoljiti i u nastupanju imovinske štete za pravno ili fizičko lice (ponekad i za celu državu), u gubitku poslovnog ugleda, gubitku poverenja u sigurnost i istinitog kompjuterskog poslovanja i uopšte kompjuterskih informacija, opasnosti od zloupotrebe po slobode i prava čoveka uopšte na razne načine i u raznim oblicima. I sami učinioci krivičnih dela u vezi sa zloupotrebom kompjutera predstavljaju posebnu često specifičnu kategoriju ljudi. Ovde se najčešće radi o nedelikventnim, nenasilnim, socijalno prilagodljivim pojedincima. To su po pravilu lica koja ipak moraju da poseduju posebna stručna i praktična znanja i veštine u domenu visoke informatičke, računarske i kompjuterske tehnologije i kojima su ovakva tehnološka sredstva dostupna.

Ova se krivična dela vrše prikriveno, često bez neke vidljive i bliske prostorne povezanosti učinioca dela i žrtve (oštećenog). Najčešće se teško otkrivaju a još teže dokazuju, a dugo vremena ostaju praktično neotkriveni sve dok oštećeni ne pretrpi neku štetu koja je vidljiva u sistemu računarskih informacija. To je kriminalitet koji brzo menja forme i oblike ispoljavanja, granice među državama kao i vrstu oštećenog[33].

Tako je Interpol još 1980. godine konstatovao sledeće:

"Danas u savremenom svetu postoji još jedan veliki usavršeni front koji je prisutan u svetskim razmerama. Veliki kriminalitet, organizacije kriminalaca sve više se orijentišu na akcije pljački u kojima je objekt kompjuter. Elektronika se zloupotrebljava. Ne beleži se pad klasičnih pljački ali se iz godine u godinu povećava nova vrsta kriminaliteta u kome se elektronika koristi kao sredstvo da se kriminalci domognu milionskih svota novca

Savremena informaciona i kompjuterska tehnologija unela je nove i drastične promene u sve sfere društvenog života.

Te promene su pored pozitivnih i korisnih novina donele i niz problema vezanih za pojavu i širenje kompjuterskog kriminaliteta različitih oblika, formi i vidova ispoljavanja. Sve te promene se mogu svesti na sledeće:

[33] *Izvor. Nikola Kitarović, Kompjuterski kriminalitet, Bilten sudske prakse Vrhovnog suda Srbije, Beograd, broj 2-3/ 1998. godine, str. 52-53*

- nove forme vrednosti,
- koncentracija podataka,
- novi ambijent delovanja,
- nove metode i tehnike delovanja,
- sužavanje vremenske skale delovanja,
- širenje geografskog prostora delovanja,
- pokretljivost,
- stabilnost rizika.

6.3. Karakteristike učinilaca krivičnih dela kompjuterskog kriminala

Ne može se govoriti o jedinstvenom profilu učinilaca kompjuterskog kriminaliteta,oni se svrstavaju u različite kategorije prema pojavnim oblicima dela koja čine, ali i prema motivima, koji ih pokreću u vršenju kriminalnih aktivnosti.

Učinioci ovih dela se mogli podeliti na:

- ✓ zlonamerne, koji mogu da deluju radi ostvarenja imovinske koristi, ili samo u cilju nanošenja štete i

- ✓ na učinioce koji nisu motivisani ne ostvarenjem koristi, niti prouzrokovanjem štetnih posledica, već jednostavno traže zadovoljstvo u neovlašćenom prodiranju u neki dobro obezbeđen informacioni sistem. To su tzv. hakeri *(hackers)*, koji koristeći
  svoje računarsko znanje, upadaju u tuđe kompjuterske sisteme.

6.3.1. Hakeri

Ovi učinioci predstavljaju kompjuterske entuzijaste, koji provaljujući u dobro čuvane informatičke sisteme iživljavaju svoju strast za avanturama po tzv „informacionim autostradama" u specifičnom *cyber-spaces*-u. Oni su često pravi „kompjuterski zavisnici" koji čak ponekad nemaju pravi kontakt s realnošću, već prvenstveno obitavaju u svom „virtuelnom svetu".

Oni vrhunsko zadovoljstvo nalaze u samom činu provaljivanja u višestruko obezbeđene informacione sisteme i što su kompjuterski sistemi bolje čuvani, to je za hakere veći izazov da se upuste u za njih spektakularno savladavanje „kriptografskih brava". Zato su na meti ovih učinilaca. često najbolje obezbeđeni informacioni sistemi kao što su kompjuterske mreže vlada savremenih država, ili vojnih laboratorija, pa i u kompjuterske sisteme Pentagona.

Hakeri mogu svesno ili nesvesno da prouzrokuju ogromne štete. Oni su prema svom profesionalnom opredeljenju najčešće programeri kompjutera, visokoobrazovani

informatičari, a ponekad je reč o osobama koje su svoju veštinu i znanje stekli baveći se kompjuterima iz hobija.

To su veoma inteligentni učinioci a jedina prava zaštita od njihovih provala je jačanje kriptografskih sistema zaštite, uz strožiju kriminalnu politiku prema ovakvim učiniocima Oni, nezavisno od motiva koji ih pokreću, realno predstavljaju veliku opasnost, naročito u situacijama kada se upuštaju u rizične informatičke avanture u tako osetljivim područjima kao što su nacionalna bezbednost, industrija naoružanja, satelitska tehnologija itd.

6.3.2. Zlonamerni učinioci kompjuterskih delikta

Zlonamerni učinioci kompjuterskih delikta najčešće su motivisani koristoljubljem. Oko 80% delikvenata čini delo prvi put, a 70% je zaposleno više od pet godina u oštećenom preduzeću.

Njihovo starosno doba je između 19 i 30 godina, pretežno su muškog pola, veoma su inteligentni; imaju uglavnom više godina radnog iskustva i važe kao savesni radnici koji prilikom obavljanja radnih zadataka ne prouzrokuju nikakve probleme, često su tehnički kvalifikovaniji nego što to zahteva radno mesto na koje su raspoređeni; ovi učinioci sebe po pravilu ne smatraju kradljivcima ili uopšte kriminalcima, već samo pozajmljivačima.

6.4. Koristoljubivi kompjuterski kriminalitet

Koristoljubivi kompjuterski kriminalitet veoma je čest u bankarstvu, finansijskim korporacijama i osiguravajućim društvima. Statistički podaci o učiniocima kompjuterskih delikta u oblasti bankarskih poslova ukazuju na najčešće profesije učinilaca: 25% čine osobe sa specijalnim ovlašćenjima sa odgovornostima u informatičkim sistemima, 18% programeri, 18% službenici koji raspolažu terminalima, 16% blagajnici. 11% operateri-informatičari i u 12% slučajeva učinioci su lica van oštećenih korporacija, u šta su uključeni i korisnici usluga.

6.5. Posledice kompjuterskog kriminaliteta

Štete nastale vršenjem kompjuterskih delikta, zavisno od pojavnog oblika kompjuterskog kriminaliteta, mogu se podeliti na:

1. finansijske – koje mogu da nastanu kada učinilac vrši delo u cilju sticanja protivpravne imovinske koristi, pa tu koristi za sebe drugo, zaista i stekne, ili je ne stekne, ali svojim delom objektivno pričini određenu štetu, ili kada učinilac ne postupa radi sticanja koristi za sebe ili drugog, ali objektivno učini finansijsku štetu.

2. nematerijalne – koje se ogledaju u neovlašćenom otkrivanju tuđih tajni , ili drugom "indiskretnom štetnom postupanju"

3. kombinovane – kada se otkrivanjem određene tajne, ili povredom autorskog prava, putem zloupotrebe kompjutera ili informatičke mreže naruši nečiji ugled, odnosno povredi moralno pravo, a istovremeno prouzrokuje i konkretna finansijska šteta.

7. MEĐUNARODNO REGULISANJE KOMPJUTERSKOG KRIMINALITETA

7.1. Kompjuterski kriminalitet u uporednom krivičnom pravu

Budući da preventivne mere (opšteg i specijalnog karaktera) često nisu dovoljne niti jedine mere kojima se društvo suprotstavlja naraslim i nabujalim oblicima i vidovima zloupotrebe kompjutera u različite svrhe, to je logično da sva savremena krivična zakonodavstva u sistemu inkriminacija poznaju jedno ili više kompjuterskih (računarskih ili informatičkih ili tehno) krivičnih dela za koja su propisane različite vrste i mere krivičnih sankcija.

Tako, iako Nemački krivični zakonik[34] ne poznaje kompjuterska krivična dela, to ne znači da ova protivpravna, nedopuštena ponašanja nisu inkriminisana. Naime, u Nemačkoj je 1986. godine donet poseban Krivični zakon za suzbijanje privrednog kriminaliteta koji predviđa niz kompjuterskih krivičnih dela i to: kompjutersku špijunažu u čl. 202a., kompjutersku prevaru u čl. 263a., falsifikovanje podataka u čl. 269., obmanu u pravnom prometu pri obradi podataka u čl. 270., promenu podataka u čl. 302a. i kompjutersku sabotaža u čl. 303a.

Krivični zakonik Austrije[35] predviđa kompjutersko krivično delo u čl. 126a. Ono se zove oštećenje podataka.

U Velikoj Britaniji je 1990. godine donet poseban Zakonik o zloupotrebi kompjutera. Ovaj zakonik predviđa niz krivičnih dela vezanih za zloupotrebu kompjutera i drugih informacionih sistema za koju se propisane veoma stroge kazne[36]

Krivični zakonik Makedonije poznaje u čl. 251. kompjutersko krivično delo pod nazivom. Upad u kompjuterski sistem[37].

Na sličan način postupa i Krivični zakonik Republike Srpske koji poznaje identično krivično delo pod nazivom: Upad u kompjuterski sistem u čl. 260[38].

Krivični zakonik Republike Slovenije (.) poznaje sledeća krivična dela i to : Protivzakoniti ulaz u zaštićenu računarsku bazu podataka u čl. 225 i Upad u računarski sistem u čl. 242[39].

---

[34] *Schonke-Schroder, Strafgesetzbuch, Munchen, 1978. godine*
[35] *E. Foregger-E. Serini, Strafgesetzbuch, Wien, 1989. godine*
[36] *Martin Wasik, The computer misuse act, The Criminal Review, 1990. godine, str. 767).*
[37] *Krivični zakonik Makedonije (Služben vesnik na Republika Makedonija, Skopje, broj 37/1996)*
[38] *Krivični zakonik Republike Srpske (Službeni glasnik Republike Srpske, Banja Luka, broj 22/2000*
[39] *B. Penko, K. Strolig, Kazenski zakonik z uvodnimi pojasnili, Ljubljana, 1999*

7.2. Pravno regulisanje kompjuterskog kriminala na nivou Evropske Unije

Od prvih pojavnih oblika, početkom 90-ih, do danas mnoga su međunarodna tela posvetila pažnju ovom kriminalu. Pored međunarodne sve je učestalija i nacionalna regulacija kompjuterskog kriminala, odnosno nekih od njegovih oblika. Dakle, regulacija se odvija na više koloseka.

Najznačajniji i najbrojniji međunarodni akti doneti su u okviru Evropske Unije 1998. godine pod vođstvom *Urliha Sieber*-a sa Univerziteta u *Virzburgu* izrađena je posebna Studija o pravnim aspektima kompjuterskog kriminala u Informacionom društvu *Legal Aspects of Computer-related Crime in the Information Society* – COMCRIME *study* koja je obuhvatala i osnove kompjuterskog kriminala, kao višeg oblika.

Ovaj akt u kombinaciji sa dokumentima sa Lisabonskog sastanka Evropskog saveta 2000. godine na kome je istaknut značaj tranzicije u konkurentnu, dinamičnu i na znanju zasnovanu ekonomiju predstavlja smernice za aktivnosti vezane za razumevanje fenomena kompjuterskog kriminala. Akcioni plan (*eEurope Action Plan*) iz iste godine vezan je za aktivnost obezbeđenja sigurnosti mreže i uspostavljanja saradnje zemalja članica i njihovog zajedničkog pristupa kompjuterskom kriminalu do 2002. godine.

Iste godine donosi se i predlog Pravnog okvira odlučivanja vezanog za napade na informacione sisteme (*Proposal for a Council Framework Decision on attacks against information systems*). Godinu dana kasnije dokument je dopunjen sa nedozvoljenim pristupom informacionim sistemima i nedozvoljenim ometanjima sistema i podataka. Doneta je 2000. godine i Direktiva o elektronskom poslovanju (*Directive on electronic commerce*) u kojoj se posebna pažnja posvećuje problemu zloupotreba

Te godine donosi se čitav set različitih akata od Odluke Saveta o sprečavanju dečije pornografije na Internetu, Konvencije o međusobnoj pomoći u krivičnoj materiji do Preporuke o strategiji za novi Milenijum u zaštiti i kontroli kompjuterskog kriminala. Potom sledi akt kojim treba da se obezbedi sigurnije Informaciono društvo kroz sigurnost informacione infrastrukture i borbe protiv kriminala vezanog za .

Naravno sa tom godinom niti počinje niti se završava borba protiv kompjuterskog, cyber, odnosno kriminala visokih tehnologija. Tako je 1996. godine započela Zajednička akcija protiv rasizma i ksenofobije, 1997. doneta je Preporuka o anonimnosti subjekata na Internetu i Deklaracija o globalnim računarskim mrežama, 1998, sačinjen je Predlog o okvirima sprečavanja seksualne eksploatacije i trgovine ljudskim bićima. Par godina kasnije donosi se i poseban akt vezan za *cyber* kriminal (*Communication on Cybercrime*).

