RAZVOJ PRAVNE REGULACIJE ELEKTRONIČKOG POTPISA, ELEKTRONIČKOG CERTIFIKATA I ELEKTRONIČKE ISPRAVE U HRVATSKOM I POREDBENOM PRAVU

Tihomir Katulić, dipl. iur. [*]

UDK 347.135.224:004.3/.4
004.3/.4:347.135.224
Pregledni znanstveni rad
Primljeno: siječanj 2011.

Uvodno autor govori o ključnoj ulozi elektroničkog potpisa u pravnoj regulaciji elektroničke trgovine kao brzorastuće grane gospodarstva koja podrazumijeva brojna pravna pitanja vezana uz utjecaj informacijske tehnologije na društvo i pravo. Počevši od ispitivanja važnosti vlastoručnog potpisa kao sredstva autentikacije autora dokumenta preko potvrđivanja sadržaja dokumenta prezentiraju se uvjeti koje elektronički potpis treba ispuniti kako bi zauzeo mjesto vlastoručnog potpisa u pravnom prometu. U nastavku, prikazuje se intenzivna zakonodavna aktivnost na području regulacije elektroničkog potpisa, od prvih zakona iz sredine devedesetih godina prošlog stoljeća do danas. Unatoč kratkom vremenskom okviru od samo petnaest godina, u bogatoj poredbenoj praksi moguće je razlikovati nekoliko različitih pristupa kojim su razna zakonodavstva širom svijeta pokušala regulirati elektronički potpis i srodna pitanja kako bi omogućili kvalitetnu razinu pravne sigurnosti elektroničkoj trgovini i drugim pravnim odnosima koji se odvijaju putem elektroničke komunikacije. Autor razlikuje nekoliko zakonodavnih etapa karakteriziranih različitim teorijskim i praktičnim stavovima o karakteru regulacije elektroničkog potpisa. U prvoj etapi problematizira se odnos dva suprotna pristupa pitanju potrebe specifikacije tehnološke osnovice elektroničkog potpisa, dok se u drugoj ispituje priroda sustava dvostrukog kolosjeka i na njemu zasnovanog pravnog okvira koji dominira u europskom pravnom krugu. Na osnovama iskustava iz poredbenog prava autor zatim analizira izabrane odredbe iz Zakona o elektroničkom potpisu, uz osvrt na utjecaj koji isti zakon ima na druge zakone, osobito Zakon o elektroničkoj ispravi. U posljednjem dijelu rada autor

[*] Tihomir Katulić, dipl. iur., asistent Pravnog fakulteta Sveučilišta u Zagrebu, Trg maršala Tita 14, Zagreb

iznosi kritiku instituta elektroničke isprave, te zaključuje osvrtom na dosadašnju primjenu elektroničkog potpisa u hrvatskoj pravnoj praksi.

Ključne riječi: elektronički potpis, napredni elektronički potpis, elektronička isprava, elektronička trgovina, elektronička komunikacija, informacijska tehnologija, Public Key Infrastructure, Electronic Data Interchange

Uvod

Upotreba informacijske tehnologije u različitim aspektima društvenog života za sobom povlači brojne socijalne, ekonomske i pravne posljedice. Utjecaj informacijske tehnologije na društvene odnose raste, razvija se i mijenja jednakom brzinom kao i sama tehnologija, a novi oblici društvenih odnosa modificiraju ili zamjenjuju postojeće.

Jedna takva aktivnost jest svakako elektronička trgovina. Pojam elektronička trgovina ili *e-commerce* odnosi se na kupnju ili prodaju proizvoda ili usluga putem informacijskih sustava i posredstvom elektroničke komunikacije. Sve potpunija prisutnost i upotreba informacijskih tehnologija omogućili su izvanredan rast granama gospodarstva koje se koriste elektroničkom trgovinom, a sama elektronička trgovina najbrže je rastući segment gospodarstva u mnogim razvijenim, ali i zemljama u razvoju.

Direktna i indirektna elektronička trgovina[1] ključni su promotori procesa ekonomske globalizacije, omogućivši prvi put istinsku globalnu ekonomsku razmjenu, ne samo među etabliranim multinacionalnim korporacijama, već i malim, lokalnim poduzetnicima. Razvoj trgovine putem interneta ubrzao je i razvoj drugih danas široko prihvaćenih tehnologija, poput elektroničkog transfera novca, internetskog marketinga, EDI tehnologija i automatske pohrane i analize podataka.

Elektronički potpis ključan je element uspjeha elektroničke trgovine, uvjet bez kojeg elektronička komunikacija, a time i elektronička trgovina, ostaje pravno nesigurna i nepouzdana. Tehnologije elektroničkog potpisa kakve danas poznajemo možda ne pružaju apsolutnu sigurnost u identitet i sadržaj elektroničke komunikacije, ali mogu omogućiti onu nužnu razinu sigurnosti, sasvim usporedivu, ako ne i kvalitetniju, od komunikacije na papiru uz vlastoručni potpis i žig.

Upotreba elektroničkog potpisa prožima sve aspekte upotrebe informacijske tehnologije u modernom pravnom prometu. Elektroničkim potpisom možemo

[1] Dragičević, D., *Kompjutorski kriminalitet i informacijski sustavi*, Informatorov Biro Sustav, Zagreb, 2004., str. 40.

autorizirati poruke elektroničke pošte, elektroničke isprave i druge dokumente (poput ugovora) u elektroničkom obliku[2], zatim zaštititi upotrebu sredstava neposredne elektroničke komunikacije u realnom vremenu, poput internetske telefonije, alata za *instant messaging* i drugih komunikacijskih servisa.

Da bismo mogli na odgovarajući način pratiti nastanak i razvoj elektroničkog potpisa, osvrnimo se načas na ulogu vlastoručnog potpisa u pravnom prometu.

Čin stavljanja potpisa, osobnog pečata ili kakvog drugog osobnog traga na rukom ili strojem ispisani dokument bilo koje vrste stoljećima se smatra temeljnim uvjetom nastanka presumpcije slaganja potpisnika sa sadržajem isprave. Bez valjana potpisa kojim stranka ugovora ili podnositelj nekog zahtjeva ili bilo koji drugi sudionik pravnog prometa izravno prihvaća sadržaj isprave koju potpisuje, sama isprava koliko god pažljivo i detaljno sročena nema pravnu snagu jer se u pravilu ne može smatrati valjanim očitovanjem volje.

Zanimljivo je pitanje gdje se i kako točno definira što je potpis.[3] Moglo bi se reći kako je potpis zapravo pravni standard[4], a da će svaki konkretan propis koji regulira neko područje zapravo sam propisati potrebne kvalitete koje potpis u konkretnom slučaju treba imati da bi se smatrao pravnovažećom potvrdom identiteta i volje nekog pravnog subjekta.

Do donošenja hrvatskog Zakona o elektroničkom potpisu u hrvatskom pravu nije bilo zakona koji bi definirali potpis, osobito u kontekstu pravno valjane isprave u elektroničkom obliku. Naravno, zakona koji određuju potpis kao uvjet bez kojeg se ne može, primjerice kod sklapanja ugovora, ima napretek. Tako Zakon o obveznim odnosima, i onaj iz 1978., i noviji iz 2005., sadržavaju odredbe koje upotrebljavaju termin potpis, podrazumijevajući pod njime čin stavljanja potpisa ili kakvog drugog neposrednog osobnog traga, ali istodobno ne definirajući od čega se potpis, odnosno potpisivanje sastoji.[5]

Isto tako, Zakon o parničnom postupku[6] također redovito navodi potpis stranke kao formalni uvjet bez kojeg se nekoj ispravi ili podnesku ne može priznati autentičnost niti valjanost. Slične odredbe sadržavaju i Zakon o ka-

---

2 Matić, T., *Elektronički potpis*, Odvjetnik, *vol.* 11–12, Zagreb, 2010., str. 8.

3 *Ibid.*, str. 8.

4 Visković, N., *Teorija države i prava*, Birotehnika CDO, Zagreb, 2001. str. 251.

5 Matić, T., *Osnove prava elektroničke trgovine*, MEP Consult, Zagreb, 2008., str. 55.

6 Npr. čl. 389. st. 3 Zakona o parničnom postupku ili čl. 186. st. 9. ZPP-a, Narodne novine, br. 84/2008.

znenom postupku[7], Zakon o općem upravnom postupku, Zakon o upravnom sporu i mnogi drugi zakoni.

Važnost elektroničkog potpisa

Pitanje definicije potpisa osobito je važno u vremenu kada intenzivno prelazimo na komunikaciju putem elektroničkih informacijskih sustava. Broj elektroničkih dokumenata u državnoj upravi, pravosuđu i gospodarstvu u stalnom je porastu. Kako informacijska tehnologija napreduje, tako se šire i mogućnosti njezine upotrebe.

Elektronički potpis kao pravni ekvivalent ručnom potpisu i pečatu sposoban je znatno ubrzati poslovanje[8], omogućujući neusporedivo više poslovnih transakcija istodobno čuvajući sigurnost i povjerljivost poslovne komunikacije u digitalnom okružju.[9]

Budući da upotreba elektroničkih informacijskih sustava u društvu u cjelini raste, gospodarski subjekti i državna uprava, žele li (p)ostati efikasni, trebaju prihvatiti i upotrebljavati moderne informacijske tehnologije poput elektroničkog potpisa u svakodnevnom radu.

Iako je u razvijenim zemljama Zapadne Europe te Sjedinjenim Državama uvođenje informacijskih tehnologija u poslovanje proces koji traje još od sedamdesetih godina prošlog stoljeća[10], i unatoč činjenici kako je prvi Zakon o informatičkoj djelatnosti u Republici Hrvatskoj donesen još davne 1977. godine kao republički zakon u sklopu bivše federativne države[11], uvođenje infor-

[7] Novi Zakon o kaznenom postupku iz 2008. u čl. 79. "Elektronička isprava" regulira potrebne uvjete za priznanje i zaprimanje elektroničke isprave te sadržaj, autentikaciju, vrijeme i način zaprimanja podnesaka elektroničkim putem. ZKP, Narodne novine, br. 152/2008.

[8] Vojković, G., *Elektronički potpis*, Godišnjak 12 Hrvatskog društva za građanskopravne znanosti i praksu, Zagreb, 2005., str. 463.

[9] Primjerice, informatizacija burzovnog poslovanja omogućila je brokerima širom svijeta da samostalno, putem informacijskih sustava, za svoje klijente prate ulaganja u dionice na dvadesetak najvećih svjetskih burzi. Nadalje, jeftine aviokompanije svakodnevno zaprimaju i prodaju stotine tisuća rezervacija i karata. Tako je irski Ryan Air prošle godine prevezao više od šezdeset milijuna putnika koji su svoje karte i ukrcajne propusnice nabavili isključivo elektroničkim putem.

[10] Dragičević, *op. cit*. u bilj. 2, str. 46.

[11] Zakon o informatičkoj djelatnosti, Narodne novine, br. 49/1977. Zanimljivo kako je prije gotovo četrdeset godina zakonodavac bio svjestan opasnosti uvođenja informacijskih tehnologija bez koordinacije i opreznog planiranja, pa je u spomenutom Za-

macijskih tehnologija u poslovanje u Republici Hrvatskoj, osobito u segmentu javne uprave, u proteklih dvadesetak godina nije bila sustavna, već sporadična pojava.

U tijelima državne uprave Republike Hrvatske u nedavnoj prošlosti događali su se razni nedorečeni pokušaji "informatizacije" i "internetizacije" bez čvrstog plana i cilja. O tome svjedoče brojne strategije i drugi okvirni dokumenti koji su iz godine u godinu usvajani bez većeg efekta u smislu konkretnijih promjena u načinu na koji državna uprava funkcionira, po uzoru na slične dokumente iz zapadnih uzora.[12]

Reguliranje elektroničke trgovine i s njom povezanih tehnologija i postupaka ozbiljnije je ušlo u fokus hrvatskog zakonodavca tek početkom novog tisućljeća, desetak godina kasnije nego na Zapadu.

U vrijeme kada su doneseni zakoni poput Zakona o elektroničkoj trgovini, Zakona o elektroničkom potpisu i Zakona o elektroničkoj ispravi dolazi do promjene u stajalištu zakonodavca prema utjecaju informacijske tehnologije na društvo i do osvještavanja potrebe da se isti odgovarajuće regulira, a sve (uglavnom[13]) pod utjecajem relevantne zakonodavne prakse u susjednim, teorijski i sustavno bliskim zakonodavstvima u postupku preuzimanja europske pravne stečevine.

Od svih pravnih pitanja i nedoumica koje prate pojavu elektroničke trgovine osobito se ističe ono o regulaciji elektroničkog potpisa. Bez elektroničkog potpisa, već smo istaknuli, nema zadovoljavajuće razine pravne sigurnosti prilikom sklapanja pravnih poslova u elektroničkom obliku.[14]

Kada govorimo o elektroničkom potpisu, valja istaknuti kako on podrazumijeva i upotrebu elektroničkog certifikata. Moglo bi se reći da elektronički potpis u širem smislu obuhvaća i elektronički potpis u užem smislu, kao metodu zaštite sadržaja elektroničkog dokumenta ili elektroničke komunikacije,

konu o informatičkoj djelatnosti upozoravao na opasnost od udvostručivanja nadležnosti i primjene raznorodnih standarda koji bi mogli popratiti informatizaciju.

[12] Teško je oteti se dojmu da su projekti reforme državne uprave poput famoznog programa Hitro.hr, kao i ostale informatizacijske "strategije" zapravo ponajprije politički projekt, za razliku od, primjerice, njemačkog plana osuvremenjivanja državne uprave *Bund*Online 2005. ili novijeg e-Government 2.0 plana za prilagodbu njemačke državne uprave *online* poslovanju.

[13] Dogodile su se i neke zakonodavne inicijative, poput nekih odredaba Zakona o elektroničkoj ispravi, koje nisu imale podlogu u komparativnoj praksi.

