

*Dr Drago Lj. Divljak, redovni profesor
Univerzitet u Novom Sadu
Pravni fakultet u Novom Sadu
D.Divljak@pf.uns.ac.rs*

PRAVNO DEJSTVO ELEKTRONSKIH POTPISA U MEĐUNARODNOJ REGULATIVI I PRAVU SRBIJE*

Sažetak: *Pravno dejstva elektronskih potpisa, koje u sebi uključuje problem njegove punovažnosti i pravne snage je jedno od bitnih pitanja elektronske trgovine. U radu se analizira pristup ovom problemu u međunarodnoj regulativi i pravu Srbije, pri čemu se on sagledava i u kontekstu nekih nacionalnih komparativnih rešenja, a posebno u kontekstu prava EU.*

Na međunarodnom planu, pravna regulativa je konceptualno skoro identična i zasiva se na načelima pravnog priznanja, funkcionalne ekvivalencije i formalne tehnološke neutralnosti. Isto tako se široko prihvata pristup o korelaciji pravnog dejstva elektronskih ugovora i njihove pouzdanosti, s tim što se razlike postoje samo u pogledu preciziranja i nivoa odnosnih zahteva. I u pravu Srbije se prihvata navedeni koncept, s tim što se ono metodološki, strukturalno i sadržinski prevashodno naslanja na pravo EU. Posebno značajno je da i u našem pravu „pouzdanost i sigurnost“ postaje ključna determinanta pravnog dejstva elektronskih potpisa. Naime, najviša pravna snaga se daje kvalifikovanom elektronskom potpisu, koji dobija isto pravno dejstvo kao i svojeručni potpis, pa čak može da zameni overu svojeručnog potpisa, ali zauzvrat on mora zadovoljiti vrlo složen sistem striktnih zahteva koji svi zajedno trebaju da obezbede visok nivo njegove pouzdanosti.

Ključne reči: *pravno dejstvo, elektronski potpisi, međunarodna regulativa, pravo Srbije, pouzdanost, kvalifovani elektronski potpis.*

* Rad je nastao kao rezultat istraživanja na projektu: “Teorijski i praktični problemi stvaranja i primene prava (EU i Srbija)“, koji se realizuje na Pravnom fakultetu Univerziteta u Novom Sadu.

UVODNE NAPOMENE

Elektronski potpisi¹ su jedan od ključnih elemenata elektronske trgovine.² Njihova pojava je u praksi otvorila je mnoštvo tehničkih, funkcionalnih i sledstveno tome i pravnih pitanja, koji predstavljaju novi pravni izazov.³ U tom kontekstu, jedno od bitnih pitanja je pitanje pravnog dejstva elektronskih potpisa, koje u sebi uključuje problem njegove punovažnosti i pravne snage. Ono je kompleksnije prirode jer je povezano sa primenom bazičnih principa modernog prava elektronske trgovine kao što su princip nediskriminacije, tehnološke neutralnosti i funkcionalne ekvivalencije, ali i sa drugim važnim problemima u datoj oblasti, posebno pitanjem sigurnosti. U radu koji sledi razmotrićemo problem pravnog dejstva elektronskih potpisa u međunarodnoj regulativi i pravu Srbije, sagledavajući ga u kontekstu nekih nacionalnih komparativnih rešenja, a posebno u kontekstu prava EU, što je logično, s obzirom da se Srbija nalazi u procesu pridruživanja EU i da u njemu imamo obavezu prilagođavanja njenim pravnim pravilima.

1. PRAVNO DEJSTVO ELEKTRONSKIH POTPISA U MEĐUNARODNOJ REGULATIVI

S obzirom na karakter elektronskih komunikacija i interneta koji ne poznaju državne granice, nužno je bilo i u oblasti elektronskih potpisa doći do značajnog nivoa konvergencije nacionalnih pravnih sistema⁴ putem procesa harmonizacije⁵ i unifikacije pravnih pravila. U kreiranju ovakvog pravnog okvira koji prepoznaje i olakšava prekogranične elektronske transakcije,⁶ od ključne važnosti je aktivnost

¹ Ne postoji univerzalno prihvaćena defincija elektronskog potpisa, ni u teoriji, niti u pravnoj regulativi. Upor: Stephen E. Blythe, „Digital signature law of the United Nations, European Union, United Kingdom and United States: Promotion of growth in E-commerce with enhanced security,” *Richmond Journal of Law & Technology*, 11.2/2005, 3; Jonathan E. Stern, „The electronic signatures in global and national commerce act,” *Berk. Tech. LJ* 16, 2001, 397; Faye Fangfei Wang, *Law of electronic commercial transactions: Contemporary issues in the EU, US and China*, Routledge 2014, 79; Sieg Eiselen, „Fiddling with the ECT act—Electronic signatures,” *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad*, 17.6./2014, 2806.

² Upor: Kalama M., Lui-Kwan, „Recent developments in digital signature legislation and electronic commerce,” *Berkeley Tech. LJ* 14/1999, 465.

³ Upor: Jeffrey B. Ritter, Judith Y. Gliniecki, „International Electronic Commerce and Administrative Law: The need for harmonized national reforms,” *Harv. JL & Tech.*, 6/1992, 263.

⁴ Upor: Justin Hughes, „The Internet and the persistence of law,” *BCL Rev.*, 44 /2002, 361.

⁵ O procesu harmonizacije u oblasti elektronske trgovine, šire: Drago Divljak, „Harmonizacija pravila o elektronskoj trgovini i pravo Srbije“, *Zbornik radova Pravnog fakulteta u Novom Sadu (Zbornik radova PFNS)*, 3/2018, 909-924.

⁶ Upor: J. E. Stern, 391.

UNCITRAL-a,⁷ koji u okviru vrlo osobenog pravnog izazova interneta,⁸ problemu elektronske trgovine, pa time i elektronskih potpisa prilazi simbiotski, gde pravna regulativa na različitim nivoima zajedno nastaje i pod međusobnim je uticajem.⁹ U tom pogledu on je izradio dva Model zakona i jedna konvenciju. To su Model zakon o elektronskoj trgovini iz 1996. godine, Model zakon o elektronskim potpisima iz 2001. godine i Konvencija UN o upotrebi elektronskih komunikacija u međunarodnim ugovorima iz 2005. godine.