Nešto manje bile su aktivnosti OECD-a, UN i Saveta Evrope. Još 1983. godine u okviru OECD usvojena je Studija o međunarodnoj primeni i harmonizaciji krivičnog prava vezanog za probleme kompjuterskog kriminala i zloupotreba, tri godine kasnije izašla je minimalna lista u okviru dokumenta Kriminal vezan za kompjutere: analiza i pravna politika, a od 1999. godinu je obeležio ceo set priručnika za sigurnost informacionih sistema kojima se uspostavljaju pravila i osnov njenog postizanja.

Savet Evrope je krajem 1998. godine objavio početak pripreme na donošenju Konvencije o cyber kriminalu, čiji predlog je aprila 2000. godine pušten u proceduru javne rasprave. Ona je danas jedan od najznačajnijih dokumenata koji su pored evropskih zemalja prihvatili i Japan, SAD; Kanada, Južna Afrika. Konvenciju, koja je stupila na snagu u julu 2004, godine prate brojni dokumenti doneti u okviru Saveta:

- *Trust and Security in Cyberspace: The Legal and Policy Framework for Addressing Cybercrime (2002);*
- *Cyber-Rights & Cyber-Liberties, Advocacy Handbook for NGOs (2003);*
- *Racism Protocol to the Convention on Cybercrime (2003);*
- *The Protocol to the Cybercrime Treaty (2002);*
- *Additional Protocol to the Cybercrime Convention Regarding "Criminalization of Acts of a Racist or Xenophobic Nature Committed through Computer Networks ";*
- *Report Revised draft of the Protocol on Racist Speech (2002);*
- *Background Materials on the Racist Speech Protocol ;*
- *Draft Protocol on Racist and Zenophobic Speech: Prelimiary draft (2001);*
- *Second Protocol on Terrorism (2002).*

U okviru grupe G8 od 1997. godine (kada je predložen Akcioni plan borbe protiv ovog kriminala, a usvojenog 1998) na predlog ekspertske grupe za kooperaciju na polju pravde i unutrašnjih poslova ministri pravde i unutrašnjih poslova u više navrata su raspravljali o principima te borbe. Poslednji sastanak bio je u maju prošle godine na kom se, između ostalog, raspravljalo i o nužnosti međunarodne saradnje u sprovođenju istraga i hvatanju počinioca, kao i prihvatanju standarda definisanih u konvenciji Saveta Evrope.

Pored toga ova organizacija donela je i:

- *Recommendations for Enhancing the Legal Framework to Prevent Terrorist Attacks;*
- *Recommendations on Special Investigative Techniques and other Critical Measures for Combating Organized Crime and Terrorism ;*
- *Recommendations for Sharing and Protecting National Security Intelligence Information in the Investigation and Prosecution of Terrorists and Those Who Commit Associated Offenses: Best Practices for Network Security, Incident Response and Reporting to Law Enforcement* i druge.

Ujedinjene nacije, takođe, su imale brojne aktivnosti i donele odgovarajuće akte koji su direktno ili posredno bili vezani za rešavanje problema kompjuterskog kriminala. Pored njih određenim aspektima ili tipovima ovog kriminala bave se i druge međunarodne organizacije kakva je WIPO, Međunarodna privredna komora, Svetska trgovinska organizacija, Azijsko pacifička organizacija za ekonomsku saradnju.

Materijalna prava postaju veoma lagana materija u odnosu na procesna koja treba da obuhvate sve postupke koji su vezani za krivične, građanske, upravne, arbitražne i druge poslove i aktivnosti.

Ova prava treba da olakšaju istražnim i pravosudnim organima prikupljanje i realizovanje podataka o učinjenim delima i počiniocima. Istovremeno upravo ove odredbe trebalo bi da olakšaju institucionalizovanje saradnje koja se mora uspostaviti između odgovarajućih organa gonjenja različitih zemalja, kao i međunarodnih policijskih organizacija.

Otuda je Evropska Unija 2000. godine donela Konvenciju o međusobnoj pomoći u kriminalnoj materiji kojom se predviđa ne samo saradnja već i usklađivanje pravnih i pravosudnih sistema zemalja članica. Saradnja se očekuje i sa relevantnim institucijama korisnika, organa za superviziju zaštite podataka, kao i industrije. Isticanje uspostavljanja efikasnosti, transparentnosti i ravnoteže među svim akterima koji treba da doprinesu odgovarajućoj borbi u sprečavanju ali i sankcionisanju cyber kriminala svakako je osnovni motiv ovog akta.

Ni grupa G8 nije ostala po strani u rešavanju praktičnih pitanja kooperacije i internacionalizacije aktivnosti vezanih za cyber kriminal.

Uspostavljena je mreža koja 24 sata 365 dana u godini obezbeđuje adekvatnu primenu principa borbe protiv kriminala visokih tehnologija. Njima se pridružuju i zemlje nečlanice, čime se krug širi, a očekivani efekti treba da budu bolji. Uspostavljen je čak i ekspertski tim koji bi trebao da identifikuje metode i tehnike i definiše standarde koje se mogu primenjivati u borbi protiv cyber kriminala, kao i u pružanju pomoći specijalizovanim telima za njegovo otkrivanje.

Taj tim čini Međunarodnu organizaciju za kompjuterske dokaze (*IOCE*) kao grupu kojoj su se priključili timovi iz Evropske Unije i njenih zemalja članica.

Tako je uspostavljena mreža čiji je cilj olakšavanje realizacije programa istraživanja i praćenja ovog kriminala[40].

[40] *Drakulić, M.: Kompjutersko pravo. Beograd, FON*

8. PROPISI REPUBLIKE SRBIJE U OBLASTI KOMPJUTERSKOG KRIMINALITETA

Što se tiče naše države, možemo reći da smo se sa velikim zakašnjenjem uključili u oblast rešavanja ovog problema, te da je prvi korak načinjen donošenjem Zakona o izmenama i dopunama Krivičnog Zakonika Republike Srbije, kada je po prvi put izvršena inkriminacija krivičnih dela koja pripadaju oblasti kompjuterskog kriminala.

To praktično znači da do donošenja ovog zakona, nije postojala zakonska regulativa u ovoj oblasti, te da su učinioci ovih krivičnih dela, bili izuzeti od krivičnog gonjenja, te da su slobodno bez bilo kakvih posledica mogli da vrše sve napred navedene oblike kompjuterskog kriminala. Kako je prema Krivičnom Zakoniku predviđeno :

„ Krivično delo je ono delo koje je zakonom predviđeno kao krivično delo, koje je protivpravno i koje je skrivljeno „[41]

Određenost u zakonu je opšte obeležje svakog krivičnog dela. Određenost u zakonu znači propisivanje svih obeležja jednog krivičnog dela, određivanje njegovog bića. Dakle, tek 2003 godine uvodi krivična dela vezana za zloupotrebu kompjutera, a koja imaju zajednički objekt zaštite - bezbednost računarskih podataka odnosno informacionih sistema u celini i poverenja u istinitost ovih podataka. Dakle, osnovni materijalni zakon koji reguliše ovu oblast je Krivični Zakonik Republike Srbije , a nedavno je i ratifikovana Konvencija o visokotehnološkom kriminalu.

8.1. Krivično materijalno pravo

Krivično materijalno pravo predviđeno je prvenstveno Krivičnim Zakonom Republike Srbije . Krivični Zakonik Republike Srbije u delu koji nosi naziv „ Krivična dela protiv bezbednosti računarskih podataka“ predviđa sledeća krivična dela[42].

Prvo krivično delo ove vrste u našem pravu jeste: **Oštećenje računarskih podataka i programa**

Delo ima osnovni i dva teža oblika. Osnovno delo se sastoji u oštećenju, prikrivanju, neovlašćenom brisanju, izmeni ili na drugi način činjenju neupotrebljivim računarskih podataka ili programa. Delo se dakle može učiniti samo u odnosu na računarski podatak ili program koji pripada nekom fizičkom licu - pojedincu (kao napadni objekt) i to sa više alternativno predviđenih delatnosti.

Cilj preduzimanja ovih delatnosti je onesposobljavanje za korišćenje u potpunosti ili delimično računarskih podataka (jednog ili više njih) ili programa.

[41] *izvor : Krivični Zakonik Republike Srbije*
[42] *izvor : Krivični Zakonik Republike Srbije*

Posledica se dakle sastoji u povredi zaštićenog dobra. Delo može učiniti svako lice a u pogledu vinosti potreban je umišljaj. Za ovo je delo propisana novčana kazna ili zatvor do tri meseca.

Prvi teži oblik ovog krivičnog dela postoji ako je preduzetom radnjom prouzrokovana šteta za neko lice u iznosu preko 450 000 dinara. Visina prouzrokovane štete je kvalifikatorna okolnost za koju zakon propisuje kaznu zatvora od tri meseca do tri godine. Najteži oblik ovog krivičnog dela za koji je propisana kazna zatvora od šest meseci do pet godina postoji ako je preduzetom radnjom prouzrokovana šteta u iznosu preko 1.500 000 dinara.

Računarska sabotaža je drugo kompjutersko krivično delo u našem pravu za koje je propisana kazna zatvora od jedne do pet godina.

Delo čini lice koje unese, uništi, izbriše, izmeni, ošteti, prikrije ili na drugi način učini neupotrebljivim računarski podatak ili program ili uništi ili ošteti računar ili drugi uređaj za elektronsku obradu i prenos podataka sa namerom da onemogući ili znatno omete postupak elektronske obrade i prenosa podataka koji su od značaja za državne organe, javne službe, ustanove, preduzeća ili druge subjekte.

Objekt napada kod ovog dela je dvojako određen. To je prvo, računarski podatak ili program (kao i kod prethodnog krivičnog dela) ali i računar odnosno drugi uređaj za elektronsku obradu ili prenos podataka. No, ovde se mora raditi i o posebnom svojstvu oštećenog. Naime, ovi objekti moraju da pripadaju državnom organu, javnoj službi ili drugim pravnim licima kao što su ustanove, preduzeća ili druge organizacije. Inače u pogledu radnje izvršenja i ostalih obeležja bića ovog dela nema razlike u odnosu na prethodno krivično delo.

Pravljenje i unošenje računarskih virusa je krivično delo predviđeno u čl. 300 Delo ima osnovni i teži oblik.

Osnovno delo čini lice koje napravi računarski virus u nameri da ga unese u tuđi računar ili računarsku mrežu. Radnja izvršenja je samo sačinjavanje, pravljenje virusa. Šta su to virusi, kako se prave, koje su njihove vrste ili karakteristike, svrha i sadržina predstavljaju pitanja koje sudsko veće mora da reši u svakom konkretnom slučaju kao faktičko pitanje. Delo je svršeno samim momentom pravljenja ovakvog virusa u nameri da se on unese u tuđi računar ili računarski sistem bez obzira da li je takva namera i ostvarena u konkretnom slučaju ili ne.

Ako je pak ovako sačinjeni, napravljeni virus i unet u tuđi računar ili računarsku mrežu čime je prouzrokovana šteta (bilo imovinska ili neimovinska i to bez obzira u kom iznosu) radi se o težem obliku ovog krivičnog dela.

Sledeće je krivično delo je **Računarska prevara**. Delo ima jedan osnovni, jedan posebni i dva teža, kvalifikovana oblika.

Osnovno delo čini lice koje unese netačan podatak ili ne unese kakav važan podatak ili ko na drugi način prikrije ili lažno prikaže podatak i tako utiče na rezultat elektronske obrade ili prenosa podataka. Bitno je da je ova radnja falsifikovanja, krivotvorenja, dovođenja u zabludu oštećenog preduzeta u nameri da se sebi ili drugom pribavi protivpravna imovinska korist odnosno da se drugome nanese kakva imovinska šteta. Za postojanje krivičnog dela dovoljno je da je radnja izvršenja preduzeta u navedenoj nameri. Tog trenutka je delo svršeno. Nije potrebno da je u konkretnom slučaju u nastupila imovinska šteta za neko lice

Poseban oblik računarske prevare za koji je propisana novčana kazna ili zatvor do dve godine postoji kada je radnja krivotvorenja podataka ili prikrivanja ili lažnog prikazivanja računarskih podataka preduzeta u nameri da se na ovaj način drugom licu nanese kakva šteta. Ta šteta ne mora da nastupi u konkretnom slučaju, ali ona mora da bude pobuda, unutrašnji pokretač učinioca na preduzimanje radnje izvršenja. Može se raditi o imovinskoj, ali i drugim vidovima neimovinske štete.

Zavisno od visine pribavljene protivpravne imovinske koristi za učinioca ili neko drugo lice, zakon razlikuje dva teža, kvalifikovana oblika ovog krivičnog dela. obliku računarske prevare za koji je propisana kazna zatvora od dve do dvanaest godina.

Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka ima osnovni i dva teža oblika ispoljavanja.

Osnovno delo čini lice koje kršeći mere zaštite (preventivno - tehničke i druge mere) neovlašćeno pristupi računaru ili računarskoj mreži ili neovlašćeno pristupi elektronskoj obradi podataka. Radnja izvršenja je pristupanje, ulazak, upad u tuđi računar ili računarsku mrežu. Bitno je da je ova radnja preduzeta neovlašćeno, dakle protivpravno i drugo kršenjem predviđenih mera zaštite. Ove okolnosti moraju biti obuhvaćene umišljajem učinioca dela.