[14] Nikšić, S., *Elektronički potpis u skladu sa smjernicom 1999/93/EC*, Pravo u gospodarstvu, *vol*. 39. *no*. 5, Zagreb, 2000., str. 258.

i elektronički certifikat čija je uloga pouzdano potvrditi identitet neke pravne ili fizičke osobe.[15]

Elektronički potpis osnovna je tehnologija provjere autentičnosti digitalnog dokumenta. O kvalitetnom pravnom i tehničkom okviru uvođenja elektroničkog potpisa u svakodnevni život ovisi i kvaliteta usluga državne uprave i gospodarstva u dobu elektroničke komunikacije.[16] Bez legalne upotrebe elektroničkog potpisa nema ni prostora za legalizaciju rada elektroničkih agenata[17], svakako ne u široj poslovnoj primjeni.

Prije analize hrvatskog i poredbenog pravnog okvira regulacije instituta elektroničkog potpisa treba istaknuti nekoliko zahtjeva koji se stavljaju pred zakonodavca i tijela državne uprave kako bi elektronički potpis zaživio.

Osnovni zahtjev koji se stavlja pred elektronički potpis je pitanje potvrđivanja izvornosti, odnosno autentičnosti potpisnika i sadržaja potpisane komunikacije. Elektronički potpis baziran na bilo kojoj tehnologiji koja neće jamčiti, u najvećoj mogućoj mjeri, da je elektronički dokument njime potpisan autentičan, sadržajno i u pogledu oznake autora, neće biti prihvaćen u pravnom prometu.[18]

Nadalje, elektronički potpis treba biti jednostavan za upotrebu i za korisnike i za tijela koja jamče njegovu autentičnost.

---

[15] Dragičević, *op. cit*. u bilj. 2, str. 87 i 88.

[16] Pitanje uređenja i upotrebe elektroničkog potpisa pitanje je od iznimne važnosti i za prelazak na moderniju i efikasniju razinu funkcioniranja cijelog državnog upravnog aparata, od tijela središnje državne vlasti poput ministarstva i središnjih državnih ureda, do mnogobrojnih agencija koje pokrivaju ostala područja od javnog interesa.

[17] Pravnu definiciju elektroničkih agenata još je 1999. dao američki *Uniform Electronic Transactions Act* (UETA). UETA je model zakon koji je pripremila američka Nacionalna konferencija povjerenika za usuglašavanje državnih zakona (National Conference of Commissioners on Uniform State Laws). Taj model zakon uključen je u državnu legislativu 47 američkih saveznih država te propise Distrikta Kolumbije te Puerto Rica i Djevičanskih otoka. National Conference of State Legislatures, http://www.ncsl.org/default.aspx?tabid=13484 (3. veljače 2011.).

[18] Elektronički potpis koji nije zaštićen nekom vrstom kriptografije, zapravo i nije potpis u užem smislu te riječi, odnosno ne može imati funkciju ekvivalentnu potpisu učinjenom rukom. Potpis učinjen rukom, osim informacije (samog teksta koji se sastoji od osobnog imena, prezimena ili znakova), i svojim grafičkim prikazom govori o identitetu potpisnika (kroz stil i način pisanja, čime se bavi znanost forenzičke analize rukopisa). Oznaka autora učinjena elektroničkim putem bez mjere osiguranja autentičnosti ne može služiti istoj svrsi, kao što ni tiskana komunikacija koja nije vlastoručno potpisana ili drukčije označena u pravilu ne može poslužiti za identifikaciju autora.

Treće, radi promicanja upotrebe elektroničkog potpisa, ali i radi više razine pravne sigurnosti, osim komercijalnih pružatelja usluge certificiranja nužan je i javni institucionalni okvir, odnosno tijelo državne uprave koje će voditi bazu podataka s registriranim elektroničkim potpisima.

I konačno, četvrti uvjet kvalitetnog usvajanja elektroničkog potpisa u svakodnevni život je izjednačavanje vrijednosti elektroničkog i vlastoručnog potpisa. Iako će se taj uvjet moći ispuniti tek nakon što prva tri budu zadovoljena, bez ovog koraka elektronički će potpis ostati samo tehnološki kuriozitet ograničen na neke aspekte elektroničke trgovine.

Donošenje Zakona o elektroničkom potpisu i s njime povezanih provedbenih propisa nužan je prvi korak, no nikako i posljednji kad je riječ o regulaciji elektroničkog potpisa i usvajanju njegove upotrebe i od javnih i od privatnih tijela, no ovu konstataciju ne treba shvatiti kao poziv na donošenje nove regulative prije nego što se teorijski i praktično ne ispita doseg i učinak postojeće.

Elektronička isprava kao poseban pravni institut

Digitalni dokument potpisan ispravnim i certificiranim elektroničkim potpisom čini praktičnu, uporabnu cjelinu koju je zakonodavac odlučio regulirati i u našem pravu.

Osiguravajući oznaku identiteta osobe i sadržaja elektroničkog dokumenta elektronički potpis i elektronički certifikat nužan su preduvjet, pravno i tehnički, definicije i bitka pojma elektroničke isprave.

Neka zakonodavstva, pa tako i hrvatsko, koriste se pojmom elektroničke isprave kako bi pripremila pravni okvir za interpretaciju sadržaja dokumenta u elektroničkom obliku i njegove pravne snage, za razliku od drugih, a osobito sustava *common lawa* koji u pravilu ne nalaze potrebnim stvoriti novi pravni institut samo da bi postigli izjednačavanje valjanosti dokumenata na papiru i onih u elektroničkom obliku.[19]

[19] Sustavi *common lawa* uključuju odredbe o elektroničkom potpisu u svoje relevantne pravne kodifikacije, a pravnu valjanost i važnost elektroničkih dokumenata postižu odredbom o zabrani njihove diskriminacije u usporedbi s onima na papiru pod uvjetom upotrebe elektroničkog potpisa koji kroz kriptografske metode jamči autentičnost sadržaja i autora (što bi uglavnom odgovaralo i u Europi prihvaćenoj definiciji naprednog elektroničkog potpisa). Primjeri koji potkrepljuju tu tvrdnju su američki *Electronic Signatures in Global and National Commerce Act* (ESIGN) ili britanski *Electronic Communications Act* iz 2000. U nekoj mjeri može se spomenuti i kanadski *Personal Information Protection and Electronic Documents Act* (PIPEDA) iz 2000., iako on po-

Valja istaknuti da je zakonodavac u konačnom prijedlogu zakona bio svjestan da je takvo normativno rješenje relativna rijetkost ne samo u svjetskoj praksi, već i u užem kontinentalnom pravnom krugu.[20]

Štoviše, ni zakonodavstvo Europske unije ne poznaje pojam elektroničke isprave kao posebnog pravnog instituta.[21]

U hrvatskom pravu Zakon o elektroničkoj ispravi s kraja 2005. posljednji je od triju zakona koji su imali zadatak pripremiti pravni okvir za elektroničku trgovinu u trenucima kad je ona, širenjem širokopojasnog interneta, postala realnost i u Republici Hrvatskoj.

Uz Zakon o elektroničkom potpisu i Zakon o elektroničkoj trgovini, Zakonom o elektroničkoj ispravi definira se posebna vrsta dokumenta, elektronička isprava koja u praksi treba biti izjednačena s ispravama izdanima na papiru (pod određenim zakonskim uvjetima), čime je po mišljenju zakonodavca tada trebao biti zaokružen potreban pravni okvir kako bi elektronička trgovina bila adekvatno regulirana i zaštićena u usporedbi s tradicionalnim oblicima poslovanja. Osnovni cilj Zakona o elektroničkoj ispravi[22] bio je dati zakonsku osnovu izjednačavanja vrijednosti tradicionalnih potpisanih dokumenata i isprava izdanih u papirnatom obliku s onima izdanima u elektroničkom obliku, što je i ispunjeno odredbom o izjednačavanju pravne snage elektroničke isprave s onom izdanom na papiru.

---

sebno definira elektroničke dokumente kao poseban pravni institut, što nije široko prihvaćen pristup problemu priznavanja dokumenata i komunikacije učinjene elektroničkim putem.

[20] Lisičar, H., *Mogućnosti uporabe elektroničke isprave i elektroničkog dokumenta u parničnom postupku*, Zbornik Pravnog fakulteta u Zagrebu, *vol.* 60, br. 6, Zagreb, 2010., str. 1395.

[21] "Potrebno je istaknuti da se u svega nekoliko zemalja započelo pristupati izdvojenom reguliranju uporabe elektroničkih dokumenata, dok se u većini zemalja u kojima se pravno uređuje uporaba elektroničkih dokumenata, parcijalno regulira ovo područje i to kroz objedinjene zakonske tekstove kojima se uređuje elektronička trgovina, elektronički potpis, elektroničke transakcije i slično. Pri izradi teksta Konačnog prijedloga Zakona o elektroničkoj ispravi izvršen je uvid u postojeća zakonodavstva u zemljama Europske unije, pri čemu je utvrđeno da nema pravne stečevine u ovom području." Središnji državni ured za e-Hrvatsku, *Obrazloženje konačnog teksta prijedloga Zakona o elektroničkoj ispravi*, Poglavlje 1, Zagreb, 2005.

[22] "Prihvaćene odrednice uključivanja Republike Hrvatske u Europsku uniju traže i uređeni pravni sustav u kojem se područje elektroničkog poslovanja zajedno s pravnom valjanosti elektroničkih isprava postavlja kao podloga za donošenje Zakona o elektroničkoj ispravi." *Ibid.*

Zakon dalje uređuje uvjete koji trebaju biti ispunjeni kako bi se neki dokument u digitalnom obliku smatrao elektroničkom ispravom, odnosno kako bi imao dokumentacijsko svojstvo.[23] Osim navedenog, predmet Zakona je i regulacija obveze pohrane elektroničke isprave i drugi zahtjevi koje izdavatelj elektroničke isprave treba ispuniti, a koji osiguravaju pravnu sigurnost pri upotrebi elektroničkih isprava u pravnom prometu.

Odlučiti se za normativno rješenje reguliranja elektroničke isprave kao posebnog pravnog instituta ili protiv toga složeno je pitanje, ne isključivo pravne prirode. Da bismo razumjeli sve razloge za takvo rješenje i protiv njega, trebamo upoznati postojeću regulaciju elektroničkog potpisa te iskustva iz poredbenog prava.

Elektronički potpis u poredbenom pravu

Donošenjem Zakona o elektroničkom potpisu 2002. godine hrvatski je zakonodavac napravio prvi korak prema usvajanju i primjeni elektroničkog potpisa.

U pripremi Zakona hrvatski zakonodavac inspiraciju je uglavnom crpio iz dokumenata Europske unije, kao i nekih multilateralnih međunarodnih organizacija poput Svjetske trgovinske organizacije ili UNCITRAL-a.

Sažeti UNCITRAL-ov model zakon ograničen je samo na pitanje primjene elektroničkog potpisa na području trgovine i u velikoj se mjeri naslanja na odredbe starijeg UNCITRAL-ova model zakona o elektroničkoj trgovini iz 1996.

UNCITRAL-ov model zakon ipak definira pojmove elektroničkog potpisa, certifikata i pružatelja usluge certificiranja i dr. na tehnološki neutralan način. Što se podrazumijeva pod pojmom tehnološke neutralnosti?

Pojam tehnološke neutralnosti u pravnoj teoriji najčešće obuhvaća dva aspekta.

Prvi aspekt odnosi se na usporedbu *on-line* i *off-line* aktivnosti, odnosno poduzimanje neke pravne radnje elektroničkim putem (elektronička komunikacija) ili klasičnom komunikacijom putem teksta ispisanog rukom ili strojno na papiru, ili davanjem izjave na zapisnik u nekom pravnom ili upravnom postupku. Ovdje zahtjevi tehnološke neutralnosti traže da se ni jedna od tih dviju aktivnosti ne diskriminira niti stavlja u povlašten položaj.

[23] Lisičar, *op. cit*. u bilj. 21, str. 1397.

Drugi aspekt tehnološke neutralnosti sastoji se od zahtjeva da se ne preferira određeno tehnološko rješenje. Drugim riječima, pravni propisi trebali bi biti sročeni na takav način da ne favoriziraju ili diskriminiraju određenu tehnologiju.[24]

Tehnološka neutralnost propisa nužan je uvjet postizanja pravne sigurnosti i efikasno osiguravanje djelovanja propisa na budućnost kada trenutačno aktualna tehnologija možda više neće biti u upotrebi.

Pitanje koje se kod određivanja sadržaja pojma tehničke neutralnosti postavlja jest: Smatra li se zakonsko određivanje upotrebe određenog tehničkog principa, odnosno dostignuća, povredom tehničke neutralnosti?

Konkretno, kod elektroničkog potpisa pitanje je je li zakonska specifikacija upotrebe arhitekture javnog i privatnog ključa, tzv. Public Key Infrastructure (PKI)[25], povreda tehničke neutralnosti.

Prva generacija zakona o elektroničkom potpisu

Primjer takvog, tehnološki pristranog (iako za svoje vrijeme svakako naprednog) propisa je *Digital Signature Act* američke savezne države Utah iz 1995. To je ujedno najstariji poznati zakon koji donosi definiciju elektroničkog potpisa, njegov doseg i specificira[26] kako se elektronički potpis treba implementirati da bi se s njegovom upotrebom mogli povezati pravni učinci.

Iz navedene odredbe jasno je da ovaj američki zakonodavac presumira upotrebu arhitekture javnog i privatnog ključa.[27]

S druge strane, UNCITRAL-ov model zakon, američki savezni zakon (*US Federal Electronic Signatures in Global and National Commerce* iz 2000.), kao i zakon savezne države Kalifornije[28] ne prejudiciraju upotrebu tehnologije javnog

[24] Reed, C., *Taking Sides on Technology Neutrality*, (2007) 4:3 *SCRIPTed* 263, Edinburgh, 2004., http://www.law.ed.ac.uk/ahrc/script-ed/vol4-3/reed.asp (3. veljače 2011.).

