Revija za evropsko pravo: II (2000) 1.
@Udruženje za pravo Evropske unije, Beograd

Prof. dr Jelena VILUS*

UDK 339.94 : 061.1EC
659.2.000.34
str. 49 - 67.
izvorni naučni rad

EVROPSKA UNIJA I ELEKTRONSKO PRAVO
- Povodom usvajanja Direktive Zajednice o elektronskim potpisima -

ABSTRACT

At the end of 1999 the European Parliament and Council adopted the Directive 1999/93/EC on a Community framework for electronic signatures. The member states are requested "to comply with this Directive before 19 July 2001". The Directive deals with questions of electronic signatures, establishment, work and liability of certification bodies (certification-service-providers). Before reviewing these issues, the author gave a short analyses of electronic commerce, electronic and digital signature and importance of authentication of the parties (sender and receiver) and integrity of the electronic message sent through closed (EDI) or open (Internet) system. The opportunities of intentional intrusion in the open network is greatly facilitated in Internet and therefore the question of security by encryption of signature became even more important. There are analyses of the role of certification body, conditions for their establishment and their duties in identifying the public and private keys of the sender,

* Evropski centar za mir i razvoj (ECPD), Beograd.

which has implication on the electronic (or digital) signature and integrity of the message.

Key words: *electronic commerce, digital and electronic signatures, authentication of signatures by certification authorities, encryption of signature, the role of public and private keys, mistakes, frauds, liability of the parties, service providers and the member states.*

I Osnovna pitanja od značaja za elektronske potpise

Uvodne napomene

Krajem decembra 1999. godine Evropski parlament i Savet usvojili su Direktivu 1999/93/EC o okviru Zajednice o elektronskim potpisima. Nema sumnje da je ovo izuzetno važan dokument jer se njime reguliše materija koja je od vitalnog značaja za funkcionisanje elektronske trgovine. Globalna trgovina se ne može zamisliti bez elektronske trgovine, a ova, pak, bez osnovnih pravnih propisa kojima se garantuju elektronski potpisi. Potreba za pravnim regulisanjem pitanja od značaja za uspešno funkcionisanje elektronske trgovine javila se onda kada su domaći propisi postali prepreka za realizovanje transakcija zaključenih korišćenjem kompjutera.

Evropska ekonomska zajednica je odavno shvatila značaj elektronskog prenosa podataka pa je od značaja istaći da je 1987. usvojila Evropski kodeks ponašanja u oblasti elektronskih plaćanja. Bankarstvo se pokazalo kao najpogodnija oblast za primenu elektronskog prenosa podataka, pa je logično što se baš u toj oblasti ovaj način u zemljama tržišne privrede brzo prihvatio jer je pokazao velike prednosti pred papirnom obradom poslova u banakrstvu. Upravo u toj oblasti počeo je proces bezpapirne trgovine (*paperless commerce).* Međutim, papirni način i obrada podataka se i dalje koriste, ali u razvijenom svetu ovaj vid sve više uzmiče

pred velikim prednostima koje pruža elektronska trgovina. U vezi sa elektronskim plaćanjem Kodeks EEZ ističe da se pod tim pojmom podrazumevaju "sve platne transakcije koje se obavljaju platnim karticama sa magnetnom trakom i mikročipom na elektronskim platnim terminalima".

1. Elektronska trgovina

Pravnim regulisanjem elektronskog načina poslovanja bave se mnoge međunarodne organizacije. Nema sumnje da centralnu ulogu u tom procesu ima Komisija UN za međunarodno trgovinsko pravo[1]. Komisija UN za međunarodno trgovinsko pravo (UNCITRAL) se bavi unifikacijom pravila iz oblasti međunarodnog prava i na tom planu od osnivanja do danas postigla je značajne rezultate. Usvojeno je dosta značajnih dokumenata u raznim oblastima (međunarodna prodaja, međunarodni prevoz, arbitraža, načini ustupanja investicionih radova), pri čemu su korišćeni razni pravni oblici (konvencije, model zakoni, jednoobrazna pravila, vodiči i sl.).

Kad je reč o elektronskoj trgovini, Komisija za međunarodno trgovinsko pravo najtešnje sarađuje sa Međunarodnom trgovinskom komorom[2], Međunarodnim pomorskim komitetom (CMI)[3], Ekonomskom

[1] Komisija je osnovana 1996. Rezolucijom Generalne skupštine Ujedinjenih nacija 2105 (XXI). Pored Komisije za međunarodno pravo, koja se bavi javnim pravom, UNCITRAL je drugi pravni organ u okviru Ujedinjenih nacija kojii se bavi privatnim pravom, tj. unifikacijom pravila namenjenih međunarodnoj trgovini. Komisija tesno sarađuje sa specijalizovanim organizacijama aktivnim na polju međunarodne trgovine. Rezolucijom je predviđeno da Komisija svoje godišnje izveštaje redovno dostavlja UNCTAD-u (*United Nations Conference on Trade and Development).*

[2] Međunarodna trgovinska komora je na planu elektronske trgovine usvojila *Jednoobrazna pravila za telekomunikacione prenose* 1988*, Opšte uzanse o bezbednoj digitalnoj trgovini* 1997. godine, a u pripremi su *E-terms - jednoobrazna pravila za tumačenje elektronskih termina* (slično kao *Incoterms*) koji bi trebalo da posluže poslovnim ljudima da se pozivanjem na neku od klauzula *E-terms*-a obezbede u slučaju da dođe do problema u toku izvršenja ugovora koji je zaključen korišćenjem elektronskog prenosa podataka. Usvajanje *E-terms*-a očekuje se tokom 2000/2001.