Prvi teži oblik za koji je propisana novčana kazna ili zatvor do dve godine čini lice koje upotrebi podatak koji je pribavio, do koga je došao neovlašćenim pristupom zaštićenom računaru ili računarskoj mreži. Ova upotreba može biti u bilo kojoj nameri ili za bilo koju svrhu ili cilj. Ako je pak usled preduzete radnje upotrebe na ovaj način pribavljenog računarskog podatka došlo do nastupanja teških posledica za drugog (drugo fizičko ili pravno lice) radi se o najtežem krivičnom delu ove vrste za koje je zakon propisao kaznu zatvora od šest meseci do pet godina. Bitno je da je posledica i to teška (a to je faktičko pitanje za sudsko veće) nastupila za drugog i da između nje i preduzete radnje upada u zaštićeni računarski sistem postoji uzročno-posledična veza.

Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži. Delo ima osnovni i teži oblik.

Objekt napada u ovom slučaju je javna računarska mreža. Osnovno delo čini lice koje neovlašćeno (dakle protivno postojećim propisima, protivzakonito) sprečava ili ometa pristup javnoj računarskoj mreži. Za ovo je delo propisana novčana kazna ili zatvor do

jedne godine. U slučaju da se kao učinilac javi službeno lice u vršenju službe tada se radi o kvalifikovanom obliku ovog dela za koji je propisana kazna zatvora do tri godine. Ovde se zapravo radi o posebnom, specijalnom obliku krivičnog dela zloupotrebe službenog položaja službenog lica koje sprečava ili ometa drugom fizičkom ili pravnom licu nesmetani pristup i korišćenje javne računarske mreže.

I poslednje delo je **Neovlašćeno korišćenje računara ili računarske mreže.** Delo čini lice koje neovlašćeno koristi računarske usluge ili računarsku mrežu u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist. Predviđena je novčana kazna ili zatvor do tri meseca.

8.2. Konvencija o visokotehnološkom kriminalu

Ova konvencija je ratifikovana od strane Narodne skupštine Republike Srbije, I na taj način uveta u domaći pravni poredak. U samom uvodu ove konvencije, data su objašnjenja i razlozi donošenja[43].

Kao osnovni razlog za donošenja ove Konvencije , države potpisnice navode :

Sprovođenje zajedničke kaznene politika u svrhu zaštite društva od kiber kriminala, *inter alia* usvajanjem odgovarajuće legislative i unapređivanjem međunarodne saradnje;

Saradnja između država i privatnih preduzeća u borbi protiv kiber kriminala i potrebu zaštite legitimnih interesa u korišćenju i razvoju informatičke tehnologije, jer efikasna borba protiv kiber kriminala zahteva povećanu, brzu i veoma funkcionalnu međunarodnu saradnju u krivičnim stvarima;

U Konvenciji se navode osnovi donošenja ovog akta, kao što su :

Duboke promene koje je donela digitalizacija, konvergencija i stalni trend ka globalizaciji kompjuterskih mreža;

Rizici da se kompjuterske mreže i elektronske informacije mogu takođe koristiti za izvršenje krivičnih dela i da dokazni materijali koji se odnose na takve prestupe mogu biti uskladišteni u tim mrežama ili prenošeni preko njih;

Dakle, osnovni cilj konvencije je sprečavanje dela usmerenih protiv poverljivosti, integriteta i dostupnosti kompjuterskih sistema, mreža i kompjuterskih podataka, kao i sprečavanja zloupotrebe tih sistema, mreža i podataka na taj način što će se predvideti kaznene mere za takva činjenja kao što je opisano u ovoj konvenciji i što će se usvojiti mere dovoljne za efikasnu borbu protiv takvih krivičnih dela, na taj način što će se na

[43]Izvor: Konvencija o visokotehnološkom kriminalu

unutrašnjem i međunarodnom nivou olakšati otkrivanje, istraga i gonjenje takvih krivičnih dela i što će se obezbediti uslovi za brzu i pouzdanu međunarodnu saradnju;

Konvencija definiše sledeće termine

Izraz "**kompjuterski sistem"** označava svaki uređaj ili grupu međusobno povezanih ili uslovljenih uređaja, od kojih jedan ili više njih, u zavisnosti od programa, vrši automatsku obradu podataka;

Izraz "**kompjuterski podaci**" označava svako izlaganje činjenica, podataka ili koncepata u obliku koji je pogodan za njihovu obradu u kompjuterskom sistemu, uključujući tu i odgovarajući program na osnovu kojeg kompjuterski sistem vrši svoju funkciju;

Izraz "**davalac usluga**" označava:

Svako javno ili privatno lice koje korisnicima pruža svoje usluge na polju komuniciranja putem kompjuterskih sistema, i

Svako drugo lice koje obrađuje ili skladišti kompjuterske podatke za račun takvih komunikacijskih usluga ili za račun korisnika takvog servisa.

Izraz "**promet podataka**" označava sve kompjuterske podatke koji su u vezi sa komuniciranjem putem kompjuterskih sistema, a koje generiše kompjuterski sistem i koji čine deo lanca komuniciranja, u kojima se sadrže podaci o poreklu, odredištu, putanji, vremenu, datumu, veličini, trajanju i vrsti predmetne usluge.

Krivična dela protiv **poverljivosti, integriteta i dostupnosti kompjuterskih podataka i sistema**

8.2.1. Nedozvoljeni pristup

Svaka članica treba da usvoji takve legislativne i ostale neophodne mere da bi se bespravno pristupanje kompjuterskom sistemu kao celini ili nekom njegovom delu, kada se učini namerno, okvalifikovalo u njenom nacionalnom pravu kao krivično delo. Članica može da uslovi da delo mora biti učinjeno kršenjem bezbednosnih mera sa namerom pribavljanja kompjuterskih podataka ili sa nekom drugom nečasnom namerom, ili učinjeno u vezi sa kompjuterskim sistemom koji je povezan sa drugim kompjuterskim sistemom.

8.2.2. Nedozvoljeno presretanje

Svaka članica treba da usvoji takve legislativne i ostale neophodne mere da bi se u njenom nacionalnom pravu kao krivično delo okvalifikovalo bespravno presretanje prenosa kompjuterskih podataka koji nisu javne prirode, ka kompjuterskom sistemu, od njega ili

unutar samog sistema, u šta spada i elektromagnetska emisija iz kompjuterskih sistema kojom se prenose takvi podaci, a kad je učinjeno sa namerom i uz pomoć tehničkih uređaja. Članica može usloviti da delo mora biti učinjeno sa nečasnim namerama, ili učinjeno u vezi sa kompjuterskim sistemom koji je povezan sa drugim kompjuterskim sistemom.

8.2.3. Ometanje podataka

Svaka članica treba da usvoji takve legislativne i ostale neophodne mere da bi se bespravno oštećenje, brisanje, kvarenje, menjanje ili prikrivanje kompjuterskih podataka okvalifikovalo u njenom nacionalnom pravu kao krivično delo, ukoliko se učini sa namerom.

Članica može rezervisati pravo da uslovi da dela iz stava 1 moraju da rezultiraju velikom štetom.

8.2.4. Ometanje sistema

Svaka članica treba da usvoji takve legislativne i ostale neophodne mere da bi se u njenom nacionalnom pravu kao krivično delo okvalifikovalo bespravno i u većem stepenu ometanje funkcionisanja kompjuterskih sistema putem unošenja, prenošenja, oštećenja, brisanja, kvarenja, menjanja ili prikrivanja kompjuterskih podataka, ukoliko je učinjeno sa namerom.

8.2.5. Zloupotreba uređaja

Svaka članica treba da usvoji takve legislativne i ostale neophodne mere da bi se u njenom nacionalnom pravu kao krivično delo, ukoliko je učinjeno sa namerom i bespravno, okvalifikovalo sledeće:

- Proizvodnja, prodaja, nabavljanje radi upotrebe, uvoz, distribucija i drugi vidovi stavljanja na raspolaganje;
- Sredstava, što podrazumeva i kompjuterske programe, projektovane ili preuređenje prvenstveno u svrhu izvršenja nekog od navedenih dela;
- Kompjuterskih lozinki, šifri za pristup, ili sličnih podataka putem kojih se može pristupiti kompjuterskom sistemu kao celini ili nekom njegovom delu sa namerom da bude upotrebljen u svrhu izvršenja nekog od navedenih dela.

8.2.6. Falsifikovanje koje je u vezi sa kompjuterima

Svaka članica treba da usvoji takve legislativne i ostale neophodne mere da bi se u njenom nacionalnom pravu kao krivično delo okvalifikovalo unošenje, menjanje, brisanje ili prikrivanje kompjuterskih podataka koje rezultira u podacima koji nisu autentični, sa

namerom da se učini da oni budu smatrani za autentične i da se sa njima u redovne svrhe postupa kao da su autentični, bez obzira na to da li su ti podaci direktno čitljivi i razumljivi. Članica može usloviti da postoji namera prevare, ili slična nečasna namera, da bi se ustanovila krivična odgovornost.

8.2.7. Prevare koje su u vezi sa kompjuterima

Svaka članica treba da usvoji takve legislativne i ostale neophodne mere da bi se u njenom nacionalnom pravu kao krivično delo okvalifikovalo nanošenje imovinske štete drugim licima kada se to učini bespravno i sa namerom, na sledeće načine:

- Bilo kakvim unošenjem, menjanjem, brisanjem ili prikrivanjem kompjuterskih podataka,
- Bilo kakvim ometanjem funkcionisanja kompjuterskih sistema,
- Sa namerom prevare ili drugom nečasnom namerom da se bespravno pribavi ekonomska dobit za sebe ili za druga lica

Pored krivičnopravnih odredaba materijalnog karaktera koje sadrži Krivični zakonik Republike Srbije, oblast pravne zaštite prava intelektualne svojine, u okviru borbe protiv visokotehnološkog kriminala, regulisana je i **Zakonom o posebnim ovlašćenjima radi zaštite prava intelektualne svojine**.

Ovim zakonom predviđena je odgovornost za privredne prestupe i prekršajna odgovornost pravnih lica za povredu prava intelektualne svojine. U pravcu kontrole proizvodnje, prometa, upotrebe i držanja robe kao i pružanja usluga kojima se povređuje pravo intelektualne svojine, posebna ovlašćenja poverena su pojedinim ministarstvima kroz inspekcijske službe (tržišna i turistička inspekcija pri Ministarstvu trgovine, turizma i usluga, poreski inspektorat i policija pri Ministarstvu finansija i dr.). Međutim, i ovde je učinjen jedan propust koji stvara dosta problema u primeni zakona.

Naime, za jedan od subjekata privrednog poslovanja, samostalne trgovinske radnje, nisu predviđeni oblici odgovornosti. To u praksi znači da se radnje koje predstavljaju kršenje prava intelektualne svojine izvršene u poslovanju ovakvih subjekta privrednog prometa ne mogu brzo i efikasno sankcionisati kroz odgovornost za privredne prestupe, što one u suštini i jesu, već se moraju posmatrati kroz izvršenje krivičnog dela neovlašćenog iskorišćavanja autorskog dela ili predmeta srodnog prava.

Ovo, sa jedne strane, podrazumeva angažovanje celokupnog mehanizma krivičnopravne zaštite koji je glomazan i ne naročito brz i efikasan u smislu ostvarivanja svrhe sankcionisanja zabranjene radnje, dok, sa druge strane, imajući vidu da naše krivično zakonodavstvo tek odskora predviđa odgovornost pravnog lica, nameće individualno sankcionisanje pojedinačne radnje jednog ili više fizičkih lica, čime se znatno otežava sankcionisanje nedozvoljenog ponašanja privrednog subjekta u privrednom i platnom prometu.

Dakle, propisivanjem krivičnih dela koja se odnose na kompjuterski kriminalitet učinjen je prvi korak u suzbijanju ovih nedozvoljenih oblika ponašanja, međutim to nije dovoljno i da bi borba protiv visokotehnološkog kriminaliteta dala određene rezultate potrebno je izvršiti I korenite promene u organizaciji i nadležnosti pravosudnih organa. To je učinjeno donošenjem Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala jula meseca 2005. godine.

9. ORGANIZACIJA I NADLEŽNOST DRŽAVNIH ORAGANA U BORBI PROTIV KOMPJUTERSKOG KRIMINALA

Bezbednost informaciono-komunikacionih mreža je jedan od osnovnih preduslova za elektronsko poslovanje, a posebno za elektronsko plaćanje. Zaštita informacija je neophodna komponenta elektronskog poslovanja koja na željeni nivo redukuje opasnosti vezane za laku dostupnost i brzu razmenljivost ogromnih količina informacija.

Brojne i raznovrsne potencijalne pretnje - opasnosti koje ugrožavaju informacione sisteme, a posebno one koji imaju karakter kriminalnih radnji, nedvosmisleno nameću potrebu izgradnje zaštite informacionih sistema. Jedan od segmenata zaštite od prevara i kriminalnih dela je i zakonska regulativa.

U Republici Srbiji je u Krivičnom zakoniku u glavi dvadeset i sedam taksativno su nabrojana krivična dela protiv bezbednosti računarskih podataka, koja smo obradili u prethodnom poglavlju ovog rada, i koja uz ostala krivična dela vezana za visoko tehnološki kriminal svakako doprinose sprečavanju vršenja krivičnih dela iz ove oblasti.

