ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA PRÁVNICKÁ

DIPLOMOVÁ PRÁCE

ELEKTRONICKÝ PODPIS V OBLASTI SOUKROMÉHO PRÁVA

JAN AMBROŽ

Plzeň 2012

ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA PRÁVNICKÁ

DIPLOMOVÁ PRÁCE

ELEKTRONICKÝ PODPIS V OBLASTI SOUKROMÉHO PRÁVA

JAN AMBROŽ

Příslušné oborové pracoviště:	Katedra soukromého práva a civilního procesu
Název studijního programu:	Právo a právní věda
Název oboru:	Právo
Jméno vedoucího práce:	JUDr. Radek Spurný
Pracoviště vedoucího práce:	Katedra forenzní psychologie a sociologie

Plzeň 2012

Prohlášení autora o původnosti práce

Prohlašuji tímto, že jsem diplomovou práci na téma „Elektronický podpis v oblasti soukromého práva“ zpracoval sám pouze s využitím pramenů v práci uvedených.

Datum: Podpis:

Jan Ambrož

Digitálně podepsal Jan Ambrož
DN: c=CZ, l=Spojařů 1222, 386 01 Strakonice, ou=P120582, cn=Jan Ambrož, serialNumber=P120582
Důvod: Jsem autor tohoto dokumentu
Datum: 2012.03.29 11:17:08 +02'00'

Poděkování

Na tomto místě bych chtěl zejména poděkovat svému vedoucímu diplomové práce JUDr. Radku Spurnému za jeho podporu při vedení diplomové práce a JUDr. Milanu Hulmákovi za úvodní konzultace a uvedení do tématu.

Dále bych rád poděkoval svým rodičům a přátelům za morální i finanční podporu při studiu.

Obsah

1. Úvod

Člověk dnes a denně využívá nástrojů usnadňujících mu každodenní život, nástrojů, které vznikly díky invenci lidstva, ale i nástrojů ovlivňujících jeho samého. Stejně jako právo dává rámec, resp. pravidla, lidskému chování, tak příroda dala rámec nejen životu, ale i vzniku a vývoji nástrojů. To příroda dává předmětům vlastnosti, jaké mají, a právě první nástroje jako křesadlo, pochodeň, kolo, kopí atp. využívají vhodných vlastností pro daný nástroj. Člověk tyto vlastnosti poznal a začal jich využívat ke svému prospěchu. Těžko by někdo dnes nazval tyto nástroje technologií, ale určitě je možné je považovat za prapůvod technologie.

Spolu s vývojem lidstva se urychloval i technologický vývoj.[1] Bylo to způsobeno nejen řadou demografických a průmyslových revolucí, ale i rozvojem samotné technologie, který byl pochopitelně umožněn již předešlými objevy na tomto poli. Těžko by bez kola mohl vzniknout parní stroj a bez parního stroje automobil. Právě technologický vývoj, ale nejen on, umožňoval další vývoj lidstva, proto se pro jednotlivé vývojové epochy začaly užívat označení dle materiálů užívaných k výrobě nástrojů a zbraní, dle způsobu získávání potravin či dle jednotlivých nástrojů charakteristických pro danou dobu.

Spolu s evolucí technologie se měnila kultura, morální hodnoty člověka, ale i sociální vazby uvnitř společnosti, obzvláště pak díky změnám ve formě a způsobu komunikace. Dokonce se lze setkat i s názory, že civilizace se spíše vytvářela díky rozvoji komunikace uvnitř společnosti a vývoji jednotlivých prostředků komunikace. Právě schopnost sdílet informace s ostatními jedinci má vliv na vývoj myšlení, chování a kultury. Díky tomu je možné vykládat vývoj lidstva pomocí odlišných epoch ve vývoji lidské komunikace.[2]

Předzvěstí nové epochy byl vznik osobního počítače a následně internetu. Internet se stal v posledních dvaceti letech jedním z největších masových médií a prostředků komunikace mezi lidmi navzájem. V dnešní době můžeme být svědky rozmachu a další diferenciace jednotlivých komunikačních prostředků v rámci internetu.

---

[1] Důkazem z dnešní doby může být tzv. Mooreův zákon, který je považován za velmi přesný odhad technologického vývoje v oboru informačních technologií. V roce 1965 chemik a spoluzakladatel firmy Intel Gordon Moore předpověděl, že počet tranzistorů v procesoru se každým rokem zdvojnásobí, tzn. že se zdvojnásobí i výpočetní výkon.

[2] DEFLEUR, M. L.; BALL-ROKEACH, S. *Theories of mass communication*. 5th Edition. New York : Longman, 1989. 4 s.

Novou etapou vývoje webových stránek je tzv. Web 2.0, který klade důraz na mnohem větší interakci samotných uživatelů, což způsobilo vznik nového fenoménu – sociálních sítí. V souvislosti s tzv. e-commerce[3] sále více a více nabývá na významu potřeba adekvátního zabezpečení transakcí. Podobný rozmach patrně čeká i oblast mobilní komunikace využívající internet.

Bylo tedy nevyhnutelné, aby se dva takové fenomény jako právo a internet setkaly. Protknutí práva a internetu nabývá na významu zejména v posledních letech spolu s nárůstem počtu právních úkonů činěných prostřednictvím tohoto komunikačního kanálu. Možnost ověřit platnost právních úkonů a pravost a neporušitelnost dat, resp. datových zpráv, které slouží jako „zprostředkovatel přenosu" těchto úkonů, je proto signifikantnější než kdykoli před tím.

Na tuto potřebu muselo nutně začít reagovat i právo[4], proto jsme v mnoha právních řádech za posledních 14 let svědky přijímání legislativy, která má za cíl regulovat obchodování prostřednictvím elektronických prostředků a v souvislosti s tím i regulovat elektronický podpis.

Podpis jako součást písemného právního úkonu, ale nejen právního úkonu, vždy naplňoval řadu funkcí, zejména pak sloužil jako prostředek sloužící k ověření totožnosti podepisující osoby a potvrzení, že ten, kdo činí právní úkon, tak opravdu učinit chtěl. Tyto aspekty nabývají na významu zejména u smluvních vztahů, kde smluvní strana jednající na základě takového úkonu si musí být jista, že jejím případným plněním jí nevznikne škoda (např. díky neplatnosti právního úkonu), která by jinak nemusela vzniknout.

Elektronický podpis, lze v určitých aspektech považovat za bezpečnější formu podpisu, která plní i některé další funkce, které běžný podpis ze své povahy ani plnit nemůže. Lze důvodně očekávat, že význam elektronického podpisu bude spolu

---

[3] E-commerce lze definovat jako široký pojem, který zahrnuje jakoukoli obchodní transakci mezi nepodnikajícími subjekty nebo podnikateli, která je uskutečňována v rámci či skrze elektronické sítě. Předmětem mohou být jak hmotné, tak nehmotné věci. Jediným důležitým faktorem je, že komunikace této transakce probíhá skrze elektronické médium. DAVIES, S. Computer Program Claims: The Final Frontier for Software. *European Intellectual Property Review*. 1998, 20, 429 s.