1.1. Model zakona o elektronskoj trgovini

Prvi osnov harmonizacije¹⁰ u oblasti elektronskih komunikacija je Model zakon o elektronskoj trgovini.¹¹ On, iako efektivno vrlo značajan za oblast elektronske trgovine,¹² pitanju elektronskih potpisa prilazi segmentirano. U skladu sa opštom namerom da ukloni formalne prepreke elektronskoj trgovini, on posebno reguliše situacije u kojima bi se koristila sredstva elektronske komunikacije umesto tradicionalnih, zasnovanih na papiru.¹³ U tom okviru regulisani su i elektronski potpisi i to u čl. 7., u kojem se utvrđuje opseg primene elektronskih potpisa u situacijama kada se zakonom zahteva postojanje potpisa ili se zakonom jednostavno predviđaju posledice za njegovo nepostajanje.¹⁴

Iz navedenog sadržaja ovog člana, vidljivo je da se u Model zakonu generalno polazi od toga da su svojeručni potpisi i potpisi u elektronskom obliku različite prirode i nijedan ne može automatski obavljati iste funkcije kao drugi, niti se pravno mogu poistovetiti. Stoga ovaj Model zakon nastoji istražiti funkcije koje potpis u tradicionalnom obliku obavlja i zatim određuje posebne kriterijume koji

⁷ Međunarodna trgovinska komora (ICC) izradila je dokument pod nazivom General Usage for International Digitally Ensured Commerce' (GUIDEC). On je usmeren ka regulisanju pitanja alokacije rizika i odgovornosti između učesnika.

⁸ O problemu konceptualnog pristupa pravnom regulisanju interneta i novih tehnologija, šire: J. Hughes, 360; Amelia H. Boss, "Searching for security in the law of electronic commerce," *Nova L. Rev.* 23/1998, 588 i dalje; Sanja Radovanović, „Zaključivanje ugovora putem Interneta-ide li pravo u korak sa vremenom“, *Zbornik radova PFNS*, 3./2008, 279-291.

⁹ Šire: Amelia H. Boss, „Electronic Commerce and the Symbiotic Relationship Between International and Domestic Law Reform,“ *Tul. L. Rev.* 72 /1997, 684.

¹⁰ UNCITRAL se odlučio za model zakon, a ne za konvenciju, shvatajući da su razlike u nacionalnim pravnim sistemima bile prevelike da bi u tom momentu bilo realnih šansi za usvajanje konvencije u ovoj blasti. Upor: S. Eiselen, 2807.

¹¹ Model Law on Electronic Commerce with Guide to Enactment, with additional article 5 bis adiptet in 1998, UNCITRAL, 1996, http://www.uncitral.org/pdf/english/texts/electcom/V1504118_Ebook.pdf, avgust 2019.

¹² Model zakona o elektronskoj trgovini je široko prihvaćen, jer ga preko 60 država širom sveta koristilo kao polaznu tačku za svoje nacionalne zakone.

¹³ Radi se o pismenom obliku informacije, potpisa i originala informacija koji su regulisani u čl. 6., 7. i 8. Model zakona o elektronskoj trgovini iz 2001. godine.

¹⁴ Čl. 7. st. 2. Model zakona o elektronskoj trgovini iz 2001. godine.

će, ako su ispunjeni, omogućiti elektronskim potpisima da datu svrhu i funkciju obavljaju na isti način kao i tradicionalni svojeručni potpisi.¹⁵ Ovakav pristup kojim se posrednim putem utvrđuje pravno dejstvo elektronskih, se najčešće označava, kao pristup ili princip funkcionalne ekvivalencije, pri čemu se u pogledu opsega pravnog dejstva elektronskih potpisa, krajnja odluka ipak prepušta nacionalnim zakonodavcima.¹⁶

U skladu s navedenim principom funkcionalne ekvivalencije, u Model zakonu o elektronskoj trgovini elektronski potpisi se u pogledu pravnog dejstva izjednačavaju sa svojeručnim potpisima, pod uslovom da su ispunjena dva uslova u vezi sa elektronskim prenosom podataka. Prvi uslov je ispunjen ako se metoda koristi da identifikuje potpisnika poruke i njegovu saglasnost sa sadržajem poruke, čime se pravno dejstvo elektronskog potpisa veže za dve primarne funkcije svojeručnog potpisa, a to su: identifikacija potpisnika poruke i dokaz da je on odobrio sadržaj dokumenta.¹⁷ Drugi uslov sadrži obavezu da metod bude pouzdan u meri koji se smatra odgovarajućim za svrhu za koju je poruka generisana ili prenesena u vezi sa svim okolnostima, uključujući i svaki relevantni sporazum.¹⁸

Može se zaključiti da se ovim Model zakonom kreiraju opšte pretpostavke i standardi u pogledu bezbednosti i verodostojnosti elektronskog potpisa, bez posebnog preciziranja. Ovakav koncept, koji je bio osnova i za druge regulatorne sisteme,¹⁹ ne uključuje dodatne sigurnosne zahteve i procedure, što se u jednu ruku može oceniti i logičnim, jer ni kod svojeručnog potpisa one nisu posebno specificirane. Međutim, u cilju lakše primene ovih pravila, ipak su u Vodiču Model zakona o elektronskoj trgovini instruktivno naznačeni brojni pravni, tehnički i komercijalni faktori koje treba uzeti u obzir pri određivanju da li je korišćena metoda dovoljno pouzdana i primerena.²⁰

¹⁵ Upor: Stephen Mason, *Electronic signatures in law*, Cambridge 2012, 96; J. Hughes, 388.

¹⁶ Tako se u Par. 76. Vodiča za primenu Model zakona o elektronskoj trgovini, koji prati ga i pruža dodatne informacije i objašnjenja kako bi se pomoglo državama u pripremi sopstvenih relevantnih zakona, napominje da kada se potpiše elektronski dokument pomoću funkcionalnog ekvivalenta svojeručnog potpisa, to ne znači automatski da su elektronski podaci pravno validni. Konačnu reč, prema konceptu ovog Model zakona daju zakoni doneti na nacionalnom nivou koji regulišu dato pitanje.