[25] Dragičević, *op. cit*. u bilj. 2, str. 272.

[26] Tako u članku 401(1) određuje upotrebu digitalnog potpisa potvrđenog od strane certifikacijskog tijela, odnosno kasnije kao presumpciju autentikacije potpisnika traži da primatelj potpisanog dokumenta nema saznanja o tome kako potpisnik dokumenta protupropisno posjeduje tajni, privatni ključ kao dio digitalnog potpisa. Digital Signature Act http://www.jus.unitn.it/users/pascuzzi/privcomp97-98/documento/firma/utah/udsa.html (3. veljače 2011.).

[27] Todd, P., *E-commerce Law*, Cavendish Publishing Limited, London, 2005. str. 127.

[28] Kalifornija je odmah nakon savezne države Utah kao druga američka savezna država regulirala primjenu elektroničkog potpisa na tehnološki neutralan i minimali-

i privatnog ključa već tehnološki neutralno i općenito navode uvjete korištenja i priznanja elektroničkog potpisa u pravnom prometu.

S druge strane, japanski Zakon o elektroničkim potpisima i certifikacijskim uslugama iz 2000., iako ne navodi na koji (tehnički) način će certifikacijski sustav biti izveden, implicira upotrebu PKI-ja.[29]

Iz navedenih primjera očito je da je pitanje tehničke neutralnosti ispočetka podijelilo zakonodavce u dva tabora, jedne koji formulirajući propise izbjegavaju određivanje neke konkretne tehnologije, i druge koji, pokušavajući specificirati sustav zaštite integriteta elektroničkog potpisa preciziraju i koji tehnički, odnosno metodološki pristupa takav sustav zaštite treba sadržavati.

U pristup tzv. funkcionalne ekvivalentnosti, odnosno pravne sustave koji ne specificiraju konkretnu tehnologiju ili pristup kojim bi se imao zajamčiti integritet sustava elektroničkog potpisa, uz UNCITRAL-ov model zakon ubrajali su se i australski Zakon o elektroničkim transakcijama[30] te već navedeni američki federalni Zakon o elektroničkim potpisima u globalnoj i nacionalnoj trgovini.[31]

U pristup tehnološke određenosti, odnosno specificiranja tehnologije (uglavnom zasnovane na modelu PKI) na kojoj će se zasnivati elektronički potpis ubrajali su se, uz navedeni propis američke savezne države Utah, i neki raniji europski propisi, poput prvog njemačkog Zakona o digitalnom potpisu (*Signaturgesetz*) iz 1997. ili talijanskog zakona[32] (tzv. Bassinijev zakon iz ožujka 1997.).

Neki autori[33] uz dva navedena pristupa izdvajaju i treći, tzv. minimalistički pristup, osnovno obilježje kojeg bi bilo svjesno odbijanje ulaženja u detaljniju

stički način, propisavši uvjete potrebne za priznavanje elektroničkog potpisa u komunikaciji s tijelima državne uprave. Smedinghoff and Hill Bro, *Electronic Signature Legislation*, FindLaw legal library, 1999.

[29] Neslužbeni prijevod japanskog zakona (*The Law concerning Electronic Signatures and Electronic Certification Services*, Law *no*. 102 of 2002) dostupan je na stranicama japanskog Ministarstva trgovine, gospodarstva i industrije na adresi www.meti.go.jp.

[30] Tako australski Zakon o elektroničkim transakcijama iz 1999. navodi kako će se dokument smatrati autentičnim ako je potpisan elektroničkim putem tako da je identificiran potpisnik te uzimajući u obzir sve relevantne okolnosti u vrijeme potpisa, ako se metoda potpisa smatra prihvatljivom.

[31] *US Federal Electronic Signatures in Global and National Commerce Act*, 2000. http://www.ftc.gov/os/2001/06/esign7.htm (3. veljače 2011.).

[32] Todd, *op. cit*. u bilj. 27, str. 127.

[33] Aalberts, B.; van der Hof, S., *Digital Signature Blindness. Analysis of legislative approaches toward electronic authentication*, Kluwer, 2000. http://rechten.uvt.nl/simone/Ds-art4.htm#_Toc468692773 (3. veljače 2011.).

regulaciju pitanja elektroničkog potpisa, ne samo s aspekta tehnologije koja bi u tu svrhu bila upotrijebljena, nego i odbijajući precizirati institucionalni okvir potreban za provedbu osiguranja kvalitetne razine zaštite i pouzdanosti elektroničkog potpisa. Minimalistički pristup[34] zadržao bi se dakle na opisu funkcija koje elektronički potpis treba obavljati, ponajprije na području trgovine, te različitim razinama sigurnosti potpisa ovisno o svrsi za koju se koristi.[35] U kontekstu razvoja pravne regulacije elektroničkog potpisa mišljenje ovog autora jest da je minimalistički pristup danas sadržan u okviru pristupa funkcionalne ekvivalentnosti i nije ništa više od povijesnog kurioziteta, svjedok brzine kojom se informacijska tehnologija, a s njom i relevantno pravo, danas razvija.

Što se preostalih dvaju modela tiče, oba imaju i dobrih i loših strana. Tehnološka određenost na razini općeg propisa može značiti pouzdanost u razinu tehničke zaštite koja zauzvrat pruža višu razinu pravne sigurnosti korisnicima.

S druge strane, apstraktnija funkcionalna ekvivalentnost znači jednostavniju mogućnost usvajanja budućih, još boljih ili jednako kvalitetnih, ali jednostavnijih ili jeftinijih tehnologija koje se mogu pojaviti u bilo kojem trenutku, bez potrebe za zakonodavnim izmjenama.

Naravno, prednosti navedenih pristupa mogu vrlo lako postati i njihove mane. Tehnološka određenost može postati tehnološki uteg razvoju pravnih odnosa baziranih na elektroničkom potpisu ako tehnologija informacijskih sustava prijeđe na neki novi nivo u kojem će arhitektura javnog i privatnog ključa biti zamijenjena nečim jednostavnijim i naprednijim. Isto tako, funkcionalna ekvivalentnost može dovesti do pravne nesigurnosti ako se usporedo sa sigurnijim tehnološkim rješenjima pod kapu ekvivalentnosti provuku i neka koja bi omogućila lakše zloporabe.

EU i sustav dvostrukog kolosijeka

Cilj druge generacije propisa koji definiraju elektronički potpis bio je na neki način pomiriti oba prijašnja pristupa, odnosno preuzeti najbolje strane i od jednog i od drugog, što je dovelo do trenda "dvostrukog kolosijeka", od-

[34] Primjer minimalističkog pristupa bio bi UNCITRAL-ov model zakon prema kojem je usvojeno nekoliko nacionalnih zakona, poput hongkonškog "Electronic Transaction Ordinance". Yun Zhao, Regulation of Electronic Signatures and Certification Services in Hong Kong, Kluwert International Encyclopaedia of Laws: Cyber Law, 280-282, str. 101.

[35] Aalberts, van der Hof, *op. cit*. u bilj. 34.

nosno, među ostalim, definiranja dviju zasebnih vrsta elektroničkog potpisa, običnog i "naprednog", odnosno kvalificiranog oblika koji se razlikuju prema uvjetima nastanka i pravnoj snazi.

Ključnu ulogu u promoviranju sustava dvostrukog kolosijeka odigrala je zakonodavna aktivnost Europske unije koja je prilično[36] kasnila u usporedbi s nacionalnim zakonodavstvima najrazvijenijih država, poput Sjedinjenih Država, Velike Britanije ili Njemačke, ali i u usporedbi s multilateralnim organizacijama poput Svjetske trgovinske organizacije ili UNCITRAL-a.

Razlozi kašnjenja bili su dvojaki. Zahvaljujući inicijativama administracije američkog predsjednika Clintona u drugoj polovici devedesetih američko zakonodavstvo pratilo je ekonomski uzlet izazvan širenjem interneta u fazi u kojoj su njime dominirale američke tvrtke i američki interesi. Europske su tvrtke komparativno sporije osvajale internetski prostor od američkih, pa je i interes za donošenjem pravnih okvira elektroničke trgovine općenito, i elektroničkog potpisa konkretno, bio na nižoj razini.

Drugi važan razlog kašnjenja bila su neslaganja među članicama EU-a u vezi s upotrebom kriptografskih standarda.[37]

"Dotcom boom", odnosno izvanredan rast američkoga gospodarstva baziran na tehnološkom napretku i komercijalnoj eksploataciji informacijske tehnologije i povezanog tržišta usluga koje se ubrzano počelo razvijati krajem devedesetih godina prošlog stoljeća potaknuo je EU na intenzivan zakonodavni rad kako bi članice uhvatile priključak sa SAD-om.

---

[36] Nazvati kašnjenje od nekoliko godina u usvajanju potrebne regulative priličnim, može se činiti tendencioznim, stoga treba ponovno upozoriti na brzinu kojom informacijska tehnologija mijenja sve društvene, pa tako i pravne odnose. Kašnjenje od pet godina barem djelomično je "zaslužno" što među deset najvrednijih tehnoloških kompanija na svijetu danas nema ni jedne europske. U popisu Wall Street Journala iz 2010. listu predvodi Cisco, a slijede Microsoft, Apple, Google, Oracle, IBM, Intel, HP, Qualcomm i Dell. Drugi, još važniji razlog, jest pitanje zaštite softverskih patenata, čemu se opiru europska pravna doktrina i praksa, za razliku od američkog pravnog sustava koji dopušta njihovu registraciju. Posljedica tog prijepora je da američke tehnološke kompanije raspolažu nevjerojatnim portfeljima patenata koji pokrivaju sva zamisliva područja informacijske tehnologije, čime su europski tehnološki giganti poput Siemensa, Ericssona ili Nokije čak i prije razvoja novih proizvoda na nekom području tehnike već u startu u nepovoljnijoj poziciji.

[37] Članice Unije prepirale su se o politici kriptografske zaštite, kao i o nedostacima valjanih tehničkih standarda, što je u konačnici prisililo naprednije članice da same donesu odgovarajuću legislativu – v. Todd, *op. cit*. u bilj. 27, str. 127 i dalje.

U relativno kratkom vremenu tijela EU-a pripremila su nekoliko dokumenata koji su trebali promovirati elektroničku trgovinu kao aktivnost od najvišeg interesa za gospodarstvo Unije.

U toj zakonodavnoj inicijativi središnju ulogu ima Direktiva o elektroničkoj trgovini.[38] Cilj Direktive o elektroničkoj trgovini bio je stvoriti pravni okvir elektroničke trgovine u Europi, baziran na načelima slobodnog tržišta, istodobno štiteći javni interes i izbjegavajući pretjeranu regulaciju.

Osim navedenoga, bitan moment koji je potaknuo nastanak Direktive o elektroničkoj trgovini bila je sve različitija praksa rješavanja sporova koji su nastajali na području elektroničke trgovine u pravnim porecima zemalja članica Unije, pa je zadatak te Direktive bio pružiti razinu pravne sigurnosti koja bi potaknula razvoj elektroničke trgovine bez straha od ishoda eventualnih sporova i za potrošače i za pružatelje raznih elektroničkih usluga te druge poslovne subjekte.

Kako je jasno da je pitanje elektroničkog potpisa iznimno važno za pravni okvir elektroničke trgovine, usporedo je, nakon četverogodišnjeg zakonodavnog postupka, na snagu početkom 2000. godine stupila i Direktiva o elektroničkom potpisu 1999/93/EC.[39]

Njezin osnovni zadatak bio je stvoriti jedinstveni zakonodavni okvir za primjenu elektroničkog potpisa na području zemalja članica kako bi se elektronički potpis mogao upotrebljavati u pravnom prometu putem elektroničkih komunikacija s istom pravnom snagom kao i potpis učinjen rukom na papiru.

Osnovna ideja Direktive jest razlikovanje dvaju tipova elektroničkog potpisa, (osnovnog) elektroničkog potpisa i naprednog elektroničkog potpisa.

Prema Direktivi, elektronički potpis su podaci u elektroničkom obliku pridruženi ili logički povezani s drugim podacima i služe kao metoda autentifikacije.

S druge strane, napredni elektronički potpis takav je elektronički potpis koji je:

---

[38] 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"), http://eur-lex.europa.eu/LexUriServ/LexUriServ do?uri=CELEX:32000L0031:EN:HTML (3. veljače 2011.).

[39] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, http://eur-lex.europa.eu/LexUriServ/LexUriServ. do?uri=CELEX:31999L0093:EN:HTML (3. veljače 2011.).

1. jedinstveno povezan s potpisnikom
2. sposoban identificirati potpisnika
3. stvoren upotrebom sredstava pod kontrolom korisnika
4. povezan s podacima tako da je moguće otkriti sve naknadne promjene podataka.

Osim elektroničkog potpisa i naprednog elektroničkog potpisa Direktiva uvodi i pojam **kvalificiranog certifikata**[40]. Navedene definicije iz Direktive svrstavale bi Direktivu u okvir tehnološki određenih propisa s obzirom na to da jasno impliciraju upotrebu tehnologije infrastrukture javnog ključa.

Ipak, u Direktivi je sadržana odredba koja omogućuje funkcionalno tumačenje, odnosno mogućnost da i drugi oblici elektroničkog potpisa, osim onog baziranog na tehnologiji infrastrukture javnog ključa, imaju pravnu snagu.