[4] Důkazem může být i uvědomění si této potřeby Evropským parlamentem a Radou, když v recitálu Směrnice 1999/93/ES, o zásadách Společenství pro elektronické podpisy, ze dne 13. prosince 1999, je uvedeno: „*Rychlost technického rozvoje a celosvětový rozměr internetu vyžadují přístup otevřený různým technologiím a službám, které umožňují ověřování pravosti dat elektronickou cestou*."

s rostoucím množstvím kontraktů uzavíraných elektronicky nabývat na síle, a proto si autor této práce zvolil výše nadepsané téma.

Tato diplomová práce si klade za cíl osvětlit využití elektronického podpisu v soukromoprávní oblasti v rámci českého právního řádu, dále upozornit a objasnit úskalí plynoucí z jeho používání. Práce se také primárně zabývá vlivem elektronického podpisu na některé náležitosti právního úkonu, možné způsoby zneužití a odpovědnostní vztahy. Práce též komparuje jednotlivé instituty a vzniklé otázky se zahraničními právními řády a případně doporučuje možné návrhy de lege ferenda.

Česká odborná právní veřejnost se tématu elektronického podpisu věnovala zejména v prvních letech účinnosti zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů (dále jen „Zákon“), když zejména komparovala vlastnoruční podpis s elektronickým a činila možné návrhy de lege ferenda. Zákon prošel za tuto dobu mnohými změnami, díky kterým jsou úvahy české právní veřejnosti již neaktuální. Mimoto zde stále zůstává mnoho zcela nezmapovaných otázek, které jsou alespoň v zahraničí částečně řešeny. Práce je jedinečná právě svojí komplexnosti, se kterou zpracovává dané téma a která se v českém prostředí v této podobě dosud neobjevila.

Při tvorbě této diplomové práce autor využil především knižních a časopiseckých zdrojů z oblasti české i zahraniční právní vědy. Pochopitelně bylo dále čerpáno z řady internetových zdrojů. Omezenou roli hraje judikatura, jelikož zejména ta česká předmětné spory zatím neřešila. Zahraniční judikatura byla používána zejména k nastínění různých forem a podob podpisu.

Práce je členěna do třech hlavních tematických kapitol, které postupně osvětlují specifika elektronického podpisu a jeho použití při činění písemných právních úkonů, dále vliv použití elektronického podpisu na některé náležitosti písemných právních úkonů a následně možnosti zneužití elektronického podpisu a z toho vyplývající odpovědnostní vztahy.

Pro účely práce se elektronickým podpisem rozumí, pokud není uvedeno jinak, kvalifikovaný elektronický podpis jako nejběžněji užívaná forma elektronického podpisu, pokud není uvedeno jinak. V práci se objevují také technické pasáže, které se autor pokusil omezit na minimum nutné pro výklad tak, aby bylo možné posoudit závěry, které v sobě zahrnují reflexi jednotlivých technologických konceptů.

2. Srovnání a charakteristika vlastnoručního podpisu, elektronického podpisu a mechanických prostředků

Dle ustanovení § 40 odst. 3 zákona č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“), je písemný právní úkon platný, je-li podepsán jednající osobou. Právní úkon činěný elektronicky může být podepsán elektronicky dle zvláštních předpisů, tímto zvláštním předpisem se rozumí Zákon. Podpis může být také nahrazen mechanickými prostředky v případech, kdy je to obvyklé. Těmito třemi prostředky pro stvrzení písemného právního úkonu a jejich formami se budeme zabývat v této kapitole.

Nejprve je však nutné vyjasnit některé základní termíny spojené s využitím těchto kontraktačních prostředků, jelikož jejich výklad není často příliš jasný.

2.1 Písemný právní úkon

Právní úkon je zákonem definovaný projev vůle směřující zejména ke vzniku, změně nebo zániku těch práv nebo povinností, které právní předpisy s takovým projevem spojují.[5]

Pokud odhlédneme od problematičnosti výkladu pojmu „směřující“, která by mohla být předmětem rozsáhlé diskuze a která není významná pro téma práce ani pro logickou posloupnost práce, z dané definice je možné vyvodit čtyři základní znaky právního úkonu, kterými se budeme věnovat dále v kapitole 3:

(i) existence nositele vůle,

(ii) existence vůle,

(iii) existence projevu vůle,

(iv) existence právní normy, která s daným projevem vůle spojuje vznik, změnu nebo zánik právního vztahu.

Český právní řád zásadně nedefinuje, co se rozumí písemnou formou právního úkonu. Pouze se zmiňuje, že písemná forma je zachována, je-li právní úkon učiněn telegraficky, dálnopisem nebo elektronickými prostředky, jež umožňují zachycení obsahu právního úkonu a určení osoby, která právní úkon učinila.[6] Byť tato definice jednoznačně neurčuje, co všechno může být písemným právním úkonem, je z ní patrné,

[5] Ustanovení § 34 občanského zákoníku.

[6] Ustanovení § 40 odst. 4 občanského zákoníku.

že zákon klade na písemný právní úkon dvě podmínky, a to zachycení obsahu právního úkonu a určení osoby, která právní úkon učinila.

Z podmínky zachycení obsahu je možné vyvodit požadavek určité formy vyjádření obsahu právního úkonu a dále požadavek na uchování tohoto vyjádření na určitém nosiči.

Ohledně formy vyjádření je z výše uvedeného zřejmé, že musí obsahovat určité právně relevantní sdělení schopné vyvolat právní následky. Aby bylo schopné vyvolat právní následky, musí být alespoň z části vyjádřeno v oblasti přirozeného jazyka (nikoliv pouze výpočty, rovnicemi, funkcemi atd.). Součástí sdělení však mohou být znaky a znakové soubory, které samy o sobě nereprodukují přirozený jazyk (např. rovnice stanovující způsob výpočtu kupní ceny), ale mohou mít určitou funkci v daném sdělení.[7]

Sdělení obsažené v písemném právním úkonu, musí být alespoň z části vyjádřené písmem, tj. systémem reprezentujícím výroky mluveného jazyka prostřednictvím stálých a patrných znaků.[8] Může se jednat o jakékoliv písmo včetně obrázkového či šifry, avšak musí být srozumitelné adresátovi právního úkonu.

V souvislosti s uchováním obsahu písemného právního úkonu, je třeba tento požadavek vykládat tak, že obsah musí být zachycen na nosiči, ze kterého je možné tento obsah reprodukovat a je možné ho takto udržet alespoň po přiměřenou dobu.

Zákon hovoří o listině, avšak její legální definici již nikde nenalezneme. S tímto si však poradila teorie, když dovodila, že jako dostačující se jeví, když byl písemný právní úkon vyjádřen písmem na takovém médiu, které je schopné písmo zaznamenat. Stav a konzistence tohoto média jsou právně irelevantní, pokud je způsobilé uchovat písmo alespoň po takovou dobu, aby písemná forma úkonu mohla být zjištěna a relevantním způsobem ověřena. Stejně tak je irelevantní volba technické pomůcky, kterou je psáno. Volba jazyka, písma nebo psacího materiálu tedy není v dané souvislosti rozhodující.[9]

V souvislosti s písemným právním úkonem učiněným elektronicky přichází v úvahu především harddisk počítače, USB flash paměť či jiné podobné médium, které

[7] ČERMÁK, K. Elektronický podpis - pohled soukromoprávní. *Bulletin advokacie*. 2002, 11, 67 s.

