

Др Драго Љ. Дивљак, редовни професор
Универзитет у Новом Саду
Правни факултет у Новом Саду
D.Divljak@pf.uns.ac.rs

ПРАВНО ДЕЈСТВО ЕЛЕКТРОНСКИХ ПОТПИСА У МЕЂУНАРОДНОЈ РЕГУЛАТИВИ И ПРАВУ СРБИЈЕ*

Сажетак: *Правно дејства електронских потписа, које у себи укључује проблем његове иновационости и правне снаге је једно од битних питања електронске трговине. У раду се анализира присуство овом проблему у међународној регулативи и праву Србије, при чему се он сагледава и у контексту неких националних компаративних решења, а посебно у контексту права ЕУ.*

На међународном плану, правна регулатива је концептуално скоро идентична и заснива се на начелима правног признања, функционалне еквиваленције и формалне технолошке неутралности. Исти иако се широко прихвата присуство о корелацији правног дејства електронских уговора и њихове поузданости, с тим што се разлике постоје само у погледу прецизирања и нивоа односних захтева. И у праву Србије се прихвата наведени концепти, с тим што се оно методолошки, структурално и садржински преваходно наслања на право ЕУ. Посебно значајно је да и у нашем праву „поузданост и сигурност“ постоје кључна дејерминанти правног дејства електронских потписа. Наиме, највиша правна снага се даје квалификованом електронском потпису, који добија исто правно дејство као и својеручни потпис, а чак може да замени оверу својеручног потписа, али заузврат он мора задовољити врло сложен систем стриктних захтева који сви заједно требају да обезбеде висок ниво његове поузданости.

Кључне речи: *правно дејство, електронски потписи, међународна регулатива, право Србије, поузданост, квалификовани електронски потпис.*

* Рад је настао као резултат истраживања на пројекту: “Теоријски и практични проблеми стварања и примене права (ЕУ и Србија)“, који се реализује на Правном факултету Универзитета у Новом Саду.

УВОДНЕ НАПОМЕНЕ

Електронски потписи¹ су један од кључних елемената електронске трговине.² Њихова појава је у пракси отворила је мноштво техничких, функционалних и следствено томе и правних питања, који представљају нови правни изазов.³ У том контексту, једно од битних питања је питање правног дејства електронских потписа, које у себи укључује проблем његове пуноважности и правне снаге. Оно је комплексније природе јер је повезано са применом базичних принципа модерног права електронске трговине као што су принцип недискриминације, технолошке неутралности и функционалне еквиваленције, али и са другим важним проблемима у датој области, посебно питањем сигурности. У раду који следи размотрићемо проблем правног дејства електронских потписа у међународној регулативи и праву Србије, сагледавајући га у контексту неких националних компаративних решења, а посебно у контексту права ЕУ, што је логично, с обзиром да се Србија налази у процесу придруживања ЕУ и да у њему имамо обавезу прилагођавања њеним правним правилима.

1. ПРАВНО ДЕЈСТВО ЕЛЕКТРОНСКИХ ПОТПИСА У МЕЂУНАРОДНОЈ РЕГУЛАТИВИ

С обзиром на карактер електронских комуникација и интернета који не познају државне границе, нужно је било и у области електронских потписа доћи до значајног нивоа конвергенције националних правних система⁴ путем процеса хармонизације⁵ и унификације правних правила. У креирању оваквог правног оквира који препознаје и олакшава прекограничне елек-

¹ Не постоји универзално прихваћена дефиниција електронског потписа, ни у теорији, нити у правној регулативи. Упор: 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 Упор: Kalama M., Lui-Kwan, „Recent developments in digital signature legislation and electronic commerce,” *Berkeley Tech. LJ* 14/1999, 465.

³ Упор: 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 Упор: Justin Hughes, „The Internet and the persistence of law,” *BCL Rev.*, 44 /2002, 361.

⁵ О процесу хармонизације у области електронске трговине, шире: Драго Дивљак, „Хармонизација правила о електронској трговини и право Србије“, *Зборник радова Правног факултета у Новом Саду (Зборник радова ПФНС)*, 3/2018, 909-924.

тронске трансакције,⁶ од кључне важности је активност UNCITRAL-а,⁷ који у оквиру врло особеног правног изазова интернета,⁸ проблему електронске трговине, па тиме и електронских потписа прилази симбиотски, где правна регулатива на различитим нивоима заједно настаје и под међусобним је утицајем.⁹ У том погледу он је израдио два Модел закона и једна конвенцију. То су Модел закон о електронској трговини из 1996. године, Модел закон о електронским потписима из 2001. године и Конвенција УН о употреби електронских комуникација у међународним уговорима из 2005. године.