¹⁷ O mogućim funkcijama elektronskog potpisa: S. Mason, 98; Kalama M., Lui-Kwan, 460.

¹⁸ Upor: S. Mason, 99.

¹⁹ Ovaj model je sledila *Evropska unija, ali i Singapur, Bermudi i sl. Ibid*, 156.

²⁰ Tako su navedeni :1) sofisticiranost opreme koju koristi svaka strana; (2) priroda njihove trgovinske delatnosti; (3) učestalost komercijalnih transakcija između strana; (4) vrsta i veličina transakcije; (5) funkciju zahteva za potpisom u datom zakonu i regularno okruženje; (6) sposobnost komunikacionih sistema; (7) poštovanje postupaka autentifikacije utvrđenih u posrednici; (8) opseg postupaka autentifikacije koji je bilo kome dostupan posrednik; (9) poštovanje trgovinskih običaja i prakse; (10) postojanje mehanizama za osiguranje osiguranja protiv neovlašćene poruke; (11) važnost i vrednost informacija sadržanih u data poruka; (12) dostupnost alternativnih metoda identifikacije i troškovi implementacije; (13) stepen prihvatanja ili neprihvatanja metode identifi-

Bitna karakteristika ovako koncipiranog Model zakona o elektronskoj trgovini je i da on ne predviđa, niti zahteva korišćenje bilo koje specifične vrste tehnologije da bi se elektronski potpisi u svom pravnom dejstvu načelno izjednačili sa svojeručnim potpisima.²¹ Na ovaj način se nominalno prihvata princip tehnološke neutralnosti, koji obavezuje na usvajanje pravnih pravila koje su neutralne u odnosu na korišćenu tehnologiju.²²

1.2. Model zakon o o elektronskim potpisima

Model zakona o elektronskim potpisima iz 2001. godine²³ je saglasno svom nazivu specijalistički usmeren ka oblasti elektronskih potpisa. Formalno gledano, pravno dejstvo elektronskih potpisa je regulisano prevashodno u čl. 6. i 7, ali i čl. 3. pri čemu se oni moraju tumačiti u kontekstu opšteg pojmovnog određenja elektronskih potpisa datog u čl. 2. ovog Modela.

U sadržinskom pogledu Model zakona o elektronskim potpisima bitno dopunjuje Model Zakona o elektronskoj trgovini²⁴ na način da se zadržavaju njegovi osnovni principi i zahtevi, uz dodatne iskorake u nekim segmentima. Tako se za specifično delovanje elektronskog potpisa isto koristi princip funkcionalne ekvivalencije za situacije kada se zakonom zahteva potpis nekog lica, odnosno jednostavno propisuju posledice nepostojanja potpisa. U skladu sa datim principom, Model zakonom o o elektronskim potpisima se predviđa da se tada umesto svojeručnog može koristiti elektronski potpis sa istovetnim pravnim dejstvom, uz ispunjenje utvrđenih preduslova i zahteva. Oni ne proizilaze samo iz čl. 6 Modela zakona, već i iz čl. 2 kojim se definiše elektronski potpis.

Ukoliko se integralno posmatraju navedene relevantne odredbe, onda se može zaključiti da su navedeni zahtevi identični se zahtevima Model zakona o elektronskoj trgovini.²⁵ Međutim, oni se Model zakonom o elektronskim potpisima dodatno preciziraju. Tako se elektronski potpisi smatraju pouzdanim ako ispunjavaju sledeće uslove: a) ako su podaci za generisanje potpisa povezani samo sa potpisnikom a ne sa drugim licima, b) ako su podaci za generisanje potpisa u vreme potpisivanja bili pod kontrolom potpisnika i nijednog drugog lica; c) ako je svaka promena u elektronskom potpisu nakon potpisivanja uočljiva; i d) ako je

kacija u relevantnoj industriji ili oblasti u oba vremena metoda je dogovorena i vreme kada je data poruka saopštena; i (14) bilo koji drugi relevantni faktor.

²¹ Upor: S. E. Blythe, 1.

²² Oni imaju za cilj da obezbede isti pravni tretman elektronskom potpisu nezavisno od tehnologije koji se koriste u njegovom nastanku, odnosno da zabrani diskriminaciju ili favorizovanje potpisa samo po navedenom osnovu.

²³ Model Law on Electronic Signatures with Guide to Enactment 2001, UNICITRAL, <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/ml-elecsig-e.pdf>, avgust 2019.

²⁴ Upor: S. Eiselen, 2809.

²⁵ Upor: S. Eiselen, 2809.

cilj pravnog zahteva da potpis obezbedi sigurnost za integritet informacija na koje se odnosi, svaka njihova izmena nakon potpisivanja mora biti uočljiva.²⁶

Napred navedeni zahtevi imali su za cilj da objektivizuju kriterijume tehničke pouzdanosti elektronskih potpisa klasifikujući ih u grupe sa različitom usmerenošću. Jedni se fokusiraju na karakteristike podataka za kreiranje potpisa koji moraju biti povezani sa potpisnikom a, drugi se bave okolnostima u kojima se koriste podaci za kreiranje potpisa, treći i četvrti su usmereni ka pitanjima integriteta elektronskog potpisa i integriteta informacija na koje se elektronski potpis odnosi.²⁷ Svi zajedno oni čine specifični „test pouzdanosti“, čije se postojanje u delu teorije problematizuje.²⁸

Navedeni zahtevi u pogledu pouzdanosti elektronskog potpisa sadržani u Model zakonu o elektronskim potpisima imaju za cilj uspostavljanje minimalnih pretpostavljenih, a ne maksimalnih standarda i imaju karakter smernica, jer se njihova stvarna konkretizacija može izvršiti eventualnim imperativnim zakonskim odredbama, ali i ugovorima između stranaka. Naime u skadu sa čl. 7 ovog Model zakona, svako lice, odnosno nadležni organ može odrediti koji tip elektronskih potpisa će zadovoljiti napred navedene zahteve iz člana 6,²⁹ pri čemu to, ipak mora biti u skladu sa priznatim međunarodnim standardima.³⁰ Isto tako, i učesnici u elektronskoj komunikaciji, mogu koristeći se načelom autonomije volje uspostaviti svoje kriterijume pouzdanosti, pod uslovom da ispunjavaju minimum navedenih zahteva,³¹ što takođe govori da su navedeni opšti uslovi pouzdanosti prilično fleksibilni i podložni primeni principu autonomije volje.