[8] SAMPSON, G. *Writing Systems: A Linguistic Introduction.* Stanford : Stanford University Press, 1985. 26 s.

[9] ELIÁŠ, K. Právní úkony na soukromých listinách se zvláštním zřetelem k jejich podepisování. *Ad Notam.* 1996, 3, 53 s.

umožňuje uchovat data po uživatelem zvolenou dobu. Naopak zejména z praktických důvodů nepřichází v úvahu operační paměť počítače, ve které je možné uchovávat data pouze po dobu chodu systému (alespoň ve většině obvyklých případů).

Pokud zákon mluví o zachování písemné formy za předpokladu, že je úkon učiněn elektronickými prostředky, je tak učiněno naprosto správně. Lze se setkat s názory, že by bylo vhodnější nahradit pojem „elektronický" pojmem „počítačový".[10] Tento přístup by byl vzhledem k novým technologiím spíše na úkor technické neutrality a potřebné míry obecnosti. Jak autor tohoto přístupu správně poznamenává, vzhledem k pojmu elektronický by bylo možné označit za písemný právní úkon i úkon učiněný telefonem. Bezesporu lze dnes učinit písemný právní úkon prostřednictvím mobilního telefonu (např. prostřednictvím elektronické pošty, která je samozřejmě přístupná i v mobilním telefonu). V případě telefonu autor zřejmě předpokládal nemožnost učinit písemný právní úkon pouhým slovem. V souvislosti s moderními technologiemi a zejména těmi mobilními, se ale rozdíly mezi osobním počítačem a mobilním telefonem smývají. Příkladem mohou být určité mezičlánky, které se prosazují zejména v poslední době a využívají prvků jak osobních počítačů, tak i mobilních telefonů (např. tzv. tablety). Lze i důvodně předpokládat, že v budoucnu obě tyto technologie nebudou ve své čisté formě existovat. Z výše uvedených důvodů je v zájmu technologické neutrality lepší zachovat současný přístup, čímž se předejde zbytečným novelizacím zákona v souvislosti s postupnými změnami technologie a zachová se tak mnohem širší koncept, který pojme veškeré výše uvedené případy.[11]

Autor „počítačového" přístupu upozorňuje i na jiné technologie (televize, vysílačky). Tyto technologie by samozřejmě naplňovaly význam slova „elektronický", avšak nebylo by možné je považovat za písemný právní úkon vzhledem k výše uvedenému požadavku vyjádření právně relevantního sdělení písmem.

Ani v angloamerické právní kultuře není požadavek písemné formy vázán pouze na úkon učiněný inkoustem na papíře. V roce 1869 soud státu New Hampshire ve Spojených státech amerických shledal telegraf za prostředek naplňující písemnou formu právního úkonu.[12] Americké soudy dále konstatovaly, že písemnou formu právního

[10] SOKOL, T. Ještě k elektronickému dokumentu. *Bulletin advokacie*. 2002, 3, 44 s.

[11] Důkazem může být i zachování tohoto přístupu v návrhu nového občanského zákoníku, konkrétně v § 562 odst. 1 Návrhu občanského zákoníku schváleného Poslaneckou sněmovnou Parlamentu ČR.

[12] Howley v. Whipple, 48 N.H. 487 (1869).

úkonu naplňují telexy[13], faxy[14], magneticky nahraná data na disku počítače[15] a dokonce i nahrávka na pásce[16].

Požadavek písemné formy právního úkony slouží k různým účelům, zejména u smluvních vztahů poskytuje hmatatelný důkaz o existenci a povaze vůle stran být smlouvou vázán; upozorňuje strany na následky vstupu do smluvního vztahu; umožňuje prokázat vůli stran i vůči třetím osobám; poskytuje záznam smluvního vztahu, který se nemění v čase; poskytuje prostředek, který je přijímán orgány veřejné moci; umožňuje snadné uchování záznamu projevu vůle.[17]

Český právní řád vychází z principu bezformálnosti právních úkonů až na úkony, o kterých to stanoví zákon nebo kdy to vyžaduje dohoda účastníků.[18] Pokud jde o vztahy v obchodním právu, přistupuje k nim ještě písemná forma vyžádaná alespoň jednou stranou.[19] V případě, že tvoří jednu smluvní stranu více osob, je nutné požadavku písemné formy vyhovět i tehdy, když na ní trvá alespoň jeden z účastníků daného právního vztahu.[20] Zákon požaduje buď prostou písemnou formu[21], nebo formu zpřísněného zápisu, tj. notářského zápisu[22]. Je patrné, že výjimek z principu

---

[13] Joseph Denunzio Fruit Co. v. Crane, 79 F. Supp. 117.

[14] Bazak International Corp. v. Mast Industries, Inc., 535 N.E.2d 633 (N.Y. 1989). Dále také American Multimedia Inc. v. Dalton Packaging, Inc., 143 Misc. 2d 295 (N.Y. Sup. Ct. 1989).

[15] People v. Avila, 770 P.2d 1330 (Colo. Ct. App. 1988). Dále také Clyburn v. Allstate, 826 F.Supp. 955 (D.S.C. 1993).

[16] Ellis Canning Co. v. Bernstein, 348 F. Supp. 1212 (D. Colo. 1972). Avšak ve věci Roos v. Aloi, 127 Misc. 2d 864 (N.Y. Sup. Ct. 1985) soud došel k závěru, že nahrávka nesplňuje požadavek písemné formy.

[17] SMEDINGHOFF, T. J.; BRO, R. H. *FindLaw* [online]. 1999 [cit. 2011-10-21]. Electronic Signature Legislation. Dostupné z WWW: <http://library.findlaw.com/1999/Jan/1/241481.html>.

[18] Ustanovení § 40 odst. 1 občanského zákoníku.

[19] Ustanovení § 272 odst. 1 zákona č. 513/1991, obchodní zákoník, ve znění pozdějších předpisů (dále jen „obchodní zákoník“).

[20] ELIÁŠ, K. Právní úkony na soukromých listinách se zvláštním zřetelem k jejich podepisování. *Ad Notam.* 1996, 3, 53 s.

[21] Písemná forma smluv je upravena v ustanovení § 46 občanského zákoníku. Prostou písemnou formu zákon požaduje v ustanoveních § 46 odst. 1, § 57 odst. 1, § 149a, § 156 odst. 1, § 476, §524, § 531 odst. 3, § 533, § 546, § 685 občanského zákoníku, § 263 odst. 2, § 272, § 289 odst. 2, § 303, § 313 a § 323 obchodního zákoníku.

[22] Forma notářského zápisu je stanovena v ustanoveních § 143 odst. 1, 2, 3, § 147, § 156 odst. 3, § 476 odst. 1, § 476d občanského zákoníku, § 57 odst. 1, 3, § 186 odst. 6, § 186a, § 190 odst. 3, § 220t odst. 3, § 224 odst. 6, § 225 odst. 3 obchodního zákoníku.

bezformálnosti je celá řada. Návrh nového občanského zákoníku v mnoha případech od požadavku písemné formy upouští.