1.1. Модел закона о електронској трговини

Први основ хармонизације¹⁰ у области електронских комуникација је Модел закон о електронској трговини.¹¹ Он, иако ефективно врло значајан за област електронске трговине,¹² питању електронских потписа прилази сегментирано. У складу са општом намером да уклони формалне препреке електронској трговини, он посебно регулише ситуације у којима би се користила средства електронске комуникације уместо традиционалних, заснованих на папиру.¹³ У том оквиру регулисани су и електронски потписи и то у чл. 7., у којем се утврђује опсег примене електронских потписа у ситуацијама када се законом захтева постојање потписа или се законом једноставно предвиђају последице за његово непостајање.¹⁴

Из наведеног садржаја овог члана, видљиво је да се у Модел закону генерално полази од тога да су својеручни потписи и потписи у електрон-

⁶ Упор: J. E. Stern, 391.

⁷ Међународна трговинска комора (ИЦЦ) израдила је документ под називом *General Usage for International Digitally Ensured Commerce* (GUIDEC). Он је усмерен ка регулисању питања алокације ризика и одговорности између учесника.

⁸ О проблему концептуалног приступа правном регулисању интернета и нових технологија, шире: J. Hughes, 360; Amelia H. Boss, "Searching for security in the law of electronic commerce," *Nova L. Rev.* 23/1998, 588 и даље; Сања Радовановић, „Закључивање уговора путем Интернета-иде ли право у корак са временом“, *Зборник радова ПФНС*, 3./2008, 279-291.

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

¹⁰ UNCITRAL се одлучио за модел закон, а не за конвенцију, схватајући да су разлике у националним правним системима биле превелике да би у том моменту било реалних шанси за усвајање конвенције у овој бласти. Упор: 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, август 2019.

¹² Модел закона о електронској трговини је широко прихваћен, јер га преко 60 држава широм света користило као полазну тачку за своје националне законе.

¹³ Ради се о писменом облику информације, потписа и оригинала информација који су регулисани у чл. 6., 7. и 8. Модел закона о електронској трговини из 2001. године.

¹⁴ Чл. 7. ст. 2. Модел закона о електронској трговини из 2001. године.

ском облику различите природе и ниједан не може аутоматски обављати исте функције као други, нити се правно могу поистоветити. Стога овај Модел закон настоји истражити функције које потпис у традиционалном облику обавља и затим одређује посебне критеријуме који ће, ако су испуњени, омогућити електронским потписима да дату сврху и функцију обави на исти начин као и традиционални својеручни потписи.¹⁵ Овакав приступ којим се посредним путем утврђује правно дејство електронских, се најчешће означава, као приступ или принцип функционалне еквиваленције, при чему се у погледу опсега правног дејства електронских потписа, крајња одлука ипак препушта националним законодавцима.¹⁶

У складу с наведеним принципом функционалне еквиваленције, у Модел закону о електронској трговини електронски потписи се у погледу правног дејства изједначавају са својеручним потписима, под условом да су испуњена два услова у вези са електронским преносом података. Први услов је испуњен ако се метода користи да идентификује потписника поруке и његову сагласност са садржајем поруке, чиме се правно дејство електронског потписа веже за две примарне функције својеручног потписа, а то су: идентификација потписника поруке и доказ да је он одобрио садржај документа.¹⁷ Други услов садржи обавезу да метод буде поуздан у мери који се сматра одговарајућим за сврху за коју је порука генерисана или пренесена у вези са свим околностима, укључујући и сваки релевантни споразум.¹⁸

Може се закључити да се овим Модел законом креирају опште претпоставке и стандарди у погледу безбедности и веродостојности електронског потписа, без посебног прецизирања. Овакав концепт, који је био основа и за друге регулаторне системе,¹⁹ не укључује додатне сигурносне захтеве и процедуре, што се у једну руку може оценити и логичним, јер ни код својеручног потписа оне нису посебно специфициране. Међутим, у циљу лакше примене ових правила, ипак су у Водичу Модел закона о електронској трговини инструктивно назначени бројни правни, технички и комерцијални фактори које треба узети у обзир при одређивању да ли је коришћена метода довољно поуздана и примерена.²⁰

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

¹⁶ Тако се у Пар. 76. Водича за примену Модел закона о електронској трговини, који прати га и пружа додатне информације и објашњења како би се помогло државама у примени сопствених релевантних закона, напомиње да када се потпише електронски документ помоћу функционалног еквивалента својеручног потписа, то не значи аутоматски да су електронски подаци правно валидни. Коначну реч, према концепту овог Модел закона дају закони донети на националном нивоу који регулишу дато питање.