Tako članak 5. Direktive određuje da zemlje članice neće uskratiti (osnovnom) elektroničkom potpisu mogućnost ostvarivanja pravnih učinaka i upotrebe elektroničkog potpisa kao dokaza u pravnim postupcima samo zato što:

1. potpis je dan u elektroničkom obliku
2. potpis nije baziran na kvalificiranom certifikatu
3. potpis nije baziran na kvalificiranom certifikatu izdanom od strane ovlaštenog certifikacijskog tijela
4. potpis nije učinjen putem posebnog uređaja za stvaranje elektroničkog potpisa.[41]

---

[40] Pojam kvalificiranog certifikata, kao i odgovornosti certifikacijskog tijela, nije sadržan u osnovnom dijelu Direktive, već u aneksima I i II. Da bi se certifikat koji izdaje certifikacijsko tijelo, a koji povezuje podatke iz elektroničkog potpisa uz identitet osobe i potvrđuje njezin identitet, smatrao kvalificiranim, certifikat treba sadržavati: oznaku da je riječ o kvalificiranom certifikatu; oznaku certifikacijskog tijela i države u kojoj je certifikacijsko tijelo osnovano; ime ili pseudonim potpisnika (u tom slučaju treba biti označeno da je riječ o pseudonimu); oznaku o nekom posebnom svojstvu potpisnika koje će biti uključeno ako je to potrebno, odnosno ako to svrha u koju je certifikat izdan zahtijeva; podatke za provjeru certifikata koji odgovaraju podacima za stvaranje potpisa, a koji su pod kontrolom korisnika naprednog elektroničkog potpisa; oznaku trajanja, odnosno početka i kraja važenja certifikata; identifikacijsku oznaku certifikata; napredni elektronički potpis certifikacijskog tijela; ograničenja upotrebe certifikata u pogledu vrste transakcija; ograničenja upotrebe certifikata u pogledu visine vrijednosti transakcija.

[41] Hrvatski Zakon o elektroničkom potpisu u prvoj varijanti nije sadržavao ovu odredbu. Preskakanje zabrane diskriminacije potpisa i ograničenja poput onih iz čl. 6 Zakona prije izmjena i dopuna iz 2008. dovode u pitanje volju zakonodavca da omogući redovitu upotrebu elektroničkog potpisa u pravnom prometu.

Ostali zakoni iz druge generacije propisa o elektroničkom potpisu

Nakon stupanja na snagu europske Direktive o elektroničkom potpisu zemlje članice prilično su brzo usvojile njezine odredbe i integrirale ih u svoje zakonodavstvo.

Među prvima to je učinila Njemačka, koja je isprva, svojim *Signaturgesetzom*[42] iz 1997., bila svrstana među zemlje koje su upotrijebile pristup tehnološke određenosti. Nakon donošenja europske Direktive njemački se zakonodavac brzo priklonio sustavu dvaju kolosijeka, pa je već 2001. na snagu stupio *Gesetz über Rahmenbedingungen für elektronische Signaturen* koji je u njemačko pravo unio definiciju elektroničkog potpisa i naprednog elektroničkog potpisa, sukladno odredbama Direktive.

Češki *Zákon o elektronickém podpisu* i slovački *Zakon o elektronickom podpise* također poznaju pojmove osnovnog i naprednog elektroničkog potpisa, kao i francuski[43], poljski[44], bugarski[45], slovenski[46] i zakoni mnogih drugih zemalja članica EU-a. Konačno, kako ćemo vidjeti, isti je pristup usvojio i hrvatski Zakon o elektroničkom potpisu.

Sustav dvostrukog kolosijeka usvojili su i pravni poreci zemalja izvan Europe. U teoriji je prikazan primjer singapurskog *Electronic Transactions Acta* iz 1998. koji također poznaje dvije kategorije elektroničkog potpisa. Singapurski zakonodavac je uz osnovni elektronički potpis za kvalificiranu kategoriju upotrijebio naziv **sigurni elektronički potpis** (*secure electronic signature*)[47]. Iako je u čl. 17 i čl. 18 singapurskog zakona zakonodavac izbjegao tehnološki pristranu definiciju, upotrijebivši funkcionalno ekvivalentan pristup, čl. 20 ipak spominje upotrebu tehnologije javnog i privatnog ključa.[48]

---

[42] Todd, *op. cit*. u bilj. 27, str. 134.

[43] Décr. No. 2002-535 18. Avr. 2002, relatif à l'évauation et à la certification de la sécurite offerte par les produits et les systémes des technologies de l'information.

[44] Ustawa o podpisie elektronicznym (Dziennik Ustaw z 2001 r. Nr 130 poz. 1450).

[45] Закон за електронния документ и електронния подпис, 2006.

[46] Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP), 2000.

[47] Todd, *op. cit*. u bilj. 27, str. 135.

[48] "(a) the digital signature was created during the operational period of a valid certificate and is verified by reference to the public key listed in such certificate", čl. 20 st. 1 singapurskog *Electronic Transactions Acta* iz 1998., http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN025623.pdf (3. veljače 2011.).

Stanje u hrvatskom zakonodavstvu i praksi prije donošenja Zakona o elektroničkom potpisu

Prije donošenja Zakona o elektroničkom potpisu zakonodavstvo Republike Hrvatske nije sadržavalo zakon ili provedbeni propis koji bi eksplicitno definirao elektronički potpis, premda je u zemljama kontinentalnog pravnog kruga pitanje elektroničkog potpisa obrađivano u nekoliko navrata od sredine devedesetih godina prošlog stoljeća.

Međutim, ako i nije bilo konkretnih zakona, to ne znači da je hrvatska pravna praksa u tom razdoblju bila potpuno nesvjesna tehnoloških promjena koje širom svijeta mijenjaju lice poslovne i upravne prakse.[49]

Tako u tom kontekstu valja izdvojiti u teoriji već spomenutu odluku Vrhovnog suda RH br. Rev. 1227/93 u kojoj Vrhovni sud smatra da je zahtjev pisanog oblika ugovora ispunjen, među ostalim, i kada se stranke sporazume nekim drugim sredstvima koja omogućuju da se sa sigurnošću utvrdi sadržaj i davatelj isprave.[50] Iz navedenog tumačenja moglo bi se iščitati kako je Vrhovni sud tehnički neutralno predvidio i važnost elektroničke komunikacije i budućih autentifikacijskih tehnologija.

Ipak, teško bi bilo tvrditi na osnovi jedne sudske presude, osobito u sustavu u kojem prethodna sudska praksa u pravilu ne vezuje sud, da je u razdoblju prije Zakona o elektroničkom potpisu postojala nakana da se elektroničkoj komunikaciji i elektroničkim ispravama sustavno prizna dokazna vrijednost u sudskim i upravnim postupcima. Kao što smo vidjeli u pregledu komparativne legislative, zakonska regulacija elektroničkog potpisa je i u svjetskim razmjerima fenomen star tek nešto više od petnaest godina.

Zakon o elektroničkom potpisu

Elektronička trgovina podrazumijeva upotrebu najrazličitije informacijske i komunikacijske tehnologije, spajajući potrošače i pružatelje usluga u virtualnom prostoru, bili oni poslovni subjekti, tijela državne uprave ili građani.[51]

Fenomen elektroničke trgovine teško se može razmatrati bez uvida u elektroničke komunikacije i u poslovnom i u pravnom smislu. Rast i razvoj elektroničke trgovine i elektroničkih komunikacija prilika su svakom društvu, a

[49] Matić, *op. cit*. u bilj. 6, str. 56.

[50] *Ibid*., str. 56.

[51] B2B, B2C, B2G.

posebno ekonomski slabije razvijenim sredinama poput naše, da se ubrza gospodarski, znanstveni i društveni razvoj.

Zbog toga je pravodoban razvitak brze, sigurne i praktične pravne zaštite elektroničke trgovine i rješavanja svih vrsta sporova koji se u vezi s njom mogu javiti pitanje od iznimnog društvenog značenja. Čak i male zemlje, bez većeg utjecaja na globalnoj političkoj pozornici, mogu postati centri trgovine, usluga i znanosti ako se dobro pozicioniraju u virtualnom prostoru.

Kao što u virtualnom prostoru postoje mjesta slabe regulative, područja bezakonja gdje *cyber* kriminalci pohranjuju ukradene osobne podatke i trguju njima bez straha od nemoćnog lokalnog pravosuđa[52], isto tako je istinito i suprotno – velike investicije u usluge i servise informacijskog društva traže ne samo jeftinu kvalificiranu radnu snagu, već i siguran pravni okvir.

Imajući to na umu, u skladu s europskom zakonodavnom praksom, Direktivom o elektroničkom potpisu i pripremnim dokumentima koji su Direktivi prethodili[53] i hrvatski je zakonodavac početkom 2002. usvojio Zakon o elektroničkom potpisu – ZEP[54], koji je do sada jedinu izmjenu i dopunu doživio sredinom 2008.[55] Na osnovi Zakona o elektroničkom potpisu (ZEP), kao i njegovih kasnijih izmjena i dopuna, doneseni su i pravilnici koji detaljnije reguliraju neke okvirne odredbe Zakona, ponajprije o pravilima, uvjetima i postupcima certificiranja, povezivanja sustava certifikacije i regulaciji registra davatelja usluga certificiranja elektroničkih potpisa.[56] Osobito u kontekstu provedbenih

[52] "Data haven", vidi Dragičević, *op. cit*. u bilj. 2, str. 13.

[53] Directive on electronic commerce, Community Framework for electronic signatures, European initiative on electronic commerce, Green Paper on the convergence of the telecommunications, media and information technology sectors and the implications for regulation, Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services.

[54] Zakon o elektroničkom potpisu (ZEP), Narodne novine, br. 10/2002.

[55] Zakon o izmjenama i dopunama Zakona o elektroničkom potpisu, Narodne novine, br. 80/2008.

[56] To su:

1. Pravilnik o tehničkim pravilima i uvjetima povezivanja sustava certificiranja elektroničkih potpisa, Narodne novine, br. 89/2002
2. Pravilnik o mjerama i postupcima uporabe i zaštite elektroničkog potpisa i naprednog elektroničkog potpisa, sredstava za izradu elektroničkog potpisa, naprednog elektroničkog potpisa i sustava certificiranja i obveznog osiguranja davatelja usluga izdavanja kvalificiranih certifikata, Narodne novine, br. 54/2002
3. Uredba o djelokrugu, sadržaju i nositelju poslova certificiranja elektroničkih potpisa za tijela državne uprave, Narodne novine, br. 146/2004

propisa Zakona o elektroničkom potpisu treba istaknuti novi pravilnik o izradi elektroničkog potpisa i uporabi sredstva za izradu elektroničkog potpisa koji kontrolira izradu i uporabu elektroničkog potpisa.

Jedan od osnovnih zadataka Zakona bio je, prvi put u hrvatskom pravu, pripremiti pravni okvir korištenja elektroničkog potpisa, odnosno ustrojiti sustav potvrđivanja izvornosti i autentičnosti elektroničke komunikacije bez kojeg nema pouzdanog elektroničkog poslovanja, elektroničke trgovine, a ni elektroničke komunikacije građana prema državnim tijelima.

Već je ranije istaknuto da elektronički potpis može biti bilo koji oblik označavanja autorstva i podrijetla elektroničkih dokumenata. Neke vrste usluga, poput internetskog bankarstva, upotrebljavaju posebne uređaje, *tokene*, kako bi osigurali autentifikaciju svojih korisnika i njihovih interakcija s bankarskim sustavom.

Upotreba posebnih autentifikacijskih uređaja, kao što su tokeni, ili biometrijskih[57] tehnologija česta je u tipiziranim i konkretnim transakcijama poput internetskog bankarstva, no u općoj elektroničkoj komunikaciji heterogenost informacijskih servisa otežava ili čak sprečava upotrebu takvih uređaja.

Stoga je nakana hrvatskog zakonodavca bila zakonom propisati i usvojiti u svjetskim razmjerima istražen i prihvaćen sustav elektroničkog potpisa zasnovan na tehnologiji infrastrukture javnog ključa, odnosno *Public Key Infrastructure* (PKI).[58] Odabir te provjerene tehnologije imao je cilj stvoriti povjerenje poslovne zajednice i najšire javnosti u pouzdanost upotrebe elektroničkog potpisa u svakodnevnom poslovanju te potaknuti njegovu najširu primjenu.

4. Pravilnik o evidenciji davatelja usluga certificiranja elektroničkih potpisa, Narodne novine, br. 54/2002, 112/2007, 107/2010.
5. Pravilnik o izradi elektroničkog potpisa, uporabi sredstva za izradu elektroničkog potpisa, općim i posebnim uvjetima poslovanja za davatelje usluga izdavanja vremenskog žiga i certifikata, Narodne novine, br. 107/2010.

Ovdje treba spomenuti i Popis normizacijskih dokumenata u području primjene Zakona o elektroničkom potpisu i Pravilnika o izradi elektroničkog potpisa, također objavljen u Narodnim novinama, br. 107/2010 koji javnosti daje na uvid europske informacijske i sigurnosne standarde i dokumente koji su poslužili kao preporuke za izradu pravilnika.

[57] Dragičević, *op. cit*. u bilj. 2, str. 97.

[58] PKI je kriptografska metoda zasnovana na koncepciji primjene dvostrukih ključeva u kriptografskoj zaštiti elektroničke komunikacije, ponajprije poruka elektroničke pošte. Svaki korisnik PKI-ja istodobno ima jedan privatni, samo njemu poznat tajni ključ, i jedan javni ključ koji će biti dostupan javnosti putem organizacijske infrastrukture.

Drugi osnovni cilj bio je urediti prava, obveze i odgovornosti fizičkih i pravnih osoba u vezi s pružanjem usluga certificiranja elektroničkog potpisa. Kao što smo već istaknuli, sustav PKI elektroničkog potpisa podrazumijeva mrežu certifikacijskih tijela koja će voditi računa o ispravnosti korisničkih certifikata, pa Zakon o elektroničkom potpisu daje i smjernice o njihovoj organizaciji.[59]

Zakonska definicija pojma elektronički potpis i drugih pojmova

Zakon o elektroničkom potpisu prvi put u hrvatskom pravu definira pojam elektronički potpis i predstavlja *lex specialis*[60] za primjenu elektroničkog potpisa i drugih pojmova vezanih uz upotrebu elektroničkog potpisa, a posebno kod upotrebe elektroničkog potpisa u sudskim i upravnim postupcima.

