Elektronické právne úkony v práve Slovenskej republiky v kontexte s úpravou v EÚ

Andrea Moravčíková*

V nasledujúcich riadkoch sa pokúsim objasniť systém umožňujúci uznať právny úkon vyhotovený v elektronickej podobe ako rovnocenný s úkonom v písomnej podobe, ktorou sa tradične rozumie podoba papierová, a to v podmienkach Slovenskej republiky v súvsťažnostiach s úpravou v EÚ.

Prvá a druhá časť príspevku je venovaná problematike elektronického podpisu, keďže podľa platného Občianskeho zákonníka [1] v ust. § 40 je písomný právny úkon považovaný za platný, ak je podpísaný konajúcou osobou. Keďže od roku 2002 je súčasťou platnej právnej úpravy zákon o elektronickom podpise, väčšia časť príspevku je venovaná jeho analýze.

S platnosťou právnych úkonov súvisí aj problematika vzniku a platnosti zmlúv, ktorej je venovaná tretia časť. Považovala som za potrebné spomenúť aj vzorovú úpravu, ktorá vznikla na pôde UNCITRALu v rokoch 1996 až 2001.

Záverečná časť príspevku stručne hodnotí možnosti a spôsoby v oblasti civilného konania a dokazovania, ktoré vzhľadom na novosť problematiky nemožno doložiť judikatúrou, keďže žiadna zatiaľ neexistuje, a to ani v dostupných európskych zdrojoch.

* JUDr. Andrea Moravčíková, Ph.D., Právnická fakulta UK Bratislava

[1] Zákon č. 40/1964 Z. z. Občiansky zákonník.

1. TRENDY V OBLASTI ELEKTRONICKEJ KOMUNIKÁCIE

V poslednej dobe sa venuje výrazná pozornosť otázkam elektronickej komunikácie vo vzťahu k možnostiam jej využitia ako pre komerčné účely tak v oblasti štátnej administratívy. Odhliadnuc od nástupu stále novších technických a programových prostriedkov pre e-commerce resp. e-business, je tu stále zreteľnejšia potreba právneho zaradenia takejto formy komunikácie. Nejde ani tak o „zaškatuľkovanie" nejakého procesu pod už známe inštitúty, je celosvetovým trendom vytváranie samostatnej legislatívy, rešpektujúcej špecifické požiadavky elektronickej komunikácie.

Legislatívne aktivity v oblasti elektronickej komunikácie treba vnímať ako prínos do tejto oblasti ľudskej činnosti Jedinou snahou regulácie je vymedziť, aký druh komunikácie, resp. aké technické a programové prostriedky komunikácie, budú považované za dostatočne bezpečné a teda následná vymožiteľnosť právnych úkonov nimi urobených bude jednoduchšie preukázateľná a bude požívať vysokú mieru dôveryhodnosti. Nemusím zdôrazňovať, že práve pre oblasť komunikácie s verejnými inštitúciami je nevyhnutné presne stanoviť stupne bezpečnosti a spôsoby bezpečnej elektronickej komunikácie.

1.1 ELEKTRONICKÝ PODPIS A JEHO PRINCÍPY

Aby mohli platiť uskutočnené právne úkony v elektronickej podobe, musí existovať minimálne taký stupeň ochrany komunikácie a vymieňaných dokumentov, aký je zaručený pri klasickej papierovej komunikácii. Z toho vyplýva potreba legislatívne definovať elektronický podpis, stanoviť záväzné pravidlá pre jeho používanie, čo by mu dalo rovnaké postavenie ako podpisu ručnému. Pre väčšinu z nás podpis znamená významnú skutočnosť týkajúcu sa vyjadrenia vôle, súhlasu s podpisovanou listinou a v nej uvedenými údajmi. Podpis je akýsi rituál – už po stáročia na znak súhlasu a platnosti úkonu pripájame k jeho písomnému zneniu svoj podpis. Podpis má niekoľko významných funkcií – identifikuje osobu, ktorá ho vyznačila, vyjadruje súhlas tejto osoby s textom, pod ktorým je podpis pripojený, resp. preukazuje, že táto osoba je buď autorom textu alebo sa s jeho obsahom stotožňuje. Z legálneho hľadiska je nevyhnutnou súčasťou písomného právneho úkonu. Písomná forma môže mať dve podoby – tzv. holograf, vlastnoručne napísaná a podpísaná listina, a tzv. alograf, listina napísaná inou osobou ako podpisujúcim. Okrem podpisu nájdeme v právnej literatúre aj zmienku o tzv. znamení vlastnej ruky, čo je „podpis" osoby, ktorá nevie alebo nemôže písať (tradične tri krížiky).[2]

Podpis ručný nie je nikde presne definovaný, elektronický podpis má z technického hľadiska viacero prejavov. Veľmi všeobecne povedané, elektronickým podpisom je čokoľvek, čo nejakým spôsobom **nasvedčuje o spojení prejavu vôle** (napr. zmluvy) **s určitou fyzickou identitou**, t.j. napr. aj „podpísanie" e-mailu vlastným menom[3]. Prirodzene, bezpečnosť takéhoto dokumentu a najmä jeho dôveryhodnosť je ohrozená. Vstupom nových počítačových technológií sa musel zmeniť aj prístup k forme právnych úkonov a právny systém sa bude musieť vysporiadať so spôsobom ich akceptácie ako platných a vynútiteľných aktov. Vzhľadom na netradičnú formu elektronických správ ešte stále pretrváva polemika, o aký právny úkon ide a akým spôsobom je možné dokazovať jeho platnosť v prípade sporu. Občiansky zákonník pred prijatím zákona o elektronickom podpise obsahoval ustanovenie § 40, podľa ktorého písomná forma právneho úkonu bola zachovaná, ak je právny úkon urobený telegraficky, ďalekopisom, alebo elektronickými prostriedkami, ktoré umožňujú zachytenie obsahu právneho úkonu a určenie osoby, ktorá úkon urobila. Napriek spresneniu tohto ustanovenia po prijatí zákona o elektronickom podpise je určenie osoby, ktorá úkon urobila, resp. s ním vyjadrila súhlas, v prípade elektronických dokumentov veľmi pertraktovanou otázkou[4]. Splnenie týchto podmienok je základným predpokladom na zabezpečenie platnosti danej správy (úkonu).