¹⁷ О могућим функцијама електронског потписа: S. Mason, 98; Kalama M., Lui-Kwan, 460.

¹⁸ Упор: S. Mason, 99.

¹⁹ Овај модел је следила *Евројска унија, али и Сингајур, Бермуди и сл. Ibid*, 156.

²⁰ Тако су наведени :1) софистицираност опреме коју користи свака страна; (2) природа њихове трговинске делатности; (3) учесталост комерцијалних трансакција између страна;

Битна карактеристика овако конципираног Модел закона о електронској трговини је и да он не предвиђа, нити захтева коришћење било које специфичне врсте технологије да би се електронски потписи у свом правном дејству начелно изједначили са својеручним потписима.²¹ На овај начин се номинално прихвата принцип технолошке неутралности, који обавезује на усвајање правних правила које су неутралне у односу на коришћену технологију.²²

1.2. Модел закон о електронским потписима

Модел закона о електронским потписима из 2001. године²³ је сагласно свом називу специјалистички усмерен ка области електронских потписа. Формално гледано, правно дејство електронских потписа је регулисано преваходно у чл. 6. и 7, али и чл 3. при чему се они морају тумачити у контексту општег појмовног одређења електронских потписа датог у чл. 2. овог Модела.

У садржинском погледу Модел закона о електронским потписима битно допуњује Модел Закона о електронској трговини²⁴ на начин да се задржавају његови основни принципи и захтеви, уз додатне искорак у неким сегментима. Тако се за специфично деловање електронског потписа исто користи принцип функционалне еквиваленције за ситуације када се законом захтева потпис неког лица, односно једноставно прописују последице непостојања потписа. У складу са датим принципом, Модел законом о електронским потписима се предвиђа да се тада уместо својеручног може користити електронски потпис са истоветним правним дејством, уз испуњење утврђених предуслова и захтева. Они не произилазе само из чл. 6 Модела закона, већ и из чл. 2 којим се дефинише електронски потпис.

Уколико се интегрално посматрају наведене релевантне одредбе, онда се може закључити да су наведени захтеви идентични се захтевима Модел

(4) врста и величина трансакције; (5) функцију захтева за потписом у датом закону и регуларно окружење; (6) способност комуникационих система; (7) поштовање поступака аутентификације утврђених у посредници; (8) опсег поступака аутентификације који је било коме доступан посредник; (9) поштовање трговинских обичаја и праксе; (10) постојање механизма за осигурање осигурања против неовлашћене поруке; (11) важност и вредност информација садржаних у дата порука; (12) доступност алтернативних метода идентификације и трошкови имплементације; (13) степен прихватања или неприхватања методе идентификација у релевантној индустрији или области у оба времена метода је договорена и време када је дата порука саопштена; и (14) било који други релевантни фактор.

²¹ Упор: S. E. Blythe, 1.

²² Они имају за циљ да обезбеде исти правни третман електронском потпису независно од технологије који се користе у његовом настанку, односно да забрани дискриминацију или фаворизовање потписа само по наведеном основу.

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>, август 2019.

²⁴ Упор: S. Eiselen, 2809.

закона о електронској трговини.²⁵ Међутим, они се Модел законом о електронским потписима додатно прецизирају. Тако се електронски потписи сматрају поузданим ако испуњавају следеће услове: а) ако су подаци за генерисање потписа повезани само са потписником а не са другим лицима, б) ако су подаци за генерисање потписа у време потписивања били под контролом потписника и ниједног другог лица; ц) ако је свака промена у електронском потпису након потписивања уочљива; и д) ако је циљ правног захтева да потпис обезбеди сигурност за интегритет информација на које се односи, свака њихова измена након потписивања мора бити уочљива.²⁶

Напред наведени захтеви имали су за циљ да објективизују критеријуме техничке поузданости електронских потписа класификујући их у групе са различитом усмереношћу. Једни се фокусирају на карактеристике података за креирање потписа који морају бити повезани са потписником а, други се баве околностима у којима се користе подаци за креирање потписа, трећи и четврти су усмерени ка питањима интегритета електронског потписа и интегритета информација на које се електронски потпис односи.²⁷ Сви заједно они чине специфични „тест поузданости“, чије се постојање у делу теорије проблематизује.²⁸