Sa aspekta pravnog dejstva elektronskih potpisa relevantan je i čl. 3. Model zakona o elektronskim potpisima kojim se formalno potvrđuje važenje principa tehnološke neutralnosti u ovoj oblasti. U ovom članu je utvrđeno da ništa u ovom Model zakonu, osim člana 5., se ne može primeniti tako da isključi, ograniči ili liši pravnog dejstva bilo koji način kreiranja elektronskog potpisa koji ispunjava njegove zahteve. S druge strane je vidljivo da zahtevi za pouzdanošću mogu implicitno pogodovati korišćenju nekih oblika i tehnologija kreiranja elektronskog potpisa.³² Međutim, ključno je da se time ne isključuju druge vrste tehnologija koje bi mogle da ispune date zahteve pouzdanosti, pri čemu je uloga pravnih pravila samo da ponudi predvidljivost u definisanju tih zahteva.³³

²⁶ Čl. 6. st 2. Model zakona o elektronskim potpisima iz 2001. godine

²⁷ Upor: S. Eiselen, 2810.

²⁸ Upor: S. Mason, 114.

²⁹ Upor: S. Eiselen, 2809.

³⁰ Čl. 7. st 2. Model zakona o elektronskim potpisima iz 2001.godine.

³¹ Upor: S. Eiselen, 2811.

³² Upor: S. E. Blythe, (2005), 6.

³³ *Ibid.*

1.3. Konvencija UN o upotrebi elektronskih komunikacija u međunarodnim ugovorima

Konvencija UN o upotrebi elektronskih komunikacija u međunarodnim ugovorima iz 2005. godine³⁴ doneta je s ciljem da reguliše upotrebu elektronskih komunikacija u vezi sa zaključenjem ili izvršenjem ugovora između strana koje imaju svoja sedišta u različitim državama.³⁵ U pogledu pravnog dejstva elektronskih potpisa je relevantan čl. 9 st. 3. Konvencije, što sugerise da se UNCITRAL odlučio da u datoj Konvenciji generalno pridržava pristupa minimalne regulacije datog u Model zakonu o elektronskim komunikacijama,³⁶ kao i njegovih sadržinskih odrednica. Tako, isto uređuje pitanje korišćenja potpisa, tj. za situacije kada zakon nalaže postojanje potpisa ili se eventualno predviđaju pravne posledice njegovog odsustva, i to na funkcionalno ekvivalentnom principu. Vidljivo je da iskazani pristup omogućava da se koristi bilo koji oblik elektronskog potpisa,³⁷ što sugerise da je načelno prihvaćen i princip tehnološke neutralnosti. Isto tako, Konvencijom se slično Model zakonu, pouzdanost utvrđuje kao bitan element za definisanje pravne snage elektronskog potpisa.

Međutim, iako slični, pristup iskazan u Konvenciji o upotrebi elektronskih komunikacija u međunarodnim ugovorima u odnosu na Model zakon o elektronskoj trgovini, svakako nije identičan, jer se drugačijim formulacijama i nekim dopunskim elementima u konvenciji ipak menja naglasak poređenju sa odredbama u Model zakonima. Prva izmena se odnosi na uslove funkcionalne ekvivalencije. Naime u Konvenciji je utvrđeno da elektronski potpis može zameniti svojeručni potpis, ako se koristi metoda za identifikaciju stranke i za ukazivanja na njenu nameru u pogledu informacija sadržanih u elektronskoj komunikaciji. Uključivanjem elementa „namere“ umesto „saglasnosti“ u pogledu informacija sadržanih u elektronskoj komunikaciji, izvršen je otklon od analognih odredbi u odnosu na oba Model zakona.³⁸ To je značajan iskorak, jer se u Konvenciji naglasak daje na identitetu stranke i njenoj nameri u pogledu elektronskih informacija, dok je u Model zakonima u prvom planu „integritet informacija“ u elektronskoj komunikaciji.

³⁴ Convention on the Use of Electronic Communications in International Contracts – CUE-CIC, UNCITRAL, 2005, https://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf, avgust 2019.

³⁵ Konvencija je stupila na snagu 2013. godine i ratifikovao je manji broj zemalja. Međutim, njen značaj se ne iscrpljuje samo u tome, jer je ona u nekim pravima bila uzor u koncipiranju nacionalnih pravila kao što je slučaj sa pravom Singapura. Vid: Eliza Mik, „Evaluating the Impact of the Un Convention on the Use of Electronic Communications in International Contracts on Domestic Contract Law-The Singapore Example,“ *Y.B. Int'l L. & Aff.* 43, 2010, 44.

³⁶ Upor: S. Eiselen, 2812.

³⁷ Upor: S. Mason, 111.

³⁸ Upor: F. F. Wang, 84.

Poseban naglasak se u Konvenciji o upotrebi elektronskih komunikacija u međunarodnim ugovorima daje elementu pouzdanosti elektronskih potpisa, pa stoga u tom pogledu je došlo da najvećih izmena u odnosu na Model zakon o elektronskoj trgovini. Naime, u Konvenciji je preuzet uslov apstraktne pouzdanosti iz Model zakona o elektronskoj trgovini koji propisuje da metod mora biti pouzdan u meri koji se smatra odgovarajućom za svrhu za koju je poruka generisana ili prenesena u vezi sa svim okolnostima, uključujući i svaki relevantni sporazum. Međutim, novina je da se ostavlja mogućnost da se može dokazati da elektronski potpis ispunjava zahteve u pogledu pouzdanosti.³⁹ Stoga se može oceniti da se postojeći koncept pouzdanosti iz Model zakona o elektronskoj trgovini koji se može nazvati „teorijskom pouzdanošću“ u datoj Konvenciji nadograđuje elementom koji se može označiti kao „faktička pouzdanost.“