Podmínkou platnosti právního úkonu, kterému zákon nebo dohoda účastníků předepisuje písemnou formu, je podpis. Je-li právní úkon učiněn elektronickými prostředky, je možné, nikoliv však nutné, ho podepsat elektronicky podle zvláštních předpisů. Z textu zákona vyplývá, že ne každý právní úkon činěný elektronicky je nutné elektronicky podepsat. I elektronicky nepodepsaný právní úkon učiněný elektronickými prostředky je možné považovat za platný, ale pouze za předpokladu, že platnost tohoto úkonu není spojována s písemnou formou.

Písemná forma není dodržena ani v případě, kdy zákon požaduje úřední ověření podpisu. V tomto případě nemá na platnost vliv skutečnost, že podpis lze úředně ověřit i následně tím, že podepsaná osoba uzná podpis za vlastní.[23]

Závěrem je nutné upozornit na následky nedodržení písemné formy. Tím je především neplatnost, která je v případě zákonem předepsané písemné formy absolutní a v případě písemné formy dohodnuté účastníky relativní.

2.2 Datová zpráva

Zákon definuje datovou zprávu jako elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou.[24]

Vzorový zákon UNCITRAL, konkrétně UNCITRAL Model Law on Electronic Signature (2001), stanoví, že datovou zprávou jsou informace vygenerované, odeslané, přijaté nebo uložené elektronickými, optickými nebo obdobnými prostředky zahrnujícími zejména EDI (electronic data interchange) systém, elektronickou poštu, telegram, telex nebo telekopii.[25]

Z těchto definic lze dovodit, že datová zpráva může obsahovat i jiná sdělení než vyjádřená písmem. Dokonce nemusí obsahovat ani smysluplné vyjádření přirozeného jazyka. Pokud však budeme mluvit o zprávě jako procesu komunikace, je důvodné předpokládat, že zpráva ve většině případů nese relevantní sdělení, které je adresát schopen vnímat a pochopit.

---

[23] ŠVESTKA, J.; SPÁČIL, J.; ŠKÁROVÁ, M.; HULMÁK, M. a kolektiv. *Občanský zákoník I, II.* 2. vydání. Praha : Nakladatelství C. H. Beck, 2009. 362 s.

[24] Ustanovení § 2 Zákona.

[25] Ustanovení článku 2 vzorového zákonu UNCITRAL Model Law on Electronic Signature (2001).

Zákon nikde nestanovuje povinnost podepisovat datovou zprávu, pouze stanoví, že datová zpráva je podepsána, pokud je opatřena elektronickým podpisem[26]. Naproti tomu písemný právní úkon ke své platnosti vyžaduje podpis. Je patrné, že ne každý právní úkon je datovou zprávou. K tomu by musel být učiněn pomocí elektronických prostředků a v případě obligatorní písemné formy také patřičně elektronicky podepsán. Na druhou stranu ne každá datová zpráva je právním úkonem, ale pouze taková, která obsahuje sdělení vyvolávající právní následky, které s nimi zákon spojuje. Datová zpráva ve vztahu k právnímu úkonu tedy není pojmem rovným, ani nadřazeným nebo podřazeným.[27]

Pokud bychom se zabývali vztahem datové zprávy a dokumentu, tak dokumentem rozumíme každou písemnou, obrazovou, zvukovou nebo jinou zaznamenanou informaci, ať již v podobě analogové či digitální, která byla vytvořena původcem nebo byla původci doručena.[28] Je tedy možné říci, že pojem datová zpráva ve svém užším významu je shodný s pojmem elektronický dokument.[29] Avšak datová zpráva v širším významu může nést více elektronických dokumentů, které budou tvořit přílohy, z čehož vyplývá, že datová zpráva v širším významu je pojem nadřazený elektronickému dokumentu. V tomto ohledu je třeba také vykládat příslušné právní předpisy, jelikož to má pro pravidla elektronické komunikace v právní praxi zásadní důsledky (k tomu v další podkapitole).[30]

Návrh nového občanského zákoníku v § 561 odst. 1 dále stanoví, že *„jiný právní předpis stanoví, jak lze při právním jednání učiněném elektronickými prostředky písemnost elektronicky podepsat“*. Autor se domnívá, že tato formulace je nepříliš vhodně zvolena, jelikož dle ustanovení § 3 odst. 1 Zákona je datová zpráva podepsána, pokud je opatřena elektronickým podpisem. Zákonodárce by měl věnovat pozornost rozdílnosti pojmů písemnost, písemnost jako právní úkon, písemný právní úkon a datová zpráva dle toho, jak je činěno výše. Dle autora by bylo vhodné při takto zvolené

[26] Ustanovení § 3 odst. 1 Zákona.

[27] ČERMÁK, K. Elektronický podpis - pohled soukromoprávní. *Bulletin advokacie*. 2002, 11, 67 s.

[28] Ustanovení § 2 zákona 499/2004, o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon o archivnictví“).

[29] Dále k tomu ustanovení § 22 odst. 2 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů (dále jen „zákon o el. úkonech“).

[30] PETERKA, J.; PODANÝ, J. Problematika elektronické podpisu v soudní praxi. *Právní rozhledy*. 2010, 19, 689 s.

formulaci deklarovat vztah těchto dvou pojmů například ve výkladových ustanoveních Zákona. Nový občanský zákoník dále již přímo neobsahuje deklaratorní ustanovení, které stanoví, že právní úkon činěný elektronicky lze podepsat, avšak výkladem výše uvedeného ustanovení lze toto bez potíží dovodit.

2.2.1 Paradigma obálky a dokumentu

Široká veřejnost má všude tam, kde dochází k právně relevantní komunikaci, zažité tzv. paradigma obálky, dle kterého je možné dokument doručit buď samostatně, např. při osobním předání návrhu smlouvy, nebo vložený do obálky při doručení poštou.

Veřejnosti je známé, že nositelem sdělení, mj. i toho právně relevantního, je pouze dokument, zatímco obálka slouží k přenosu dokumentů a nenese žádné relevantní sdělení, kromě údajů o adresátovi, případně i odesílateli a okolnostech přepravy (např. datum předání držiteli poštovní licence či využití zvláštních prostředků přepravy zásilky – lodní či letecká). Stejně tak je veřejnost seznámena s tím, že podpisem dokumentu projevuje souhlas s obsahem tohoto dokumentu, kdežto podpisem obálky, což je samo o sobě velice neobvyklé, se vyjadřuje pouze, že dokument do obálky vložila a obálku zalepila právě osoba podepsaná.[31]

V elektronické sféře je situace složitější o to, že elektronický objekt může nést současně obě funkce, tj. jednak být nositelem dalších dokumentů a jednak nést i určité právně relevantní sdělení. V tomto smyslu je tedy nutné rozlišovat 3 různé varianty[32]:

1. čisté dokumenty – objekty, které obsahují pouze sdělení, ale již neobsahují další objekty charakteru dokumentů (např. čistě textový soubor ve formátu TXT);
2. čisté obálky – objekty, které pouze nesou další dokumenty, avšak nenesou žádné vlastní sdělení (např. zpráva přenášená informačním systémem datových schránek);
3. hybridy – objekty, které nesou vlastní sdělení a současně jsou i nositelem dalších dokumentů (např. e-mail nesoucí přílohy).