[3] Komitet je 1990. izradio *Pravila za elektronske konosmane*. Ova pravila su izuzetno značajna, jer je konosman (kao svojinski dokument) izuzetno važan kod otvaranja dokumentarnog akreditiva, a značajan je u i u vezi međunarodnog (naročito pomorskog) prevoza robe.

komisijom UN za Evropu odnosno njenim specijalizovanim Centrom CEFACT (*Centre for Facilitation of Procedures and Practices for Administration, Commerce and Transport)* koji se bavi izradom standarda, bez kojih se uopšte ne može zamisliti razvoj elektronske trgovine[4] kao i sa Evropskom ekonomskom zajednicom tj. Evropskom unijom.

Evropska unija je, slično kao i druge međunarodne organizacije, shvatila značaj pravnog regulisanja nekih osnovnih pitanja, pri čemu se koristi već usvojenim dokumentima drugih međunarodnih organizacija. Treba navesti da EU (slično kao i druge međunarodne organizacije) prilikom formulisanja svojih tekstova naročito uzima u obzir pravila koja su već usvojena u okviru Komisije UN za međunarodno trgovinsko pravo (UNCITRAL) kako bi se na taj način u najvećoj meri usaglasili propisi namenjeni regulisanju međunarodne trgovine. Nema sumnje da je Direktiva o elektronskim potpisima (dalje "Direktiva") od izuzetnog pravnog značaja, tim pre što čl. 13. Direktive nalaže državama članicama (navodi se da su one "dužne") "da donesu zakone, propise i administrativne odredbe neophodne za usaglašavanje sa ovom Direktivom najkasnije do 19. jula 2001. godine". O tome su, navodi se u istom članu, "dužne da odmah obaveste Komisiju".

U vezi sa obradom pitanja o elektronskim potpisima koja čine predmet Direktive, važno je razmotriti pitanja elektronskih i digitalnih potpisa, utvrđivanja verodostojnosti takvih potpisa i ulogu i značaj certifikacionih tela kojima se poverava uloga izdavanja certifikata, čime se pravno obezbeđuje sigurnost učesnicima elektronske trgovine.

2. Elektronski potpis

Prema čl. 2. Direktive "elektronski potpis" označava podatke u elektronskom obliku koji su priloženi ili se logički povezuju sa drugim elektronskim podacima i služe kao metod za svrhe utvrđivanja verodostojnosti". U praksi postoji obični i "pojačani elektronski potpis" Za ovaj drugi je neophodno da se ispune uslovi prema kojima: postoji

[4] CEFACT je najveći broj definitivno usvojenih standarda (koji nose oznaku "2") usvojio u oblasti dokumentarnih akreditiva, iako se intenzivno radi na velikom broju drugih standarda za elektronsko poslovanje.

jedinstvena veza sa potpisnikom; u stanju je da se identifikuje potpisnik, stvoren je korišćenjem sredstava tako da ga potpisnik može držati pod svojom sopstvenom kontrolom kao i da je povezan sa podacima na koje se odnosi na takav način da se svaka naknadna izmena može da otkrije. U Direktivi se dalje navode definicije za bezbedno stvaranje potpisa, za proveru tih potpisa, za certifikat i za provajdera-certifikacione-usluge *(cetification-service-provider),* kako se u Direktivi naziva certifikaciono telo. Pre nego što se ukaže na elektronske potpise, potrebno je osvrnuti se na digitalne popise jer su u toj oblasti Američki savez pravnika *(American Bar Association - ABA)* 1996. i Međunarodna trgovinska komora 1997. objavili opširne publikacije posvećene digitalnim potpisima. Oba ova dokumenta značajno su uticala na kasnija jednoobrazna pravila koja su u ovoj oblasti usvojena (kao što je slučaj sa Direktivom). Ova pravila, kao i Direktiva EU se pažljivo razmatraju i čine podlogu za izradu nacrta Međunarodnih jednoobraznih pravila UNCITRAL-a o elektronskim pravilima (čije usvajanje se očekuje tokom 2000).

3. Digitalni potpisi

Kao što je navedeno, ABA je 1996. usvojila Vodič o digitalnim potpisima (*Digital Signature Guidelines)* koji na preko 130 stranica daje objašnjenja o digitalnim potpisima, certifikatima i certifikacionim telima kojima je poverena uloga izdavanja certifikata. Prema ovom Vodiču "digitalni potpis" je transformacija poruke[5] korišćenjem asimetričkog kriptosistema i *hash*[6] funkcije tako da lice koje poseduje inicijalnu poruku i potpisnikov javni ključ mogu precizno da utvrde: da li je izvršena transformacija korišćenjem privatnog ključa koji odgovara javnom ključu potpisnika i da li je inicijalna poruka izmenjena pošto je izvršena transformacija. Opšte uzanse MTK o

[5] Za "poruku" *Model zakon UNCITRAL-a o elektronskoj trgovini* od 1996. navodi da ona ožnačava "informaciju koja je generisana, poslata, primljena ili sačuvana elektronskim, optičkim ili sličnim načinom i obuhvata, ali se ne ograničava, na elektronski prenos podataka (EDI), elektrtonsku poštu, telegram ili faks".