Osnovni i napredni elektronički potpis

Zakon definira elektronički potpis kao "...skup podataka u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koji služe za identifikaciju potpisnika i vjerodostojnosti potpisanog elektroničkog dokumenta."[61]

Dakle, zakonodavac tumači da je elektronički potpis skup podataka u elektroničkom obliku koji je pridružen nekoj elektroničkoj komunikaciji, poput elektroničke pošte ili nekom elektroničkom dokumentu, a identificira korisnika i potvrđuje potpunost i točnost potpisane komunikacije ili dokumenta.

Sljedeći pojam koji Zakon definira jest pojam naprednog elektroničkog potpisa. Kao što smo u uvodnom izlaganju istaknuli, dualitet osnovnog i naprednog elektroničkog potpisa, odnosno sustav dvostrukog kolosijeka, danas

[59] Čl. 1. ZEP-a glasi: "Ovim se Zakonom uređuje pravo fizičkih i pravnih osoba na uporabu elektroničkog potpisa u upravnim, sudskim i drugim postupcima, poslovnim i drugim radnjama, te prava, obveze i odgovornosti fizičkih i pravnih osoba u svezi s davanjem usluga certificiranja elektroničkog potpisa, ako posebnim zakonom nije drukčije određeno".

[60] Tako odredbe Zakona o parničnom postupku, Zakona o općem upravnom postupku i Zakona o upravnom sudu u vezi s upotrebom elektroničkog potpisa treba razmatrati u skladu s odredbama Zakona o elektroničkom potpisu.

[61] Vidi čl. 2 i čl. 3 ZEP-a. Definicija iz članka 3 neznatno se razlikuje od objašnjenja pojma u čl. 2. Objašnjenje pojma u čl. 2 izravan je prijevod odredaba čl. 2 europske Direktive o elektroničkom potpisu na temelju koje je Zakon o elektroničkom potpisu i nastao. Nije jasno zašto je zakonodavac u čl. 3 tu definiciju ponešto skratio, iako se njezin smisao time nije bitno izmijenio.

prevladava u većini zakonodavstava koja su donijela propise koji reguliraju elektronički potpis.

Napredan elektronički potpis je potpis[62]:

1. koji je povezan isključivo s potpisnikom
2. koji nedvojbeno identificira potpisnika
3. koji nastaje upotrebom sredstava kojima potpisnik može samostalno upravljati i koja su isključivo pod nadzorom potpisnika
4. koji sadržava izravnu povezanost s podacima na koje se odnosi i to na način na koji nedvojbeno omogućuje uvid u bilo koju izmjenu izvornih podataka.

Uvjeti koji se postavljaju pred napredni elektronički potpis prilično su strogi, no nužni ako je cilj njime zamijeniti tradicionalni potpis na papiru.

Naravno, kao što je i ručni potpis na papiru tehnički moguće krivotvoriti sa svim posljedicama koje to predstavlja za pravnu sigurnost, isto se može reći i za napredni elektronički potpis. Međutim, uvjeti koje zakonodavac propisuje u najvećoj mogućoj mjeri osiguravaju dokumente i komunikaciju potpisanu naprednim elektroničkim potpisom od zloporabe.[63]

Što se pravne snage naprednog elektroničkog potpisa tiče, on ima istu pravnu snagu i zamjenjuje vlastoručni potpis ili pečat.[64]

Već je ranije istaknuto da je jedna od osnovnih zadaća Zakona promovirati upotrebu elektroničkog potpisa u trgovini, među poslovnim subjektima, ali i u komunikaciji države i građana. Kako bi zakonodavac zabranio diskriminaciju elektroničkog potpisa, odnosno potaknuo njegovu upotrebu, Zakon zabranjuje njegovo osporavanje:

1. zato što je potpis dan u elektroničkom obliku
2. zato što nije zasnovan na kvalificiranom certifikatu
3. zato što kvalificiran certifikat nije izdan od strane akreditiranog davatelja usluga certifikacije

---

[62] Vidi čl. 2 i čl. 4 ZEP-a.

[63] Iako u čl. 4 Zakona upotreba PKI-ja nije izrijekom spomenuta, odredba iz st. 1 točke 4 o "... izravnoj povezanosti s podacima na koje se odnosi i to na način na koji nedvojbeno omogućava uvid u bilo koju izmjenu" nagovještava upotrebu PKI-ja ili neke slične tehnologije u kojoj je upotreba osobnog ključa i pripadajućeg uređaja pod nadzorom potpisnika jedini ispravan način potpisivanja komunikacije ili elektroničkog dokumenta, a naknadne ili neovlaštene izmjene dovest će do neispravnog potpisa i upozorenja za primatelje i potpisnika kod izdavanja sigurnosnog certifikata.

[64] Vidi čl. 5 ZEP-a.

4. zato što elektronički potpis nije izrađen upotrebom sredstva za izradu naprednog elektroničkog potpisa.[65]

U izvornom tekstu Zakona iz 2002. čl. 6 sadržavao je iznimke od zabrane diskriminacije elektroničkog potpisa samo zato što je dan u elektroničkom obliku i ostalih razloga. Te su iznimke bile znatna ograničenja na polje primjene elektroničkog potpisa.[66]

Vjerojatan razlog uključivanja takve odredbe bio je izdvojiti pravne poslove i akte od posebnog društvenog interesa, koji bi bio ugrožen eventualnim zloporabama elektroničkog potpisa, pa je zakonodavac isključio mogućnost primjene elektroničkog potpisa u sklapanju navedenih pravnih poslova.

Uzimajući u obzir opreznost zakonodavca, argumenti protiv takvog ograničenja čine se ipak uvjerljivijima. Cilj svakog propisa o elektroničkom potpisu trebao bi biti promocija naprednijeg, bržeg, efikasnijeg i sigurnijeg poslovanja, a ne njegova sabotaža. Premda je u noveli Zakona iz 2008. sporni članak promijenjen, a poduža lista ograničenja izbačena, zbog šest godina koje je ZEP tako oslabljen proveo na snazi ostaje dojam kako zakonodavac u tom trenutku zapravo nije shvaćao prednosti koje elektronička komunikacija pruža ili je bio skeptičan oko njezine mogućnosti primjene pa je donosio propise samo zato što je to politički trenutak tražio.

Konačno, ako zakonodavac za neke konkretne pravne poslove želi postaviti ograničenje koje će spriječiti da se oni obavljaju na daljinu i/ili uz upotrebu elektroničke komunikacije i elektroničkog potpisa, onda neka takvu odredbu unese u zakone koji reguliraju to područje, primjerice Zakon o nasljeđivanju,

---

[65] Vidi čl. 6 ZEP-a. Nepostojanje ove odredbe u originalnom tekstu Zakona iz 2002. još je jedan primjer pretjerane opreznosti zakonodavca oko ozbiljnije upotrebe elektroničkog potpisa.

[66] Članak 6 ZEP-a u izvornom obliku glasio je: "Ne može se odbiti prihvaćanje dokumenta samo zbog toga što je sačinjen i izdan u elektroničkom obliku s elektroničkim potpisom ili naprednim elektroničkim potpisom. Iznimno, stavak 1. ovoga članka ne odnosi se na: 1. pravne poslove kojima se vrši prijenos vlasništva na nekretninama ili se uspostavljaju druga stvarna prava na nekretninama, 2. oporučne poslove, 3. imovinske predbračne, odnosno bračne ugovore, 4. opterećenje i otuđenje imovine za koje je potrebno odobrenje centra za socijalnu skrb, 5. ugovore o predaji i raspolaganju s imovinom za života, 6. ugovore o doživotnom uzdržavanju i sporazume u svezi s nasljeđivanjem, 7. darovne ugovore, 8. druge pravne poslove za koje je posebnim zakonom propisano da se sastavljaju u obliku javnobilježničkog akta, odnosno isprave, 9. druge pravne poslove ili radnje za koje je posebnim zakonom ili na temelju zakona donesenim propisom izričito određena uporaba vlastoručnog potpisa u dokumentima na papiru ili ovjera vlastoručnog potpisa."

Zakon o vlasništvu i drugim stvarnim pravima itd. Ipak, bilo bi mudro u takvom djelovanju suspregnuti strah od novog i ograničenja zadržati na razini u kojoj najmanje utječu na dinamiku suvremenih društvenih odnosa.

Pojam i uloga vremenskog žiga (digitalnog vremenskog biljega)

Originalna inačica Zakona o elektroničkom potpisu iz 2002. godine nije uključivala definiciju vremenskog žiga. Izmjenama i dopunama iz 2008. pojam "vremenski žig" uveden je za oznaku digitalnog vremenskog biljega.

Vremenski žig, odnosno digitalni vremenski biljeg metoda je označavanja nastanka elektroničkog dokumenta i bilježenja promjena njegova sadržaja kroz vrijeme, odnosno riječ je o mehanizmu provjere kada je digitalni dokument kreiran, odnosno promijenjen, što je važno za utvrđivanje vjerodostojnosti dokumenata.[67]

Zakonodavac u točki 3 prvog stavka čl. 2 Zakona definira pojam i ulogu vremenskog žiga kao elektronički potpisanu potvrdu izdavatelja koja potvrđuje sadržaj podataka na koje se odnosi u navedenu vremenu.

Elektronički zapis

U točki 5 istog stavka zakonodavac je unio definiciju elektroničkog zapisa kao cjelovitog skupa podataka koji su elektronički generirani, poslani, primljeni ili sačuvani na elektroničkom, magnetnom, optičkom ili drugom mediju.[68]

Zakonodavac dalje navodi kako "sadržaj elektroničkog zapisa uključuje sve oblike pisanog i drugog teksta, podatke, slike i crteže, karte, zvuk, glazbu, govor, računalne baze podataka".[69]

---

[67] Dragičević, *op. cit*. u bilj. 2, str. 107.

[68] Nabrajanje vrsta medija koji služe za pohranu elektroničkih podataka je, iz razloga tehničke neutralnosti, suvišno. Sve navedene tehnologije medija služe istoj svrsi, pohrani podataka. Je li elektronički zapis pohranjen na postojećem magnetnom, optičkom ili *flash* mediju, ili budućem biološkom – s aspekta pravne znanosti potpuno je svejedno.

[69] ZEP, čl. 2 st. 1 točka 5. Uz ovu definiciju elektroničkog zapisa ostaje pitanje što je s, primjerice, videozapisima ili metapodacima stvorenima od strane pretraživačkih servisa. Očito su i te dvije kategorije, izvan svake sumnje, elektronički zapisi, no zakonodavac ih nije uključio u zakonsku definiciju.

Potpisnik elektroničkog potpisa

Potpisnik elektroničkog potpisa, u smislu odredaba Zakona o elektroničkom potpisu, jest osoba koja posjeduje sredstvo za izradu elektroničkog potpisa kojim se potpisuje, a djeluje u svoje ime ili u ime fizičke ili pravne osobe koju predstavlja.

Dakle, elektroničkim potpisom može se služiti svaka fizička osoba u vlastito ime, kao i kategorije osoba koje imaju pravo zastupanja pravnih osoba ili drugih fizičkih osoba.[70]

Sredstva i podaci za izradu elektroničkog i naprednog elektroničkog potpisa

Za izradu elektroničkog potpisa potrebna su sredstva za izradu, odnosno odgovarajuća računalna oprema ili računalni program kojima se potpisnik koristi pri izradi elektroničkog potpisa.

Ovdje može biti riječ o prilagođenim računalima opće namjene s nekim od javno i komercijalno dostupnih softverskih rješenja, a moguća je i upotreba specijaliziranih rješenja koja kombiniraju *proprietary* hardverska i softverska rješenja.

Za izradu naprednog elektroničkog potpisa zakonodavac propisuje određene zahtjeve bez ispunjenja kojih se elektronički potpis ne može kvalificirati kao napredni elektronički potpis:

1. da se podaci za izradu naprednog elektroničkog potpisa mogu pojaviti samo jednom te da je ostvarena njegova sigurnost
2. da se podaci za izradu naprednoga elektroničkog potpisa ne mogu ponoviti te da je potpis zaštićen od krivotvorenja pri korištenju postojeće raspoložive tehnologije
3. da podatke za izradu naprednoga elektroničkog potpisa potpisnik može pouzdano zaštititi protiv korištenja od strane drugih[71]
4. da sredstvo za izradu naprednoga elektroničkog potpisa ne smije prilikom izrade naprednoga elektroničkog potpisa promijeniti podatke koji se potpisuju ili onemogućiti potpisniku uvid u te podatke prije procesa izrade naprednoga elektroničkog potpisa.

[70] Odvjetnici, članovi uprava ili upravnih odbora dioničkih društava, članovi uprava društava ograničene odgovornosti, prokuristi, osobe ovlaštene za zastupanje udruga građana itd.

[71] Čl. 2 st. 1 točka 7 i čl. 9 ZEP-a.

Navedeni zahtjevi, osobito jedinstvenost podataka za izradu naprednog elektroničkog potpisa i zaštita od krivotvorenja presumiraju upotrebu kriptografskih računalnih tehnologija poput PKI-ja. Upotreba kriptografskih algoritama generira jedinstvene javne i privatne ključeve koji su jedinstveni za svakog potpisnika i ne mogu se rekonstruirati ili reproducirati bez potpisnikova znanja.

Sredstva i podaci za verificiranje elektroničkog potpisa

Dokumenti i komunikacija potpisana elektroničkim potpisom moraju odgovarati zabilježenom jedinstvenom elektroničkom potpisu potpisnika. Svaka komunikacija i dokument potpisan elektroničkim potpisom trebaju se moći podvrgnuti provjeri (verifikaciji, ovjeri).