Ve vztahu elektronického podpisu k těmto variantám je význam podpisu následující:

1. elektronický podpis na čistém elektronickém dokumentu vyjadřuje souhlas podepsané osoby s obsahem dokumentu, tedy projevem vůle;

[31] Tamtéž.

[32] Tamtéž.

2. elektronický podpis na čisté obálce není projevem vůle, ale značí, že obsah obálky sestavila podepsaná osoba;
3. elektronický podpis na hybridu je nutné interpretovat dvěma možným způsoby současně:
    a) vůči obsahu, který je sdělením, jako vyjádření souhlasu,
    b) vůči obsahu, který je přílohou, jako potvrzení, že právě podepsaná osoba přílohu do hybridu vložila.

Dnešní právní praxe, zejména tak postupuje mnoho soudů, si počíná v mnoha ohledech nesprávně, když vztahuje elektronický podpis zprávy i na přílohu.

Ústavní soud v rozhodnutí sp. zn. IV. ÚS 319/05 judikoval, že povinnost stěžovatele uvedená v ustanovení § 42 odst. 3 zákona 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů (dále jen „OSŘ“), tedy písemně doplnit své elektronické podání do tří dnů, se nevztahuje na podání v elektronické podobě, jestliže je k němu připojen uznávaný elektronický podpis dle ustanovení § 11 odst. 1 Zákona. Reagoval, tak na chybu zákonodárce, který stanovoval, že veškerá podání činěná v elektronické podobě, je třeba do tří dnů doplnit předložením jeho originálu, případně písemným podáním shodného znění, jinak k těmto podáním soud nepřihlíží. OSŘ bylo již novelizováno tak, že zmíněný nedostatek odstranilo.

Ústavní soud ovšem ve výše zmíněné věci také neuznal elektronicky přiloženou plnou moc advokáta, jelikož se nejednalo o originál, a vyzval k doplnění. Advokát v tomto případě originál plné moci doplnil, pročež mohl Ústavní soud přistoupit k meritornímu projednání věci.

Advokát se mohl vyhnout doplnění plné moci v papírové podobě tak, že by dodal plnou moc podepsanou pomocí elektronického podpisu založeného na kvalifikovaném certifikátu vydaným akreditovaným poskytovatelem certifikačních služeb nebo mohl provést autorizovanou konverzi papírové plné moci. S tímto názorem se shoduje odborná právní veřejnost z řad soudců[33] i z řad autorů vydávající komentářovou literaturu, když uvádí: „*Ten, kdo předložil soudu pouze neověřené kopie (opisy) listin nebo konverzí neautorizované dokumenty (datové zprávy) v elektronické podobě, musí být připraven na výzvu soudu poskytnout jejich originály*“.[34]

[33] PETERKA, J.; PODANÝ, J. Problematika elektronické podpisu v soudní praxi. *Právní rozhledy*. 2010, 19, 689 s.

[34] DRÁPAL, L.; BUREŠ, J. a kol. Občanský soudní řád I, II. Komentář. 1. vydání. Praha : Nakladatelství C. H. Beck, 2009. 272 s.

Problém tedy může nastat v případě, kdy u přílohy převedené neautorizovanou konverzí není zajištěna nezměnitelnost této přílohy ještě ve stádiu své papírové formy a dále také originalita, když pouze provedením autorizované konverze má její výstup stejné právní účinky.[35] Dalším ryze praktickým problémem je, že soudy ve své praxi pracují spíše s přílohami, které se často uvnitř soudního systému přeposílají, a přeposláním se ztrácí podpis z původní datové zprávy. V případě přejímání podpisu z datové zprávy na přílohy, soudce tak nemusí být schopen ověřit, kdo tuto přílohu podepsal, případně zda byla vůbec podepsána či nebyla dokonce pozměněna.

Z výše uvedeného je zřejmé, že v případě podání činěného prostřednictvím emailu, kdy bychom v textu uvedli pouze: „V příloze zasílám podání.“, dále přiložili samotné podání, které by však nebylo elektronicky podepsané, a email elektronicky podepsali, by nás soud měl vyzvat k doplnění. Sami bychom se přiznali k tomu, že podáním je pouze dokument v příloze a nikoliv text emailu, který sám nepochybně nesměřuje k uplatnění práva, ke splnění povinnosti nebo k jiným procesněprávním následkům, které s ním spojují právní předpisy.

V případě soukromoprávních úkonů je tedy nutné aplikovat stejné závěry, když je nezbytné si uvědomit, jaký objekt hraje roli obálky, dokumentu nebo hybridu. Příkladem může být jednostranné odstoupení od písemné smlouvy zaslané druhé smluvní straně v příloze elektronicky podepsaného emailu, aniž by samotná příloha byla elektronicky podepsána a aniž by text emailu obsahoval jakékoliv další sdělení. Je zřejmé, že v tomto případě by nebylo platně odstoupeno od smlouvy a smlouva tak nebyla zrušena.[36]

2.3 Podpis

Již od vzniku prvních písemností se objevují nástroje pro ověření pravosti písemnosti, proto není překvapivé, že právě Sumerové, kteří jsou považováni za první civilizaci zaznamenávající písmo do kamene a později na hliněné destičky, vynalezli první mechanismus ověření pravosti. Využívali k tomu nástroj v podobě válce, který by mohl být přirovnán k dnešnímu pečetidlu. Pečetě se k naplnění této funkce používaly primárně až do nedávné doby.[37]

[35] Ustanovení § 22 odst. 2 zákona o el. úkonech.

[36] Vzhledem k ustanovení § 40 odst. 2 a 3 občanského zákoníku.

[37] POSTGATE, J. N. *Early Mesopotamia - Society and Economy at the Dawn of History.* New York : Routledge, 1992. 282 s.

Použití podpisu je zaznamenáno již v Talmudu, kde měl podpis sloužit jako prostředek pro zamezení úprav dokumentu. Praxe ověřování pravosti dokumentu připojením podpisu se začala využívat na území římské říše již v roce 439 našeho letopočtu za vlády Valentiniána III. Na konci dokumentu bývalo připsáno slovo „*subscripto*“, případně krátká věta o tom, že strany dokument podepsaly. Dále byla připojena pečeť jednající osoby. Pečeť byla postupem času nahrazena ručně psaným jménem podepisující osoby. Tato metoda se rozšířila natolik, že přetrvala následujících 1400 let.[38]

V roce 1677 byl v Anglii schválen zákon „*An Act for Prevention of Frauds and Perjuries*“, který vyžaduje u určitých typů smluv písemnou formu a podpis. Mnoho právních řádů v rámci této právní kultury poté přijalo podobný zákon označovaný jako „*Statute of frauds*“.[39]

2.3.1 Forma podpisu

Český právní řád s pojmem podpis na řadě míst operuje. Jedním z nejvýznamnějších případů je výše uvedené ustanovení § 40 odst. 3 občanského zákoníku. Samotný termín však nikde v pozitivní právní úpravě není definován stejně jako v jiných právních řádech nejen kontinentálního právního systému.