1.2 VŠEOBECNÉ POŽIADAVKY NA PLATNOSŤ ELEKTRONICKÉHO PODPISU

Pre použitie elektronického dokumentu je potrebné dosiahnuť naplnenie troch základných požiadaviek na jeho platnosť, zaručenú stupňom ochrany poskytnutej pri tvorbe a prenose dokumentu. Už v procese vytvárania dokumentu je potrebné použitím vhodného softvéru zabezpečiť:

- autorizáciu správy, t.j. preukázateľnosť, že daný dokument vytvorila skutočne označená osoba.
- autenticitu správy, t.j. overenie miesta, o ktorom sa predpokladá, že z neho správa pochádza.
- zachovanie integrity správy – znamená to, že správa nebude počas jej cesty od odosielateľa k adresátovi nijako modifikovaná, resp. dôjde úplná a nezmenená.
- nemožnosť popretia prijatia a odoslania správy.

Pre naplnenie uvedených požiadaviek sa v sú-

[2] Pozri LUBY, Š.: Základy všeobecného súkromného práva. III. vydanie pôvodného diela. Šamorín, Heuréka 2002, str. 82.

[3] V tomto prípade teba odlišovať technické pojmy od legálnych, keďže v zákone o elektronickom podpise už definíciu elektronického podpisu nájdeme, viď ďalší text.

[4] Bližšie v poslednej kapitole textu.

časnosti ako najbezpečnejší javí systém PKI (Public Key Infrastructure). Systém je postavený na princípe dvoch kľúčov, ktoré spolu súvisia a len za použitia oboch je systém funkčný (princíp asymetrického kryptografického algoritmu RSA). Osoba, ktorá sa rozhodne komunikovať elektronicky a podpisovať svoje dokumenty najdôveryhodnejším spôsobom, si vytvorí dva kľúče – jeden tajný a druhý verejný. Tajný kľúč musí udržať v tajnosti a ak chce zachovať jeho nezneužiteľnosť, nesmie ho nikomu ďalšiemu sprístupniť (zvyčajne sa uchováva pomocou smart kariet alebo na disketách). Verejný kľúč, jediný a jedinečný ku kľúču tajnému, zverejní prostredníctvom servera alebo oznámením osobám, s ktorými hodlá komunikovať.

Ak následne takáto osoba chce odoslať správu, podpíše ju s použitím tajného kľúča a adresát overí platnosť podpisu s použitím príslušného verejného kľúča. Adresát má tak záruku, že správa prišla skutočne od držiteľa príslušného tajného kľúča, keďže zakódovanie tajným kľúčom nemožno prelomiť. Pre účely identifikácie účastníkov na sieti a zabezpečenia súladu fyzickej identity osoby s identitou elektronickou, slúžia tzv. certifikačné a registračné autority. Ich úlohou je distribúcia verejných kľúčov potrebných na overenie platnosti podpisu, ku ktorým vydávajú certifikáty (zverejňujú ako zoznamy platných, tak zrušených certifikátov).

Digitálny podpis, resp. podľa terminológie slovenského zákona o elektronickom podpise – podpis elektronický, nie je teda podpis v tradičnom zmysle slova. Nie je to podpis osoby prenesený elektronickými prostriedkami do počítača – je to systém ochrany, postavený na báze tzv. asymetrického kryptografického algoritmu (poznáme aj šifrovane symetrické, ktoré však pre účely našej právnej úpravy nie je považované za elektronický podpis). V končenom dôsledku je podpisom súslednosť znakov, v ktorom je inkorporovaná identita podpisujúceho (hovoríme o autentifikácii) a zároveň text, ku ktorému sa podpis pripája.

2. SLOVENSKÁ PRÁVNA ÚPRAVA ELEKTRONICKÉHO PODPISU V KONTEXTE SO SMERNICOU PRE ELEKTRONICKÉ PODPISY

2.1 ZÁKLADNÉ CIELE A ÚČEL SMERNICE

Smernica 1999/93/EC Európskeho parlamentu a Rady zo dňa 13. Decembra 1999 o rámci spoločenstva pre elektronické podpisy[5] (ďalej len „Smernica") bola prijatá po úvahách Komisie, či k takejto úprave vôbec treba pristúpiť a akým spôsobom. V súvislosti s vývojom v OECD a na pôde UNCITRALu[6] bol zvolený prístup technologickej neutrality a smernica nie je zameraná na jeden určitý typ elektronického podpisu. Hoci v súčasnosti je jedným z najširšie používaných systémov elektronického podpisovania systém asymetrického šifrovania PKI, „neexistuje záruka, že tak bude aj v budúcnosti"[7]. Jedným z najdôležitejších zámerov smernice bolo dosiahnutie technologickej neutrality ako záruka jej pretrvania do budúcnosti, čo dokazuje aj dlhotrvajúci proces prípravy smernice v porovnaní s prijímaním legislatívy v iných, dokonca aj členských, krajinách. Určitým poučením bol aj vývoj po prijatí zákona v štáte Utah, USA, v roku 1995, ktorý je zameraný výlučne na systém certifikačných autorít, avšak nie je dostatočne určitý a právne problémy spôsobili jeho ťažkú aplikáciu v praxi[8].

Ako sa uvádza v Smernici, k jej prijatiu viedlo presvedčenie, že elektronická komunikácia a obchod vyžadujú „elektronické podpisy" a s tým súvisiace služby umožňujúce overovanie údajov. Vzhľadom na to, že odlišné pravidlá pre právne uznávanie elektronických podpisov a akreditáciu poskytovateľov certifikovaných služieb v členských štátoch môžu vytvárať veľkú prekážku pri používaní elektronickej komunikácie

[5] Directive 1999/93/EC of the Parliament and of the Council of 13. December 1999 on a Community framework for electronic signatures OJ L13, 19. 1. 2000, str. 12.