[6] Izraz "*hashing*" označava sažimanje osnovne poruku u manju, pod uslovom da se u toj manjoj zadrži osnovni smisao poruke. Zbog teškoće u vezi sa prevođenjem ovaj izraz se koristi u svom izvornom obliku

međunadno bezbednoj digitalnoj trgovini (*General Usage for International Digitally Ensured Commerce - GUIDEC)* od 1997. su na preko 40 stranica dale značajan doprinos kodifikaciji i popularizaciji ove vrste potpisa. U pogledu "digitalnog potpisa" Uzanse sadrže definiciju koja je identična onoj koju sadrži ABA Vodič. U vezi sa kriptosistemom *(cryptosystem)* navodi se da taj termin označava mogućnost asociranja date poruke sa određenim kriptografskim ključem kao i jednu ili više operacija za utvrđivanje da li je data poruka apsolutno podudarna sa onom kada je operacija ranije izvršavana. Kad je reč o asimetričnom kriptosistemu (*asymetric cryptosystem),* koji se često naziva "kriptosistem javnog ključa", navodi se da je to "jedan ili više algoritama kojima se obezbeđuje uparivanje ključeva odn. kojim se potvrđuje da privatni ključ odgovara javnom ključu. Ono što je bitno, podvlače Uzanse, je da digitalni potpis bude sa sigurnošću i nedvosmisleno vezan za poruku. Sve dotle dok se ta veza održava, učesnici mogu biti sigurni da je njihova poruka autentična i da nije izmenjena.

Digitalni potpis je po mnogo čemu sličan elektronskom "pojačanom" potpisu kod koga se traži utvrđivanje verodostojnosti pošiljaoca i primaoca poruke i potvrda da integritet poruke nije doveden u pitanje, tj. da je ona od slanja do primanja ostala neizmenjena.

4. Utvrđivanje verodostojnosti

Utvrđivanje verodostojnosti *(authentication)* poruke, pošiljaoca i primaoca je od izuzetnog značaja, jer se inače može desiti (naročito na otvorenim mrežama Internet-a), da se poruke preinače i da se time oštete učesnici. Drugim rečima, pitanje utvrđivanja verodostojnosti poruke i učesnika znači veliku sigurnost za elektronski promet. Time se obezbeđuje zaštita podataka i sprečava neovlašćeni pristup sistemu. Drugim rečima, uvek postoji mogućnost - bez obzira što može biti mala - da neko neovlašćeno lice sazna za sadžinu poruke i time dovede u pitanje njen integritet. Ovi rizici mogu biti umanjeni metodima kriptovanja (šifrovanja) koji se uveliko koriste, mada u nekim državama za određene oblasti nisu dozvoljene[7].

[7] Kriptografska tehika u nekim zemljama nije dozvoljena jer se smatra da se njome može da onemogući krivično gonjenje. Kriptovanje može da bude zabranjeno i u pogledu izvoza

a) Greške u prenosu

Greške u prenosu su moguće (nekad se i ne otkriju) i često mogu da nanesu velike štete licu naročito u slučaju kada su ponude o prodaji robe ili usluge lansirane preko Internet-a. U pogledu nenamerne greške zanimljiv je slučaj engleske multinacionalne kompanije Argos koja svoje proizvode prodaje preko kataloga. U jednoj od svojih ponuda 1999. godine na Argos *web site*-u lansirana je prodaja najnovijih televizora u boji po ceni od 2.99 GBP umesto 299, što je dovelo do potražnje koja je iznenadila kompaniju. Samo jedan od klijenata poručio je 1.700 televizora. Argos je odmah dao javnu izjavu da je u pitanju greška, ali je poveden spor koji se još uvek vodi. Nije sigurno da će Argos biti oslobođen odgovornosti za obeštećenje zavedenih potrošača. Ponuda na *web site* smatra se ponudom i na nju se primenju sva pravila koja za ponudu inače važe. S ovim u vezi izuzetno je važno da se kompanije koje reklamiraju ili nude svoju robu ili usluge preko Internet-a pozovu na svoje opšte uslove, ukoliko ih imaju, kojim su detaljno regulisana prava i obaveze ugovornih strana[8].

b) Namerne greške

Namerne greške su upadi u sistem tzv. hakera (*hackers)* koji neovlašćeno upadaju u mreže i "skidaju" programe koje zatim prodaju. U mnogim zemljam tako postoje piratski programi koji se prodaju po ceni koja je daleko niža od prave cene, a na kojima neovlašćena lica zarađuju ogromne pare.

Slučaj pornografskih filmova i onih sa agresivnom sadržinom koji se lansiraju preko Internet-a predstavljaju ozbiljan vid zloupotrebe. Ovo se

---

software. Zanimljive su s ovim u vezi odredbe *Evropskog EDI Model sporazuma* u kome se navodi (čl.7.3) da se "stranke mogu sporazumeti da koriste poseban oblik zaštite za određene poruke, kao što je metod kriptovanja u meri u kojoj je to dopušteno pravom bilo koje njihove odnosne zemlje".