U cilju sprovođenja Krivičnog zakonika vezano za oblast iz glave dvadeset i sedam s obzirom na specifičnost ovih krivičnih dela donet je Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala jula meseca 2005. godine[44].

9.1. Posebno tužilaštvo

Kako je članom 4. Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala predviđeno za krivična dela protiv bezbednosti računarskih podataka i krivičnih dela protiv intelektualne svojine, imovine i pravnog saobraćaja kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarske mreže i računarski podaci, za postupanje u predmetima navedenih krivičnih dela nadležno je Okružno javno tužilaštvo u Beogradu za teritoriju Republike Srbije. Obrazuje se posebno odeljenje za borbu protiv visokotehnološkog kriminala.

[44] *Izvor Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala*

Radom Posebnog tužilaštva rukovodi posebni tužilac za visokotehnološki kriminal, koga postavlja Republički javni tužilac iz redova javnih tužilaca i zamenika javnih tužilaca. Prednost imaju javni tužioci odnosno zamenici javnih tužilaca koji poseduju posebna znanja iz oblasti informatičkih tehnologija. Mandat posebnog tužioca je četiri godine i može biti ponovo postavljen. Posebni tužilac ima prava i dužnosti kao javni tužilac.

Kada dođe do saznanja da se u jednom krivičnom predmetu radi o slučajevima predviđenim za nadležnost Posebnog tužioca, isti se pismeno obraća Republičkom javnom tužiocu zahtevajući od njega da mu poveri ili prenese u nadležnost taj predmet.

Republički javni tužilac, na predlog Posebnog tužioca, donosi poseban akt o unutrašnjoj organizaciji i sistematizaciji radnih mesta u posebnom tužilaštvu uz saglasnost ministra za poslove pravosuđa.

9.2. Služba za borbu protiv visokotehnološkog kriminala

Članom 9 istog zakona je predviđeno da se obrazuje posebna služba za borbu protiv visokotehnološkog kriminala u okviru Ministarstva unutrašnjih poslova. Ministar unutrašnjih poslova po pribavljenom mišljenju Posebnog tužioca postavlja i razrešava starešinu Službe i bliže uređuje njen rad u skladu sa zakonom. Služba postupa po zahtevima Posebnog tužioca u skladu sa zakonom.

9.3. Nadležnost i organizacija sudova

Za postupanje u predmetima krivičnih dela iz oblasti visokotehnološkog kriminala za teritoriju Republike Srbije je nadležan Okružni sud u Beogradu. Za odlučivanje u drugom stepenu nadležan je neposredno viši sud .

U okružnom sudu u Beogradu se obrazuje Veće za borbu protiv visokotehnološkog kriminala. Sudije u to veće raspoređuje predsednik Okružnog suda iz reda sudija tog suda uz njihovu saglasnost. Prednost imaju sudije koje poseduju posebna znanja iz oblasti informacionih tehnologija

Sudije se raspoređuju u Veće najduže na dve godine a može im biti produžen mandat odlukom predsednika Okružnog suda u Beogradu.

9.4. Dosadašnja primena ovih zakona

Zakon je donet 2005. godine. Posebno tužilaštvo je formirano aprila 2007. godine Za krivična dela protiv bezbednosti računarskih podataka podignute su do sada optužnice

protiv 8 lica. Za krivična dela protiv intelektualne svojine u 2007. godini podignuta je optužnica protiv 95 lica .

U toku 2008 godine Posebnom tužilaštvu za borbu protiv visoko tehnološkog kriminala podnete su krivične prijave protiv 166 lica, što predstavlja značajan porast u odnosu na prethodnu godinu. Zahtev za sprovođenje istrage stavljen je protiv 147 lica. Protiv 75 lica podignute su optužnice.

U toku 2008 godine, policijski službenici Odeljenja za borbu protiv visokotehnološkog kriminala, SBPOK – a MUP-a Republike Srbije, od izvršilaca ovih krivičnih dela oduzeli su ukupno 53 računara i 48.400 kom. optičkih diskova, sa hiljadama neovlašćeno umnoženih autorskih dela u vidu filmova, muzika, softvera, računarskih igrica i drugih mulitimedijalnih sadržaja.

U toku 2008 godine, na teritoriji Republike Srbije izvršeno je ukupno 1.313 krivičnih dela visokotehnološkog kriminala. U prethodnoj godini taj broj je uznosio 1.095[45].

Od osnivanja Posebnog tužilaštva za borbu protiv viskotehnološkog kriminala 55 lica je optuženo, 43 lica je pravosnažno osuđeno, a protiv 42 lica postupak je još uvek u toku. Pozitivnopravnim propisima RS, iz stvarne nadležnosti Posebnog tužilaštva izostavljan su krivična dela koja se odnose na zloupotrebu platnih kartica i internet pornografiju.

[45]izvor http://www.tuzilastvovtk.sr.gov.yu/index.php/index.html

10. PROBLEM KOMPJUTERSKOG KRIMINALITETA IZ UGLA PROCESNOG ZAKONODAVSTVA

Na terenu procesnih odredaba koje su u direktnoj vezi sa otkrivanjem krivičnih dela visokotehnološkog kriminala možemo konstatovati da važeći Zakonik o krivičnom postupku ne predviđa posebne dokazne radnje niti posebna ovlašćenja vezana za otkrivanje ovih krivičnih dela. U postupku otkrivanja krivičnih dela visokotehnološkog kriminala i prikupljanja i izvođenja dokaza, koriste se opšte odredbe Zakonika o krivičnom postupku koje se odnose i na sva druga krivična dela.

Zakonik o krivičnom postupku je osnovni izvor procesnog zakonodavstva, koji utvrđuje pravila sa ciljem da niko nevin ne bude osuđen, a da se učiniocu krivičnog dela izrekne krivična sankcija pod uslovima koje predviđa krivični zakon i na osnovu zakonito sprovedenog postupka.

Dakle, za sva krivična dela pa i za krivična dela kompjuterskog kriminala, potrebno je da prvenstveno delo bude predviđeno kao krivično delo, što je i učinjeno u Krivičnom Zakoniku, a nakon toga potrebno je da u zakonom propisanom postupku prikupiti neophodne dokaze, a zatim utvrditi da li je optuženi učinio krivično delo i da li je krivično odgovoran.

Postupak otkrivanja učinioca krivičnih dela započinje u pretkrivičnom postupku uz saradnju nadležnog javnog tužioca i organa unutrašnjih poslova. Nakon toga pokretaće se krivični postupak. Dakle, potrebno je otkriti da je izvršeno krivično delo, zatim otkriti učinioca krivičnog dela, zatim sprovesti postupak prikupljanja dokaza (istraga) i na kraju sprovesti dokazni postupak u kome će se izvesti svi predloženi i prikupljeni dokazi i utvrditi činjenično stanje.

Prema našem Zakoniku o krivičnom postupku, krivični postupak obuhvata stadijum prethodnog postupka koji obuhvata istragu i stavljanje okrivljenog pod optužbu i stadijum glavnog postupka koji obuhvata pripremanje glavnog pretresa, glavni pretres, donošenje i objavljivanje presude i postupak pravnih lekova. Ovako organizovanom formalnom postupku prethodi tzv. pretkrivični postupak, koji nije sudski postupak i koji ima za cilj otkrivanje i prijavljivanje krivičnih dela. U ovom radu mi ćemo pre svega ukazati na probleme koji se javljaju u vezi sa prikupljanjem i korišćenjem dokaza u sudskom postupku.

Dakle, pre svega treba obraditi fazu istrage i fazu glavnog pretresa.

Istraga je prva faza prethodnog postupka koju rešenjem otvara istražni sudija ili veće, na *zahtev* ovlašćenog tužioca, protiv određenog lica, kad postoji osnovana sumnja da je to lice učinilo krivično delo. Istragu sprovodi istražni sudija.

Istraga se otvara koordiniranom aktivnošću dva procesna subjekta: ovlašćenog tužioca, koji podnosi zahtev za sprovođenje istrage istražnom sudiji nadležnog suda. U sadržini zahteva za sprovođenje istrage se mora naznačiti: lice protiv koga se zahteva

istraga, opis dela (zakonska obeležja) zakonski naziv krivičnog dela (kvalifikacija), okolnosti iz kojih proizlazi osnovanost sumnje za označeno lice i dokazi koji potvrđuju činjenice. Uz zahtev se dostavljaju i krivična prijava, spisi i zapisnici o formalnim i neformalnim radnjama. Ako se složi sa zahtevom ovlašćenog tužioca doneće rešenje o sprovođenju istrage.

Svrha istrage je u prikupljanju dokaza i podataka koji su potrebni za odluku o podizanju optužnice ili obustavi postupka, kao i za prikupljanja dokaza za koje postoji opasnost da se neće moći ponoviti na glavnom pretresu, i onih čije se izvođenje smatra celishodnim.

Od radnji i ovlašćenja relevantnih za visokotehnološki kriminal, ukazujemo na sledeće:[46] članom 77. ZKP propisana je radnja dokazivanja koja se sastoji u pretresanju stana (relevantna za obezbeđenje dokaza koji se nalaze u stanu počinioca, članom 82. ZKP regulisano je privremeno oduzimanje predmeta (npr. pečaćenje kućišta računara, rad sa kopijama, itd), član 85. ZKP predviđa mogućnost kontrole pisama i pošiljki osumnjičenog (npr. elektronska pošta), dokazna radnja veštačenja uređena je članom 114. ZKP (veštaci informatičke struke), članom 220. ZKP predviđena je obaveza svih državnih organa da sudovima i drugim organima koji učestvuju u krivičnom postupku pruže potrebnu pomoć, naročito ako se radi o otkrivanju krivičnih dela i pronalaženju učinilaca, član 232. ZKP propisuje uslove pod kojima je moguće preduzeti radnje snimanja razgovora i lica (restriktivna odredba, samo u taksativno navedenim slučajevima), a član 234. ZKP predviđa uslove za izdavanje naredbe za dostavljanje podataka o stanju na poslovnim ili ličnim računima osumnjičenog lica.

Zakonik navodi da su radnje dokazivanja procesne radnje suda, koje sud preduzima_ da bi formirao svoje ubeđenje o postojanju ili nepostojanju činjenica koje su bitne za njegovu odluku.

Činjenice koje su predmet dokazivanja utvrđuju se u krivičnom postupku korišćenjem određenih dokaznih sredstava:

1. Saslušanje okrivljenog
2. Saslušanje svedoka
3. Uviđaj i rekonstrukcija
4. Veštačenje

Zbog specifičnosti krivičnih dela kompjuterskog kriminala od najvećeg značaja za dokazni postupak je dokaz koji se izvodi veštačenjem. Iskaz veštaka je izjava koja sadrži stručni nalaz ili stručno mišljenje procesno nezainteresovanog lica o činjenicama za čije utvrđivanje pravna sprema i opšte obrazovanje sudije nije dovoljno

[46] *Izvor: Zakonik o krivičnom postupku*

Lica koja po naredbi suda daju iskaz na osnovu stručnog znanja, nazivaju se veštaci. Od veštaka se mogu tražiti stručni nalaz (utvrđivanje činjenica) ili mišljenje (stručni sud o utvrđenim činjenicama) ili i nalaz i mišljenje.

Izvođenje veštačenja se sastoji od pripremanja veštačenja, samog veštačenja i davanja iskaza. Dakle, kada se u krivičnom postupku pojavi neko od krivičnih dela kompjuterskog kriminala, učešće IT veštaka je obavezno. Naročito, imajući u vidu činjenicu da se kod ovih krivičnih dela izvođenje dokaza vrše posredno, što predstavlja odstupanje, odnosno izuzetak od osnovnog načela neposrednosti po kome se radnje potrebne za formiranje sudske odluke moraju izvesti pred sudijom koji će odluku doneti. Ovo načelo uspostavlja vezu između radnji dokazivanja i radnji odlučivanja

Na primer Krivični Zakonik RS kao jedno od krivičnih dela u ovoj oblasti predviđa **Pravljenje i unošenje računarskih virusa**. Delo ima osnovni i teži oblik. Osnovno delo čini lice koje napravi računarski virus u nameri da ga unese u tuđi računar ili računarsku mrežu. Radnja izvršenja je samo sačinjavanje, pravljenje virusa.

Šta su to virusi, kako se prave, koje su njihove vrste ili karakteristike, svrha i sadržina predstavljaju pitanja koje sudsko veće mora da reši u svakom konkretnom slučaju kao faktičko pitanje. U tome im stručnu pomoć moraju da pruže lica sa posebnim znanjima i veštinama - veštaci informatičke struke.

Dakle, Zakonik o krivičnom postupku predstavlja osnovni zakon po kome se utvrđuje činjenično stanje i izvode dokazi za sva krivična dela iz materijalnog zakonika, pri tome potpuno zanemaruje sve posebnosti i specifičnosti pojedinih krivičnih dela, predviđajući istu proceduru i ista osnovna načela i principe.

Kao jedna od najvažnijih oblasti koja se bavi kompjuterskom kriminalom sa procesnog aspekta je digitalna forenzička nauka koja obezbeđuje primenu naučno deriviranih i dokazanih metoda za: *čuvanje, sakupljanje, validaciju, identifikaciju, analizu, interpretaciju, dokumentovanje i prezentaciju* digitalnih dokaza iz različitih izvora digitalnih podataka sa ciljem rekonstrukcije događaja krivičnog dela kompjuterskog kriminala ili zloupotrebe računara[47].