Наведени захтеви у погледу поузданости електронског потписа садржани у Модел закону о електронским потписима имају за циљ успостављање минималних претпостављених, а не максималних стандарда и имају карактер смерница, јер се њихова стварна конкретизација може извршити евантуалним императивним законским одребама, али и уговорима између странака. Наиме у складу са чл. 7 овог Модел закона, свако лице, односно надлежни орган може одредити који тип електронских потписа ће задовољити напред наведене захтеве из члана 6,²⁹ при чему то, ипак мора бити у складу са признатим међународним стандардима.³⁰ Исто тако, и учесници у електронској комуникацији, могу користећи се начелом аутономије воље успоставити своје критеријуме поузданости, под условом да испуњавају минимум наведених захтева,³¹ што такође говори да су наведени општи услови поузданости прилично флексибилни и подложни примени принципу аутономије воље.

Са аспекта правног дејства електронских потписа релевантан је и чл 3. Модел закона о електронским потписима којим се формално потврђује ва-

²⁵ Упор: S. Eiselen, 2809.

²⁶ Чл. 6. ст 2. Модел закона о електронским потписима из 2001. године

²⁷ Упор: S. Eiselen, 2810.

²⁸ Упор: S. Mason, 114.

²⁹ Упор: S. Eiselen, 2809.

³⁰ Чл. 7. ст 2. Модел закона о електронским потписима из 2001.године.

³¹ Упор: S. Eiselen, 2811.

жење принципа технолошке неутралности у овој области. У овом члану је утврђено да ништа у овом Модел закону, осим члана 5., се не може применити тако да искључи, ограничи или лиши правног дејства било који начин креирања електронског потписа који испуњава његове захтеве. С друге стране је видљиво да захтеви за поузданошћу могу имплицитно погодovati коришћењу неких облика и технологија креирања електронског потписа.³² Међутим, кључно је да се тиме не искључују друге врсте технологија које би могле да испуне дате захтеве поузданости, при чему је улога правних правила само да понуди предвидљивост у дефинисању тих захтева.³³

1.3. Конвенција УН о употреби електронских комуникација у међународним уговорима

Конвенција УН о употреби електронских комуникација у међународним уговорима из 2005. године³⁴ донета је с циљем да регулише употребу електронских комуникација у вези са закључењем или извршењем уговора између страна које имају своја седишта у различитим државама.³⁵ У погледу правног дејства електронских потписа је релевантан чл. 9 ст. 3. Конвенције, што сугерише да се UNCITRAL одлучио да у датој Конвенцији генерално придржава приступа минималне регулације датог у Модел закону о електронским комуникацијама,³⁶ као и његових садржинских одредница. Тако, исто уређује питање коришћења потписа, тј. за ситуације када закон налаже постојање потписа или се евентуално предвиђају правне последице његовог одсуства, и то на функционално еквивалентном принципу. Видљиво је да исказани приступ омогућава да се користи било који облик електронског потписа,³⁷ што сугерише да је начелно прихваћен и принцип технолошке неутралности. Исто тако, Конвенцијом се слично Модел закону, поузданост утврђује као битан елемент за дефинисање правне снаге електронског потписа.

³² Упор: S. E. Blythe, (2005), 6.

³³ *Ibid.*

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

³⁵ Конвенција је ступила на снагу 2013. године и ратификовао је мањи број земаља. Међутим, њен значај се не исцрпљује само у томе, јер је она у неким правима била узор у конципирању националних правила као што је случај са правом Сингапура. Вид: 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 Упор: S. Eiselen, 2812.

³⁷ Упор: S. Mason, 111.

Међутим, иако слични, приступ исказан у Конвенцији о употреби електронских комуникација у међународним уговорима у односу на Модел закон о електронској трговини, свакако није идентичан, јер се другачијим формулацијама и неким допунским елементима у конвенцији ипак мења нагласак поређењу са одредбама у Модел законима. Прва измена се односи на услове функционалне еквиваленције. Наиме у Конвенцији је утврђено да електронски потпис може заменити својеручни потпис, ако се користи метода за идентификацију странке и за указивања на њену намеру у погледу информација садржаних у електронској комуникацији. Укључивањем елемента „намере“ уместо „сагласности“ у погледу информација садржаних у електронској комуникацији, извршен је отклон од аналогних одредби у односу на оба Модел закона.³⁸ То је значајан искорак, јер се у Конвенцији нагласак даје на идентитету странке и његовој намери у погледу електронских информација, док је у Модел законима у првом плану „интегритет информација“ у електронској комуникацији.