[6] Valné zhromaždenie OSN prijalo dňa 12. Decembra 2001rezolúciu, ktorou Vzorový zákon pre elektronické podpisy spolu so vzorovým zákonom o elektronickom obchode z roku 1996 v znení jeho doplnku z roku 1998 odporúča do pozornosti členským štátom ako vhodné riešenia otázok elektronickej komunikácie. Vzorový zákon o elektronickom podpise bol pripravovaný tak, aby bol plne konzistentný so vzorovým zákonom o elektronickom obchode, a to ako do obsahu tak terminológie. Vzorový zákon o elektronickom podpise plne preberá definície a ustanovenia zákona o elektronickom obchode týkajúce sa oblasti použitia, základných definícií, interpretácie, možnosti zmeny dohodou strán a základných náležitostí podpisu (ako je uvedené v čl. 7 vzorového zákona o elektronickom obchode). Ďalej preberá a zachováva základné princípy ako:

- Princíp technologickej neutrality
- Princíp funkčne ekvivalentného/rovnocenného prístupu
- Rešpektovanie zmluvnej autonómie strán (dispozitívnosť podľa čl. 5)
- Vymedzenie minimálnych štandardov pre použitie v otvorených ako aj uzavretých systémoch.

[7] DICKIE, J.: Internet and Electronic Commerce Law in the European Union. Hart Publishing, Oxford – Portland Oregon 1999. Str. 40.

[8] O aktuálnom vývoji v rámci EÚ, ktorý sa prikláňa k iným technológiám ako k uvedenej PKI, svedčí aj vyjadrenie írskej ministerky pre informačnú povinnosť M. Hanafin na medzinárodnej konferencii ITAPA 2003: „Digitálny podpis je fantastická technológia, ale zložito implementovateľná medzi bežnou populáciou. Tým, že nám občania doručia maximum svojich údajov elektronicky a to i pri využití jednoduchších spôsobov elektronickej autentifikácie, štátu vznikajú obrovské úspory." zdroj Parlamentný kuriér 6/2004 str. 46.

a elektronického obchodu bolo potrebné prijať jasný rámec Spoločenstva, pokiaľ ide o podmienky používania elektronických podpisov a posilniť dôveru a všeobecné uznanie nových technológií.

Vnútorný trh umožňuje poskytovateľom certifikovaných služieb rozvíjať ich cezhraničné činnosti s cieľom zvýšiť svoju konkurenčnú schopnosť a tým poskytnúť spotrebiteľom a podnikom nové príležitosti pre bezpečnú elektronickú výmenu informácií a obchod bez ohľadu na hranice. Za účelom stimulácie certifikovaných služieb v rámci celého spoločenstva prostredníctvom otvorených sietí smernica zaručuje poskytovateľom certifikovaných služieb možnosť poskytovať tieto služby bez predchádzajúceho povolenia.

Podľa Smernice regulačný rámec nie je potrebný pre elektronické podpisy, používané výlučne v **uzavretých systémoch**[9]. Elektronické podpisy, ktoré spĺňajú požiadavky definované v Smernici a ktoré sa používajú v uzavretých systémoch užívateľov však musia byť právne uznané. Musí byť rešpektované právo strán dohodnúť sa medzi sebou na podmienkach, za ktorých budú akceptovať elektronicky podpísané údaje, a to v súlade s existujúcim národným právom.

Smernica sa nesnaží harmonizovať národné predpisy týkajúce sa zmluvného práva, najmä uzatváranie a plnenie zmlúv. Ustanovenia týkajúce sa právneho účinku elektronických podpisov by tak nemali porušiť požiadavky na formu zmluvy, definované v národnom práve, pokiaľ ide o uzatváranie zmlúv alebo predpisy určujúce, kde má byť zmluva uzatvorená.

Národné právo kladie rôzne požiadavky na právoplatnosť **vlastnoručných podpisov**. Certifikáty sa môžu použiť na potvrdenie identity osoby, podpisujúcej sa elektronicky; zaručené elektronické podpisy vychádzajúce z kvalifikovaných certifikátov majú ešte vyššiu úroveň bezpečnosti a zaručené elektronické podpisy, ktoré vychádzajú z kvalifikovaného certifikátu a ktoré vytvorilo bezpečné zariadenie na tvorbu podpisov už možno považovať za právne ekvivalentné vlastnoručným podpisom, pokiaľ napĺňajú požiadavky na vlastnoručný podpis.

Smernica ponecháva úpravu zodpovednosti na členských štátoch a jej obsahom je len vymedzenie veľmi stručného rámca, na ktorom si členské štáty majú vybudovať vlastný systém elektronických podpisov[10].

2.2 ANALÝZA PLATNÉHO PRÁVNEHO STAVU V SR V SÚVISLOSTIACH S POŽIADAVKAMI SMERNICE

Právna úprava elektronického podpisu, ako základný predpoklad uznania platnosti elektronických právnych úkonov, je v Slovenskej republike účinná od 1. mája 2002, a to na základe zákona č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov (ďalej ZEP). V nasledujúcej analýze sa zameriam na súlad, resp. nesúlad, zákona s požiadavkami smernice, keďže nedostatky tejto právnej úpravy spôsobili neexistenciu platnej elektronickej komunikácie v SR. Základnými právnymi predpismi pre oblasť elektronickej komunikácie v zmysle platnosti právnych úkonov, sú:

1. zákon č. 215/2002 Z. z. o elektronickom podpise spolu s vykonávacími vyhláškami Národného bezpečnostného úradu zverejnenými v zbierke zákonov:
   a) 537/2002 Z. z. o vyhotovení a overovaní elektronického podpisu a časovej pečiatky
   b) 538/2002 Z. z. o kvalifikovaných certifikátoch
   c) 539/2002 Z. z. o produktoch elektronického podpisu
   d) 540/2002 Z. z. o podmienkach na poskytovanie akreditovaných certifikačných služieb a požiadavkách na audit, rozsah auditu a kvalifikáciu audítorov
   e) 541/2002 Z. z. o obsahu a rozsahu prevádzkovej dokumentácie vedenej certifikačnou autoritou a bezpečnostných pravidlách a pravidlách na výkon certifikačnej činnosti
   f) 542/2002 Z. z. o spôsobe a postupe používania elektronického podpisu v obchodnom a administratívnom styku
2. zákon č. 22/2004 Z. z. o elektronickom obchode.

Kľúčové problémy platnej právnej úpravy [11]

Pri porovnaní ZEP so smernicou, resp. štandardnou úpravou v zahraničí, možno vybadať niekoľko kľúčových problémov:

[9] Uzavretým systémom sa rozumie podľa zákona o elektronickom podpise systém slúžiaci výlučne pre vlastné potreby jeho účastníkov, ktorý vznikol na základe dohody účastníkov systému a ku ktorému majú prístup len účastníci systému (typicky sú to banky a ich klienti pri službách ako homebanking, uzavreté dodávateľské siete apod.).