Navedeni iskoraci u Konvenciji o upotrebi elektronskih komunikacija u međunarodnim ugovorima u odnosu na oba Model zakona se svakako mogu pozitivno oceniti. Međutim, i pored pomaka u tom pogledu, predstavljeni koncept pouzdanosti elektronskih potpisa ostaje i dalje i nedovoljno konkretizovan što može biti njegov hendikep u praksi.⁴⁰ Na konceptualnom planu se kao njen veći nedostatak može navesti što i dalje primenom principa funkcionalne ekvivalencije rešava praktičan problem primene elektronskih potpisa, ali ne daje decidne odgovore o vezi njihovog pravnog važenja.⁴¹

2. PRAVNO DEJSTVO ELEKTRONSKIH POTPISA U PRAVU SRBIJE

Polazeći od toga da je “pravna nesigurnost antiteza jakih i efikasnih tržišta”,⁴² i nacionalnom nivou su zakonodavci morali pristupiti pravnoj regulaciji elektronskih potpisa. U kontekstu pravnog dejstva elektronskih potpisa, ključni korak je omogućavanje njihovog pravnog priznanja i punovažnosti, kojim se dozvoljava da se strane obavezuju ugovorom i putem elektronskog potpisa.⁴³ Ukoliko bi se elektronskim dokumentima uskratila mogućnost i elektronskog potpisivanja, oni bi morali dopunjeni papirnim zapisima sa svojeručnim potpisima, što nije samo skuplja, manje konkurentna, manje efikasna varijanta,⁴⁴ već i varijanta koja bi svojom komplikovanošću

³⁹ Upor: S. Eiselen, 2812.

⁴⁰ Upor: F. F. Wang, 87.

⁴¹ *Ibid*, 85.

⁴² Upor: J. E. Stern, 392.

⁴³ Upor: J. E. Stern, 397.

⁴⁴ Upor: Andrew Barofsky, „The European Commission’s Directive on Electronic Signatures: Technological Favoritism Towards Digital Signatures,“ *BC Int’l & Comp. L. Rev.* 24/2000, 146; Kalama M. Lui-Kwan, 470.

vanošću bitno usporila rast elektronske trgovine. Tek prizanjem punovažnosti elektronskih potpisa se dosledno efektuirao princip da se ugovori zaključeni i “potpisani” u potpunosti elektronskim sredstvima smatraju pravno validnim.⁴⁵

U pravu Srbije je prvi put Zakonom o elektronskim potpisima⁴⁶ iz 2004. godine učinjen najvažniji prvi iskorak u pogledu pravnog legitimisanja i priznanja elektronskih potpisa. Ovakvim normativnim pristupom ranije srpsko zakonodavstvo u opcionom obliku inkorporira elektronski potpis u naš pravni sistem, pri čemu parcijalno problematizira samo njegovu dokaznu snagu u zakonom uređenom postupku.⁴⁷

Zakon o elektronskim potpisima je zamenjen Zakonom o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju iz 2017. godine.⁴⁸ On se i po nazivu i sadržini naslanja na važeće pravo EU iz ove oblasti sadržano u Uredbi o elektronskoj identifikaciji i uslugama od poverenja za elektronske transakcije na unutrašnjem tržištu,⁴⁹ kojom se između ostalog, reguliše i elektronski potpis,⁵⁰ ali se delom zadržava i nadležnost država članica u ovoj oblasti.⁵¹

Donošenjem novog Zakona o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju je ne samo potvrđen, već i osnažen princip pravnog priznanja i punovažnosti elektronskih ugovora, u nešto drugačijoj stilizaciji nego u u važećoj uredbi EU.⁵² To je učinjeno izričitom formulacijom da se elektronskom potpisu ne može osporiti punovažnost ili dokazna snaga samo zbog toga što je u elektronskom obliku, ili što ne ispunjava uslo-

⁴⁵ Upor: A. Barofsky, 146.

⁴⁶ *Sl glasnik RS*, br. 135/2004.

⁴⁷ Naime, utvrđeno je da 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. Upor: Čl.6. Zakona o elektronskom potpisu.

⁴⁸ *Sl glasnik RS*, br. 94/2017.

⁴⁹ Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Ona je je derogirala Direktivu 1999/93/EC o elektronskom potpisu. Šire o njoj: Jos Dumortier, et al., *The legal and market aspects of electronic signatures*, Interdisciplinary centre for Law & Information Technology, Katholieke Universiteit Leuven, 2003; S. E. Blythe, 8.

⁵⁰ Čl. 1. Uredbe o elektronskoj identifikaciji i uslugama od poverenja za elektronske transakcije na unutrašnjem tržištu – UEDUPETUT.

⁵¹ Naime, u oblasti pravnog dejstva elektronskih potpisa je podeljena nadležnost između nivoa EU i država članica, pa je osim zahteva predviđenih u Uredbi prema kojima bi kvalifikovani elektronski potpis trebao imati jednako pravno dejstvo kao svojeručni potpis, sve ostalo potrebno je odrediti nacionalnim pravima država članica. Upor: Par. 49. Preambule UEDUPETUT.

⁵² Utvrđeno je da se elektronskom potpisu se kao dokazu u sudskim postupcima ne može uskratiti pravno dejstvo i dopuštenost samo zbog toga što je on u elektronskom obliku ili zbog toga što ne ispunjava sve zahteve za kvalifikovani elektronski potpis. Upor: Čl. 25 st. 1. UEDUPETUT.

ve za kvalifikovani elektronski potpis.⁵³ Međutim, navedeni načelni pristup o pravnom priznanju elektronskih potpisa u našem pravu nije apsolutan, jer se pravila o punovažnosti elektronskih potpisa ne primenjuju na pravne poslove za koje je posebnim zakonom predviđeno da se ne mogu preuzeti u elektronskoj formi, odnosno na ugovore i druge pravne poslove za koje je posebnim zakonom predviđeno da se sačinjavaju u formi overe potpisa, javno potvrđene (solemnizovane) isprave, ili u formi javnobeležničkog zapisa.⁵⁴ Ograničenje domašaja ovog principa je prisutno i u drugim pravima, ali ona često nisu identična.⁵⁵

Za detaljniju analizu pravnog dejstva elektronskih potpisa u pravu Srbije su posebno relevantne i odredbe čl. 2 i čl. 50 navedenog zakona. Tek njihovim kompletnim razmatranjem se može utvrditi pozicija našeg aktuelnog prava u datoj oblasti.