Ne ulazeći u pitanje samog postupka digitalne forenzičke istrage, u ovom radu ukazaćemo pre svega na značaj digitalnog dokaza i mogućnost njegove primene u postupku dokazivanja.

[47]Izvor M. Milosavljević, G. Grubor „ Digitalna forenzička istraga kompjuterskog kriminala“, Univerzitet Singidunum, 2009

10.1. Digitalni dokaz

Prema definiciji IOCE u oblasti digitalne forenzičke nauke, *digitalni dokaz* je svaka informacija u digitalnom obliku koja ima dokazujuću vrednost, a koja je ili uskladištena ili prenesena u takvom obliku. Pojam digitalnog dokaza uključuje kompjuterski uskladištene i kompjuterski generisane dokazne informacije, digitalizovane audio i video dokazne signale, signale sa digitalnog mobilnog telefona, informacije sa digitalnih faks mašina i signale drugih digitalnih uređaja.

Znači, digitalni dokaz je bilo koja informacija generisana, obrađivana, uskladištena, ili prenesena u digitalnom obliku na koju se sud može osloniti kao validnu, tj. svaka binarna informacija, sastavljena od digitalnih 1 i 0, uskladištena ili prenesena u digitalnoj formi, kao i druge moguće kopije originalne digitalne informacije koje imaju dokazujuću vrednost i na koje se sud može osloniti, u kontekstu forenzičke akvizicije, analize i prezentacije dokaza pred sudom.

Digitalni kompjuterski dokaz formira se iz gomile *posrednih* stvarnih dokaza, od kojih se ni jedan ne sme isključiti iz bilo kog razloga. Dokazi moraju biti potpuni, da se međusobno dopunjuju (prepliću) i da nemaju tzv. pukotina za donošenje zaključaka, odnosno za utvrđivanje *čvrstog digitalnog dokaza*[48].

Dakle, najčešće u pretkrivičnom postupku ili eventualno u stadijumu istrage , nadležni državni organi specijalizovani za oblast kompjuterskog kriminala pokreću proces prikupljanja podataka koji će kasnije poslužiti kao dokaz u sudskom postupku.

O postupku prikupljanja dokaza, prof. Gojko Grubor navodi »treba sakupljati sve posredne dokaze sa lica mesta, ne samo što digitalni forenzičar misli da treba, nego i sve ono što može potencijalno indicirati šta se stvarno dogodilo. U procesu akvizicije digitalnih dokaza, treba generalno snimiti listu fajlova i logova kao dokaze, čak i bez ikakve ideje šta se stvarno dogodilo. Treba imati u dokaznom materijalu svaki fajl koji potencijalno može sadržavati dokaz, pre nego što se fajl prepiše, ili izmeni. Nakon inicijalne pretrage (bez privremenog oduzimanja računara), treba se okrenuti prvobitnoj hipotezi i dograditi je detaljnije sa prikupljenim dokazima.

Velika je verovatnoća da je propušten neki važan dokaz, što je dobar argument da se računar privremeno oduzme, dok traje istraga, što nije uvek lako. Svaki posredni dokaz, koji zajedno čine dokazni materijal, treba tretirati kao da direktno vodi ka nepobitnom dokazivanju izvršenog krivičnog dela i kao da su svi jednako važni i kritični za konkretni slučaj. Tek tada počinje proces izgradnje dokaza bez tzv. pukotina, odnosno, izgradnja neoborivog dokaza. Potrebno je, dakle, mnogo posrednog dokaznog materijala za jedan mali čvrsti dokaz.«

[48] Izvor M. Milosavljević, G. Grubor „ Digitalna forenzička istraga kompjuterskog kriminala“, Univerzitet Singidunum, 2009

Nakon prikupljanja dokaznog materjala, otvaranja sudskog postupka, ponovo dolazimo na problem izvođenja dokaza. Naime, sudije nisu edukovani da bi u potpunosti razumeli problematiku kompjuterskog kriminala, oni pre svega kao neophodnu pomoć u postupku angažuju veštake, u ovom slučaju IT veštake, koji će na osnovu prikupljenog dokaznog materjala, dati svoj nalaz i mišljenje. Međutim, tu se postupak ne završava, jer poslednju reč, naravno , imaju sudije da li će neku od činjenica uzeti kao dokazanu ili ne zavisi samo od slobodnog sudijskog uverenja. Kako će oceniti dokaz koji je izveden veštačenjem, takođe, zavisi samo od slobodnog sudijskog uverenja.

O značaju digitalnog dokaza za sudski postupak , prof. G. Grubor navodi i sledeće »Očekuje se da forenzička analiza digitalnih dokaza otkrije najviše potrebnih podataka za izgradnju čvrstog, neoborivog digitalnog dokaza, jer postoji velika razlika između kompjuterskog digitalnog dokaza u računaru (*computer evidence*) i čvrstih, neoborivih dokaza (*proof*) prihvatljivih na sudu. Neoborivi, čvrsti dokaz nepobitno uspostavlja činjenice, ali je to i subjektivna interpretacija kompjuterskog digitalnog dokaza koji izvodi forenzičar. Kompjuterski digitalni dokaz u računaru je objektivan digitalni podatak i može se koristiti u meri u kojoj se može dokazati da nije izmenjen.

Pri akviziciji kompjuterskih digitalnih dokaza treba uvek verovati u indikacije koje pokazuje istraga, sve dok se ne sastave svi delići posrednih digitalnih dokaza u čvrsti dokaz bez tzv. pukotina. Treba tražiti nekonzistentnosti, ali prihvatiti i ono što se vidi, bez racionalizacije. Ako se u toku forenzičke akvizicije digitalnih dokaza dobiju konfliktni podaci, treba se vratiti korak unazad i pokušati otkriti šta se stvarno vidi. Možda konflikt uopšte i ne postoji. Ukoliko konflikt postoji, ne pokušavati njegovo rešavanje racionalizacijom.

Ni u kom slučaju ne menjati ništa u ispitivanim računarima, sa kojih se u procesu akvizicije digitalnih dokaza sakupljaju digitalni podaci i ne objavljivati nalaze forenzičke analize digitalnih dokaza u toku istrage. Treba uvek računati da će slučaj ići na sud, a napadač bi u međuvremenu mogao izmeniti svoj računar i izbrisati sve podatke i eventualne tragove napada, koji mogu biti potencijalni digitalni dokazi.“

Dakle, postojeći zakonik ne daje nikakvu definiciju dokaza, a samim tim ni definiciju digitalnog dokaza koji se pojavljuju u vezi sa izvršenjem krivičnih dela visokotehnološkog kriminala. Međutim, digitalni dokazi imaju istu vrednost kao i svi drugi materijalni dokazi i za njih važe potpuno ista procesna pravila kao i za sve ostale dokaze.

Zbog svega navedenog, potrebno je najpre izvršiti promene, kako u materijalnom, tako i u procesnom zakonodavstvu, i naravno obučiti sudije tako da mogu da bez problema i teškoća učestvuju kako u postupku prikupljanja dokaza, tako i u postupku izvođenja i ocene dokaza.

10.2. Međunarodni aspekt digitalnog dokaza

Razlike između pravnih sistema zemalja članica UN-a nametnule su problem usklađivanja pravne regulative kao prioritet međunarodne zajednice. Problematika prepoznavanja određenog ponašanja kao ilegalnog u jednoj zemlji i tretiranje istog tipa ponašanja kao legalnog u nekoj drugoj, pruža veliki prostor za izbegavanje krivične odgovornosti.

Drugi problem koji se javlja je problem nadležnosti. Kod ove vrste problema, kao i u prvom slučaju, problem nastaje korišćenjem tehnologije koja omogućava rad sa udaljenih lokacija, odnosno upotrebu resursa u jednoj zemlji za obavljanje aktivnosti u drugoj dok se operativni rad obavlja u nekoj trećoj zemlji. Ovakvo delovanje nemoguće je u svetu klasičnog kriminala. Upravo iz razloga koordinacije i efikasne borbe protiv kriminala neophodno je međusobno razumevanje i uvažavanje kako organa gonjenja tako i pravosuđa. Pre svega neophodno je što više približiti zakonsku regulativu, a potom uskladiti i procese prikupljanja i analiziranja digitalnih dokaza.

Organizacije

U međunarodnoj borbi protiv kompjuterskog kriminala, kao i u definisanju i predviđanju potencijalnih opasnosti, najznačajnije u manjoj ili većoj meri su:

- ✓ Ujedinjene Nacije
- ✓ Organizacija za Međunarodnu Saradnju i Razvoj (OECD)
- ✓ Savet Evrope
- ✓ Evropska Unija
- ✓ G-8

Savet Evrope

Savet Evrope je internacionalna organizacija sa sedištem u Strazburu. Osnovana je 1949. godine od strane deset zemalja zapadne Evrope. Danas je to pan-Evropska organizacija koja obuhvata i Rusiju i Tursku.

Glavna uloga Saveta Evrope je jačanje demokratije, ljudskih prava i vladavine prava u okviru država članica. U sferi krivičnog prava održano je preko dvadeset konvencija i usvojeno je više od osamdeset preporuka. 1989. godine Komitet Ministara, sastavljen od ministara inostranih poslova država članica, usvojio je preporuku o zaštiti podataka .

Ova preporuka poziva države članice da razmotre uvođenje nekih propisa u vezi kompjuterskog kriminala. Tek 1995. godine Savet Evrope donosi Preporuku 95 kojom predstavlja procedure za implementaciju prethodne preporuke. Preporuka 95 predstavlja prvi momenat definisanja procedura pretrage i zaplene, nadgledanja, elektronskih dokaza, šifrovanja i internacionalne kooperacije .

U februaru 1997. godine, formira se Komitet Eksperata o Kriminalu u Cyberprostoru (PC-CY). Zadatak ovog komiteta je bio ispitivanje kompjuterskog kriminala i vezane problematike u krivično procesnom pravu. Krajnji cilj rada ovog komiteta je bio definisanje prestupa, nadležnosti, pretrage i zaplene, zaštite podataka i odgovornosti Internet provajdera. Kao rezultat tog rada nastala je 31. novembra 2001. godine u Budimpešti Konvencija o Kompjuterskom Kriminalu. Ova konvencija predstavlja prekretnicu u borbi protiv kompjuterskog kriminala ali i jasnu smernicu svim zemljama kako pravosuđe treba tretirati prestupe u ovoj sferi.

Definišući mere koje treba preduzeti na nacionalnom nivou, Savet Evrope dao je spisak potpunih definicija zločina protiv privatnosti, integriteta i dostupnosti kompjuterskih podataka i sistema, potpune definicije od ilegalnog pristupa sistemima i podacima do dečije pornografije.

Na ovaj način omogućeno je svakoj zemlji da prepozna vrstu zločina i kao takvu je uvrsti ili definiše u svom pravosudnom sistemu. Savet Evrope nije dao smernice za sankcionisanje ovih zločina, on je samo omogućio da počinioce mogu biti kažnjeni „efektivnim, proporcionalnim i oštrim sankcijama koje uključuju lišavanje lica slobode" u slučaju kada je počinilac pravno lice. Predviđena je i mera novčane kazne.

Savet Evrope nije išao dalje u definisanju već je ostavio svakoj svojoj članici da svoju pravnu regulativu uredi na način na koji ona smatra odgovarajućim. Takav pristup dovodi do razlika koje su prihvatljivije u smislu različitosti sredina i sistema državnog uređenja.

Evropska Unija

Evropska Unija (EU), formirana je 50-tih godina dvadesetog veka. Danas su skoro sve zemlje Evropskog kontinenta njene članice. Uz sopstvenu monetu, zastavu i himnu, EU ima i sopstvene zakone, kao i direktive kojima uređuje slabo definisane i nedefinisane aspekte u sferi kompjuterskog kriminala.

Januara 1995. godine usvojena je direktiva kojom se uspostavljaju kriterijumi za zaštitu građana EU a u vezi sa elektronski obrađenim podacima. Ova direktiva je ustanovila pravo svakog građana da zna koji se podaci čuvaju i obezbedila zaštitu transfera privatnih podataka u zemlje koje nisu članice EU ukoliko te zemlje ne poseduju adekvatne mehanizme čuvanja privatnosti podataka .

Decembra 1997. godine usvaja se direktiva kojom je osigurana privatnost telekomunikacija . Ovom direktivom se od telekomunikacionih kompanija zahteva da obrišu sve podatke o obavljenom saobraćaju odmah nakon kraja transmisije (odnosno transfera podataka), osim za potrebe naplate organa unutrašnjih poslova ili državne bezbednosti.

Da bi se osigurala informatička povezanost među svim državama EU kao i njenim građanima, a pogotovu da bi svi građani koristili pogodnosti informacionih tehnologija i Interneta, decembra 1999. godine EU usvaja eEurope inicijativu. Ključni momenti ove inicijative se odnose na povezivanje mladih sa novim tehnologijama, jeftiniji Internet pristup, pokretanje elektronskog poslovanja i brži pristup studentima i đacima. Ipak, kada je odobren akcioni plan eEurope inicijative akcenat je stavljen na značaj sigurnosti kompjuterskih mreža i borbe protiv kompjuterskog kriminala.

U dokumentu koji je usvojen 26. januara 2001. godine pod nazivom „Kreiranje sigurnijeg informatičkog društva“, naglašava se značaj akcije u smislu prevencije kriminalnih aktivnosti zajedno sa jačanjem informatičke infrastrukture. Na taj način se osiguravaju odgovarajuća sredstva za delovanje organa gonjenja članica EU.