[10] K poslednému vývoju implementácie smernice pozri viac KELM, S.: On the implementation of the 1999 European Directive on electronic signatures. In: e-Signature Law Journal Vol. 2, Nr. 2, 2005, str. 5–14.

[11] Pripravuje sa novela zákona o elektronickom podpise, a to aj vzhľadom na viaceré problémy, ktoré bránia jeho aplikovateľnosti v praxi, na ktoré upozorňuje autorka na verejných fórach od platnosti zákona; jej znenie je prístupné na verejnú diskusiu na stránkach www.nbusr.sk, avšak zatiaľ nie je možné predvídať nadobudnutie účinnosti novely (podľa autorky nedostatočne reagujúcej na v analýze uvedené problémy).

a) Vymedzenie 24 nových pojmov (Smernica obsahuje 13) je neštandardným najmä z toho dôvodu, že niektoré sa viažu výlučne na jednu technológiu, samostatné definovanie služieb a činností navodzuje dojem rozdielnosti subjektov, ktoré sa nimi zaoberajú, terminológia ako súkromný kľúč, verejný kľúč, autorita nie je legislatívne vhodná. Táto terminológia nie je použitá ani v smernici ani v ďalších medzinárodne akceptovaných dokumentoch.

b) Definícia elektronického podpisu je postavená do roviny jedinej technológie a to takej, ktorá používa súkromné a verejné kľúče. Vychádzajúc zo smernice, tzv. obyčajný elektronický podpis by nemal byť takto vymedzený. Viazanie zaručeného podpisu na kvalifikovaný certifikát je tiež v rozpore zo smernicou.

c) V súvislosti s náležitosťami platného certifikátu jeho delenie na „telo" a „podpis" je právne nadbytočné, a hoci technicky sa certifikát takto prejavuje, z právneho hľadiska je to irelevantné a nič to nemení na tom, čo certifikát je a aké povinnosti majú subjekty s ním nakladajúce. Taktiež to možno považovať za prvok narúšajúci technologickú neutralitu, keďže budúce technológie nemusia takéto členenie poznať. Analogicky sa to týka zoznamov zrušených certifikátov.

d) Za diskriminačnú možno považovať povinnosť preukazovať oprávnený záujem na získaní informácií týkajúcich sa chodu certifikačnej autority (§ 14 ods. 3 písm. b)) a možno tiež hovoriť o rozpore s princípmi poskytovania takýchto služieb (za určitých okolností môže ísť o rozpor so zákonom č. 211/2000 Z. z. o slobodnom prístupe k informáciám).[12]

e) Veľmi nevhodnou sa javí úprava uznávania zahraničných certifikátov, keďže podľa platnej právnej úpravy bez bilatelárnej dohody medzi SR a cudzím štátom nemožno žiaden zahraničný kvalifikovaný certifikát považovať za platný v SR, a to aj napriek tomu, že jedným z cieľov takejto právnej úpravy má byť zjednodušenie uznávania platnosti elektronických právnych úkonov v rámci únie.[13]

V ďalšom texte sa zameriame na komparáciu legálnych textov a na vymedzenie podstaty platnej právnej úpravy, vysvetlenie jej základných náležitostí a na odchýlky od požiadaviek Smernice.

Terminológia

Smernica pomerne podrobne definuje základné pojmy objavujúce sa v súvislosti s elektronickým podpisom. Na rozdiel napr. od Vzorového zákona pre elektronické podpisy UNCITRAL rozoznáva niekoľko stupňov podpisov a rozlišuje aj ich bezpečnostnú a právnu úroveň. K určitej diskrepancii medzi Smernicou a ZEP dochádza v obsahu a počte definovaných pojmov, z čoho najdôležitejší je nesúlad definícií najpodstatnejších termínov obsiahnutých v týchto normách – elektronický podpis, podpisotvorné dáta a podpisovateľ.

Smernica definuje elektronický podpis, zaručený elektronický podpis (ako vyššiu úroveň a záruku bezpečnosti), podpisovateľa, dáta a zariadenia na vytvorenie elektronického podpisu a zariadenie na vytvorenie bezpečného elektronického podpisu (v súlade s prílohou III. Smernice), dáta a zariadenia na overenie podpisu, ďalej definuje certifikát, kvalifikovaný certifikát, poskytovateľa certifikačných služieb, produkty pre elektronický podpis (t.j. hardvér a softvér) a napokon dobrovoľnú akreditáciu.

ZEP vymedzuje nezvyčajné množstvo nových pojmov (až 24 nových termínov), napr. definuje také pojmy ako dokument, digitálny dokument, elektronický dokument, podpísaný elektronický dokument, súkromný kľúč, verejný kľúč (čo svedčí o viazaní predpisu na jednu technológiu), prostriedok na vyhotovenie elektronického podpisu, bezpečné zariadenie na vyhotovenie elektronického podpisu, prostriedok na overenie elektronického podpisu, ako aj tzv. produkt pre elektronický podpis. Zákon dokonca odlišne od Smernice či Vzorového zákona UNCITRAL rozlišuje pojmy certifikačná služba, certifikačná činnosť, poskytovateľ certifikačných služieb ako fyzická osoba alebo právnická osoba, ktorá vykonáva certifikačné služby a certifikačná autorita, ktorou je poskytovateľ certifikačných služieb, ktorý spravuje certifikáty. Takéto delenie považujem za veľmi nadbytočné a mätúce, keďže je to vždy jedna osoba a v zaužívanej terminológii ide jednoznačne vždy o poskytovateľa certifikačných služieb. Zákon ďalej rozlišuje medzi podpisovateľom a držiteľom certifikátu, čo je z právneho hľadiska pomerne nezvyčajné.

Smernica definuje **elektronický podpis** ako dáta v elektronickej forme, ktoré sú priložené alebo logicky súvisia s inými elektronickými údajmi a ktoré slúžia ako overovacia metóda. **Zaručený elektronický podpis**, ktorý naviac napĺňa požiadavky, že:

[12] Text zo zákona.