[8] Ukoliko je *Argos* u svojoj ponudi pomenuo svoje Opšte uslove, u tom slučaju, ti opšti uslovi čine sastavni deo ponude i ugovora (*incorporation be reference)* i *Argos* bi bio oslobođen odgovornosti za grešku prilikom lansiranja prodaje televizora za cenu koja bi svakom razumnom čoveku odmah morala biti smešno niska.

naročito odnosi na negativan uticaj ovakvih filmova na omladinu i decu. U mnogim propisima Evropske unije zabranjeno je reklamiranje cigareta i alkoholnih pića preko televizije i Internet-a, što se u mnogim državama (sem u državama-članicama EU) ne poštuje.

Napred naveden primeri nenamernih i namernih grešaka na Internetu govore o značaju utvrđivanja verodostojnosti poruke. U zatvorenim mrežama (*closed network)* mogućnost zloupotreba je mnogo manja nego što je to slučaj na otvorenim mrežama *(open network)*, kao što je Internet. Otuda je šifrovanje poruke jedan od načina da se poruka sačuva u svom izvornom, originalnom obliku. Šifrovanje se definiše kao metod i proces transformisanja informacije iz svog izvornog (razumljivog) u šifrovani (nerazumljivi)) oblik i dobijanje originalne poruke nazad iz šifrovanog oblika kroz obrnut proces. U pogledu savremenog načina šifrovanja u primeni su "blokovsko šifrovanje", sistem metodom "javnog ključa" kao i zaštita lozinki baze podataka šifrovanjem. Ključevi verodostojnosti su tajni kriptografski ključevi koji su prethodno razmenili pošiljalac i primalac a koji se koriste u algoritmima za utvrđivanje verodostojnosti[9].

5. Certifikaciona tela

Uloga ceritifikacionih tela (*certification authorities - CA)* je značajna jer se preko njih obezbeđuje pravna sigurnost elektronske trgovine. Treba, međutim, naglasiti da efikasnost trećeg lica kao certifikacionog tela zavisi od toga koliko se usluge određenog CA priznaju kao praktične, pouzdane i pravno obavezujuće. Ovo priznanje velikim delom zavisi od načina na koji CA obavljaju svoje usluge, od toga da li su certifikati dokumentovani i transparentni i u kojoj meri zainteresovana lica i javnost mogu imati uvid u rad certifikacionog tela.

[9] D. Bulatović i B. Trifunović: *Šifrovanje i zaštita podataka u elektronskom prenosu novca*, izd. Stručna knjiga, Beograd 1995, str. 160. Autori navode da je "bolje poruke ne šifrovati nego loše šifrovati jer ovo drugo čini da se stvori utisak o lažnoj sigurnosti". Isti autori dalje navode da "šifarske transformacije koje treba izvesti u konkretnom slučaju zavise od pretnji kojima je izložen sistem. Ponekad i najjednostavnija transformacija može zaštiti informacije, ali zato i mudro napravljeno šifrovanje može se pokazati beskorisno ukoliko treba da ga savlada profesionalni kriptoanalitičar".

Certifikaciona tela postoje u mnogim zemljama u svetu, s tim što su se najpre javila u SAD i tamo ostvarila zapažene rezultate, tako da su druge države (preko Interneta i na druge načine) preuzele praksu SAD u pogledu osnivanja i rada svojih CA. Pitanja digitalnih potpisa *(digital signatures)* i certifikacionih tela *(certification authorities),* su, u stvari, tesno povezana, jer certifikaciono telo treba da izda certifikat u vezi sa kriptografskim ključevima (o podudarnosti javnog i tajnog ključa) koji se koriste u vezi sa digitalnim potpisima[10]. Ono što se u ovom pogledu smatra važnim je činjenica da certifikaciono telo mora da poseduju infrastrukturu koja će omogućiti pružanje usluge koja se od njega očekuje; da zaposleni kadrovi moraju imati stručno znanje, iskustvo i kvalifikacije koje su neohodne za obavljanje pomenutih usluga; mora se obezbediti beleženje svih relevantnih informacija koje se tiču certifikata za određeni rok, a naročito se moraju obezbediti dokazi o certifikatu u slučaju spora. Ovo zabeležavanje *(recording)* može da bude u elektronskoj formi. Certifikaciono telo mora biti spremno da u svako doba objavi sve dostupne informacije koje se tiču korišćenih postupaka i primenjene prakse, kao ugovora i uslova koji se odnose na pitanje odgovornosti za pokretanje tužbe za slučaj spora. Sve ove informacije moraju biti izražene na lak, jednostavan i pristupačan način.

Certifikaciona tela izdaju certifikat kojim se potvrđuje da je certifikaciono telo poštovalo pravila koja se tiču njegovog rada (profesionlna odgovornost); da prema znanju tog tela ne postoje materijalne činjenice koje su u certifikatu izostavljene koje bi mogle negativno da utiču na pouzdanost informacija sadržanih u certifikatu. Pored ovih osnovnih podataka u certifikat se unose i podaci o činjenici da su javni i privatni ključevi "upareni" (da predstavljaju *functioning key pair)*, da je u vreme izdavanja certifikata privatni ključ pripadao potpisniku (subjektu, licu) koji je identifikovan u

[10] U svetu ne postoji saglasnost o tome kako bi ovo telo trebalo da se zove. U zemljama Latinske Amerike, na primer, u kojima je izuzetno važna uloga javnog beležnika, smatra se da se upravo njima treba poveriti uloga izdavanja certifikata. Čak su dobili naziv *Cyber Notaries*, dok se u nacrtu *Međunarodnih jednobraznih pravila UNCITRAL*-a nazivaju davaoci certifikacione usluge, a Direktiva EU o elektronskim potpisima ova tela naziva provajderima-certifikacione-usluge. Nije zauzet jedinstven stav ni u pogledu nadležnosti i odgovornosti ovih tela. Ono što je u ovom trenutku izvesno, to je da odluku o osnivanju i radu ovih organa donose nacionalne države, što je logično jer jednoobrazna pravila u ovom pogledu ne bi bila moguća.

certifikatu, kao i da privatni ključ odgovara javnom ključu navedenom u certifikatu.