U čl. 2 koji se bavi definisanjenjm zakonskih kategorija, faktički elektronski potpisi se u našem pravu klasifikuju na tri kategorije i to elektronske potpise, napredne i kvalifikovane elektronske potpise. Taj pristup je u identičnom obliku preuzet iz prava EU.⁵⁶ Ukoliko navedenu klasifikaciju stavimo u kontekst već navedenog pravila da se elektronskom potpisu ne može osporiti punovažnost ili dokazna snaga samo zbog toga što je u elektronskom obliku ili što ne ispunjava uslove za kvalifikovani elektronski potpis, onda se logično mogu izvući određeni zaključci o bitnim odrednicima prava Srbije u pogledu pravnog dejstva elektronskih potpisa.

Prvo, svaki elektronski potpis, koji ispunjava generalne tehničke i funkcionalne uslove koje su date u pojmovnom određenju elektronskog potpisa⁵⁷ je punovažan i ima određenu dokaznu pravnu snagu i dejstvo. Ona je vezana za potvrđivanje integriteta podataka koji se potpisuju i identiteta potpisnika, ali će konkretnu sadržinu tog dejstva dati poslovna i sudska praksa u budućnosti. Činjenica da se u našem pravu na ovaj način daje dokazna snaga i potpisu koji ne ispunjava uslove za kvalifikovani elektronski potpis, ukazuje da ovakvi „nekvalifikovani“ potpisi nisu formalno ograničeni dodatnim kriterijumima sigurnosti, kao što je to učinjeno u nekim uporednim pravima.⁵⁸

⁵³ Čl.50. st. 1. Zakona o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju – ZEDEIUPEP.

⁵⁴ Čl. 50. st.3. i 4 ZEDEIUPEP.

⁵⁵ O pristupu kineskog prava: Stephen E.Blythe, „China’s New Electronic Signature Law and Certification Authority Regulations: A Catalyst for Dramatic Future Growth of E-Commerce,“ *Chi.-Kent J. Intell. Prop.*, 7/2007, 16.

⁵⁶ Upor: čl. 3. UEDUPETUT koji takođe predviđa tri vrste elektronskog potpisa:elektronski potpis, napredni elektronski potpis i kvalifikovani elektronski potpis.

⁵⁷ Elektronski potpis u našem pravu je generalno određen kao skup podataka u elektronskom obliku koji su pridruženi ili logički povezani sa drugim (potpisanim) podacima u elektronskim obliku tako da se elektronskim potpisom potvrđuje integritet tih podataka i identitet potpisnika. Čl. 2. st. 1.tač. 20. ZEDEIUPEP.

⁵⁸ Takav je slučaj u pravu Kine. Upor: S.E.Blythe, (2007), 29.

Drugo, svi elektronski potpisi nemaju isto pravno dejstvo. Za razliku od navedenih „običnih“ ili „nekvalifikovanih“ elektronskih potpisa koji imaju ograničenu pravnu snagu, najviša pravna snaga se daje kvalifikovanom potpisu, koji dobija isto pravno dejstvo kao i svojeručni potpis, pa čak može da zameni overu svojeručnog potpisa, ako je to propisano posebnim zakonom.⁵⁹ Na ovaj način se kreira diferencirana šema pravnog dejstva elektronskih potpisa, u kome postoje dve njihove pravne relevantne kategorije, gde je kvalifikovani elektronski potpis ključan i iz kojeg se izvodi kako pravno određenje, tako i pravno dejstvo „običnih“ ili „nekvalifikovanih“ elektronskih potpisa. Kreiranje ovakvog sistema pravnog dejstva elektronskih potpisa u našem pravu je zasnovano na pravu EU,⁶⁰ ali je generalno sličan sistem prisutan i u uporednom pravu, kao što je slučaj u Kini.⁶¹ Zbog sadržine pravnog dejstva koje ima kvalifikovani elektronski potpis, on iako dobrovoljan, ovakvim normativnim sistemom može postati ne samo poželjan, već i faktički skoro obavezan.⁶²

Treće, u pravu Srbije, punovažnost i pravno dejstvo elektronskih ugovora se formalno ne vezuje za konkretni oblik tehnologije koja se koristi za kreiranje elektronskog potpisa, što je česta praksa u uporednom pravu.⁶³ Time se ukazuje da je u našem pravu implicitno načelno prihvaćen princip tehnološke neutralnosti, za razliku od prava EU koje se eksplicitno poziva na njega,⁶⁴ što je svakako dobar pristup.⁶⁵ Međutim, striktnim zahtevima u vezi sigurnosti se faktički favorizuju digitalni potpisi⁶⁶ i drugi oblici elektronskog potpisa sa visokim performansama sigurnosti,⁶⁷ čime se naše pravo faktički približava hibridnom modelu regulacije koji se zasniva na ograničenoj tehnološkoj neutralnosti, sa svim svojim implikacijama.⁶⁸

⁵⁹ Čl.50. st. 2. i 3. ZEDEIUPEP.

⁶⁰ Čl. 25. st. 1. i 2. ZEDEIUPEP.

⁶¹ U Kini je je u tom smislu kreiran tzv. pouzdan elektronski potpis, koji bi mogao biti pandan našem kvalifikovanom elektronskom potpisu. O zahtevima koje moraju ispuniti takvi potpisi: S. E. Blythe. (2007), 16-17.

⁶² Upor: Stephen E. Blythe „Hong Kong Electronic Signature Law and Certification Authority Regulations: Promoting E-commerce in the World’s Most Wired City.“ *NCJL & Tech.* 7/2005, 9.

⁶³ Upor: F. F. Wang, 79.

⁶⁴ U par. 26.i 27. Preambule UEDUPETUT je navedeno da pravni učinci koji se njome osiguravaju trebali bi biti ostvarivi bilo kojim tehničkim sredstvima pod uslovom da su zahtevi ove Uredbe ispunjeni. U tom smislu se i pledira za otvorenost za tehnološke inovacije u ovoj oblasti.

⁶⁵ Upor: Kalama M. Lui-Kwan, 478.