[13] Porovnaj § 17 ZEP a Stanovisko NBU zverejnené na oficiálnej stránke NBU www.nbusr.sk v časti Elektronický podpis, Legislatíva, Rôzne (stránka navštívená 28.2004). V závere Stanoviska sa konštatuje: „Nakoľko platnosť zahraničného kvalifikovaného certifikátu nemožno hodnoverne overiť, na uznanie zahraničného kvalifikovaného certifikátu (certifikátu zahraničnej akreditovanej certifikačnej autority) je nutné, aby bola uzavretá medzinárodná dohoda medzi SR a príslušným štátom (členský štát EÚ ako aj štát, ktorý nie je členom EÚ), v ktorej by sa oba štáty po porovnaní príslušných právnych noriem a akreditačných schém recipročne zaviažu, že i budú vzájomne uznávať vydávané kvalifikované certifikáty."

a) je jednoznačne spojený podpisovateľom,
b) je schopný identifikovať podpisovateľa,
c) je vytvorený pomocou prostriedkov, ktoré sú pod výlučnou kontrolou podpisovateľa a
d) je spojený s dátami, na ktoré sa vzťahuje, a to takým spôsobom, ktorý umožní odhaliť každú následnú zmenu týchto dát.

Elektronický podpis podľa ZEP je informácia pripojená alebo inak logicky spojená s elektronickým dokumentom, ktorá musí spĺňať tieto požiadavky:

a) nemožno ju efektívne vyhotoviť bez znalosti súkromného kľúča a elektronického dokumentu,
b) na základe znalosti tejto informácie a verejného kľúča patriaceho k súkromnému kľúču použitému pri jej vyhotovení možno overiť, že elektronický dokument, ku ktorému je pripojená alebo s ním inak logicky spojená, je zhodný s elektronickým dokumentom použitým na jej vyhotovenie.

Zaručený elektronický podpis podľa ZEP je elektronický podpis, ktorý musí spĺňať podmienky pre elektronický podpis a zároveň:

a) je vyhotovený pomocou súkromného kľúča, ktorý je určený na vyhotovenie zaručeného elektronického podpisu,
b) možno ho vyhotoviť len s použitím bezpečného zariadenia na vyhotovovanie elektronického podpisu,
c) spôsob jeho vyhotovovania umožňuje spoľahlivo určiť, ktorá fyzická osoba zaručený elektronický podpis vyhotovila,
d) na verejný kľúč patriaci k súkromnému kľúču použitému na vyhotovenie zaručeného elektronického podpisu je vydaný kvalifikovaný certifikát.

Z vyššie uvedeného je zjavné, že v bazálnych termínoch sú výrazné obsahové odlišnosti a slovenská právna úprava sa odklonila od požiadaviek Smernice smerom k rigidnosti právnej úpravy aj v oblasti, ktorá takýto zásah nepotrebuje, teda oblasť „obyčajného" elektronického podpisu. Takýto prístup považujem za porušenie princípu technologickej neutrality a za príkry rozpor s účelom Smernice.[14]

Prístup na trh

V súlade so Smernicou štáty môžu zaviesť systémy dobrovoľnej akreditácie, zamerané na zvýšenie úrovne poskytovania certifikačných služieb. Všetky podmienky súvisiace s týmito systémami musia byť objektívne, transparentné, primerané a nediskriminačné. Členské štáty nemôžu obmedziť počet akreditovaných poskytovateľov certifikačných služieb z dôvodov, ktoré spadajú do rámca smernice.

Členské štáty majú zabezpečiť vytvorenie vhodného systému, ktorý umožní kontrolu poskytovateľov certifikačných služieb so sídlom na ich území, a ktorý vydávajú kvalifikované certifikáty verejnosti (práve kvalifikované certifikáty majú zaručovať charakter elektronického podpisu ako podpisu vlastnoručného). Za týmto účelom budú poverené kontrolou zhody bezpečných zariadení na tvorbu podpisov s požiadavkami definovanými v Prílohe III orgány určené členskými štátmi. Členské štáty môžu podriadiť používanie **elektronických podpisov vo verejnom sektore** splneniu ďalších požiadaviek.

ZEP nepriamo podmieňuje výkon činnosti aj neakreditovaných certifikačných autorít, keďže zavádza povinnosť 30 dní pred začatím činnosti takéhoto subjektu oznámiť úradu začiatok svojej činnosti. V súvislosti s akreditovanými certifikačnými autoritami zavádza systém akreditácie a auditu, podrobne upravených v zákone a vykonávacích predpisoch.

Účinnosť elektronického podpisu

Podľa smernice majú zaručené elektronické podpisy založené na kvalifikovanom certifikáte a vytvorené bezpečným zariadením na tvorbu podpisov charakter vlastnoručného podpisu a takto je potrebné ich v legislatíve definovať. Zároveň je potrebné zabezpečiť, aby boli prípustné ako dôkazy pri súdnych procesoch.

Elektronickému podpisu **nesmie byť odoprená právna účinnosť** a prípustnosť ako dôkazu v súdnych procesoch iba preto, že:

- má elektronickú formu, alebo
- nevychádza z kvalifikovaného certifikátu, alebo
- nevychádza z kvalifikovaného certifikátu vydaného akreditovaným poskytovateľom certifikačných služieb, alebo
- nebol vytvorený bezpečným zariadením na tvorbu podpisov.

Podľa ZEP ak možno v styku s verejnou mocou používať elektronický podpis, **tento elektronický podpis musí byť zaručeným elektronickým podpisom.**
Zároveň je takýto podpis uznaný ako **platný**, ak

a) existuje kvalifikovaný certifikát verejného kľúča patriaceho k súkromnému kľúču použitému pri vyhotovení daného elektronického podpisu,
b) je preukázateľné, že kvalifikovaný certifikát bol

[14] Navyše, opäť v rozpore so Smernicou, vychádzajúc z vyhlášky NBU č. 542/2002 Z. z., pokiaľ vytváraný zaručený elektronický podpis má slúžiť ku komunikácii prostredníctvom elektronickej podateľne (čo bude zjavne vo väčšine prípadov), k nemu musí byť pripojená aj časová pečiatka. Časová pečiatka je služba, ktorú výlučne poskytujú akreditované certifikačné autority.

platný v čase vyhotovenia daného elektronického podpisu,

c) elektronický dokument, ku ktorému je zaručený elektronický podpis pripojený alebo s ním inak logicky spojený, je zhodný s dokumentom použitým na jeho vyhotovenie, čo sa overilo použitím verejného kľúča uvedeného v kvalifikovanom certifikáte.