Посебан нагласак се у Конвенцији о употреби електронских комуникација у међународним уговорима даје елементу поузданости електронских потписа, па стога у том погледу је дошло да највећих измена у односу на Модел закон о електронској трговини. Наиме, у Конвенцији је преузет услов апстрактне поузданости из Модел закона о електронској трговини који прописује да метод мора бити поуздан у мери који се сматра одговарајућом за сврху за коју је порука генерисана или пренесена у вези са свим околностима, укључујући и сваки релевантни споразум. Међутим, новина је да се оставља могућност да се може доказати да електронски потпис испуњава захтеве у погледу поузданости.³⁹ Стога се може оценити да се постојећи концепт поузданости из Модел закона о електронској трговини који се може назвати „теоријском поузданошћу“ у датој Конвенцији надограђује елементом који се може означити као „фактичка поузданост.“

Наведени искораци у Конвенцији о употреби електронских комуникација у међународним уговорима у односу на оба Модел закона се свакако могу позитивно оценити. Међутим, и поред помака у том погледу, представљени концепт поузданости електронских потписа остаје и даље и недовољно конкретизован што може бити његов хендикеп у пракси.⁴⁰ На концептуалном плану се као њен већи недостатак може навести што и даље применом принципа функционалне еквиваленције решава практичан проблем примене електронских потписа, али не даје децидне одговоре о вези њиховог правног важења.⁴¹

³⁸ Упор: F. F. Wang, 84.

³⁹ Упор: S. Eiselen, 2812.

⁴⁰ Упор: F. F. Wang, 87.

⁴¹ *Ibid*, 85.

2. ПРАВНО ДЕЈСТВО ЕЛЕКТРОНСКИХ ПОТПИСА У ПРАВУ СРБИЈЕ

Полазећи од тога да је “правна несигурност антитеза јаким и ефикасним тржишта”,⁴² и националном нивоу су законодавци морали приступити правној регулацији електронских потписа. У контексту правног дејства електронских потписа, кључни корак је омогућавање њиховог правног признања и пуноважности, којим се дозвољава да се странке обавезују уговором и путем електронског потписа.⁴³ Уколико би се електронским документима ускратила могућност и електронског потписивања, они би морали допуњени папирним записима са својеручним потписима, што није само скупља, мање конкурентна, мање ефикасна варијанта,⁴⁴ већ и варијанта која би својом компликованосту битно успорила раст електронске трговине. Тек признањем пуноважности електронских потписа се доследно ефектуирао принцип да се уговори закључени и “потписани” у потпуности електронским средствима сматрају правно валидним.⁴⁵

У праву Србије је први пут Законом о електронским потписима⁴⁶ из 2004. године учињен најважнији први искорак у погледу правног легитимисања и признања електронских потписа. Оваквим нормативним приступом раније српско законодавство у опционом облику инкорпорира електронски потпис у наш правни систем, при чему парцијално проблематизира само његову доказну снагу у законом уређеном поступку.⁴⁷

Закон о електронским потписима је замењен Законом о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању из 2017. године.⁴⁸ Он се и по називу и садржини наслања на важеће право ЕУ из ове области садржано у Уредби о електронској идентификацији и услугама од поверења за електронске трансакције на унутрашњем тржишту,⁴⁹ којом се између осталог, регулише и електрон-

⁴² Упор: J. E. Stern, 392.

⁴³ Упор: J. E. Stern, 397.

⁴⁴ Упор: 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.

⁴⁵ Упор: A. Barofsky, 146.

⁴⁶ *Сл ђласник РС*, бр. 135/2004.

⁴⁷ Наиме, утврђено је да електронски потпис може имати правно дејство и може се користити као доказно средство у законом уређеном поступку, осим када се, у складу са посебним законом, захтева да само својеручни потпис има правно дејство и доказну снагу. Упор: Чл.6. Закона о електронском потпису.