U tu svrhu služi odgovarajuća računalna oprema i računalni programi kao sredstva te kontrolni kodovi, odnosno javni ključevi kao podaci dostupni certifikacijskim tijelima kako bi se provela provjera autentičnosti i integriteta podataka zaštićenih elektroničkim potpisom.[72]

Certifikati i kvalificirani certifikati

Digitalni, odnosno elektronički certifikat je isprava u digitalnom obliku kojom se potvrđuje identitet neke fizičke ili pravne osobe.[73] Najčešći oblik digitalnog certifikata je onaj kriptografski zaštićen, povezan s upotrebom javnih ključeva u PKI-ju. Digitalni certifikat služi za provjeru pripadnosti javnog ključa nekoj fizičkoj ili pravnoj osobi.

Digitalni certifikat izdaje davatelj usluge izdavanja digitalnih certifikata, odnosno neko tijelo javne vlasti ili trgovačko društvo koje pruža tu vrstu usluge – tzv. *Certificate Authority*.[74] Certifikacijsko tijelo izdaje certifikate pod određenim uvjetima. Ono je odgovorno svojim korisnicima za podatke sadržane u certifikatima.[75]

ZEP definira elektronički certifikat kao "...potvrdu u elektroničkom obliku koja povezuje podatke za verificiranje elektroničkog potpisa s nekom osobom i potvrđuje identitet te osobe."[76]

---

[72] ZEP, čl. 2 st. 1 točka 9 i 10.

[73] Dragičević, *op. cit*. u bilj. 2, str. 106.

[74] *Ibid*., str. 106.

[75] ZEP, čl. 9.

[76] ZEP, čl. 2 st. 1 točke 11 – 13.

Zakon uvodi i pojam kvalificiranog certifikata. Kvalificirani certifikat je elektronička potvrda kojom davatelj usluge izdavanja kvalificiranih certifikata potvrđuje napredni elektronički potpis.

Poput naprednog elektroničkog potpisa koji certificira, kvalificirani certifikat treba zadovoljiti neke dodatne uvjete u usporedbi s osnovnim certifikatom. Ispunjenje tih uvjeta uvjetuje valjanost kvalificiranog certifikata, a s time i valjanost i pravnu snagu naprednog elektroničkog potpisa.

Uvjeti koje ZEP propisuje za valjanost kvalificiranog certifikata odnose se na sadržaj kvalificiranog certifikata i traže da kvalificirani sadržaj sadržava[77]:

1. oznaku o tome da se radi o kvalificiranom certifikatu
2. identifikacijski skup podataka o osobi koja izdaje certifikat (osobno ime; ime oca ili majke; nadimak, ako ga osoba ima; datum rođenja; prebivalište, odnosno boravište; naziv pravne osobe i sjedište, ako certifikat izdaje pravna osoba)
3. identifikacijski skup podataka o potpisniku (osobno ime, ime oca ili majke, nadimak, ako ga osoba ima, datum rođenja, prebivalište, odnosno boravište)
4. podatke za verificiranje elektroničkog potpisa koji odgovaraju podacima za izradu elektroničkog potpisa koji su pod kontrolom potpisnika
5. podatke o početku i kraju važenja certifikata
6. identifikacijsku oznaku izdanog certifikata (brojčanu ili drugu oznaku te datum izdavanja)
7. napredni elektronički potpis davatelja usluge izdavanja kvalificiranih certifikata
8. ograničenja vezana za uporabu certifikata, ako ih ima
9. ograničenja u odnosu na važnost pravnih radnji za koje se daje certifikat, ako ih ima.

Obveze i odgovornost davatelja certifikacijskih usluga

Upotreba elektroničkog potpisa, osobito naprednog elektroničkog potpisa, u najužoj je mjeri povezana s uspostavljanjem sustava certifikacije elektroničkog potpisa, odnosno uspostavljanjem mreže tijela koja će jamčiti autentičnost i ispravnost elektroničkog potpisa.

[77] ZEP, čl. 11 st. 2.

Usluga certifikacije elektroničkog potpisa teško je usporediva s nekom aktivnošću u stvarnom, materijalnom svijetu.[78] Možda bismo mogli usporediti jedan aspekt te aktivnosti, provjeru identiteta pošiljatelja elektroničke komunikacije zaštićene elektroničkim potpisom s provjerom osobnih dokumenata, primjerice osobne iskaznice, kada šaljemo preporučenu poštansku pošiljku.

Međutim, drugi aspekt elektroničkog potpisa i elektroničkog certifikata, onaj koji jamči integritet sadržaja poruke kroz primjenu kriptografskih metoda, nema odgovarajućeg pandana u stvarnoj, materijalnoj komunikaciji.

U sustavu zaštite elektroničke komunikacije infrastrukturom javnog ključa (PKI), središnje mjesto zauzimaju davatelji usluge certifikacije (*Certification Authority*, CA), odnosno tijela koja pohranjuju ključeve, odnosno elektroničke kodove koji služe za autentikaciju i kriptografsku zaštitu elektroničke komunikacije.

Njihova je uloga prepoznata i regulirana i u hrvatskom pravu odredbama Zakona o elektroničkom potpisu.[79] Načelno, certifikacijska tijela mogli bismo podijeliti u dvije kategorije, ovisno o motivu za bavljenje tom djelatnosti.

Komercijalna certifikacijska tijela su takvi davatelji usluge certifikacije koji svoju djelatnost, izdavanje elektroničkih certifikata, naplaćuju. Javna certifikacijska tijela su tijela državne uprave, javne institucije i druga javna tijela koja djelatnost izdavanja elektroničkih certifikata ne naplaćuju.

I komercijalna i javna certifikacijska tijela dužna su prijaviti svoju djelatnost Ministarstvu gospodarstva, rada i poduzetništva u roku od osam dana prije započinjanja s radom. Ministarstvo o davateljima usluge certificiranja vodi središnju evidenciju propisanu Pravilnikom o evidenciji davatelja usluga certificiranja elektroničkih potpisa.[80]

Kako bi neki davatelj usluga certifikacije mogao davati uslugu certifikacije kvalificiranog certifikata, potrebnu za certifikaciju naprednog elektroničkog potpisa, mora ispuniti uvjete propisane Zakonom koji osiguravaju sigurnost i kvalitetu usluge certifikacije.[81] U prvom redu riječ je o sposobnosti davatelja

[78] Reed, C., *Internet Law: Text and Materials*, Cambridge University Press, 2nd Edition, Cambridge, 2004., str. 161.

[79] Konkretnije, njihove obveze i odgovornost reguliraju čl. 15 – 18 te osobito IV. glava Zakona pod nazivom Prava, obveze i odgovornosti potpisnika i davatelja usluga certificiranja (čl. 23 – 35 Zakona).

[80] Čl. 16 ZEP-a i čl. 1 Pravilnika o registru davatelja usluga certificiranja elektroničkih potpisa koji izdaju kvalificirane certifikate, Narodne novine, br. 54/2002 i 112/2007.

[81] Lista uvjeta za izdavanje kvalificiranog certifikata iz članka 17 Zakona u osnovi je prenesena iz Aneksa II europske Direktive.

usluga da osigura pouzdanu i sigurnu uslugu, vodi ažuran upisnik potpisnika kako bi se u svakom trenutku moglo identificirati potpisnika ili mu u kratkom vremenu omogućiti opoziv usluge certificiranja.

Od davatelja usluge traži se da raspolaže odgovarajuće osposobljenom tehničkom službom koja ima odgovarajuća specijalistička znanja i iskustvo na području primjene tehnologija elektroničkog potpisa i njima srodnih sigurnosnih tehnologija. U tu svrhu, premda zakonodavac to nije posebno istaknuo, procjenu o odgovarajućoj osposobljenosti valja gledati kroz primjenu međunarodnih standarda za informacijsku sigurnost.[82]

Među ostalim uvjetima valja izdvojiti zahtjev osiguranja pohrane svih relevantnih podataka koji se odnose na kvalificirani certifikat tijekom odgovarajućeg razdoblja. Od davatelja usluge certificiranja traži se pohrana podataka o potpisnicima, izdanim certifikatima, listama opozvanih certifikata, kao i tehničke podatke nastale bilježenjem rada sustava. Za sve navedene podatke Uredba od davatelja usluga certifikacije traži i izradu sigurnosnih kopija (*backupa*[83]) podataka pohranjenih na zaštićenome mjestu.[84]

Zanimljiva je odredba točke 8 st. 1 čl. 17 Zakona o osiguranju financijskih sredstava za djelovanje u skladu s odredbama Zakona. Zakonodavac svjestan tehnološki intenzivne prirode djelovanja certifikacijskih tijela, potrebe koju ona imaju za visoko specijaliziranom obrazovanom radnom snagom i važnošću djelatnosti kojom se imaju baviti, Zakonom propisuje kao uvjet postojanje "osigurane zadovoljavajuće razine financijskih resursa".[85] Naravno, ni u ZEP-u ni u provedbenim propisima nigdje se ne daje konkretan okvir što će se, od strane zakonodavca ili nadzornih tijela poput Ministarstva gospodarstva, rada i poduzetništva ili Državnog inspektorata, smatrati "zadovoljavajućom razinom financijskih resursa".

---

[82] Najpoznatiji međunarodni standardi na području informacijske sigurnosti su ISO 17799, odnosno ISO 27000 serija standarda, uključivši najnoviji ISO 27003:2010.

[83] Dragičević, *op. cit*. u bilj. 2, str. 82. Izrada *backupa* ili sigurnosnih kopija podrazumijeva redovitu pohranu podataka i programa i njihovo čuvanje na zaštićenome mjestu.

[84] Rok za pohranu podataka određen je na deset godina, s opaskom da Uredba zahtijeva da elektronički mediji koji će poslužiti za pohranu tih podataka trebaju jamčiti opstojnost podataka na rok od najmanje dvadeset godina.

[85] Točka 8 st. 1 čl. 17 ZEP-a glasi: "8. osiguranu zadovoljavajuću razinu financijskih resursa kako bi mogli djelovati u skladu sa zahtjevima utvrđenima ovim Zakonom".

O odgovornosti davatelja usluge izdavanja elektroničkog certifikata

Čl. 6 europske Direktive o elektroničkom potpisu daje minimalni okvir odgovornosti davatelja usluge izdavanja elektroničkog certifikata.[86] Prema odredbama Direktive davatelj usluge izdavanja elektroničkog certifikata odgovara:

1. za preciznost vremena izdavanja i eventualnog povlačenja certifikata
2. za sadržaj podataka sadržanih u certifikatu u trenutku izdavanja certifikata
3. za komplementarnu upotrebu podataka za izradu i verifikaciju (certifikaciju) elektroničkog potpisa u slučaju da davatelj usluge generira oba ova skupa podataka
4. za nepravovremeno djelovanje u slučaju povlačenja ili suspenzije certifikata.

Hrvatski zakonodavac pitanje odgovornosti davatelja usluga certifikacije elektroničkog potpisa u tekstu Zakona povezuje s obvezom ugovaranja osiguranja rizika od odgovornosti za štetu zbog obavljanja usluge izdavanja elektroničkog certifikata.[87] Zakon, dakle, propisuje obvezu ugovaranja osiguranja za sve davatelje usluge certificiranja.

Sukladno odredbama europske Direktive, i hrvatski Zakon za davatelja usluga certifikacije uključuje odgovornost za štetu nastalu uporabom certifikata bilo kojem tijelu, odnosno pravnoj ili fizičkoj osobi do koje je došlo zbog propuštanja certifikacijskog tijela da nadzire certifikacijski postupak, odnosno odgovara za točnost podataka sadržanih u kvalificiranom certifikatu u vrijeme izdavanja certifikata te za ispunjavanje ostalih uvjeta koje Zakon traži za izdavanje kvalificiranog certifikata.[88] U slučaju nastanka štete prema potpisniku ili

[86] Čl. 6 st. 1 Direktive o elektroničkom potpisu.

[87] Zakonodavac je u Zakon prenio odredbe o odgovornosti davatelja usluga iz europske Direktive. Tako u čl. 18 Zakona kojim je određena obveza za davatelja usluga da osigura rizik od odgovornosti za štetu na temelju obavljanja usluge izdavanja elektroničkog certifikata, odnosno certifikacije elektroničkog potpisa ističe slučajeve odgovornosti za štetu u svezi s točnošću podataka u certifikatu (točka 1 i 2).

[88] Čl. 29 ZEP-a u tom smislu navodi obveze certifikacijskog tijela: 1. osigurati da svaki kvalificirani certifikat sadrži sve potrebne podatke; 2. provesti potpunu provjeru identiteta potpisnika za kojega provodi usluge certificiranja; 3. osigurati točnost i cjelovitost podataka koje unosi u evidenciju izdanih certifikata; 4. u svaki certifikat unijeti osnovne podatke o sebi; 5. omogućiti svakoj zainteresiranoj osobi uvid u identifikacijske podatke davatelja usluga certificiranja i uvid u dozvolu za izdavanje kvalificiranih certifikata; 6. voditi ažurno točnu i sigurnosnim mjerama zaštićenu

trećima davatelj usluga odgovarat će za štetu, osim ako uspije dokazati da je postupao s dužnom pažnjom, u skladu s pravilima o davanju usluge certifikacije, odnosno da nije postupao nemarno.[89]

Tekst Zakona u vezi s odgovornošću davatelja certifikacijskih usluga nepotrebno je nomotehnički nejasan i nepregledan. Odredbe europske Direktive za minimalni okvir odgovornosti davatelja certifikacijskih usluga jasne su. Iz nepoznatih razloga hrvatski zakonodavac ni u izmjenama i dopunama Zakona nije otklonio nomotehničke nelogičnosti[90] iz izvornog teksta Zakona, pa postoji stvarna mogućnost pogrešne interpretacije Zakona, osobito u pogledu sadržaja odgovornosti davatelja usluga. Imajući u vidu utjecaj europske Direktive na sadržaj čitavog Zakona o elektroničkom potpisu, kao opći trend usvajanja europskih propisa zbog usuglašavanja hrvatskog i europskog pravnog okvira, trebalo bi u teoriji i praksi što prije zauzeti stajalište o podudarnosti sadržaja odgovornosti davatelja usluga iz obaju ovih propisa.