Z uvedeného vyplýva, že nároky ZEP sú v rozpore s požiadavkami Smernice.

3. PRÁVNE ÚKONY V OBLASTI ZMLUVNÉHO PRÁVA

Od 1. februára 2004 je účinný nový zákon o elektronickom obchode č. 22/2004 Z. z.[15] a je odrazom Smernice 2000/31/ES Európskeho parlamentu a Rady z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode (ďalej len „Smernica o elektronickom obchode"). Týmto zákonom sa do právneho poriadku SR preberajú určené právne akty Európskych spoločenstiev[16].

Pre fungujúci systém platných úkonov v elektronickej podobe je potrebné nájsť odpovede na nasledujúce problémy:

1. uznávanie dátovej správy (resp. informácie v elektronickej podobe) ako rovnocennej s požiadavkami na písomnú formu,
2. v oblasti zmluvného práva určením podmienok pre vznik a platnosť zmlúv v elektronickej podobe.

3.1 PÍSOMNÝ ÚKON A DÁTOVÁ SPRÁVA

Ak porovnáme Vzorový zákon UNCITRAL pre elektronický obchod[17] a Smernicu EÚ pre elektronický obchod, zistíme určité odlišnosti ako v rozsahu upravovanej problematiky, tak v prístupe k spôsobu oznamovania prijatia dátových správ, čo je rozhodujúce pre moment vzniku zmluvy. Smernica má na rozdiel od Vzorového zákona širší záber napr. vymedzením úpravy zodpovednosti poskytovateľov služieb informačnej spoločnosti a niektorých ďalších požiadaviek na výkon činností v informačnej spoločnosti.

Z môjho pohľadu je veľmi inšpirujúci prístup Vzorového zákona jednoduchosťou definovania pojmov a požiadaviek na platnosť úkonov. Hoci pri definovaní pojmov súvisiacich s elektronickou komunikáciou slovenský zákon o elektronickom obchode vychádza zo Smernice, uvádzam niekoľko ustanovení Vzorového zákona, ktoré považujem za vhodnejšie ako existujúce riešenie.

Článok 5 Vzorového zákona hovorí:

„Informácii nemožno uprieť právne účinky, platnosť alebo vykonateľnosť výlučne z dôvodu, že je vo forme dátovej správy."[18] Článkom 5bis[19] bola takáto účinnosť rozšírená aj na informáciu, ktorá síce nie je súčasťou dátovej správy, ale táto obsahuje na ňu odkaz (dôležité pre platnosť napr. obchodných podmienok, ktoré sú súčasťou zmluvy, ale sú samostatným dokumentom k nej pripojeným, resp. uloženým na inom obom stranám prístupnom mieste.)

Veľmi jednoduchou a zrozumiteľnou je definícia požiadavky na zrovnoprávnenie elektronickej formy s požiadavkami na písomnú formu v čl. 6 ods. 1:

„Tam, kde zákon vyžaduje, aby informácie mali písomnú formu, spĺňa dátová správa túto požiadavku, ak v nej obsiahnuté informácie sú dostupné do tej miery, aby bolo možné sa na ne v budúcnosti odvolávať". V tejto definícii je skĺbená aj požiadavka na uchovávanie dokumentov v čitateľnej podobe, čo považujeme za nesmierne dôležité vzhľadom na rýchly vývoj technológií a s tým spojené zastarávanie, teda aj riziko, že časom bude určitá informácia nedostupná z dôvodu nemožnosti jej zobrazenia či vnímania modernými komunikačnými prostriedkami.

Následne vo vzťahu k zmluvám je podstatný čl. 11:

„Pri vzniku zmluvy je možné ponuku a prijatie ponuky vyjadriť vo forme dátovej správy, ak sa zmluvné strany nedohodli inak. V prípadoch, kedy bola k vzniku zmluvy použitá dátová správa, nemožno zmluve uprieť platnosť či vykonateľnosť výhradne z toho dôvodu, že pre uvedený účel bola použitá dátová správa."

Podobnú formuláciu nájdeme v čl. 9 Smernice, t.j. vymedzenie kategórií zmlúv, na ktoré nebude možné takéto zrovnoprávnenie použiť, a to:

[15] Zákon NR SR z 3. decembra 2003 číslo 22/2004 Z. z. o elektronickom obchode a o zmene a doplnení zákona č. 128/2002 Z. z. o štátnej kontrole vnútorného trhu vo veciach ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov v znení zákona č. 284/2002 Z. z.

[16] Smernica č. 2000/31/ES (OJ L 178, 17. 7. 2000, str. 1–16), Smernica 98/34/ES (OJ L 204, 21. 7. 1998, str. 37–48), Smernica 98/48/ES (OJ L 217, 5. 8. 1998, str. 18–26).

[17] Prijatý dňa 12. júna 1996 Komisiou OSN pre medzinárodné obchodné právo UNCITRAL, a následne ho prijalo Valné zhromaždenie ako Rezolúciu 16. decembra toho istého roku.

[18] Dátovou správou sa pre účely Vzorového zákona rozumejú informácie vytvárané, odosielané, prijímané alebo uchovávané elektronickými alebo optickými a podobnými prostriedkami vrátane, ale bez obmedzenia, elektronickej výmeny dát (EDI), elektronickej pošty, telegramu, ďalekopisu alebo telefaxu.

[19] Prijatým Komisiou v júni 1998 na 31. zasadnutí.

- zmluvy, ktoré vytvárajú alebo prevádzajú práva k nehnuteľnému majetku, s výnimkou nájomných práv;
- zmluvy, ktoré si podľa práva vyžadujú účasť súdov, verejných orgánov alebo profesií výkonu verejných právomocí;
- ručiteľské zmluvy a zmluvy o dodatočnom zabezpečení cennými papiermi, ktoré sú poskytnuté osobami konajúcimi za účelom, ktorý je mimo rámca ich obchodu, podnikania alebo povolania;
- zmluvy, ktoré sa riadia rodinným právom alebo dedičským právom.

3.2 VZNIK ZMLUVY

Na požiadavku zrovnoprávnenia foriem komunikácie nadväzuje požiadavka na jednoznačné určenie momentu vzniku zmluvy. Ustanovenie § 43a Občianskeho zákonníka v odseku 1 hovorí, že:

„Prejav vôle smerujúci k uzavretiu zmluvy, ktorý je určený jednej alebo viacerým určitým osobám, je návrhom na uzavretie zmluvy, ak je dostatočne určitý a vyplýva z neho **vôľa navrhovateľa**, aby bol viazaný v prípade jeho prijatia."