Avšak české právo rozlišuje v mnoha zákonech několik různých forem podpisu:

- podpis,
- vlastnoruční podpis,
- ověřený podpis,
- elektronický podpis (včetně jeho vyšších forem – viz podkapitola 2.4 této práce).

Z logiky rozlišování jednotlivých forem podpisu, lze souhlasit s názorem, že podpis (bez dalších adjektiv) je pojmem nejobecnějším a jeho náležitost je splněna jakoukoli další vyšší formou podpisu[40], přičemž elektronický podpis je považován za ekvivalentn podpisu.

---

[38] NICHOLAS, B. *An Introduction to Roman Law.* Oxford : Clarendon Press, 1962. 256 s.

[39] FORD, W.; BAUM, M. S. *Secure electronic commerce: building the infrastructure for digital signatures and encryption*. New Jersey : Prentice Hall, 1997. 42 s.

[40] MATEJKA, J.; CHUM, V. K právní úpravě elektronického podpisu. *Bulletin advokacie.* 2002, 3, 28 s.

2.3.1.1 Podpis a vlastnoruční podpis

Při odlišení podpisu a vlastnoručního podpisu nelze souhlasit s názorem, že v případě podpisu si lze vystačit se strojovým či jinak mechanicky na listině vyznačeným podpisem.[41] To by bylo možné pouze za předpokladu, že tímto vytištěným podpisem, resp. uvedením jména, bylo myšleno nahrazení podpisu mechanickým prostředkem tam, kde je to obvyklé, ale v takovém případě se nejedná o podpis v právním slova smyslu. Tuto nepřesnost může vyvolávat například to, že český jazyk tuto distinkci nezná a pojem podpis používá i pro vytištěné jméno, které se nezřídka objevuje s dodatkem v. r. (např. v případě právních předpisů vydaných ve Sbírce zákonů). Je zcela zjevné, že vytištěný podpis je v intencích ustanovení § 40 odst. 3 občanského zákoníku považován za mechanický prostředek nahrazení podpisu.

V rámci tohoto posuzování je nutné se zamyslet, zda podřazení pod mechanické prostředky nahrazení podpisu je závislé na prostředcích sloužících k vytvoření této náhražky. V tomto ohledu lze namítnout, že pero a inkoust je také mechanickým prostředkem, který slouží k vyhotovení podpisu, ale tyto prostředky na rozdíl od tiskárny znatelněji zohledňují lidskou individualitu, proto výtvor těchto prostředků je mnohem méně náhražkou podpisu než jméno vytištěné strojem, tiskárnou nebo uvedené za textem elektronického dokumentu. Pouhé uvedení jména na dokumentu, však postrádá jakékoli propojení s lidskou individualitou a mohlo být vytvořeno kýmkoliv a je také komukoliv známé. Lze však učinit závěr, že i tištěné jméno může naplňovat podmínky podpisu podobně, jako je tomu v případě prostého elektronického podpisu. Musí ale kromě vlastního jména obsahovat ještě takové údaje, o kterých je zřejmé, že jsou schopné identifikovat osobu, a se kterými nemohl disponovat nikdo jiný.

Pro srovnání soudy angloamerického právního sytému judikovaly v souvislosti s touto problematikou, že podpisem se rozumí i vytištěné jméno[42] či otisk razítka[43].

Požadavek vlastnoručního podpisu zákonodárce stanovil zejména tam, kde je zvýšená potřeba ověřit, kdo skutečně právní úkon činí, a potvrdit projevenou vůli, což může podepisující osobu i upozornit na případné právní následky takto projevené vůle.

---

[41] MATEJKA, J.; CHUM, V. K právní úpravě elektronického podpisu. *Bulletin advokacie.* 2002, 3, 29 s.

[42] Brydges v. Dix, 7 TLR 215 (1891); France v. Dutton, 2 Q.B. 208 (1891); Newborne v. Sensolid (Great Britain), Ltd., 1 QB 45 (1954).

[43] Lazarus Estates, Ltd. v. Beasley, 1 QB 702 (1956); London County Council v. Vitamins, Ltd., London County Council v. Agricultural Food Products, Ltd., 2 QB 218 (1955); Goodman v. J. Eban Ltd., 1 QB 550 (1954).

Zákonodárce tak zejména vylučuje nahrazení podpisu mechanickými prostředky, případně použití elektronického podpisu, což svědčí o jeho rovnosti s podpisem, nikoli však tím vlastnoručním.

Nejvyšší soud se vyjádřil ke způsobu provedení vlastnoručního podpisu, když judikoval, že v případě holografní závěti musí být všechny náležitosti závěti (celý text, včetně data a podpisu) napsány vlastní rukou zůstavitele[44], přičemž pojem vlastní rukou, resp. vlastnoruční, je z hlediska ustanovení § 476a občanského zákoníku na místě vykládat jako požadavek, aby pořizovatel celou závěť napsal vlastní rukou, popřípadě, aby ji, je-li zdravotně postižen, napsal např. nohou, či za pomoci protézy, je-li tento způsob psaní u něj možný a obvyklý a nese-li současně takový způsob psaní charakteristické znaky rukopisu pořizovatele závěti[45]. Rozhodnutí se vztahuje i na další právní úkony, jelikož Nejvyšší soud také upozornil na nezbytnost nevymezit podpis závěti, jakožto písemného právního úkonu, zcela odlišně od obecně judikaturou i doktrínou přijímaných požadavků na podpis jiných písemných právních úkonů.[46]

Judikatura tak dovodila, že pojem vlastnoruční podpis v sobě zahrnuje i provedení podpisu jinak než vlastní rukou, avšak pouze za předpokladu, že je tento způsob u podepisující osoby obvyklý a nese charakteristické znaky rukopisu. Podobně se k tomuto vyjadřuje právní teorie, dle které je rozhodující pouze, že jednající osoba sama listinu podepsala bez ohledu, jaký její tělesný úd nahradil funkci ruky.[47]

2.3.1.2 Ověřený podpis

Ověřený podpis je považován za jakousi nejvyšší formu podpisu, která je výsledkem legalizace. Dle ustanovení § 74 zákona č. 352/1992 Sb., o notářích a jejich činnosti, ve znění pozdějších předpisů, legalizací notář ověřuje, že fyzická osoba v jeho přítomnosti listinu vlastnoručně podepsala nebo podpis na listině se již nacházející před ním uznala za vlastní. Je zajímavé, že zákonodárce v tomto ustanovení kombinuje dvě různé formy podpisu – podpis a vlastnoruční podpis.

---

[44] Rozhodnutí Nejvyššího soudu ze dne 17.11.1998, sp.zn. 21 Cdo 586/98, uveřejněné ve Sbírce soudních rozhodnutí a stanovisek pod č. 44/1999.