U osnovi ovog dokumenta zapravo leži potreba da se obezbede adekvatne kazne za dečiju pornografiju na Internetu, a u dugoročnom smislu i celokupna pravna regulativa vezana za visoko tehnološki kriminal. Zajedno sa propisima, namera ove Komisije bila je u promovisanju potrebe kreiranja specijalizovanih odreda ministarstava unutrašnjih poslova za kompjuterski kriminal, i to na nacionalnom nivou država članica.

Naredne godine donet je i pravni okvir u smislu napada na informacione sisteme . Njime su definisani tipove napada na informacione sisteme :

- nedozvoljeni pristup (hakovanje)
- sprečavanje rada informacionih sistema (DoS)
- izvršavanje malicioznih programa (virusi, trojanci...)
- presretanje komunikacija (*sniffing*)
- zlonamerno pogrešno predstavljanje (*spoofing*).

U daljem tekstu detaljno su definisani termini vezani za kompjutere kao i kompjuterski kriminal. Takođe utvrđuju se i vrste napada pomoću nedozvoljenog pristupa informacionom sistemu kao i mnogi drugi detalji neophodni za formiranje pravnog okvira koji će tretirati ovakve prestupe.

Ova odluka predstavlja zatvaranje procesa definisanja prestupa kao i procedura koje će se suprotstaviti kompjuterskom kriminalu. Napori Evropske Unije da približi visoko tehnološki kriminal članicama sa nedovoljno razvijenom IT strukturom, kao i budućim članicama, traju od momenta donošenja ove Odluke do danas.

Organizacija G-8

Najveći doprinos borbi protiv kompjuterskog kriminala dala je grupa osam najrazvijenijih zemalja (G-8) formiranjem takozvane Lionske grupe. Ova grupa formirana je nakon samita 1995. godine u Halifaksu . Sastavljena je od grupe eksperata kojima je dat zadatak da pregledaju i sastave sporazume i mehanizme za borbu protiv globalnog organizovanog kriminala. Već 1996. godine u Lionu, ova grupa je predstavila četrdeset preporuka za borbu protiv organizovanog kriminala. Ove preporuke su podržane od strane

Nakon samita u Lionu formirane su specifične podgrupe koje će se kasnije baviti specifičnim problemima vezanim za organizovani kriminal (visokotehnološki kriminal, trgovina ljudima, deljenje dokaza u krivičnim procesima, imigracijske prevare i terorizam).

Ovih pet podgrupa imaju za cilj implementaciju preporuka usvojenih 1996. Podgrupa za visokotehnološki kriminal imala je cilj da poveća mogućnosti zemalja članica da spreče, istraže i procesiraju zločine u vezi sa kompjuterima, mrežama i drugim novim tehnologijama. Zemlje su u ovoj grupi zastupljene multidisciplinarnim delegacijama sačinjenim od istražitelja i tužilaca, pravnih eksperata i kompjuterskih forenzičara. Već 1997. godine usvojeno je deset principa za borbu protiv kompjuterskog kriminala, kao i deset stavki akcionog plana .

Ključi momenti u radu ove grupe su: kreiranje globalnog (trenutno 40 članova) direktorijuma za kritične informacije (direktorijum je dostupan samo vladinim institucijama zemalja članica), razni dokumenti o najboljoj praksi (uputstva za sigurnost kompjuterskih mreža, internacionalni zahtevi za podršku, globalno praćenje komunikacija i dr.) i održavanje konferencija za obuku nacionalnih službi bezbednosti, a u vezi sa kompjuterskim kriminalom.

Treba napomenuti da je ova grupa odgovorna za preispitivanje mnogih pravnih sistema u cilju lakšeg suočavanja sa visokotehnološkim kriminalom, kao i za kreiranje principa transnacionalnih pretraga i zaplena (usvojen u Moskvi 1999. godine). Postojanje ovih principa, kao i brojnih dokumenata koji opisuju najbolju praksu, značajno olakšava operacije sprečavanja i borbe protiv globalnog kompjuterskog kriminala.

10.2.1. Priznavanje dokazne snage po nacionalnim pravima

Iako pravna regulativa u mnogim zemljama već pokriva osnovne prestupe poput prevare, nedozvoljenog pristupa i zloupotrebe, regulisanje velikog broja zločina iz sfere kompjuterskog kriminala sigurno će trajati godinama.

Mnoge zemlje širom sveta se trude da, pre svega, svojim građanima omoguće Internet pristup, druge malo razvijenije, se trude da isti pristup učine kvalitetnijim. Ovaj, kao i mnogi drugi faktori utiču na sporije donošenje zakona u odnosu na razvoj tehnologije.

Moguće je da će tek poneki globalni incident naterati vlasti da se ozbiljnije uhvate u koštac sa kompjuterskim kriminalom, kao što je to bio slučaj sa virusom „ILOVEYOU" .Kako je razvoj informacionih tehnologija i elektronskog poslovanja jedan od značajnih pokretača socijalnih i ekonomskih promena, pogotovu u društvima u tranziciji poput našeg, neophodno je pravno regulisati najznačajnije oblasti kompjuterski kriminal i zaštitu informacionih sistema. Nedostatak adekvatnih propisa značajno će umanjiti ili čak u potpunosti sprečiti razvoj ovih oblasti. Pravni okvir je ključan faktor kako za privlačenje novih investicija tako i za održavanje već postojećeg poslovnog okruženja.

Razlozi za to su višestruki :

- neophodno je sigurno okruženje i zaštita podataka za bilo kakvu aktivnost koja podrazumeva procesiranja podataka
- Internet tehnologije kao i elektronsko poslovanje zahtevaju sigurnost podataka i kompjuterskih mreža
- velike kompanije neće dozvoliti da se osetljivim podacima barata u zemljama koje nemaju adekvatnu pravnu regulativu u smislu zaštite od špijunaže, kompjuterskog kriminala, napada na infrastrukturu ili zloupotrebu telekomunikacija
- neophodni su i zakoni o privatnosti podataka.

Priznavanje dokazne snage po nacionalnom pravu SAD

Digitalni, kao i svi drugi dokazi, moraju biti prihvatljivi na sudu da bi se pomoću njih procesuirao slučaj. Bez dovoljne količine validnog dokaznog materijala tužilac će imati slab ili nikakav slučaj. Da bi se izbeglo odbacivanje dokaza neophodno je dokazati da su svi nalozi za pretragu i zaplenu bili legitimni. U SAD je neophodno dokazati osnov po kome su nalozi izdati kao i autentičnost samog dokaznog materijala.

Osnovana sumnja i nalog za pretres

Kao prvi realni problem u svim kriminalističkim istragama i krivičnim procesima javlja se legalnost u vršenju inicijalne pretrage i zaplene dokaznog materijala od strane nadležnih organa.

U nacionalnom pravu SAD-a ovim pitanjem se bavi Četvrti Amandman Ustava SAD odnosno njegove interpretacije u krivičnom zakonu. Četvrti Amandman ograničava mogućnosti istražiteljima u smislu pretrage i pronalaženja dokaza. Sudovi u SAD, nezavisno od toga da li je dokaz u elektronskom ili bilo kakvom drugom obliku, vode računa o razumnom očekivanju privatnosti.

Ovim se onemogućava pretraga po dokumentima i datotekama na ličnom kompjuteru neke osobe bez osnovane sumnje. Kada se dokaže da nije bilo osnovane sumnje a pretraga i zaplena su izvršene, sud će odbaciti sav dokazni materijal prikupljen tom prilikom.

Da bi dokazni materijal koji se prikuplja bio validan, neophodno je pre pretrage dokazati osnovanu sumnju i tim povodom pribaviti validni nalog za pretragu. U slučaju kompjutera kao i svih drugih uređaja u kojima se skladište informacije i podaci termin pretraga odnosi se zapravo na analizu sadržaja nekog medija.

Kako sudovi širom SAD imaju različite stavove povodom analize sadržaja nekog medija, tako se razlikuju i nalozi za pretragu koje oni izdaju. Čest je slučaj da se od tužioca traži eksplicitno formulisanje vrsta datoteka koje će biti pregledane i analizirane (npr. Word

dokumenti i Excel tabele), dok drugi sudovi dozvoljavaju pretragu i analizu kompletnog sadržaja medija.

Problematika naloga za pretragu zapravo je bazirana na neverovatno velikoj količini informacija koje može sadržati jedan medij. Potencijalni stepen kolizije odnosno zabune oko pravila očekivane privatnosti je vrlo veliki kada se u priču ubace kompjuteri. Ponekad nalog za pretragu nije ni potreban, ne zbog nekog izuzetka definisanog zakonom, već zbog odsustva legitimnog očekivanja privatnosti od strane osumnjičenog.

Na primer, ukoliko osumnjičeni koristi kompjuter koji je (otvoreno) dostupan i nije zaštićen lozinkom, ili na radnom mestu gde je poznato da administrator mreže može pristupiti svakom kompjuteru, on zapravo odbacuje sva prava garantovana Četvrtim Amandmanom zbog tako javne upotrebe kompjutera.

Druga pitanja se bave pronalaženjem dokaza od strane trećeg lica. U slučaju kvara na kompjuteru osoba ga odnosi u servis. Serviser radeći na kompjuteru nailazi na inkriminišuće dokaze odnosno informacije i prijavljuje ih nadležnim organima. U principu, ove informacije bi se tretirale kao validne, ali su sudovi u nekoliko slučaja već presudili u korist tuženog vodeći se idejom da osoba koja je odnela kompjuter u servis nije zapravo napustila princip očekivane privatnosti već je pristup informacijama dozvolila samo serviserima u toj kompaniji (SAD vs. Barth, Teksas, 1998).

Iako je neophodno štititi privatnost građana, kao što Četvrti Amandman i nalaže, potrebno je formirati nalog za pretres na najširi mogući način u skladu sa osnovanom sumnjom. Na taj način istraživači će biti u mogućnosti da obave najširu moguću analizu, a u skladu sa osnovanom sumnjom za potencijalnim inkriminišućim sadržajem koji će biti prihvaćen od strane suda.

Pretraga bez naloga

Ukoliko vreme i okolnosti dozvole, najbolje je u pretragu ići sa nalogom. Međutim, ukoliko istražitelji odluče da izvrše pretres bez naloga, taj pretres mora pripadati nekom od izuzetaka da bi se njegovi rezultati prihvatili na sudu.

Izuzeci su sledeći:

- dobrovoljni pristanak osumnjičenog
- mogućnost fizičkog uništavanja dokaza
- inkriminišući sadržaj je očevidan
- prilikom legalnog lišavanja slobode.

Iako su jasne odrednice pod kojima je ovakva pretraga moguća, postoji veliki prostor za kasnije odbacivanje ovako stečenog dokaznog materijala tako da se svim istražiteljima savetuje da ako ikako mogu izbegavaju ove metode pretresa.

Relevantni akti

Postoje brojni zakoni i amandmani koji mogu uticati na istragu a odnose se na privatnost.

Pre svega Akt Zaštite Privatnosti koji štiti slobodu govora odnosno slobodu objavljivanja i postavljanja materijala na Internet servisima. Ukoliko je materijal koji je prikupljen zaštićen Prvim Amandmanom, onda ovaj akt utiče na pretragu. Naravno postoje izuzeci kada su u pitanju legitimne pretrage u vezi sa počinjenim zločinom ili prevencijom mogućeg zločina.

U svakom slučaju istražitelji moraju sa oprezom pristupiti bilo kojoj pretrazi čiji je materijal potencijalno izmešan sa onim materijalom koji je pod zaštitom Prvog Amandmana. Istražitelj mora na svaki način izbeći kontakt sa takvim materijalom inače će celokupna istraga biti proglašena za nelegalnu.

Još jedan akt se mora razmotriti, a to je Akt Privatnosti Elektronskih Komunikacija koji se bavi zaštitom nedužnih trećih lica koji čuvaju skladištene podatke, kao što su internet provajderi. Ideja ovog zakona zapravo nije zaštita same kompanije koja pruža uslugu pristupa internetu već zaštita privatnosti ostalih korisnika te kompanije čiji se podaci takođe nalaze na serverima zajedno sa onim podacima za koje postoji nalog.

Postoje mnogi drugi akti na koje se mora obratiti pažnja i sa kojima se istražitelji u državnim službama moraju upoznati, da bi njihova istraga u sudu bila prihvaćena kao legitimna i legalna.

Autentičnost dokaza

Kada se digitalni dokaz pronađe i pravilno prikupi, da bi bio prihvaćen od strane suda, tužilac mora dokazati autentičnost dokaza. Po pravilu 901(a) FRE „zahtev za autentifikacijom ili identifikacijom je preduslov da bi se zadovoljila prihvatljivost dokaznog materijala dovoljnog da podrži nalaze koje prezentuje podnosioc zahteva za uvođenje dokaza“. Ovo pravilo u stvari nalaže tužbi da na neki način dokaže da je digitalni dokaz koji se uvodi u slučaj identičan onom inkriminišućem koji je prikupljen iz kompjutera ili nekog drugog uređaja okrivljenog.

Znači, iako je digitalni dokaz prikupljen i analiziran po svim propisima, porota ga može proglasiti neprihvatljivim ukoliko tužilac ne dokaže autentičnost dokaza na samom sudu. Ovaj standard je isti i kod klasičnih dokumenata. Obično se zahteva svedočenje nekog ko je bio u kontaktu sa dokumentom koji je u pitanju i ko može potvrditi njegovu verodostojnost.