⁶⁶ U teoriji se ponekad termin digitalni potpis koristi kao sinonim za elektronski potpis uopšte. Međutim, on je samo jedan podoblik elektronskih potpisa. Vid: E. Blythe, (2005), 3. Šire o digitalnim potpisima: F. F. Wang, 81.

⁶⁷ U teoriji je izvršena klasifikacija potpisa po osnovu stepena njihove bezbednosti na četiri grupe. Šire: S. E. Blythe, (2005), 3 i dalje.

⁶⁸ Ovakav model ima svoje dobre i loše strane. S jedne strane, ovakav pristup je samo prirodan otisak sličnih pristupa u oblasti potpisa uopšte, a s druge strane, hibridni modeli su fleksibilniji i prilagodljiviji novim tehnološkim dostignućima, uz postojanje bazične sigurnosti.

Četvrto, saglasno međunarodnoj regulativi, u pogledu koncipiranja pravnog dejstva elektronskih ugovora u našem pravu opravdano se polazi od faktora pouzdanosti i sigurnosti. Time “sigurnost” postaje ključna determinanta ne samo u kontekstu elektronske trgovine,⁶⁹ već i kontekstu dejstva elektronskih potpisa. Upravo je kreiranje napred navedenih kvalifikovanih elektronskih potpisa kao složene pravne konstrukcije rezultat takvog pristupa, iako je jasno da se “sigurnost” ne može „zakonski regulisati,“ jer je to kombinacija faktora koji nisu samo pravni, već u bitnoj meri i tehnološki i zavise od upotrebljene tehnologije u elektronskoj komunikaciji.⁷⁰ Pod kvalifikovanim elektronskim potpisom se u našem pravu podrazumeva napredni elektronski potpis koji je kreiran kvalifikovanim sredstvom za kreiranje elektronskog potpisa i koji se zasniva na kvalifikovanom sertifikatu za elektronski potpis.⁷¹ U skladu sa ovakvim određenjem, u našem pravu su kreirane tri vrste zahteva, koji svi zajedno trebaju da obezbede visok nivo verodostojnosti i bezbednosti.

Prvi zahtev se vezuju za napredne potpise, odnosno za njegove performanse, kao što je to učinjeno u pravu EU, iako u teoriji postoje razložna pravila koja generalno osporavaju njihovu tehničku i pravnu zasnovanost,⁷² ili opravdano ukazuju na njihove negativne implikacije.⁷³ I u našem pravu on podrazumeva elektronski potpis koji ispunjava dodatne uslove za obezbeđivanje višeg nivoa pouzdanosti potvrđivanja integriteta podataka i identiteta potpisnika u skladu sa ovim zakonom,⁷⁴ čime je naravljen iskorak u pravcu objektivizacije kriterijuma i pravnoj sigurnosti u datoj oblasti u odnosu na ranije srpsko zakonodavstvo. Saglasno tome, da bi jedan potpis u našem aktuelnom pravu imao tretman naprednog potpisa mora da ispuni dodatne uslove, koji su identični uslovima koji se traže u pravu EU.⁷⁵ To su sledeći uslovi; 1) na nedvosmislen način da bude povezan sa potpisnikom; 2) da omogućava utvrđivanje identiteta potpisnika; 3) da bude izrađen korišćenjem podataka za izradu elektronskog potpisa koje potpisnik odnosno pečatilac može, uz visok nivo pouzdanosti, koristiti pod svojom isključivom kontrolom; 4) da bude povezan sa elektronskim potpisnikom, na način da se može utvrditi bilo koja naknadna izmena tih podataka.

Drugi zahtev sadrži obavezu kreiranja potpisa kvalifikovanim sredstvom za kreiranje elektronskog potpisa, a to je sredstvo koje ispunjava uslove propisane zakonom.⁷⁶ Zakonom je propisano da kvalifikovano sredstvo za kreiranje elek-

⁶⁹ Upor: A. H. Boss, (1998), 590.

⁷⁰ *Ibid.*

⁷¹ Čl. 2. st.1 . tač. 30. ZEDEIUPEP.

⁷² Šire: S. Mason, 152 i dalje.

⁷³ One se posebno vide u komplikanosti. Upor: Hughes, 389. S. Eiselen, 2814.

⁷⁴ Čl.2 , st. 1, tač. 29. ZEDEIUPEP.

⁷⁵ Čl. 26. UEDUPETUT.

⁷⁶ Čl. 2, st. 1, tač. 31. ZEDEIUPEP.

tronskog potpisa mora da, pomoću odgovarajućih tehničkih rešenja i postupaka, obezbedi: 1) poverljivost podataka za kreiranje elektronskog potpisa; 2) da se podaci za kreiranje elektronskog potpisa, pojavljuju samo jednom; 3) da se podaci za kreiranje elektronskog potpisa, ne mogu dobiti izvan sredstava za kreiranje elektronskog potpisa, upotrebom dostupne tehnologije u razumnom vremenu; 4) da je elektronski potpis, pouzdano zaštićen od falsifikovanja upotrebom dostupne tehnologije; 5) mogućnost pouzdane zaštite podataka za kreiranje elektronskog potpisa, od neovlašćenog korišćenja.⁷⁷ Vrlo bitno je da sredstva za kreiranje kvalifikovanog elektronskog potpisa, prilikom kreiranja elektronskog potpisa, ne smeju promeniti podatke koji se potpisuju ili onemogućiti potpisniku, uvid u te podatke pre procesa kreiranja kvalifikovanog elektronskog potpisa.⁷⁸

Treći zahtev se tiče obavezne zasnovanosti elektronskog potpisa na kvalifikovanom sertifikatu za elektronski potpis, koji je definisan kao sertifikat za elektronski potpis koji izdaje kvalifikovani pružalac usluga od poverenja i koji ispunjava striktno uslove predviđene zakonom.⁷⁹

ZAKLJUČAK

Zbog svog značaja za elektronsku trgovinu, problem pravnog dejstva elektronskih potpisa je predmet pažnje pravne regulative kako na međunarodnom, tako i na nacionalnom planu. Na međunarodnom planu, pravna regulativa je u sadržinskom pogledu konceptualno slična i zasniva se na načelima pravnog priznanja, funkcionalne ekvalencije i formalne tehnološke neutralnosti. Isto tako se široko prihvata pristup o korelaciji pravnog dejstva elektronskih ugovora i njihove pouzdanosti, s tim što razlike postoje samo u pogledu preciziranja i nivoa odnosnih zahteva.