[45] Rozhodnutí Nejvyššího soudu ze dne 31.03.2009, sp. zn. 21 Cdo 51/2008, uveřejněné ve Sbírce soudních rozhodnutí a stanovisek pod č. 13/2010.

[46] Tamtéž.

[47] ELIÁŠ, K. Právní úkony na soukromých listinách se zvláštním zřetelem k jejich podepisování. *Ad Notam.* 1996, 3, 55 s.

Pravost ověřovaných podpisů lze ověřit dvěma způsoby podle okolností. Obsahuje-li listina již podpis, notář osvědčí prohlášení dotčené osoby, kterým uznává podpis na listině za vlastní. V tomto případě je pravost podpisu ověřena zprostředkovaně prostřednictvím osoby, která prohlásila, že podpis na listině je jejím podpisem.[48] Teorie k tomuto ne příliš přesvědčivě uvádí, že z právního hlediska je zřejmě lhostejné, kdo se na listinu fakticky podepsal. Platí zde právní fikce, že takto uznaný podpis je podpisem uznávajícího bez ohledu, zda tento podpis skutečně vytvořil vlastní rukou nebo byl vytvořen rukou třetí osoby.[49] Dle názoru autora je možné zvolit v tomto případě i formu elektronického podpisu, avšak pouze za předpokladu, že listina byla předem autorizovaně konvertována, teprve s takto konvertovanou listinou je možné jít k notáři. Neznalý notář bude ale zřejmě požadovat klasický podpis. Jiný postup než skrze autorizovanou konverzi by patrně nebyl možný, jelikož by bylo obtížné do některých elektronicky podepsaných dokumentů připojit ověřovací doložku a dále zcela nemožné připojit otisk úředního razítka notáře. Zde můžeme nalézt určitý prostor pro návrhy de lege ferenda v oblasti elektronizace notářství, které je v našem právním řádu zatím v počátcích.

Podepsala-li určitá osoba listinu před notářem, osvědčuje notář tuto skutečnost.[50] V tomto ohledu by se mohl zdát neobvyklým případ, kdy je podpis učiněn například tiskacím písmem nebo levou rukou, když podepisující osoba se obyčejně podepisuje rukou pravou. Zde by však notář nemohl ničeho namítat, jelikož podpis byl učiněn vlastnoručně. V tomto případě ale nelze uvažovat o ověřování elektronických podpisů.

Obecně tedy není možné ověřit elektronický podpis přímo na elektronickém dokumentu.

Ohledně ověření podpisu advokátem je advokát oprávněn nahradit úřední ověření podpisu vyžadované zvláštními právními předpisy svým prohlášením se stejnými účinky podle § 25a zákona č. 85/1996 Sb., o advokacii, ve znění pozdějších předpisů. Toto je možné pouze na:

a) listině, kterou sám sepsal a osoba, jejíhož podpisu se prohlášení o pravosti podpisu týká, listinu před ním podepsala, nebo

[48] BÍLEK, P.; DRÁPAL, L.; JINDRŘICH, M.; WAWERKA, K. *Notářský řád a řízení o dědictví*. 4. vydání. Praha : C. H. Beck, 2010. 303 s.

[49] SOKOL, T. Podpis, jeho podstata a role při právních úkonech. *Právní rádce*. 2004, 12, 6. s.

[50] BÍLEK, P.; DRÁPAL, L.; JINDRŘICH, M.; WAWERKA, K. *Notářský řád a řízení o dědictví*. 4. vydání. Praha : C. H. Beck, 2010. 303 s.

b) jiné listině, pokud ji jednající osoba před ním podepsala.

Jednou z možností ověření elektronického podpisu, kterému dle názoru autora zákon nijak nebrání, je podepsat elektronicky dokument v přítomnosti advokáta, dále u advokáta provést autorizovanou konverzi a advokát poté provede běžné ověření.

Patrně by bylo nemožné provést ověření, způsobem přidání kompletního prohlášení na konec samotného dokumentu při jeho tvorbě, poté nechat jednající osobu dokument elektronicky podepsat a nakonec přidat elektronický podpis advokáta. Tento postup naráží na překážku vyhotovení prohlášení, které lze provést pouze způsobem stanoveným v čl. 5 odst. 3 Usnesení představenstva České advokátní komory č. 4/2006 Věstníku, ve znění pozdějších stavovských předpisů, dle kterého je možné prohlášení vyhotovit mj. tiskem, což je u čistě elektronického dokumentu samozřejmě v rozporu s jazykovým výkladem termínu „tiskem“. Jiné možnosti vyhotovení prohlášení nepřicházejí v úvahu.

2.3.2 Podoba podpisu

Soudy angloamerického právního systému bohatě judikovaly, že podpisem nemusí být pouze vlastnoručně napsané úplné jméno, ale i různé modifikace tohoto přístupu, například křížky[51], iniciály[52], pseudonym[53], fráze identifikující osobu[54], pouhé příjmení[55], obchodní jméno[56], zkratka jména[57], částečný podpis[58].

Obdobným přístupům se věnovala i česká judikatura při řešení řady praktických otázek. Předně jaký podpis je dostatečný pro naplnění významu tohoto termínu, tedy zda například postačuje označení „*Tvá matka*“, „*Váš syn Jan*“ atp., dále jak úplný podpis z hlediska práva je dostatečný, případně zda musí být uvedeno skutečné a úplné jméno tak, jak je uvedeno v matrice a osobních dokladech.

---

[51] Baker v. Dening, 8 A&E 94 (1838); Harrison v. Harrison, 8 Ves Jun 185, 32 ER 324 (1803).

[52] Phillimore v. Barry, 1 Camp 512, 170 ER 1040 (1808); Hill v. Hill, Ch 231 (1947).

[53] Reddings Goods, 14 Jur 1052, 2 Rob. Ecc. 338 (1850).

[54] Murison v. Cook, 1 All ER 689 (1960). Podpisem zde bylo „*Your loving mother*“. Selby v. Selby, 3 Mer 2, 36 ER 1. Rozdílně např. Berdan v Berdan, 39 Cal App 2d 478 (1940). Zde nebylo jako podpis uznáno označení „mother“.

[55] Lobb and Knight v. Stanley, 5 QB 574, 114 ER 1366 (1844).

[56] Cohen v. Roche, 1 KB 169 (1927).

[57] Barrletts de Reya v. Bryne, 127 SJ 69 (1983).

[58] Chalcraft v. Giles, P 222 (1948).