U slučaju fotografije dovoljna je izjava svedoka da fotografija koja je u pitanju predstavlja „fer i preciznu“ sliku onoga što je i on sam video i ta fotografija postaje validno uvedeni dokazni materijal. Ista stvar važi i za kompjuterske dokumente. Dovoljno je svedočenje nekog o sastavu tih dokumenata da bi se postavio osnov o autentičnosti dokaza.

Nije potreban programer ili analitičar koji bi svedočio o strukturi same datoteke. Potrebno je svedočenje o sadržaju iste pri čemu poštovanje svih prethodnih procedura osigurava autentičnost strukture.

Pravilo najboljeg dokaza

Kada se u obzir uzmu i pisani i zvučni dokazi ili fotografije, sud nekada zahteva originalni dokaz. Ovaj zahtev je osmišljen ne bi li sprečio svedoke od pogrešne interpretacije određenih materijala tako što bi se oslonio jedino na njihov iskaz u vezi sa sadržajem. Sa razvojem tehnologije, postalo je izuzetno jednostavno kreirati identične kopije dokumenata ili dokaznog materijala uopšte. Pravilo najboljeg dokaza kaže da se pitanje da li je prezentovan materijal u svom izvornom obliku može pojaviti u smislu osporavanja autentičnosti, pouzdanosti ili preciznosti dokaznog materijala, i u tom smislu ukoliko je moguće treba prezentovati originalni materijal.

Kada je reč o digitalnim dokazima, tehnologija je omogućila kreiranje kopija koje su u svakom smislu verne originalu. U ovom slučaju prezentovanje kopije je u principu prihvatljivo uprkos postojanju i dostupnosti originala. U praksi se čak preferira prezentovanje kopija zbog otklanjanja svake sumnje u mogućnost izmene originala. Čak se i štampani oblik digitalnog dokumenta smatra validnim, osim u slučaju u kome on ne može prikazati sve informacije neophodne za proces.

Direktni i posredni dokazi

Direktni dokaz predstavlja činjenicu. Posredni dokaz potencijalno može ukazati na činjenicu. Uobičajena zabluda u vezi sa digitalnim dokazima predstavljena je dovođenjem u pitanje mogućnosti da digitalni dokaz uopšte može biti direktni dokaz zbog svoje elektronske prirode. Međutim, iako u elektronskom obliku, digitalni dokaz u svakom slučaju može dokazati činjenicu.

Ako se kao primer uzme dovođenje u pitanje sigurnosti nekog kompjuterskih sistema, ta sigurnost se može dokazati jedino digitalnim dokazom. Iako digitalni dokazi uopšteno samo ukazuju na pojedine ljudske, odnosno korisničke, aktivnosti ili navike, posredni dokaz može biti podjednako značajan u utvrđivanju neke činjenice kao i direktni dokaz. Ovaj primer najbolje se ilustruje prisustvom logova o uspešnom prijavljivanju na sistem određenog korisnika.

Direktni dokaz u ovom slučaju predstavlja sam zapis da je određeni nalog prijavljen sistemu u datom vremenu, međutim upotreba naloga koji je prijavljen sistemu od strane konkretne osobe predstavlja posredni dokaz. Zloupotreba ili krađa naloga kao sama mogućnost zahteva dodatna dokazivanja, a to je da jedino osoba može biti u mogućnosti da pristupi određenom kompjuteru u određeno vreme.

10.2.2. Priznavanje dokazne snage u Republici Srbiji

Iako postoje brojni pokušaji da se sistem kompjuterskog kriminala, a samim tim i digitalnih dokaza uredi, sama stabilnost političko-pravnog sistema kao i celokupnog društvenog uređenja bitno utiče na veliki zaostatak u ovoj kao i u drugim oblastima.

Krivični zakonik, donet 2001. godine (Službeni list SRJ, br. 70/2001) uvodi novu ulogu državnog tužioca u krivičnom postupku. Daje mu veća ovlašćenja a policiji ostavlja prostor da samostalno istražuje samo ona krivična dela za koja je predviđena maksimalna kazna od pet godina. Ovim postupkom bitno se utiče na pouzdanost istrage kao i na kvalitet prikupljenih dokaza. Kasnije izmene donele su definisanje „automatskog računarskog pretraživanja ličnih i drugih podataka" (član 155).

Ovaj član definiše vrste dela za koje se može obaviti pretraživanje i obrada digitalnih dokaza, i navodi:

- krivično delo protiv ustavnog uređenja i bezbednosti Republike Srbije
- krivično delo protiv čovečnosti i drugih dobara zaštićenih međunarodnim
- pravom
- krivično delo organizovanog kriminala
- krivično delo protiv polne slobode
- ubistvo, teško ubistvo, razbojništvo, krađu, falsifikovanje, zloupotrebu službenog položaja...

Takođe se dozvoljava pretraga i obrada digitalnih dokaza u slučaju da okolnosti ukazuju na pripremu nekog od navedenih krivičnih dela, a ono se na drugi način ne može sprečiti. Dalje se u tekstu kaže: „posebnu radnju (pretragu) naređuje istražni sudija na predlog javnog tužioca", i u nekim slučajevima omogućava javnom tužiocu da je samostalno naredi. Proces obrade i prikupljanja digitalnih dokaza ograničava se na tri meseca, ali se predviđa i mogućnost produžavanja za najviše tri meseca. Takođe određuje se i ko može sprovoditi ovu vrstu naredbe i to: policija, bezbednosno informativna agencija, organ carinske službe ili drugi državni organ odnosno pravno lice koja na osnovu zakona vrše određena javna ovlašćenja.

Takođe rok za uništavanje ovako prikupljenih dokaza određen je za šest meseci ukoliko se ne pokrene krivični postupak.

Javnost je imala velika očekivanja kada je jula 2005. godine donet „Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala" kojim je formirano posebno odeljenje za borbu protiv visokotehnološkog kriminala. Nažalost, specijalni tužilac postavljen je tek 2007.

Kako je sam proces postavljanja posebnog tužioca na ovu poziciju trajao dve godine, u svetu u kome se velike promene dešavaju u tom periodu, proces uređenja svih oblasti vezanih za prikupljanje, skladištenje, analiziranje i prezentovanje digitalnih dokaza u konkretnom krivičnom postupku deluje beskonačan.

Ako ovoj oblasti dodamo međunarodne regulative i veoma značajan aspekt zaštite privatnosti građana, postaje jasno da se regulativa mora donositi u hodu.

Domaće pravosuđe se najviše oslanja na istražnog sudiju, njegove sposobnosti i mogućnosti procene. Takođe, u našem pravnom sistemu jedna odnosno druga strana moraju svoje stavove nametnuti sudskom veću ili samo jednom sudiji.

Veliki broj stvari je na sudskoj slobodnoj proceni, snaga dokaza, ispravnost postupka, autentičnost dokaza i pouzdanost svedoka. Ceo proces oslonjen je na jednog čoveka, koji na kraju kao veštake poziva one navedene u spisku veštaka, ili poziva nekog po sopstvenoj proceni.

U svetu digitalnih dokaza, gde su ključni elementi za istragu osetljivi, nezahvalno je tražiti od veštaka da svojim ugledom garantuje za sadržaj čije se poreklo ne zna niti se može proveriti. Kako se celokupni sistem oslanja na sudsku slobodnu procenu, neophodno je kreiranje posebne institucije, pri institutu za veštačenja ili odvojeno od njega, koja bi bila uključena od samog početka u istragu.

Prikupljanje dokaza, dokumentovanje i analizu, kao i čuvanje digitalnih dokaza, trebale bi voditi stručne i obučene osobe. U godinama koje slede neophodno je formirati edukativni centar koji bi obučavao novi kadar, sposoban za adekvatno i profesionalno bavljenje istragom u digitalnom svetu.

Takođe, neophodno je ograničiti pristup državnim organima u smislu vrste podataka koje za određenu istragu treba da se prikupe. Trenutna situacija u našoj zemlji po tom pitanju je alarmantna. Privatnost građana se ne štiti ni na koji način niti je izgledno da će se to u skorijoj budućnosti dogoditi.

Celokupni pravni sistem ogleda se u pravičnom vođenju krivičnog postupka tako da niko nevin ne bude osuđen, a da se učiniocu krivičnog dela izrekne krivična sankcija pod uslovima predviđenim Krivičnim zakonikom i na osnovu zakonito sprovedenog postupka . U smislu digitalnih dokaza, koji će u narednom periodu predstavljati najrealniji izvor činjenica, trenutno ne postoji mogućnost da se tvrdnja montiranog procesa opovrgne kao ni to da se zahtev za nepristrasnom analizom ili superveštačenjem uopšte sprovede.

11. DISKUSIJA

Informacione i komunikacione tehnologije ključni su nosilac razvoja svuda u svetu. Njihov presudni doprinos nacionalnim ekonomijama ogleda se u visokom rastu proizvodnje i izvoza u samom ICT sektoru, ali, još važnije, kroz povećanje konkurentnosti svih ostalih privrednih sektora koji koriste nove tehnologije. Usvajanje predloženih mera zato će doprineti ne samo ICT sektoru, nego i povećanju konkurentnosti i ekonomskom rastu cele srpske ekonomije, kao i otvaranju brojnih novih radnih mesta.

Naš ICT sektor danas poseduje intelektualni i tehnološki potencijal uporediv sa najrazvijenijim delovima sveta. Najveća prepreka njihovom razvoju je nepostojanje odgovarajućeg pravnog okvira.

Naime, u Srbiji ne postoje čak ni osnovni zakoni koji garantuju bezbednost elektronskog poslovanja, zaštita intelektualne svojine je slaba, onemogućena je konkurencija na polju telekomunikacija, krivično zakonodavstvo je nedovoljno usaglašeno sa brzim informacionim razvojem.

Zbog toga je neophodno da država što pre preduzme mere koje će garantovati sledeće osnovne principe, bez kojih funkcionisanje i razvoj ICT sektora nije moguć:

1. **Pravnu sigurnost** korišćenja ICT usluga i proizvoda, uključujući pravnu sigurnost elektronskih transakcija i pravnu zaštitu elektronskih podataka.
2. **Zaštitu kritične infrastrukture,** kao osnovu za razvoj informacionih tehnologija
3. **Borba protiv visokotehnološkog kriminala –** čiji su temelji postavljeni donošenjem adekvatnih zakonskih propisa a čiji je razvoj neophodan radi stvaranja adekvatne pravne sigurnosti učesnika u elektronskom poslovanju.

Pored obezbeđivanja pravnog okvira, podrška države ICT sektoru ostvaruje najbolje rezultate putem "liderstva kroz primer", odnosno promovisanjem ICT usluga i proizvoda kroz njihovu upotrebu. Omogućujući pristup javnim službama i obavljanje administrativnih procedura preko interneta (projekat *e-Government*), državna uprava bi postala vodeći kupac ICT proizvoda i usluga, kao što je to slučaj u većem delu sveta. Tako bi država podstakla razvoj i konkurenciju ICT kompanija i omogućila brži i efikasniji rad javnih službi. Takođe, komunikacija i poslovi građana sa organima uprave postali bi neuporedivo brži i jeftiniji.

Sve predložene mere u skladu su sa programom ekonomskih reformi i nizom usvojenih dokumenta, kao što su Akcioni plan Vlade za otklanjanje administrativnih prepreka za strana ulaganja, Evropska povelja o malim preduzećima i eSEE Agenda z a razvoj Informacionog društva u regionu.

Uporedni pristup razvoja elektronskog poslovanja u svetu i donošenja pravnih akata u ovoj oblasti, dovodi nas do zaključka da jedino brza i efikasna uloga države kroz

donošenje adekvatnih zakonskih i podzakonskih propisa može da ubrza razvoj ove oblasti u našoj zemlji.

Razvoj informacionog društva treba usmeriti ka iskorišćenju potencijala za povećanje efikasnosti rada, ekonomski rast, veću zaposlenost i podizanje kvaliteta svih građana Republike Srbije.

Motor razvoja informacionog društva čine :

- Otvoren, svima dostupan i kvalitetan pristup Internetu
- razvijeno e- poslovanje, uključujući e – upravu, e-trgovinu, e- pravosuđe, e-zdravlje i e-obrazovanje.
- pravna sigurnost i relevantna zakonska regulativa u ovoj oblasti.

U Republici Srbiji bi u najskorije vreme trebalo urediti sve aspekte informacione bezbednosti i formirati odgovarajuće institucionalne okvire. Informaciona bezbednost znači zaštitu sistema, podataka i infrastrukture u cilju očuvanja poverljivosti, integriteta i raspoloživosti informacija.

Odgovarajući stepen informacione bezbednosti u svim oblicima primene IKT jedan je od preduslova stvaranja održivog informacionog društva.

Razvojem informacione bezbednosti postiže se
- poverenje korisnika u bezbedno funkcionisanje informacionih sistema i poverenje građana u zaštićenost podataka o ličnosti u informacionim sistemima;
-zaštitu podataka;
-zaštitu informacionih i telekomunikacionih sistema
-bezbednost elektronskih transakcija
- efikasni mehanizmi zaštite i ostvarivanje prava u procesima elektronskog poslovanja i elektronske razmene podataka.