V prípade elektronických zmlúv môže vzniknúť pochybnosť, či danú správu (návrh zmluvy) je možné prisúdiť odosielateľovi tak, aby ňou bol viazaný. Zákon o elektronickom obchode obsahuje ustanovenie o objednávke a potvrdení jej prijatia, podľa ktorého sa tieto považujú za doručené, ak poskytovateľ služieb a príjemca služieb alebo spotrebiteľ majú k nim na elektronickom prostriedku prístup. Analogicky takýto postup možno použiť na proces uzatvárania zmluvy.

V Smernici nájdeme len určitý návod ako riešiť prijatie objednávky, ktorý je však pomerne nejednoznačný a nie je z neho zjavné, či takýmto spôsobom dochádza len k oznámeniu prijatia objednávky alebo priamo k potvrdeniu prijatia objednávky (t.j. k viazanosti objednávkou), a to v čl. 11:

„Členské štáty musia zabezpečiť, s výnimkou prípadov, ak je medzi zmluvnými stranami, ktoré nie sú spotrebiteľmi, dohodnuté inak, aby sa v prípadoch, kedy príjemca služby zadáva svoju objednávku prostredníctvom technologických prostriedkov, uplatňovali tieto zásady:

- poskytovateľ služby musí potvrdiť príjem príjemcovej objednávky bez zbytočného odkladu a elektronicky,
- objednávka a potvrdenie príjmu sú považované za obdržané, ak zúčastnené strany, ktorým sú adresované, k nim majú prístup."

Vzhľadom na špecifický charakter elektronických dokumentov bolo potrebné upraviť požiadavky na originál. Elektronické dokumenty všeobecne nemajú charakter originálu alebo kópie, keďže všetky prezentované prejavy elektronického dokumentu sú totožné. Zákon ustanovuje, že pokiaľ je potrebné prezentovať alebo uchovať písomný právny úkon v elektronickej podobe, táto požiadavka je naplnená, pokiaľ sú vytvorené podmienky jeho nezmeniteľnosti a spoľahlivosti od jeho prvého prezentovania v konečnej podobe a možno ho v tejto podobe prezentovať osobe, ktorej je určený.[20]

S informačnými povinnosťami súvisia aj povinnosti poskytovateľa služieb pri uzatváraní zmluvy on-line. V týchto prípadoch ide o vypĺňovanie elektronických formulárových objednávok, kedy musí byť príjemcovi služieb zabezpečená možnosť návratu pri jednotlivých krokoch, možnosti opravy a zmeny objednávky, ako poskytnutie informácií o všetkých úkonoch potrebných na uzatvorenie zmluvy, technických prostriedkoch na zistenie a opravu chýb v objednávke. Poskytovateľ služieb musí informovať aj o tom, kde bude zmluva uložená a či bude príjemcovi služieb dostupná a taktiež musí uviesť, v akom jazyku bude zmluva uzavretá.

V prípade uzatvárania zmlúv medzi podnikateľmi, títo sa môžu dohodnúť na odlišnom režime uzatvárania zmlúv v elektronickej podobe[21]. Vtedy sa na nich uvedené povinnosti nevzťahujú.

Zákon obsahuje aj výluku z možnosti použitia elektronických zariadení pri uzatváraní zmlúv, na ktoré je potrebné rozhodnutie súdu, orgánu verejnej správy alebo notára a pri zmluvách o zabezpečení záväzkov, tak ako to umožňuje Smernica o elektronickom obchode.

4. SÚVISLOSTI ÚPRAVY ELEKTRONICKEJ KOMUNIKÁCIE S ÚPRAVOU DOKAZOVANIA V CIVILNOM KONANÍ

ZEP zavádza do elektronickej komunikácie rozdielne nároky v závislosti od druhu systému, v ktorom komunikácia prebieha. Z pôsobnosti zákona sú vylúčené tzv. uzavreté systémy (zákon sa na vyhotovenie a používanie elektronického podpisu v uzavretých sys-

[20] Táto požiadavka súvisí nielen s médiom, na ktorom je úkon zaznamenaný, ale aj s povinnosťou mať k dispozícii po dobu potrebnú na uchovanie média aj zariadenie, ktoré bude schopné sprístupniť zachytený právny úkon. Napr. ak je úkon zaznamenaný na „3,5" diskete, je možné, že o pár rokov sa tieto vôbec nebudú používať a nebudú dostupné ani príslušné diskové mechaniky – je preto potrebné záznam preniesť na iné médium alebo mať k dispozícii potrebnú mechaniku.

[21] Obdobný režim ustanovuje ZEP v § 1 ods. 3 pre tzv. uzavreté systémy (podľa § 2 je uzavretým systémom systém slúžiaci výlučne pre vlastné potreby jeho účastníkov, ktorý vznikol na základe dohody účastníkov systému a ku ktorému majú prístup len účastníci systému) – tieto budú používať zrejme predovšetkým podnikatelia pri elektronickom obchodovaní.

témoch použije, ak sa jeho účastníci nedohodnú inak). Zároveň však došlo k novelizácii Občianskeho zákonníka, ktorý v ust. § 40 ods. 4 uvádza:

„Písomná forma je zachovaná, ak je právny úkon urobený telegraficky, ďalekopisom alebo elektronickými prostriedkami, ktoré **umožňujú zachytenie obsahu** právneho úkonu a **určenie osoby**, ktorá právny úkon urobila. **Písomná forma je zachovaná vždy, ak právny úkon urobený elektronickými prostriedkami je podpísaný zaručeným elektronickým podpisom** (s odkazom na zákon o elektronickom podpise)"

Z uvedeného vyplýva, že pokiaľ si účastníci **uzavretého systému** dohodnú odlišné podmienky pre elektronickú komunikáciu (t.j. vylúčia použitie ZEP, čo im zákon umožňuje), v prípade sporu bude pre súd rozhodujúce, ako podporí svoje tvrdenia strana napádajúca platnosť elektronického podpisu vytvoreného druhou stranou a bude teda niesť dôkazné bremeno.