⁴⁸ *Сл ђласник РС*, бр. 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. Она је је дерогирала Директиву 1999/93/EC о електронском

ски потпис,⁵⁰ али се делом задржава и надлежност држава чланица у овој области.⁵¹

Доношењем новог Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању је не само потврђен, већ и оснажен принцип правног признања и пуноважности електронских уговора, у нешто другачијој стилизацији него у у важећој уредби ЕУ.⁵² То је учињено изричитом формулацијом да се електронском потпису не може оспорити пуноважност или доказна снага само због тога што је у електронском облику, или што не испуњава услове за квалификовани електронски потпис.⁵³ Међутим, наведени начелни приступ о правном признању електронских потписа у нашем праву није апсолутан, јер се правила о пуноважности електронских потписа не примењују на правне послове за које је посебним законом предвиђено да се не могу преузети у електронској форми, односно на уговоре и друге правне послове за које је посебним законом предвиђено да се сачињавају у форми овере потписа, јавно потврђене (солемнизоване) исправе, или у форми јавнобележничког записа.⁵⁴ Ограничење домашаја овог принципа је присутно и у другим правима, али она често нису идентична.⁵⁵

За детаљнију анализу правног дејства електронских потписа у праву Србије су посебно релевантне и одредбе чл. 2 и чл. 50 наведеног закона. Тек њиховим комплементарним разматрањем се може утврдити позиција нашег актуелног права у датој области.

У чл. 2 који се бави дефинисањем законских категорија, фактички електронски потписи се у нашем праву класификују на три категорије и то елек-

потпису. Шире о њој: 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 Чл. 1. Уредбе о електронској идентификацији и услугама од поверења за електронске трансакције на унутрашњем тржишту – УЕДУПЕТУТ.

⁵¹ Наиме, у области правног дејства електронских потписа је подељена надлежност између нивоа ЕУ и држава чланица, па је осим захтева предвиђених у Уредби према којима би квалификовани електронски потпис требао имати једнако правно дејство као својеручни потпис, све остало потребно је одредити националним правима држава чланица. Упор: Пар. 49. Преамбуле УЕДУПЕТУТ.

⁵² Утврђено је да се електронском потпису се као доказу у судским поступцима не може ускратити правно дејство и допуштеноост само због тога што је он у електронском облику или због тога што не испуњава све захтеве за квалификовани електронски потпис. Упор: Чл. 25 ст. 1. УЕДУПЕТУТ.

⁵³ Чл. 50. ст. 1. Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању – ЗЕДЕИУПЕП.

⁵⁴ Чл. 50. ст. 3. и 4 ЗЕДЕИУПЕП.

⁵⁵ О приступу кинеског права: 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.

тронске потписе, напредне и квалификоване електронске потписе. Тај приступ је у идентичном облику преузет из права ЕУ.⁵⁶ Уколико наведену класификацију ставимо у контекст већ наведеног правила да се електронском потпису не може оспорити пуноважност или доказна снага само због тога што је у електронском облику или што не испуњава услове за квалификовани електронски потпис, онда се логично могу извући одређени закључци о битним одредницама права Србије у погледу правног дејства електронских потписа.

Прво, сваки електронски потпис, који испуњава генералне техничке и функционалне услове које су дате у појмовном одређењу електронског потписа⁵⁷ је пуноважан и има одређену доказну правну снагу и дејство. Она је везана за потврђивање интегритета података који се потписују и идентитета потписника, али ће конкретну садржину тог дејства дати пословна и судска пракса у будућности. Чињеница да се у нашем праву на овај начин даје доказна снага и потпису који не испуњава услове за квалификовани електронски потпис, указује да овакви „неквалификовани“ потписи нису формално ограничени додатним критеријумима сигурности, као што је то учињено у неким упоредним правима.⁵⁸

Друго, сви електронски потписи немају исто правно дејство. За разлику од напред наведених „обичних“ или „неквалификованих“ електронских потписа који имају ограничену правну снагу, највиша правна снага се даје квалификованом потпису, који добија исто правно дејство као и својеручни потпис, па чак може да замени оверу својеручног потписа, ако је то прописано посебним законом.⁵⁹ На овај начин се креира диференцирана шема правног дејства електронских потписа, у коме постоје две њихове правне релевантне категорије, где је квалификовани електронски потпис кључан и из којег се изводи како правно одређење, тако и правно дејство „обичних“ или „неквалификованих“ електронских потписа. Креирање оваквог система правног дејства електронских потписа у нашем праву је засновано на праву ЕУ,⁶⁰ али је генерално сличан систем присутан и у упоредном праву, као што је случај у Кини.⁶¹ Због садржине правног дејства које има квалификовани

⁵⁶ Упор: чл. 3. УЕДУПЕТУТ који такође предвиђа три врсте електронског потписа: електронски потпис, напредни електронски потпис и квалификовани електронски потпис.

⁵⁷ Електронски потпис у нашем праву је генерално одређен као скуп података у електронском облику који су придружени или логички повезани са другим (потписаним) подацима у електронским облику тако да се електронским потписом потврђује интегритет тих података и идентитет потписника. Чл. 2. ст. 1. тач. 20. ЗЕДЕИУПЕП.