II Direktiva EU o elektronskim potpisima

1. Razlozi za usvajanje Direktive

U preambuli Direktive[11] se navodi da su elektronske komunikacije i trgovina nametnuli potrebu donošenja pravila o elektronskih potpisima i sličnim uslugama čime se omogućava utvrđivanje verodostojnosti podataka. Različita pravila u odnosu na priznavanje elektronskih potpisa i ovlašćenja certifikacionih tela država članica mogu da predstavljaju značajnu prepreku za korišćenje elektronskih komunikacija i elektronske trgvine. S druge strane, jasni okviri Zajednice u vezi sa uslovima koji se primenjuju na elektronske potpise znače jačanje poverenja u opšte prihvatanja novih tehnologija. Zakonodavstva država članica ne mogu ni na koji način da ometaju slobodnu razmenu robe i usluga na unutrašnjem tržištu.

Unutrašnje tržište obezbeđuje slobodno kretanje lica i s tim u vezi građani i stanovnici Evropske unije u mnogo većoj meri su prinuđeni da se obraćaju vlastima država članica koje nisu one u kojoj oni borave; elektronska komunikacija u tom pogledu pruža im velike mogućnosti da na lak i jednostavan način obave usluge, što je za njih od ogromnog značaja. Izuzetno brz tehnološki razvoj i globalni karakter Internet-a zahtevaju pristup koji je otvoren za razne tehnologije i usluge koj su u stanju da utvrde verodostojnost elektronskih podataka.

Prema Direktivi certifikacione usluge mogu da pružaju javna ili privatna lica odn. pravna ili fizička lica pod uslovom da ispunjavaju uslove koje zahteva domaće pravo. Da li će država članica da obezbedi nadzor nad radom kompanija kojima je data dozvola da obavljaju certifikacione usluge u skladu sa odredbama navedenim u Direktivi, ne sprečava privatni sektor da

[11] Tekst Direktive objavljen u *Official Journal,* L 13/12 19.01.2000.

obezbedi ovaj nazor. Direktiva ne zahteva od provajdera-certifikacionih-usluga da se podvrgnu nadzoru od strane bilo kog ovlašćenog organa. Bitno je podvući da se Direktiva bazira na dobrovoljnoj osnovi i da se na učesnike primenjuju pravila privatnog (obligacionog) prava. Ukoliko se strane slože da svoje poslovanje obavljaju elektronski u smislu odredbi domaćeg prava, onda tu njihovu volju moraju da poštuju sve države članice i elektronski potpisi na tako zaključenim poslovima imaju dokaznu snagu pred sudovima svih država članica.

Za organe Evropske unije je bitno da se ovom Direktivom stvori jedan koherentni pravni okviri na teritoriji cele Zajednice, pri čemu se ne dira u pravo svake države da ima posebna pravila za svojeručne potpise na papirnim dokumentima. Bitno je da se ostvari jednoobrazna primena obezbeđenih (pojačanih) potpisa. S tim u vezi smatra se da pojačani i overeni potpisi imaju, u pogledu pravne snage i valjanosti dokaza istu snagu kao svojeručno dati potpisi.

Da bi se doprinelo opštem prihvatanju metoda koji se primenjuju radi utvrđivanja verodostojnosti, stav Zajednice je da se elektronski potpisi u svim državama članicama moraju izjednačiti sa svojeručnim potpisima i da takvi potpisi mogu da se koriste kao dokazi u svim državama članicama. Pravno priznanje elektronskih potpisa treba da se zasniva na objektivnim kriterijumima, a ne treba da se vezuje za certifikate. Drugim rečima, Direktiva ne želi da se suprotstavlja domaćem pravu u slučaju da to pravo ima odredbe koje se u ovom pogledu razlikuju od onih koje sadrži Direktiva. Ovo stoga što se odgovornost certifikacionog tela procenjuje prema domaćem pravu u zemlji u kojoj je dobilo ovlašćenje za vršenje takvih usluga.

Da bi bila u toku sa brzim promenama koje se u ovoj oblasti odvijaju, Direktiva predviđa obavezu za Komisiju da dve godine posle primene Direktive u praksi, proveri da li nove tehnologije koje se u praksi primenjuju ili izmene pravnih propisa predstavljaju prepreku za slobodno odvijanje trgovinske razmene između država članica.