Pre dôkaz o existencii písomného záväzku (resp. písomného akéhokoľvek úkonu) bude následne potrebné preukázať ako schopnosť zachytenia obsahu právneho úkonu elektronickými prostriedkami, tak aj určenie osoby, ktorá úkon urobila. Zároveň sa bude musieť dokázať, že boli zachované požiadavky na takúto komunikáciu stanovené zmluvnými stranami.

Pokiaľ pôjde o **otvorený systém**, pri použití zaručeného elektronického podpisu v súlade so systémom vytvoreným podľa ZEP, platí nevyvrátiteľná právna domnienka platnosti písomného právneho úkonu bez potreby dokazovania zachytiteľnosti obsahu úkonu a určovania osoby, ktorá úkon urobila. Pre platnosť úkonov vyhotovených podľa zákona má veľký význam vyhláška NBÚ č. 542/2002 Z. z. o spôsobe a postupe používania elektronického podpisu v obchodnom a administratívnom styku. Pri pochybnosti o platnosti úkonu (pochybnosti o platnosti podpisu) je možné jedine najskôr napadnúť použitý systém podpisovania a až po preukázaní neplatnosti certifikátu, resp. iných chýb spôsobujúcich neplatnosť podpisu, bude možné domáhať sa neplatnosti úkonu ako takého. V týchto prípadoch však už pôjde aj o zodpovednosť príslušnej certifikačnej autority.

Napokon je potrebné vziať do úvahy fázu prejednávania sporu pred súdom. Občiansky súdny poriadok v ustanovení § 125 uvádza, že **„za dôkaz môžu slúžiť všetky prostriedky, ktorými možno zistiť stav veci"**. Ďalej je uvedené, že **„Pokiaľ nie je spôsob vykonania dôkazu predpísaný, určí ho súd."**

V prípade digitálneho záznamu a použitia elektronického podpisu v uzavretom systéme je potrebné súd uspokojiť v dvoch veciach: v otázke prípustnosti záznamu ako dôkazného prostriedku a autentičnosti záznamu ako takého.

Prípustnosť záznamu je v podstate riešená vyššie citovaným ustanovením, teda sudca nemôže odmietnuť záznam ako neprípustný dôkaz. Otázkou je, či bude záznam posudzovaný ako postačujúci a rovnocenný záznamu písomnému, ktorý sa predkladá súdu v origináli resp. v overenej kópii. V prípade elektronických záznamov dokonca originál neexistuje, každý výtlačok je originál a teda je nevyhnutné zabezpečiť, aby jeho pôvodnosť bola zaistená pravidelným vykonávaním archivácie a bezpečnostnými opatreniami v zmysle ako organizačných a fyzických tak logických spôsobov ochrany dát[22].

Autentičnosť záznamu znamená, že súd je potrebné presvedčiť o tom, že obsah záznamu nebol pozmenený, informácie pochádzajú zo zdroja, ktorý je v zázname označený, identifikačné údaje ako napr. dátum zodpovedajú skutočnosti, počas prenosu záznamu nemohlo dôjsť k jeho zmene alebo k neoprávnenému prístupu.

Podľa ust. § 127 Občianskeho súdneho poriadku ak závisí rozhodnutie súdu od posúdenia skutočností, na ktoré treba odborné znalosti, ustanoví súd po vypočutí účastníkov znalca. Namiesto posudku znalca možno použiť potvrdenie alebo odborné vyjadrenie príslušného orgánu, o správnosti ktorých nemá súd pochybnosti. V súčasnosti je podľa našich informácií možné získať znalecký posudok z oblasti bezpečnosti informačných technológií (odbor najbližší relevantnej problematike) len od troch znalcov.

Závažnou okolnosťou vplývajúcou na výsledok sporu je, že uplatňovanie práva sa koná pred sudcami, ktorí sa v tak komplikovanej problematike budú veľmi ťažko orientovať a prvé súdne spory budú nesmierne nákladnou a odborne náročnou záležitosťou. Zo strany súdu nebude možné očakávať aktivitu, ako napr. určenie spôsobu vykonania dôkazu súdom v prípade, že tento nie je predpísaný (podľa § 125 OSP), keďže ani súd nepozná ten najvhodnejší spôsob. V takej neštandardnej oblasti akou nesporne elektronický obchod je, nemožno počítať so stanovenými postupmi, keďže žiadne neexistujú.

Ak si sudca chce plniť svoju úlohu nezávislého a nestranného arbitra, môže sa stať, že konanie bude veľmi náročné časovo aj finančne (náklady na znalcov, zaobstaranie listín, ohliadky, prípadné dožiadania na vykonanie dôkazov mimo pojednávania ap.). Súd disponuje voľným hodnotením dôkazov a je možné odôvodnene prezumovať, že za určitých okolností súd nedostatočne porozumie predloženej problematike a nerozhodne tak, ako by v prípade dôkladného a správneho vykonania dokazovania a orientácie v problematike, rozhodnúť mal.

[22] Zákon o elektronickom obchode rieši aj túto dilemu v ust. § 4, podľa ktorého ak sa vyžaduje, aby písomný právny úkon bol predložený alebo uchovaný v origináli, elektronický dokument túto požiadavku spĺňa, ak sú vytvorené podmienky jeho nezmeniteľnosti a spoľahlivosti, odkedy bol prvýkrát vyhotovený v konečnej podobe a zároveň osoba, ktorej je určený, sa s ním môže oboznámiť.

SYNOPSA

Príspevok sa zaoberá analýzou platného právneho stavu v oblasti právnych úkonov vykonaných v elektronickej podobe. Okrem platnej právnej úpravy v Slovenskej republike v ňom nájdeme komparáciu s úpravou elektronického podpisu a obchodu v EÚ ako aj niekoľko poznámok o úprave vzorových zákonov UNCITRAL pre túto oblasť. Autorka sa snaží vymedziť a analyzovať kľúčové problémy platnej právnej úpravy a upozorniť na nesúlad niektorých ustanovení slovenského zákona o elektronickom podpise s nárokmi smernice. Hoci úprava elektronického podpisu je základňou pre možnosť vzniku platných právnych úkonov v elektronickej podobe, nemenej závažnou sa javí otázka momentu vzniku takéhoto právneho úkonu z pohľadu časového momentu, ako aj uznania dátovej správy ako rovnocennej s písomnosťou v tradičnom zmysle slova.