⁵⁸ Такав је случај у праву Кине. Упор: S.E. Blythe, (2007), 29.

⁵⁹ Чл. 50. ст. 2. и 3. ЗЕДЕИУПЕП.

⁶⁰ Чл. 25. ст. 1. и 2. ЗЕДЕИУПЕП.

⁶¹ У Кини је је у том смислу креиран тзв. поуздан електронски потпис, који би могао бити пандан нашем квалификованом електронском потпису. О захтевима које морају испунити такви потписи : S. E. Blythe. (2007), 16-17.

електронски потпис, он иако добровољан, оваквим нормативним системом може постати не само пожељан, већ и фактички скоро обавезан.⁶²

Треће, у праву Србије, пуноважност и правно дејство електронских уговора се формално не везује за конкретни облик технологије која се користи за креирање електронског потписа, што је честа пракса у упоредном праву.⁶³ Тиме се указује да је у нашем праву имплицитно начелно прихваћен принцип технолошке неутралности, за разлику од права ЕУ које се експлицитно позива на њега,⁶⁴ што је свакако добар приступ.⁶⁵ Међутим, стриктним захтевима у вези сигурности се фактички фаворизују дигитални потписи⁶⁶ и други облици електронског потписа са високим перформансама сигурности,⁶⁷ чиме се наше право фактички приближава хибридном моделу регулације који се заснива на ограниченој технолошкој неутралности, са свим својим импликацијама.⁶⁸

Четврто, сагласно међународној регулативи, у погледу конципирања правног дејства електронских уговора у нашем праву оправдано се полази од фактора поузданости и сигурности. Тиме “сигурност” постаје кључна детерминанта не само у контексту електронске трговине,⁶⁹ већ и контексту дејства електронских потписа. Управо је креирање напред наведених квалификованих електронских потписа као сложене правне конструкције резултат таквог приступа, иако је јасно да се “сигурност” не може „законски регулисати,“ јер је то комбинација фактора који нису само правни, већ у битној мери и технолошки и зависе од употребљене технологије у електронској комуникацији.⁷⁰ Под квалификованим електронским потписом се у нашем праву подразумева напредни електронски потпис који је креиран

⁶² Упор: 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 Упор: F. F. Wang, 79.

⁶⁴ У пар. 26. и 27. Преамбуле УЕДУПЕТУТ је наведено да правни учинци који се њоме осигуравају требали би бити оствариви било којим техничким средствима под условом да су захтеви ове Уредбе испуњени. У том смислу се и пледира за отвореност за технолошке иновације у овој области.

⁶⁵ Упор: Kalama M. Lui-Kwan, 478.

⁶⁶ У теорији се понекад термин дигитални потпис користи као синоним за електронски потпис уопште. Међутим, он је само један подоблик електронских потписа. Вид: E. Blythe, (2005), 3. Шире о дигиталним потписима: F. F. Wang, 81.

⁶⁷ У теорији је извршена класификација потписа по основу степена њихове безбедности на четири групе. Шире: S. E. Blythe, (2005), 3 и даље.

⁶⁸ Овакав модел има своје добре и лоше стране. С једне стране, овакав приступ је само природан отисак сличних приступа у области потписа уопште, а с друге стране, хибридни модели су флексибилнији и прилагодљивији новим технолошким достигнућима, уз постојање базичне сигурности.

⁶⁹ Упор: A. H. Boss, (1998), 590.

⁷⁰ *Ibid.*

квалификованим средством за креирање електронског потписа и који се заснива на квалификованом сертификату за електронски потпис.⁷¹ У складу са овакавим одређењем, у нашем праву су креиране три врсте захтева, који сви заједно требају да обезбеде висок ниво веродостојности и безбедности.

Први захтев се везују за напредне потписе, односно за његове перформансе, као што је то учињено у праву ЕУ, иако у теорији постоје разложна правила која генерално оспоравају њихову техничку и правну заснованост,⁷² или оправдано указују на њихове негативне импликације.⁷³ И у нашем праву он подразумева електронски потпис који испуњава додатне услове за обезбеђивање вишег нивоа поузданости потврђивања интегритета података и идентитета потписника у складу са овим законом,⁷⁴ чиме је нарављен искорак у правцу објективизације критеријума и правној сигурности у датој области у односу на раније српско законодавство. Сагласно томе, да би један потпис у нашем актуелном праву имао третман напредног потписа мора да испуни додатне услове, који су идентични условима који се траже у праву ЕУ.⁷⁵ То су следећи услови; 1) на недвосмислен начин да буде повезан са потписником; 2) да омогућава утврђивање идентитета потписника; 3) да буде израђен коришћењем података за израду електронског потписа које потписник односно печатилац може, уз висок ниво поузданости, користити под својом искључивом контролом; 4) да буде повезан са електронским потписником, на начин да се може утврдити било која накнадна измена тих података.