2. Pristup tržištu

U Direktivi se navodi da države članice neće donositi odredbe prema kojima bi certifikacione usluge bile podložne prethodnoj autorizaciji. Države članice mogu, s druge strane, da donesu odredbe po kojima će uslove akreditacije da podignu na viši stepen. Međutim, svi ti uslovi, navodi se u Direktivi, moraju biti "objektivni transparentni i nediskriminatorski". Državama članica se zabranjuje da ograniče broj akreditovanih tela za pružanje certifikacionih usluga. Važno je istaći da se Direktivom predviđa da države članice obezbede "osnivanje odgovarajućeg sistema koji će omogućiti nadzor" nad radom tela koja su osnovana na teritoriji države članice sa pravom da izdaju kvalifikovane certifikate za javnost. U Direktivi su u posebnom Dodatku navedeni vrlo detaljni uslovi koje moraju da ispune pravna ili fizička lica koja žele da se bave ovom vrstom aktivnosti. Ti uslovi su vrlo rigorozni i mogu da ih ispune zaista samo visoko kvalifikovana lica, jer se jedino time obezbeđuje sigurnost elektronskih potpisa i elektronske trgovine uopšte. Navodi se da Komisija može u skladu sa određenim postupkom objaviti referentne brojeve opšte priznatih standarda za proizvode certifikacionih tela.

Direktivom se predviđa da se u cilju poštovanja principa unutrašnjeg tržišta države članice obavezuju da će primenjivati odredbe koje se donesu u skladu sa Direktivom. Navodi se, takođe, da države članice "ne mogu da ograniče odredbe o uslugama certifikacije koje potiču iz druge države članice u oblastima na koje se ova Direktiva odnosi".

3. Pravna dejstva elektronskih potpisa

Direktivom se izričito predviđa da se elektronski potpisi koji se baziraju na kvalifikovanom certifikatu sačinjenom na osnovu sredstva-osiguranog-potpisa[12] izjednačavaju sa svojeručnim potpisom koji se baziraju

[12] Prema definiciji "bezbedno-sredstvo-stvaranja potpisa" znači sredstvo stvaranja potpisa koji je sačinjen u skladu sa zahtevima navedenim u Dodatku III. U tom Dodatku se navode sledeći uslovi: generisanje potpisa može da se pojavi samo jednom jer se time razumno obezbeđuje njegova tajnost; ne mogu se isporučiti sa razumnom sigurnošću jer je potpis

na papirima i da su dopušteni kao dokazi u pravnim postupcima[13]. Isto tako se podvlači da elektronski potpisi koji su u skladu sa Direktivom mogu slobodno da cirkulišu na internom tržištu.

4. Odgovornost

Nema sumnje da je pitanje odgovornosti centralno pravno pitanje, pa nije neobično što se našlo i u Direktivi EU kojim se regulišu elektronski potpisi i rad certifikacionih tela. U stvari, Direktivom se reguliše odgovornost certifikacionog tela i navodi da takvo telo (davalac certifikacione usluge) odgovara "za štetu koje bi imalo bilo koje pravno ili fizičko lice koje bi se razumno oslonilo na certifikat". Drugim rečima, treća lica u svakom slučaju mogu da se oslone na certifikat i podatke sadržane u njemu. Postoje brojni uslovi koji se zahtevaju u pogledu odgovornosti a odnose se na tačnost svih informacija u vreme izdavanja certifikata, potpisa kao i metoda kojim je utvrđen osigurani potpis[14]. S ovim u vezi značajno je dodati da se u nacrtu Jednoobraznih pravila UNCITRAL-a dodaje da bi u certifikat trebalo da se unesu i podaci o činjenici da su javni i privatni ključevi "upareni" (da predstavljaju *functional key pair)*, da je u vreme izdavanja certifikata privatni ključ pripadao potpisniku (subjektu, licu) koje je navedeno u certifikatu.

U vezi sa isključenjem ili ograničenjem odgovornosti certifikacionog tela u praksi se postavilo pitanje pod kojim uslovima bi to bilo moguće. Iako se o ovom pitanju vode diskusije, opšti stav je da certifikaciono telo ne bi

---

zaštićen protiv zloupotreba korišćenjem tekuće postojeće tehnologije; stvaranje potpisa podataka za generisanje potpisa mogu istinski da budu zaštićeni protiv korišćenja od strane drugih.

[13] Ovaj stav je u saglasnosti sa *Model zakonom UNCITRAL-a o elektonskoj trgovini* kojim se predviđa dopuštenost i dokazna snaga poruka. S tim u vezi navodi se da "u bilo kojim pravnim postupcima, ništa u vezi sa primenom pravila postupka se neće primeniti što bi značilo negiranje dopuštenosti poruke kao dokaza".

[14] U nacrtu *Jednobraznih pravila UNCITRAL-a o elektronskim potpisima* navodi se još da certifikaciono telo izdavanjem certifikata tvrdi da "ne postoje materijalne činjenice koje su u certifikatu izostavljene koje bi mogle negativno da utiču na pouzdanost informacija sadržanih u certifikatu kao i da je certifikaciono telo dalo izjavu o certifikacionoj praksi (*Certification Practice Statement-CPS).*

moglo da se oslobodi svoje odgovornosti ako bi to bilo suviše nekorektno *(grossly unfair)*, uzimajući u obzir cilj ugovora. Direktiva ne reguliše pitanje opoziva, suspenzije i registrovanja certifikata, smatrajući da je to u nadležnosti država članica. Na ovom mestu, ipak, treba napomenuti da je od značaja uspostavljanje i uredno vođenje Regtra certifikata (*Regiter of certificates)* koji predstavlja javnu ispravu, jer se u njemu nalaze svi podaci relevantni za certifikat (da li je važeći, opozvan, suspendovan). Od naročitog značaja je činjenica da li je certifikat opozvan, jer se time štiti javnost od zloupotreba i obezbeđuje poverenje u rad certifikacionih tela.