Kao osnovne i neophodne mere za razvoj ICT sektora, a na osnovu istraživanja koja su opisana u ovom radu, predlažemo sledeće:

Pravna sigurnost

Iskustva tržišno razvijenih zemalja ukazuju da vlade tih zemalja izbegavaju nametanje nepotrebnih ograničenja elektronskom poslovanju. Najčešće se propisuju minimalni i konzistentnu uslovu neophodni za funkcionisanje pravnog okruženja, uz razumevanje značaja Interneta. Na tom planu u poslednje dve godine je dosta učinjeno , pa je tako donet Zakon o elektronskoj trgovini koji uređuje uslove i način pružanja usloga informacionog društva, obaveze informisanja korisnika usluga, komercijalne poruke, pravila u vezi sa zaključenjm ugovora u elektronskom obliku, odgovornost pružalaca usluga informacionog društva, nadzor i prekršaje. Tim zakonom su stvoreni preduslovi za razvoj i funkcionisanje sistema e-trgovine po ugledu na rešenja razvijenih zemalja sveta i EU. Zakon o elektronskom potpisu i zakon o elektronskom dokumentu, dopunjuju okvir koji omogućava poslovanje elektronskim putem ravnopravno sa klasičnim poslovanjem

U radu je već detaljno obrađeno postojeće stanje zakonske regulative u ovoj oblasti, pa kao rezultat istraživanja predlažemo donošenje propisa iz oblasti informacione bezbednosti kojima će se dodatno urediti standardi informacione bezbednosti, područja informacione bezbednosti, kao i nadležnosti i zadaci pojedinih institucija u ovoj oblasti.

Potrebno je formirati instituciju koja u oblasti informacione bezbednosti obavlja poslove verifikacije i sertifikacije metoda, softverskih aplikacija, uređaja i sistema, kao i istraživanje i razvoj. Ova institucija treba da nadzire i primenu standarda informacione bezbednosti u državnim organima.

Zaštita kritične infrastrukture

Potrebno je razvijati i unapređivati zaštitu od napada primenom informacionih tehnologija na kritične infrastrukturne sisteme, što pored IKT sistema mogu biti i drugi infrastrukturni sistemi kojima se upravlja korišćenjem IKT, poput elektro-energetskog sistema

U vezi toga je potrebno dodatno urediti kriterijume za utvrđivanje kritične infrastrukture sa stanovišta informacione bezbednosti, kriterijume za karakterizaciju napada primenom informacionih tehnologija na takvu infrastrukturu u odnosu na klasične oblike napada , kao i uslove zaštite u ovoj oblasti.

Trenutno je u ovoj oblasti stanje najkritičnije, tako da se aktivnosti na zakonodavnom planu tek očekuju u narednom periodu.

Borba protiv kompjuterskog kriminala

Ubrzan razvoj borbe protiv visokotehnološkog kriminala započeo je donošenjem izmena i dopuna Krivičnog Zakonika RS, kao i Zakona o organizaciji i nadležnosti organa za borbu protiv visokotehnološkog kriminala. Ovim zakonom je prvi put u domaćem zakonodavstvu definisan pojam visokotehnološkog kriminala kao vršenje krivičnih dela kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarske mreže, računarski podaci , kao i njihovi proizvodi u materijalnom ili elektronskom obliku. Najsveobuhvatniji pokušaj da se pravno uredi borba protiv visokotehnološkog kriminala na međunarodnom nivou, a koji ima uticaja i na Republiku Srbiju, predstavlja Konvencija Saveta Evrope iz 2001 godine, a koju je Narodna skupština ratifikovala 2009 godine,

U narednom periodu potrebno je usvojiti nova i unaprediti već postojeća rešenja u našem zakonodavstvu, kako bi se omogućila veća usklađenost, a samim tim u efikasnija primena Konvencije čime bi se, u zajedničkom dejstvu i drugih državnih činilaca koji imaju javni interes za suzbijanje visokotehnološkog kriminala, omogućilo postizanje optimalnih rezultat u ovoj oblasti.

Veoma značajan korak sa aspekta procesnog krivičnog zakonodavstva imalo bi donošenje Zakona o digitalnom dokazu, kojim bi se definisao pojam digitalnog dokaza i stvorile mogućnosti za primenu istog u krivičnom postupku. Naime, da bi se bilo koja od

kompjuterskih zloupotreba dokazala neophodno je prisustvo digitalnih dokaza. Iako postoje i drugi načini dokazivanja malicioznih ponašanja, jedini neposredni dokaz nalazi se sačuvan u digitalnom obliku. Nažalost, u Srbiji, kao i u mnogim drugim oblastima, ne postoji sistemski rešen problem svedoka eksperta – veštaka, čiji ce iskaz sud smatrati validnim. Neophodno je utvrditi pravila po kojima će se iskaz određenih stručnjaka prihvatati kao validan i urediti načine na koje će se ovi dokazi prikupljati.

12. ZAKLJUČAK

U savremenim globalnim uslovima poslovanja primena informaciono-komunikacionih tehnologija i e-poslovanja postaje ključan faktor konkurentnog i profitabilnog poslovanja preduzeća i dotiče sve sektore i grane privredjivanja. Time pitanje pravilnog uvođenja i široke primene IKT i e-poslovanja postaje bitan deo kreiranja razvojnih politika Srbije koji mora biti tretiran na visokom nivou.

Praćenje trendova razvoja i primene e-poslovanja u Evropi i svetu jasno potvrđuje da je uvodjenje elektronskog poslovanja u domaća preduzeća nužan preduslov za ostvarivanje učešća srpske privrede na globalnim tržištima kroz konkurentniju ponudu domaćih proizvoda i usluga i kroz šire mogućnosti nabavke proizvoda i usluga sa svetskog tržišta.

Proces razvoja e-poslovanja u nacionalnoj ekonomiji obuhvata brojna pitanja - tehnička, pravna, ekonomska i institucionalna, tako da implementacija e-poslovanja podrazumeva multidisciplinarni i timski rad u koji moraju biti aktivno uključeni predstavnici i javnog i privatnog sektora.

U pogledu pravne infrastrukture neophodno je rešiti opšte pravne prepreke na državnom nivou i doneti sve neophodne zakone koji regulišu područje elektronskog poslovanja. Kao ključne oblasti koje moraju biti ugrađene u nacionalni legalni okvir za e-poslovanje možemo navesti sledeće: elektronska trgovina, elektronski dokument, elektronski potpis, zaštita ličnih podataka, informaciona sigurnost, zaštita tajnosti podataka, sigurno formulisanje ugovora (zakonski i komercijalno), regulisanje Internet okruženja, zaštita potrošača, prodaja na daljinu, e-privatnost, pitanja rešavanja sporova (uključujući regulisanje sporova online), a pre svega zaštita od kompjuterskog kriminala.

Komercijalizacija računarske tehnologije i njena masovna primena u poslovne i privatne svrhe, kao i sve razvijeniji sistemi komunikacije među ljudima, uslovili su pojavu nove vrste nedozvoljenog ponašanja – kompjuterskog kriminala. Kompjuterski kriminal ima dosta zajedničkih elemenata s postojećim oblicima kriminalnog ponašanja, ali poseduje i specifične elemente, na koje smo ukazivali u ovom radu. Analiza najvažnijih međunarodnih dokumenata i nacionalnih zakonodavstava pojedinih zemalja otkriva kakve se promené mogu očekivati u ovoj oblasti narednih godina. Analize i iskustva koja su sakupljena na ovaj način, mogu se koristiti kao putokaz daljeg delanja na polju visokotehnološkog kriminala u Srbiji.

Na osnovu stanja pozitivnog zakonodavstva u Republici Srbiji, a imajući u vidu činjenicu da je visokotehnološki kriminal nov pojavni oblik kriminaliteta, možemo da konstatujemo da je država preduzela značajan i odlučan korak u pravcu konstituisanja specijalizovanih organa, kao i usvajanja odgovarajućih pravnih propisa, prevashodno materijalne prirode, koji predstavljaju osnov za efikasan krivični progon počinioca krivičnih dela visokotehnološkog kriminala.

Sa druge strane, neophodno je veoma ozbiljno analizirati primedbe i preporuke koje dolaze od stručnih lica koja su angažovana na poslovima otkrivanja i gonjenja

računarskog kriminala, i izvršiti korekciju i dopunu materijalnog i procesnog zakonodavstva koja bi omogućila postizanje optimalnih rezultata u borbi protiv visokotehnološkog kriminaliteta.

Dakle, možemo zaključiti da je razvoj informacionih tehnologija i elektronskog poslovanja jedan od značajnih pokretača socijalnih i ekonomskih promena, pogotovu u društvima u tranziciji poput našeg, da je neophodno pravno regulisati najznačajnije oblasti i to pre svega, kompjuterski kriminal i zaštitu informacionih sistema. Nedostatak adekvatnih propisa značajno će umanjiti ili čak u potpunosti sprečiti razvoj ovih oblasti. Pravni okvir je ključan faktor kako za privlačenje novih investicija tako i za održavanje već postojećeg poslovnog okruženja. Bez adekvatnog domaćeg zakonodavstva nema pravne sigurnosti za učesnike elektronskog poslovanja.

13. LITERATURA

[1]. Bequai A., *Computer crime*, Lexington, str. 4, 1978.
Convention on Cybercrime, ETS No.185, Budapest, 23.XI 2001.
[2]. Dave Chaffey, E-Business and E- Commerce Management, Prentice Hall
[3]. *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain aspects of Information Society services, in particular electronic commerce, in the Internal Market.*
[4]. Drakulić M., Intelektualna svojina i ePoslovanje, 2000
[5]. Drakulić M., Privatnost i informacione tehnologije, 1996
[6]. Drakulić M., Osnovi Poslovnog prava, Beograd, FON, 2001.
[7]. Drakulić, M.: Kompjutersko pravo. Beograd, FON, 1992.
[8]. Foregger E. E. Serini, *Strafgesetzbuch*, Wien, 1989.
Ignjatović Đ., *Pojmovno određivanje kompjuterskog kriminaliteta*, Anali Pravnog fakulteta u Beogradu, Beograd, broj 1-3, str. 14,1991.
[9]. Jovašević D., *Leksikon krivičnog prava*, JP Službeni list SRJ, Beograd, 2002.
[10]. *Konvencija o visokotehnološkom kriminalu.*
[11]. *Krivični zakonik Makedonije,* Služben vesnik na Republika Makedonija, Skopje, broj 37/1996.
[12]. *Krivični zakonik Republike Srbije*, Službeni glasnik RS, br. 85/05, 88/05 i 107/05.
[13]. *Krivični zakonik Republike Srpske,* Službeni glasnik Republike Srpske, Banja Luka, broj 22/2000
[14]. K.C Laudon, C.G. Traver « E – commerce, business, technologz, sociez « 3 edition, Addison Wesley 2006.
[15]. Keegan, W.J., Global marketing managment, Prentice – Hall 2002
[16]. King D., Electronic commerce, Prentice Hall, New Jersey, 2002. godine
[17]. Kotler P., Marketing Menagment, Prentice - Hall International, London, 1991.
[18]. Kotler, P., Keller K.L., Marketing Menagment
[19]. Milosavljević M., Grubor G., *Osnovi bezbednosti i žaštite informacionih sistema*, Univerzitet Singidunum, 2006.
[20]. Parker D., *Computer abuse*, Springfild, str. 70, 1973.
[21]. Penko B., Strolig K., *Kazenski zakonik z uvodnimi pojasnili*, Ljubljana, 1999.
[22]. Petrović R. S., *Kompjuterski kriminal*, Beograd, 2002.
[23]. Schonke-Schroder, *Strafgesetzbuch*, Munchen, 1978.
[24]. Wasik M,, *The computer misuse act, The Criminal Review, str. 767, 1990.*
[25]. *Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala*, Službeni glasnik RS, broj 61/05, 18. jul 2005.
[26]. *Zakon o posebnim ovlašćenjima radi zaštite prava intelektualne svojine*, Službeni glasnik RS, broj 46/06.
[27]. *Zakonik o krivičnom postupku republike Srbije,* www.gov.rs.

Internet izvori:

www.computerworl.com (pristupljeno: 22.02.2010) primeer – uneti za svaku adresu!
www.emarket.com

www.customers.com
www.e-trgovina.co.yu
www.ebusinessassociation.org
www.ecommercetimes.com
www.emarketer.com
www.internet.com
www.ebstrategy.com
www.e-trgovina.co.yu
www.etrgovina.org/sr
www.ecommerce. Com
www.etrgovina.org/
www.economy.rs
www.esrbija.net
www.ekapija.com
www.emagazin.co.yu
www.ec.europa.eu
www.ebusiness.com
www.law.georgetown.edu/iiel/journiel.html
www.eur-lex.europa.eu
www.bc.edu
www.uncitral.org/
www.euractiv.com
www.selfgov.net/
www.srbija.gov.rs
www.nauka.gov.rs
www.parlament.sr.gov.yu/
www.spamrecycling.com
www.sk.co.yu/2001/09/skin04.html
www.elitesecurity.org/
www.prafak.ni.ac.rs/files/nast_mat/Kompjuterski_kriminal.pdf
www.mikro.rs/main/index.php?q=vestiarhiva
www.mup.vladars.net/novosti/novosti.php
www.telekomunikacije.rs
www.tuzilastvovtk.sr.gov.yu/docs/index29633.doc
www.itvestak.org.rs/
www.fpp.edu.yu/files/silabus2009pfu
http://www.techterms.com/definition/cybercrime
http://www.netalert.gov.au/advice/risks/e-crime/what_is_e-crime.html
http://europa.eu.int/information_society/topics/telecoms/internet/crime/index_en.htm
http://www.crime-research.org
http://computerhacker.newstrove.com/