Други захтев садржи обавезу креирања потписа квалификованим средством за креирање електронског потписа, а то је средство које испуњава услове прописане законом.⁷⁶ Законом је прописано да квалификовано средство за креирање електронског потписа мора да, помоћу одговарајућих техничких решења и поступака, обезбеди: 1) поверљивост података за креирање електронског потписа; 2) да се подаци за креирање електронског потписа, појављују само једном; 3) да се подаци за креирање електронског потписа, не могу добити изван средстава за креирање електронског потписа, употребом доступне технологије у разумном времену; 4) да је електронски потпис, поуздано заштићен од фалсификовања употребом доступне технологије; 5) могућност поуздане заштите података за креирање електронског потписа, од неовлашћеног коришћења.⁷⁷ Врло битно је да средства за креирање квалификованог

⁷¹ Чл. 2. ст.1 . тач. 30. ЗЕДЕИУПЕП.

⁷² Шире: S. Mason, 152 и даље.

⁷³ Оне се посебно виде у компликаности. Упор: Hughes, 389. S. Eiselen, 2814.

⁷⁴ Чл.2 , ст. 1, тач. 29. ЗЕДЕИУПЕП.

⁷⁵ Чл. 26. УЕДУПЕТУТ.

⁷⁶ Чл. 2, ст. 1, тач. 31. ЗЕДЕИУПЕП.

⁷⁷ Чл. 46, ст. 1. ЗЕДЕИУПЕП.

електронског потписа, приликом креирања електронског потписа, не смеју променити податке који се потписују или онемогућити потписнику, увид у те податке пре процеса креирања квалификованог електронског потписа.⁷⁸

Трећи захтев се тиче обавезне заснованости електронског потписа на квалификованом сертификату за електронски потпис, који је дефинисан као сертификат за електронски потпис који издаје квалификовани пружалац услуга од поверења и који испуњава стриктне услове предвиђене законом.⁷⁹

ЗАКЉУЧАК

Због свог значаја за електронску трговину, проблем правног дејства електронских потписа је предмет пажње правне регулативе како на међународном, тако и на националном плану. На међународном плану, правна регулатива је у садржинском погледу концептуално слична и заснива се на начелима правног признања, функционалне екваленције и формалне технолошке неутралности. Исто тако се широко прихвата приступ о корелацији правног дејства електронских уговора и њихове поузданости, с тим што разлике постоје само у погледу прецизирања и нивоа односних захтева.

И у праву Србије се прихвата наведени концепт, с тим што се наше право методолшки, структурално и садржински превасходно наслања на право ЕУ. Посебно значајно је да и у њему „поузданост и сигурност“ постаје кључна детерминанта дејства електронских потписа. Наиме, највиша правна снага се даје квалификованом потпису, који добија исто правно дејство као и својеручни потпис, па чак може да замени оверу својеручног потписа, али заузврат он мора задовољити врло сложен систем стриктних захтева који сви заједно требају да обезбеде висок ниво његове поузданости.

ЛИТЕРАТУРА И ИЗВОРИ

- 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;

⁷⁸ Чл. 46, ст. 2. ЗЕДЕИУПЕП.

⁷⁹ Чл. 2, ст. 1. тач. 32. ЗЕДЕИУПЕП.

- 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, август 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;
- Дивљак, Д., „Хармонизација правила о електронској трговини и право Србије“, *Зборник радова Правног факултета у Новом Саду (Зборник радова ПФНС)*, 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 adopted in 1998*, UNICITRAL, http://www.uncitral.org/pdf/english/texts/electcom/V1504118_Ebook.pdf, август 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>, август 2019;
- Ritter, J. B., Gliniecki, J. Y., "International Electronic Commerce and Administrative Law: The need for harmonized national reforms," *Harv. JL & Tech.*, 6/1992;
- Радовановић, С., „Закључивање уговора путем Интернета-иде ли право у корак са временом“, *Зборник радова ПФНС*, 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>; август 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;

Закон о електронским потписима из 2004. године, *Сл љласник РС*, бр. 135/2004;
Закон о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању из 2017. године, *Сл љласник РС*, бр. 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.*

Датум пријема рада: 10.09.2019.