I u pravu Srbije se prihvata navedeni koncept, s tim što se naše pravo metodolški, strukturalno i sadržinski prevashodno naslanja na pravo EU. Posebno značajno je da i u njemu „pouzdanost i sigurnost“ postaje ključna determinanta dejstva elektronskih potpisa. Naime, najviša pravna snaga se daje kvalifikovanom potpisu, koji dobija isto pravno dejstvo kao i svojeručni potpis, pa čak može da zameni overu svojeručnog potpisa, ali zauzvrat on mora zadovoljiti vrlo složen sistem striktnih zahteva koji svi zajedno trebaju da obezbede visok nivo njegove pouzdanosti.

⁷⁷ Čl. 46, st. 1. ZEDEIUPEP.

⁷⁸ Čl. 46, st. 2. ZEDEIUPEP.

⁷⁹ Čl. 2, st. 1. tač. 32. ZEDEIUPEP.

LITERATURA I IZVORI

- Barofsky, A., "The European Commission's Directive on Electronic Signatures: Technological Favoritism Towards Digital Signatures," *BC Int'l & Comp. L. Rev.* 24/2000;
- Blythe, S. E., "Digital signature law of the United Nations, European Union, United Kingdom and United States: Promotion of growth in E-commerce with enhanced security," *Richmond Journal of Law & Technology*, 11.2/2005;
- Blythe, S. E., "Hong Kong Electronic Signature Law and Certification Authority Regulations: Promoting E-commerce in the World's Most Wired City." *NCJL & Tech.* 7/2005;
- Blythe, S. E., "China's New Electronic Signature Law and Certification Authority Regulations: A Catalyst for Dramatic Future Growth of E-Commerce," *Chi.-Kent J. Intell. Prop.*, 7/2007;
- Boss, A.H., "Electronic Commerce and the Symbiotic Relationship Between International and Domestic Law Reform," *Tul. L. Rev.* 72 /1997;
- Boss, A.H., "Searching for security in the law of electronic commerce," *Nova L. Rev.* 23/1998;
- Convention on the Use of Electronic Communications in International Contracts – CUECIC*, UNICITRAL, 2005, https://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf, avgust 2019;
- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')*, Official Journal of the European Communities (OJ) L 178, 17. 07. 2000, pp. 1-16;
- Divljak, D., „Harmonizacija pravila o elektronskoj trgovini i pravo Srbije“, *Zbornik radova Pravnog fakulteta u Novom Sadu (Zbornik radova PFNS)*, 3/2018;
- Dumortier, J. et al., *The legal and market aspects of electronic signatures*, Interdisciplinary centre for Law & Information Technology, Katholieke Universiteit Leuven, 2003;
- Eiselen, S., "Fiddling with the ECT act–Electronic signatures." *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad*, 17.6./2014;
- Hughes, J., "The Internet and the persistence of law," *BCL Rev.*, 44 /2002;
- Lui-Kwan, K. M., "Recent developments in digital signature legislation and electronic commerce," *Berkeley Tech. LJ* 14/1999;
- Mason, S., *Electronic signatures in law*, Cambridge, 2012;
- Mik, E., „Evaluating the Impact of the Un Convention on the Use of Electronic Communications in International Contracts on Domestic Contract Law-The Singapore Example,“ *Y.B. Int'l L. & Aff.* 43, 2010;
- Model Law on Electronic Commerce with Guide to Enactment, with additional article 5 bis adiptet in 1998*, UNICITRAL, http://www.uncitral.org/pdf/english/texts/electcom/V1504118_Ebook.pdf, avgust 2019,
- Model Law on Electronic Signatures with Guide to Enactment 2001*, UNICITRAL, <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/ml-elecsig-e.pdf>, avgust 2019;

- Ritter, J. B., Gliniecki, J. Y., "International Electronic Commerce and Administrative Law: The need for harmonized national reforms," *Harv. JL & Tech.*, 6/1992;
- Radovanović, S., „Zaključivanje ugovora putem Interneta-ide li pravo u korak sa vremenom“, *Zbornik radova PFNS*, 3,/2008;
- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN>; avgust 2019;
- Stern, J. E., "The electronic signatures in global and national commerce act," *Berk. Tech. LJ* 16, 2001;
- Wang, F.F., *Law of electronic commercial transactions: Contemporary issues in the EU, US and China*, Routledge 2014, 79;
- Zakon o elektronskim potpisima iz 2004. godine, *Sl glasnik RS*, br. 135/2004;
- Zakon o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju iz 2017. godine, *Sl glasnik RS*, br. 94/2017.

*Drago Lj. Divljak, Ph.D., Full Professor
University of Novi Sad
Faculty of Law Novi Sad
D.Divljak@pf.uns.ac.rs*

The Legal Effect of Electronic Signatures in International Legislation and in Serbian Law

Abstract: *The legal effect of electronic signatures, which includes the problem of its validity and legal power, is one of the important issues of electronic commerce. The paper analyzes the approach to this problem in the international legislation and the law of Serbia, considering it in the context of some national comparative solutions, especially in the context of the EU law.*

At an international level, legislation is conceptually nearly identical and is based on the principles of legal recognition, functional equivalence and formal technological neutrality. Additionally, the approach on the correlation of the legal effect of electronic contracts and their reliability is also widely accepted, with differences only in terms of specifying and the level of related requirements. The law of Serbia also accepts the above-mentioned concept; however, methodologically, structurally and substantively it relies primarily on the EU law. It is particularly important that in our law “reliability and security” becomes a key determinant of the legal effect of electronic signatures. Namely, the highest legal power is given to a qualified electronic signature, which has the same legal effect as a handwritten signature, and can even replace the legalization of a handwritten signature, but in turn it must satisfy a very complex system of strict requirements that all together need to ensure a high level of its reliability.

Keywords: *legal effect, electronic signatures, international legislation, law of Serbia, reliability, qualified electronic signature.*

Datum prijema rada: 10.09.2019.