Kad je reč o odgovornosti certifikacionih tela prema trećim licima Direktiva navodi da su ta tela odgovorna "za štetu koju je pretrpelo bilo koje pravno ili fizičko lice koje se razumno oslanjalo na certifikat zbog propusta da se registruje opoziv certifikata". Certifikaciono telo se može osloboditi odgovornosti ako dokaže da je postupalo sa pažnjom koja se u radu takvih tela pretpostavlja. Od značaja je, takođe, navesti da Direktiva predviđa mogućnost da države članice donesu propise kojim se može predvideti ograničenje upotrebe tog certifikata, "pod uslovom da ograničenja mogu da prepoznaju treća lica".

U Direktivi se navodi da certifikaciono telo u certifikatu može označiti granicu vrednosti transakcije za koje se certifikat može koristiti "pod uslovom da je to ograničenje prepoznatljivo trećim stranama". Ugovorne strane se mogu dogovoriti o maksimalnom iznosu štete koju je certifikaciono telo dužno da plati za slučaj nastanka štete trećim licima u vezi sa certifikatom. Međutim, takva mogućnost postoji samo ako je odredba u tom smislu uneta u certifikat. U Direktivi se navodi da u tom slučaju provajder-certifikacione-usluge "neće odgovarati za štetu koja premašuje maksimalna ograničenja".

5. Međunarodni aspekti

Za dobro funkcionisanje unutrašnjeg tržišta Evropske unije od značaja je da se certifikati izdati u jednoj državi članici priznaju u svim drugim državama članicama Zajednice. Da bi se ovim pravom koristile države članice potrebno je da se dokaže da certifikaciono telo ispunjava

zahteve sadržane u Direktivi i pod uslovom da je akreditovano na osnovu "dobrovoljne akreditacione šeme koja je utvrđena u državi članici". Potrebno je, takođe, dokazati da certikaciono telo garantuje za certifikat i da je certifikat "priznat na osnovu bilateralnog ili multilateralnog sporazuma između Zajednice i trećih lica ili međunarodnih organizacija". Ukoliko bi neka preduzeća imala teškoće u vezi sa pristupom na tržišta trećih zemalja, "Komisija može podneti Savetu predlog za donošenje odgovarajućeg ovlašćenja u cilju pregovaranja o komparativnim pravima za preduzeća Zajednice u tim zemljama", o čemu Savet odlučuje kvalifikovanom većinom.

6.Zaštita podataka

U Direktivi se izričito predviđa da su certifikaciona tela dužna da vode računa o primeni Direktive[15] kojom se obezbeđuje zaštita pojedinaca u odnosu na obradu ličnih podataka prilikom slobodne razmene takvih podataka". Dalje se navodi da se podaci poverljive prirode mogu dobiti samo uz izričitu saglasnost lica (subjekta) od koga se traže i "samo koliko je neophodno za ciljeve izdavanja ili održavanja certifikata", što znači da se ovako dobijeni podaci ne mogu da koriste za bilo koju drugu svrhu bez izričite saglasnosti subjekta podataka". Direktivom se predviđa da certifikaciona tela mogu da prihvate pseudonim umesto pravog imena potpisnika.

7. Primena

Direktiva navodi (čl. 13) da su države članice dužne da svoje domaće propise usaglase sa odredbama Direktive najkasnije do 19. jula 2001. godine, o čemu su dužne da odmah obaveste Komisiju. Dalje se ističe da su države članice dužne da Komisiji dostave "tekst osnovnih odredbi domaćeg prava koje budu usvojile u oblasti na koju se odnosi ova Direktiva".

Kao što je napomenuto uz Direktivu su data četiri vrlo detaljna Dodatka koji se odnose na uslove za kvalifikovane certifikate (dodatak I),

[15] Direktiva 95/46/EC; *Official Journal*, L 281, 23.11.1995, p. 31.

uslove za certifikaciona tela, tj. provajdere-certifikacionih usluga koji izdaju kvalifikovane certifikate (dodatak II), zahteve u pogledu sredstava za stvaranje sigurnih potpisa (dodatak III) i preporuke za proveru sigurnosnog potpisa (dodatak IV).

Možda je za svrhe ovog članka od posebnog značaja dodatak II kojim se određuju uslovi za pravna ili fizička lica koja se bave izdavanjem certifikata. Prema ovom dodatku koji sadži 12 opširnih odredbi da bi se jedno lice moglo baviti ovom vrstom delatnosti potrebno je da: demonstrira pouzdanost koja je neophodna za obezbeđenje certifikacionih usluga; obezbedi rad brzog i sigurnog Registra kao i sigurne i brze usluge opoziva; vreme i datum kad je certifikat izdat ili opozvan; zaposleni personal poseduje stručno znanje, iskustvo i kvalifikacije neophodne za usluge koje se daju a naročito "stručno znanje u pogledu tehnologije elektronskih potpisa i bliskost sa odgovarajućim bezbednim procedurama"; koristi pouzdane sisteme i proizvode koji su zaštićeni protiv izmena i obezbedi tehničku i kriptografsku zaštitu procesa koji se njima omogućavaju. Dalje se navodi da certifikaciono telo mora preduzeti mere protiv falsifikovanja i održavati dovoljne finansijske izvore da bi se poslovalo u skladu sa zahtevima koji su postavljeni u Direktivi, a naročito snositi rizik odgovornosti za štetu, što se može obezbediti pribavljanjem odgovarajućeg osiguranja.