U poslovanju davatelja usluge certificiranja javit će se situacije gdje će biti potrebno bez odgađanja ukinuti postojeći certifikat. Kao što, primjerice, banke od svojih korisnika traže da bez odgađanja prijave gubitak kartice, kako eventualni kradljivac ili nepošteni nalaznik ne bi zloporabom napravio štetu, tako i certifikacijska tijela trebaju voditi evidenciju o potpisnicima koje certificiraju na način da je, zbog saznanja o gubitku ili krađi korisničkih podataka, moguće brzo staviti certifikatom zaštićeni potpis izvan snage.

Odredbe hrvatskog Zakona u kontekstu ukidanja certifikata prate odredbe Direktive. Čl. 30 Zakona regulira uvjete pod kojima davatelj usluga certificiranja ima obvezu prekidanja te usluge, odnosno stavljanja certifikata, a time i

evidenciju certifikata koja mora biti javno dostupna; 7. voditi točnu i sigurnosnim mjerama zaštićenu evidenciju nevažećih certifikata; 8. osigurati vidljiv podatak o točnom datumu i vremenu (sat i minuta) izdavanja odnosno opoziva certifikata u evidenciji izdanih certifikata; 9. čuvati sve podatke i dokumentaciju o izdanim certifikatima najmanje 10 godina pri čemu podaci i prateća dokumentacija mogu biti i u elektroničkom obliku; 10. primjenjivati odredbe zakona i drugih propisa kojima je uređena zaštita osobnih podataka.

[89] U pravnim sustavima *common lawa* uobičajen je obrnut pristup. Davatelju usluga odgovornost za štetu treba dokazati, Todd, *op. cit*. u bilj. 27, str. 154 – 155.

[90] Ponajprije, riječ je o nejasnom definiranju okvira odgovornosti. Dok u čl. 25 zakonodavac sasvim jasno definira odgovornost potpisnika, odnosno korisnika usluge certifikacije elektroničkog potpisa, isto se ne može reći i za okvir odgovornosti davatelja usluga. Osobitu zabunu unosi činjenica da je čl. 18 Zakona, ključan za interpretaciju opsega odgovornosti davatelja usluga, izdvojen iz Glave IV. Zakona, koja se zove Prava, obveze i odgovornosti potpisnika i davatelja usluga certificiranja.

certificiranog elektroničkog potpisa, izvan snage.

Iz tehnologije elektroničkog potpisa i elektroničkog certifikata, odnosno izabrane metode PKI-ja proizlazi mogućnost da fizička ili pravna osoba posjeduje više elektroničkih potpisa, odnosno više elektroničkih certifikata. Ovisno o razlozima ukidanja, takva pravna okolnost može i ne mora imati utjecaja na opstojnost ostalih elektroničkih potpisa, odnosno certifikata kojima se potpisnik koristi. Primjerice, smrt ili gubitak poslovne sposobnosti fizičke osobe sigurno će utjecati i na opoziv ostalih certifikata, ali promjena statusa ili neke kvalitete (primjerice, potpisnik je prestao biti broker, odvjetnik itd.) može se odnositi samo na jedan od njegovih elektroničkih identiteta (npr. elektronički certifikat koji odvjetnicima izdaje Odvjetnička komora), dok na ostale nema nikakva utjecaja.

O priznanju certifikata izdanih od davatelja usluga certifikacije sa sjedištem u inozemstvu

Sve moderne informacijske tehnologije namijenjene su upotrebi u okolišu svjetske informacijske mreže – interneta. Zahtjevi elektroničke trgovine okrenuti su otvorenoj komunikaciji koja ne poznaje granice država, nacionalnih pravnih poredaka ni pravnih tradicija čitavih kultura.

Svaki pokušaj regulacije elektroničke trgovine i elektroničke komunikacije treba stoga imati u vidu nesporni globalni karakter tih društvenih fenomena.

Zakonodavni rad tijela Europske unije kontinuirano promovira zajednički europski pravni okvir razvoja elektroničke trgovine i elektroničke komunikacije. Sukladno tim smjernicama, i Direktiva o elektroničkoj trgovini traži od zemalja članica Unije da ne diskriminiraju rad certifikacijskih tijela smještenih u drugim državama, pod uvjetom da ona poštuju pravila koja Unija kroz Direktivu stavlja pred certifikacijska tijela u zemljama članicama.

Hrvatski je zakon izjednačio valjanost domaćih certifikata, odnosno certifikata izdanih od strane certifikacijskih tijela sa sjedištem u Republici Hrvatskoj, i onih sa sjedištem u nekoj od zemalja članica Europske unije.

Što se valjanosti certifikata izdanih od strane certifikacijskih tijela sa sjedištem izvan Republike Hrvatske i Europske unije tiče, hrvatski zakon (sukladno odredbama europske Direktive) priznat će njihovu valjanost ako davatelj usluga certificiranja ispunjava uvjete za izdavanje kvalificiranih certifikata iz ZEP-a te je dobrovoljno akreditiran u Republici Hrvatskoj ili jednoj od zemalja članica Europske unije, ako neki domaći davatelj usluga certificiranja koji

ispunjava uvjete za izdavanje kvalificiranih certifikata iz ovoga Zakona jamči za takve certifikate jednako kao da su njegovi, ako tako odredi bilateralni ili multilateralni sporazum između Republike Hrvatske i drugih zemalja ili međunarodnih organizacija te ako tako odredi bilateralni ili multilateralni sporazum između Europske unije i trećih zemalja ili međunarodnih organizacija.[91]

Elektronički potpis u drugim hrvatskim propisima

U razdoblju od donošenja izvornog teksta Zakona o elektroničkom potpisu u siječnju 2002. do donošenja izmjena i dopuna Zakona u srpnju 2008. izgubljeno je mnogo vremena, a elektronički potpis nije zaživio u praksi.

Izmjene i dopune Zakona približile su regulaciju elektroničkog potpisa u hrvatskom pravu odredbama europske Direktive u mjeri u kojoj, uz neke iznimke, više ne postoje bitne razlike u regulaciji elektroničkog potpisa i elektroničkog certifikata.

Sredinom 2008. zakonodavac je sustavno počeo uvoditi pojam elektroničkog potpisa i elektroničke komunikacije u postupovne propise hrvatskog prava. Zakon o općem upravnom postupku i Zakon o kaznenom postupku izravno upotrebljavaju pojam elektroničkog potpisa, dok Zakon o parničnom potpisu upućuje na posebno zakonodavstvo.

Elektronički potpis u Zakonu o općem upravnom postupku

U novom Zakonu o općem upravnom postupku[92] zakonodavac uvodi mogućnost pokretanja postupka, odustanka od zahtjeva, ulaganja podnesaka, obavještavanja, dostave i izdavanja potvrda elektroničkim putem.[93]

Osobito je važan čl. 75 ZUP-a koji u st. 2 kaže: "Podnesci dostavljeni u elektroničkom obliku s elektroničkim potpisom sukladno zakonu smatrat će se vlastoručno potpisanim". Ova odredba u skladu s odredbama europske Direktive o elektroničkom potpisu u vezi sa zabranom diskriminacije elektroničkog potpisa u hrvatskom upravnom postupku napokon izjednačuje elektroničku komunikaciju s onom tradicionalnom, putem podnesaka ispisanih na papiru.

---

[91] ZEP, čl. 30.

[92] Zakon o općem upravnom postupku, Narodne novine, br. 47/2009.

[93] Čl. 41, čl. 46, čl. 71, čl. 75, čl. 83, čl. 94 i čl. 159 Zakona o općem upravnom postupku.

Zanimljivo je da zakonodavac u ZUP-u izričito ne traži primjenu naprednog elektroničkog potpisa, iako se samo upotreba naprednog elektroničkog potpisa, zaštićenog valjanim kvalificiranim elektroničkim certifikatom, može smatrati ravnopravnom zamjenom za vlastoručni potpis. Ipak, odredbu st. 2 trebalo bi tumačiti isključivo kao uputu na Zakon o elektroničkom potpisu, a mogućnost izjednačavanja elektroničkog potpisa s vlastoručnim potpisom promatrati isključivo kroz odredbe Zakona o elektroničkom potpisu.

Elektronički potpis u Zakonu o kaznenom postupku

Novi Zakon o kaznenom postupku donesen krajem 2008. predviđa mogućnost elektroničke komunikacije i podnošenja podnesaka u obliku elektroničkih isprava.[94]

ZKP izričito u čl. 79 st. 1 spominje elektronički potpis kao nužan uvjet kako bi se neki podnesak mogao podnijeti i zaprimiti elektroničkim putem, istaknuvši elektronički potpis kao osigurano utvrđenje jednoznačnog obilježja kojim se utvrđuje sastavljač elektroničke isprave.[95] U kontekstu elektroničkog

[94] Zakon o kaznenom postupku, Narodne novine, br. 152/2008.

[95] Članak 79 ZKP-a pod naslovom "Elektronička isprava" navodi uvjete pod kojima je moguća elektronička komunikacija sa sudom, ali i postupanje suda, državnog odvjetništva i policije u slučaju da elektronička komunikacija nije potpuna, te odredbe o trenutku primitka elektroničke komunikacije, koja se smatra zaprimljenom u trenutku registracije poruke u informacijskom sustavu suda, za razliku od, primjerice, pisane komunikacije upućene poštom, koja se smatra zaprimljena trenutkom zaprimanja u poštanskom uredu:

(1) Podnesci koji se prema ovom Zakonu pisano sastavljaju i potpisuju, mogu se podnijeti u obliku elektroničke isprave ako su izrađeni, otpremljeni, primljeni i pohranjeni primjenom dostupne informacijske tehnologije, i osiguravaju utvrđivanje jednoznačnog obilježja kojim se utvrđuje sastavljač elektroničke isprave (elektronički potpis).

(2) Podnesak u obliku elektroničke isprave smatra se zaprimljenim u informacijskom sustavu ili uređaju suda, državnog odvjetništva, policije ili odvjetničkog ureda, trenutkom registracije njihovog prijema u tom sustavu ili uređaju. Primatelj osigurava uredno djelovanje automatiziranog sustava potvrde prijema. Ako pošiljatelj ne zaprimi potvrdu prijema, obavijestit će o tome primatelja, pa ukoliko u roku kojeg je odredio ne primi tu potvrdu, smatra se da podnesak u obliku elektroničke isprave nije poslan.

(3) O podnesku u obliku elektroničke isprave iz stavka 2. ovog članka, sud, državno odvjetništvo i policija sastavljaju službenu zabilješku. U slučaju nerazumljivog ili nepotpunog podneska postupit će se prema članku 78. stavku 3. i 4. ovog Zakona.

potpisa ovu odredbu valja tumačiti kao uputu na upotrebu naprednog elektroničkog potpisa potvrđenog kvalificiranim certifikatom.

Elektronički potpis u Zakonu o parničnom postupku

Recentnim izmjenama i dopunama Zakona o parničnom postupku iz 2008.[96] u hrvatski parnični postupak uvedena je zakonska mogućnost elektroničke komunikacije suda i stranaka.

ZPP sintagmom "elektroničkim putem u skladu s posebnim zakonom" upućuje na poseban zakon koji bi regulirao elektronički vid dostave dokumenata u parničnom postupku. Iz teksta Zakona moglo bi se zaključiti kako nije riječ o zakonima koji reguliraju elektronički potpis i elektroničku ispravu, što su rješenja koja su prihvaćena u ZKP-u i ZUP-u, već da se za ostvarenje odredaba ZPP-a čeka donošenje posebnog zakona.[97]

ZPP tako omogućuje dostavu pismena[98], zakazivanje ročišta[99] te dostavu obrazaca i drugih očitovanja u sklopu ostvarivanja pravosudne suradnje u Europskoj uniji, sukladno odredbama Uredbe br. 1393/2007 Europskog parlamenta i Vijeća o dostavi sudskih i izvansudskih isprava u građanskim i trgovačkim predmetima u državama članicama.[100] Pitanje dostave jedno je od kontroverznijih u hrvatskom parničnom postupku jer iz prakse je razvidno da stranke u postupku izbjegavanjem primitka pismena i obavijesti mogu nepovoljno utjecati na tijek i ukupno trajanje parničnog postupka. Tome bi se možda moglo stati na kraj uvođenjem "e-procesa"[101], odnosno mogućnosti da se pojedine parnične radnje i cijele etape parničnog postupka odvijaju u virtualnom prostoru, a ne u sudnici.

(4) U ocjeni pitanja pravne valjanosti, uporabe, prometa, čuvanja i tajnosti podnesaka u obliku elektroničke isprave odgovarajuće se primjenjuju odredbe posebnih propisa.

(5) Ministar nadležan za pravosuđe donijet će posebne propise o tehničkim uvjetima za podnošenje elektroničke isprave.

96 Izmjene i dopune Zakona o parničnom postupku, Narodne novine, br. 84/2008.

97 Lisičar, *op. cit*. u bilj. 21, str. 1411.

98 Zakon o parničnom postupku, st. 1 čl. 133, koji glasi: "Pismena se dostavljaju preko pošte ili preko određenoga sudskog službenika, odnosno sudskog namještenika, preko nadležnoga tijela uprave, preko javnoga bilježnika ili neposredno u sudu odnosno elektroničkim putem u skladu s posebnim zakonom".

99 ZPP, čl. 495.

100 ZPP, čl. 507.

101 Lisičar, *op. cit*. u bilj. 21, str. 1401.

U kojoj je mjeri zakonska mogućnost elektroničke komunikacije u praksi uistinu primjenljiva, nije sasvim jasno s obzirom na to da postojeći sustav za upravljanje sudskim spisima (eSpis) ne pruža sve potrebne mogućnosti[102] komunikacije koje bi bile potrebne da bi se moglo reći kako je e-proces praktična mogućnost.

Elektronička isprava u poredbenom i hrvatskom pravu

Hrvatski je zakonodavac Zakonom o elektroničkoj ispravi napravio normativni iskorak u kontekstu regulacije elektroničkog potpisa i pravne važnosti dokumenata nastalih i distribuiranih u digitalnom obliku.

Prevladavajući model regulacije pravne važnosti elektroničkih dokumenata oslanja se ponajprije na regulaciju elektroničkog potpisa. Stvaranje novog pravnog pojma "elektroničke isprave" kao posebnog pravnog pojma, iako intrinzično povezanog s pojmom elektroničkog potpisa i elektroničkog certifikata, trebalo bi, smatrao je zakonodavac, unaprijediti pravni okvir, pripremiti ga za promjene koje upotreba informacijskih tehnologija donosi i u odnosu poslovnih subjekata (B2B, B2B itd.[103]) i u odnosu državnih tijela i građana (G2G, G2B[104]).

Komparativnopravno, pojam elektroničke isprave u smislu odredaba Zakona o elektroničkoj ispravi relativno je rijetko rješenje. Posvetiti poseban zakon regulaciji elektroničke isprave još je veći raritet. Neke od zemalja čija su zakonodavstva odlučila posebno regulirati elektroničku ispravu tako su primjerice Azerbejdžan, Filipini, Kanada i Litva.[105]

Hrvatski Zakon o elektroničkoj ispravi

Strukturno sastojeći se od triju glavnih dijelova, općih odredaba, definicije elektroničke isprave i odredaba vezanih za njezino stavljanje u promet, Zakon načelno određuje da elektronička isprava ima istu pravnu snagu kao i ona izdana na papiru, osim u slučaju da se drugim zakonima izričito traži isprava na papiru.

---

[102] *Ibid*., str. 1407.

[103] Dragičević, *op. cit*. u bilj. 2, str. 41.

[104] *Ibid*., str. 42.

[105] Lisičar, *op. cit*. u bilj. 21, str. 1395.

Mnogi hrvatski zakoni izričito spominju papirnate isprave, a tek neki u posljednje vrijeme dopunjeni ili doneseni tehnološki neutralno (bez posebne oznake) podrazumijevaju izdavanje elektroničke isprave ili izričito dopuštaju da se ona izda i u elektroničkom obliku.

Zakon daje dvojaku definiciju elektroničke isprave, pa bi se moglo izdvojiti definiciju elektroničke isprave u širem smislu, kao jednoznačno povezan cjelovit skup podataka koji su elektronički oblikovani (izrađeni s pomoću računala i drugih elektroničkih uređaja), poslani, primljeni ili sačuvani na nekom (elektroničkom, magnetnom, optičkom ili drugom) mediju i koji sadržavaju svojstva kojima se utvrđuje izvor (stvaratelj), utvrđuje vjerodostojnost sadržaja te dokazuje postojanost sadržaja u vremenu.

U užem smislu, elektronički dokument je elektronička isprava koja ima pravnu valjanost jednaku onoj isprave izdane na papiru koja se sastoji od dvaju neodvojivih dijelova, općeg koji čini sam sadržaj elektroničke isprave, i posebnog koji čine jedan ili više ugrađenih elektroničkih potpisa i podaci o vremenu nastajanja (završetka izrade) elektroničke isprave, kao i druga dokumentacijska svojstva.[106]

Ti uvjeti odnose se na primjenu elektroničkog potpisa i elektroničkog certifikata kako bi se nedvojbeno i jednoznačno utvrdio autor i sadržaj elektroničke isprave, kao i njezina cjelovitost i nepovredivost.[107]

Autor ovog rada smatra da je zakonska definicija elektroničke isprave konkretno i općenito donošenje posebnog zakona samo nova manifestacija stare zablude da će donošenje novih propisa riješiti neki postojeći problem ili potaknuti neko novo, korisno djelovanje. Iako je ponekad teško procijeniti realni utjecaj općih propisa na neko društveno ponašanje, u ovom slučaju, samo zato što već pet godina imamo Zakon o elektroničkoj ispravi, teško da smo kao tranzicijsko društvo bliže informatičkom društvu i gospodarstvu baziranom na visokoj tehnologiji.

Osnovni argument u prilog ovoj tezi bio bi broj rezervi, poput odredbe iz čl. 1 Zakona, o tome kako se elektronička isprava neće prihvaćati u situacijama u kojima drugi zakoni izričito traže izdavanje isprave otisnute na papiru.

---

[106] Čl. 7 Zakona o elektroničkoj ispravi, Narodne novine, br. 150/2005.

[107] Članci 5, 6, i 7 Zakona o elektroničkoj ispravi. Zakon traži od izdavača elektroničke isprave da omogući pristup sadržaju elektroničke isprave kroz cijelo vrijeme dokumentacijskog ciklusa, kao i da se koristi oblikom zapisa koji čitatelju omogućuje jednostavno čitanje sadržaja.

Naravno, takvih zakona je izrazito mnogo, čime je u startu doseg Zakona o elektroničkoj ispravi i upotreba elektroničke isprave u pravnom prometu nepotrebno ograničen.

Drugi bi argumenti bili više sociološkog i psihološkog karaktera, o čemu je u stručnim publikacijama već bilo govora.[108] Otpor novim tehnologijama, nepoznavanje prednosti koje one nude i preuveličan strah od opasnosti koje prijete u digitalnom okružju osnovni su razlozi zadržavanja na tradicionalnom papirnatom obliku komunikacije. Srećom, kako dolazi vrijeme generacija odraslih s informacijskom tehnologijom, tako će i strah od digitalnog ustupiti mjesto čuđenju prema papirnatom.

Iz današnje perspektive čini se vjerojatnije da je Zakon o elektroničkoj ispravi trebao poslužiti više političkoj nego pravnoj svrsi, kao poželjan normativni paket dobrih želja i namjera bez čvrste veze s realnošću.

Bilo bi mnogo korisnije da je pitanje elektroničke isprave, ako je uopće potrebna posebna regulacija digitalnog dokumenta zaštićenog naprednim elektroničkim potpisom, riješeno u okviru Zakona o elektroničkom potpisu te u okviru propisa koji reguliraju rad tijela državne uprave i drugih javnih tijela.

Zaključne napomene

Hrvatski je zakonodavac u hrvatski pravni sustav uveo elektronički potpis sukladno recentnoj komparativnopravnoj praksi. Suvremeni okvir zakonske regulacije elektroničkog potpisa počinje usvajanjem europske Direktive o elektroničkom potpisu 1999. godine, koja je u pravnu teoriju uvela razlikovanje između osnovnog elektroničkog potpisa i njegova kvalificiranog oblika, naprednog elektroničkog potpisa.

Unatoč očekivanjima stručne i poslovne zajednice[109], kao i unatoč odredbama o zabrani diskriminacije elektroničkog potpisa, realnost je da u hrvatskoj poslovnoj i upravnoj praksi elektronički potpis nije zamijenio ručni, što je znak da prednosti usvajanja informacijskih tehnologija još nisu u dovoljnoj mjeri prepoznate u hrvatskom društvu i pravnoj praksi.

Hrvatski zakonodavac još je u izvornoj inačici Zakona o elektroničkom potpisu usvojio većinu rješenja sadržanih u europskoj Direktivi. Izmjene i dopune Zakona o elektroničkom potpisu iz 2008. godine dodatno su usuglasile pravni

[108] Vojković, *op. cit*. u bilj. 9, str. 469.

[109] *Ibid.*, str. 469.

okvir elektroničkog potpisa i elektroničkog certifikata u Republici Hrvatskoj s onim na snazi u EU-u.

Od 2008. godine do danas važni postupovni zakoni, poput Zakona o kaznenom postupku, Zakona o parničnom postupku i Zakona o općem upravnom postupku usvojili su odredbe koje omogućuju elektroničku komunikaciju osiguranu elektroničkim potpisom, a u pripremi su i drugi propisi kojima se proširuje utjecaj Zakona o elektroničkom potpisu.

S druge strane, Zakon o elektroničkoj ispravi nepotrebno je ograničio upotrebu elektroničkih dokumenata. S jedne strane inzistirati na posebnom propisu i novom pravnom institutu, a s druge ograničiti njegovu primjenu do razine nepotrebnosti, nikako neće ubrzati tranziciju u informacijsko društvo.

U svrhu usvajanja elektroničkog potpisa i aktivnije upotrebe elektroničke komunikacije u pravnom prometu, a osobito u radu državnih tijela, treba još poraditi na institucionalnom okviru. Priroda tehnologije PKI-ja koja je trenutačna tehnička osnova sustava elektroničkog potpisa zahtijeva agilna i sposobna certifikacijska tijela, ali i odgovarajuću stručnost i tehničku opremljenost korisnika, osobito pravosuđa i tijela državne uprave.

U ovom trenutku čini se da tijela državne uprave tome još nisu dorasla, a brojne zakonske obveze i odgovornost povezana s postupkom certificiranja elektroničkog potpisa čine djelatnost certifikacije neprivlačnom privatnom sektoru.

Summary

Tihomir Katulić *

THE DEVELOPMENT OF LEGAL REGULATION OF THE ELECTRONIC SIGNATURE, ELECTRONIC CERTIFICATE AND ELECTRONIC DOCUMENT IN CROATIAN AND COMPARATIVE LAW

In the introduction the author talks about the key role of electronic signature in the legal regulation of electronic commerce as a fast growing branch of economy concerned with numerous legal issues regarding the impact of information technology on the society and law. The article analyses the conditions to be met electronic signature in order to replace hand signature in legal transactions, including an assessment of the importance of hand signature as a means of authenticating the author of a document, and confirming its contents. Further, the author gives an outline of the intensive legislative activity in the area of electronic signature, starting from the first laws of the mid 1990s to date. In spite of the short timeframe of 15 years, several different approaches have developed in the regulation of electronic signature and related issues, applied by legislatures worldwide, in order to provide substantial legal security in electronic commerce and other legal relations established via electronic communication. The author differentiates between several legislative phases with different theoretical and practical outlooks on the character of the regulation of electronic signature. The first phase looks at the relationship between two opposing approaches to the necessity to specify the technological basis of electronic signature, while the second analyses the nature of the two-track system and the legal framework based thereupon, predominant in the European legal circle. Based on experiences of comparative law, the auther goes on to analyse selected provisions from the Electronic Signature Act, taking a look at its impact on other laws, particularly the Electronic Document Act. In the final part of the article the author takes a critical look at the institute of electronic document, to conclude with an overview of the application of electronic signature in the Croatian legal practice to date.

Key words: electronic signature, advanced electronic signature, electronic document, electronic commerce, electronic communication, information technology, Public Key Infrastructure, Electronic Data Interchange

* Tihomir Katulić, LL. B., Assistant, Faculty of Law, University of Zagreb, Trg maršala Tita 14, Zagreb

Zusammenfassung

Tihomir Katulić *

DIE ENTWICKLUNG DER RECHTLICHEN REGELUNG DER ELEKTRONISCHEN SIGNATUR, DES ELEKTRONISCHEN ZERTIFIKATS UND DER ELEKTRONISCHEN URKUNDE IM KROATISCHEN RECHT UND IN DER RECHTSVERGLEICHUNG

Einführend stellt der Autor die Schlüsselrolle der elektronischen Signatur in der rechtlichen Regelung des elektronischen Handels als schnell wachsendem Wirtschaftszweig dar, der zahlreiche rechtliche Fragen im Zusammenhang mit dem Einfluss der Informationstechnik auf Gesellschaft und Recht aufwirft. Angefangen bei der Prüfung, wie wichtig die eigenhändige Unterschrift als Mittel der Authentifizierung des Verfassers eines Dokuments ist, bis zur Bestätigung des Dokumentinhalts werden die Voraussetzungen vorgestellt, die von der elektronischen Signatur zu erfüllen sind, um die eigenhändige Unterschrift im Rechtsverkehr ersetzen zu können. Danach wird die intensive gesetzgeberische Aktivität im Bereich der Regelung der elektronischen Signatur von den ersten Gesetzen Mitte der neunziger Jahre des letzten Jahrhunderts bis heute präsentiert. Trotz des kurzen Zeitraums von nur fünfzehn Jahren lassen sich in der reichhaltigen vergleichenden Praxis mehrere unterschiedliche Ansätze verfolgen, wie verschiedene Gesetzgeber in der Welt versuchten, die elektronische Signatur und verwandte Fragen zu regeln, um im elektronischen Handel und anderen rechtlichen Beziehungen, die im Wege elektronischer Kommunikation vollzogen werden, eine angemessene rechtliche Sicherheit zu ermöglichen. Der Autor unterscheidet einige Etappen in der Gesetzgebung, die von verschiedenen theoretischen und praktischen Standpunkten zum Wesen der Regelung der elektronischen Signatur geprägt sind. In der ersten Etappe wird das Verhältnis zwischen zwei gegensätzlichen Ansätzen bezüglich der Spezifizierung der technischen Grundlagen der elektronischen Signatur thematisiert, während in der zweiten die Natur des doppelgleisigen Systems und der darauf beruhende im europäischen Rechtskreis dominante rechtliche Rahmen besprochen werden. Aufgrund von Erfahrungen aus der Rechtsvergleichung analysiert der Autor ausgewählte Bestimmungen aus dem Gesetz über die elektronische Signatur und nimmt dabei Bezug auf den Einfluss dieses Gesetzes auf andere, insbesondere das Gesetz über die elektronische Urkunde. Im letzten Teil des Beitrags wird die Kritik am Institut der elektronischen Signatur behandelt. Der Autor schließt mit einem Kommentar zur bisherigen Anwendung der elektronischen Signatur in der kroatischen Rechtspraxis.

Schlüsselwörter: elektronische Signatur, fortschrittliche elektronische Signatur, elektronische Urkunde, elektronischer Handel, elektronische Kommunikation, Informationstechnik, Public Key Infrastructure, Electronic Data Interchange

* Tihomir Katulić, Dipl-Jurist, Assistent an der Juristischen Fakultät in Zagreb, Trg maršala Tita 14, Zagreb