Pre nego što stupi u ugovorni odnos sa licem koje zahteva certifikat kojim bi dokazao svoj elektronski potpis certifikaciono telo je dužno da obavesti to lice "o preciznim terminima i uslovima koji se tiču korišćenja certifikata, uključujući svako ograničenje njegovog korišćenja, postojanje dobrovoljne šeme akreditacije i procedura za žalbe i rešavanje sporova". Takva informacija mora biti pismena (iako može da se dostavi i elektronski), jasna i data na jeziku koji može da se razume. Relevantni delovi ove informacije "moraju takođe biti stavljeni na raspolaganje na zahtev trećih strana koja se oslanjaju na certifikat".

U vezi sa čuvanjem certifikata u poverljivom obliku u dodatku se na kraju navodi da se taj uslov postiže tako što: samo ovlašćena lica mogu da vrše upis izmene; informacija može da se proveri u pogledu autentičnosti; javno je moguće obezbediti da se certifikat vrati u prvobitni oblik u onim slučajevima kada je dobijena saglasnost nosioca certifikata i svaka tehnička

izmena kojom se usaglašavaju ovi zahtevi u pogledu sigurnosti su vidljivi za operatera[16].

Nema sumnje da su ovi dodatni uslovi jako značajni za uspešno funkcionisanje odredbi koji se tiču primene Direktive u praksi. Ukupno posmatrano zanimljivo je zaključiti na koji način su odvojena čisto pravna od tehničko-tehnoloških pitanja, kao i o tome da su oba ova pristupa od značaja kad je reč o primeni i uspešnom funkcionisanju elektronske trgovine.

Zaključne napomene

Kao što se iz napred navedene analize odredi Direktive o Zajednice o elektronskim potpisima usvojene krajem 1999. godine može zaključiti, cilj usvajanja je bio da se elektronski (digitalni) potpisi po svom pravnom dejstvu izjednače sa svojeručnim potpisima. Da bi se to postiglo bilo je neophodno usvojiti odredbe (koje velikim delom baziraju na Model zakonu UNCITRAL-a o elektronskoj trgovini od 1996) o osnivanju, radu i odgovornosti cetifikacionih tela. Prema Direktivi certifikaciona tela mogu biti pravna ili fizička lica koja ispunjavaju dosta rigorozne uslove postavljene u dodaku I koji je naveden kao sastavni deo Direktive.

Drugi važan razlog za usvajanje Direktive je da se njome potvrdi i podstakne razvoj savremenih elektronskih tehnologija i obezbedi jednakost svih državljana i građana Zajednice bez obzira u kojoj državi članici se nalaze, čime se obezbeđuje jedinstvo evropskog tržišta. Odredba navedena na kraju Direktive o obavezi Komisije (i posebno osnovanog Komiteta za elektronske potpise) o praćenju razvoja elektronskih tehnologija i potrebi usaglašavanja, odn. revizije propisa je svakako od velikog značaja. Ova misao je decidirano formulisana u čl. 1. Direktive u kome se navodi da je "cilj Direktive da olakša korišćenje elektronskih potpisa i da doprinese njihovom pravnom priznanju". Dalje se dodaje da se time "stvara pravni okvir za elektronske potpise i određene usluge izdavanja certifikata u cilju obezbeđenja unutrašnjeg tržišta". Analizom ove Direktive može se zaključiti

[16] Za bliže podatke o uslovima za zahteve u pogledu sredstava za stvaranje sigurnih potpisa i preporuke za proveru sigurnog potpisa, vidi dodatake III i IV koji su dati uz Direktivu.

da se njome jedinstveno regulišu određena osnovna pitanja od značaja za elektronske potpise, a da se veliki deo propisa koji će omogućiti uspešno funkcionisanje Direktive prepušta državama članicama.

Jelena VILUS, Ph. D.

EUROPEAN UNION AND ELECTRONIC LAW
On Occasion of the Community Directive
of Electronic Signatures

SUMMARY

The purpose of thee adoption of the Community Directive of electronic signatures, adopted at the end of 1999 was to equalize the legal effect of electronic (digital) signatures with personal ones. To achieve this, it was necessary to adopt regulations (mostly based on the Model Act of UNCITRAL on electronic trade, of 1999) on foundation, work and responsibility of certification bodies. According to the Directive, certification bodies can be legal or physical persons which fulfill quite rigorous conditions, placed in the Appendix I, which is quoted as the integral part of the Directive.

The second important reason for the adoption of the Directive is to confirm and stimulate development of contemporary electronic technologies and to ensure the equality of all citizens and inhabitants of the Community no matter in which state they live, thus providing the unity of European market. The regulation quoted at the end of the Directive about the obligation of the Commission to follow the development of electronic technologies and the need for harmonization, i. e. the revision of regulations, is certainly of great importance. This intonation is decidedly formulated in the Article 1 of the Directive, where it is said that "the aim of the Directive is to make easier the use of electronic signatures and to contribute to their legal recognition". Further it is

added that in the way "the legal frame for electronic signatures and certain services of certificate issuing, in order to secure the internal market, has been made." By the analyses of this Directive, it can be concluded that certain basic questions are regulated by it, basic question that are of importance for electronic signatures, and that a large part of regulations that would enable successful functioning of the Directive, is left to the discretion of the Member States.