Ideálním stavem, je samozřejmě situaci, kdy podepisující osoba vlastnoručně podepíše listinu jejím skutečným a úplným jménem, tedy takovým, „*které přesně odpovídá tomu, jak je formálně zapsáno v matrice a osobních dokladech jednající osoby, tedy s vypsáním jména osobního (křestního) i rodového (příjmení) a má-li jednající osoba tituly, jež jsou součástí jména, pak rovněž s jejich uvedením.*“[59] Je vhodné v případě nečitelného podpisu doplnit ho o strojově vytištěné jméno podepisující osoby a v zájmu jednoznačného určení totožnosti i o další údaje (datum narození, bydliště, dodatek „*mladší*“ či „*starší*“).[60]

Situace je však v praxi zcela odlišná. Na otázku určení, jaký podpis je dostatečný pro písemný právní úkon, je nutné odpovědět zcela obecně. V zásadě se rozumí takové označení, z něhož je objektivně možné identifikovat osobu, která úkon učinila. Musí z něj být tedy zjistitelná identita osoby, která právní úkon činí. Je-li splněna tato základní podmínka, lze za podpis uznat i podpisovou zkratku (šifru, resp. parafu) nebo dokonce i podepsání úkonu pseudonymem.[61] Podpis pseudonymem přichází v úvahu i u kvalifikovaného elektronického podpisu, naproti tomu podpis šifrou nebo heslem přichází v úvahu pouze u prostého elektronického podpisu.

Strany vícestranného právního úkonu si mohou sjednat mezi sebou určité podmínky či charakter podpisu. Toho využívají zejména peněžní ústavy, které musí provádět kontrolu podpisu s veškerou požadovanou pečlivostí. Zde je potřeba zmínit rozhodnutí Vrchního soudu v Praze ze dne 10.11.1994 sp. zn. 5 Cmo 179/94, který judikoval, že banka neodpovídá za škodu vzniklou neprovedením dispozic klienta, u kterých je zpochybněna jejich pravost nebo platnost, i když se později prokáže, že dispozice nijak vadné nebyly. Stejná situace může nastat při využití elektronického podpisu, pokud má banka důvěryhodnou informaci, například přímo od klienta, že klientův podpis byl zneplatněn, avšak samotná informace o zneplatnění ještě nebyla zveřejněna. To je možné zejména s ohledem na konkrétní certifikační politiku jednotlivých certifikačních autorit, které zveřejní zneplatnění certifikátu elektronického

[59] ELIÁŠ, K. Právní úkony na soukromých listinách se zvláštním zřetelem k jejich podepisování. *Ad Notam.* 1996, 3, 56 s.

[60] Tamtéž.

[61] Tamtéž.

podpisu nejdéle do 12 hodin (PostSignum[62]), resp. 24 hodin (I. CA[63], eIdentity[64]). V porovnání slovenská právní úprava stanovuje lhůtu pro zneplatnění certifikátu certifikační autoritou v podzákonném předpise jednotně na 24 hodin[65] nebo estonská právní úprava předepisuje zveřejnit zneplatnění do 24 hodin po oznámení.[66] Jedním z návrhů de lege ferenda by mohlo být zavedení lhůty pro zveřejnění informace o zneplatnění do Zákona.

Odlišná situace ohledně podoby podpisu platí překvapivě v případě závěti. Dle ustanovení § 476a a § 476b občanského zákoníku vyžaduje závěť podpis vlastní rukou. Dřívější i dnešní judikatura[67] však v zásadě dovodila, že vlastnoruční podpis musí obsahovat alespoň křestní jméno nebo příjmení (přípustné je i dívčí jméno[68]), a to pouze pokud je možné zůstavitele jednoznačně identifikovat[69], například i vzhledem k logické vazbě mezi oslovením adresátů a podpisem[70] nebo v případě uvedení příjmení

---

[62] Certifikační politika PostSignum Qualified CA pro kvalifikované osobní certifikáty. ČESKÁ POŠTA, s.p. *Certifikační autorita PostSignum* [online]. 2.0. 30.01.2010 [cit. 2012-02-11]. Dostupné z: <http://www.postsignum.cz/files/politiky/QCA_osobni_crt_v2-0.pdf>.

[63] CERTIFIKAČNÍ POLITIKA VYDÁVÁNÍ KVALIFIKOVANÝCH CERTIFIKÁTŮ. PRVNÍ CERTIFIKAČNÍ AUTORITA, a.s. *I.CA.* [online]. 3.1. [cit. 2012-02-11]. Dostupné z: <http://www.ica.cz/Userfiles/files/politika/CP_QCv31.pdf>.

[64] ACAeID10.1 Certifikační politika - QC. AKREDITOVANÝ POSKYTOVATEL CERTIFIKAČNÍCH SLUŽEB EIDENTITY A.S. *APCS eIdentity a.s.* [online]. 2.2. 10.02.2010 [cit. 2012-02-11]. Dostupné z: <http://www.acaeid.cz/aca2/cp-qc.pdf>.

[65] Ustanovení § 5 vyhlášky č. 538/2002 Z. z., o formáte a obsahu kvalifikovaného certifikátu, o správe kvalifikovaných certifikátov a o formáte, periodicite a spôsobe vydávania zoznamu zrušených kvalifikovaných certifikátov.

[66] Dle ustanovení § 22 Digitaalallkirja seadus (Estonská republika).

[67] Rozhodnutí Nejvyššího soudu ze dne 31.03.2009, sp. zn. 21 Cdo 51/2008, uveřejněné ve Sbírce soudních rozhodnutí a stanovisek pod č. 13/2010.

[68] Sammlung von Civilrechtlichen Entscheidungen des k. k. obersten Gerichtshofes, heraugegeben von J. Glaser Lind J. Unger, Bd. I., Verlag von Tedler & Comp., Wien, 1910; Nr. 5242. Cit. dle: ELIÁŠ, K. Právní úkony na soukromých listinách se zvláštním zřetelem k jejich podepisování. *Ad Notam.* 1996, 3, 57 s.

[69] Civ. rozh. Vážného sbírky č. 9010 z roku 1929. Cit. dle: ELIÁŠ, K. Právní úkony na soukromých listinách se zvláštním zřetelem k jejich podepisování. *Ad Notam.* 1996, 3, 57 s.

[70] Sammlung von Civilrechtlichen Entscheidungen des k. k. obersten Gerichtshofes, heraugegeben von J. Glaser Lind J. Unger, Bd. I., Verlag von Tedler & Comp., Wien, 1859; Nr. 1211. Cit. dle: ELIÁŠ, K. Právní úkony na soukromých listinách se zvláštním zřetelem k jejich podepisování. *Ad Notam.* 1996, 3, 57 s.

zůstavitele ve spojení s jeho titulem, za situace, kdy o totožnosti tohoto vlastnoručního podpisu nejsou pochybnosti[71]. Zásadně se však nepřipouští pouhá označení „*Tvoje matka*“, „*Tvůj otec*“ atp., případně jiné šifry či označení, a to i za předpokladu, že zůstavitel je jednoznačně určen, třeba tím, že dědic má pouze jednu matku.

Důvodem je zejména, že ustanovení § 578 Obecného zákoníku občanského, vyhlášeného císařským patentem ze dne 1.6.1811, č. 946 Sb. z. s., který byl pro území Republiky československé recipován zákonem č. 11/1918 Sb., ve znění pozdějších předpisů, požadoval, aby pořizovatel holografní závěti ji „*vlastní rukou podepsal svým jménem*“. Určení „*svým jménem*“ se neobjevilo již ani v ustanovení § 542 zákona č. 141/1950 Sb. (střední občanský zákoník) a nepočítá se s ním ani v ustanovení § 1522 návrhu nového občanského zákoníku. Otázkou může být, proč judikatura dále zastává totožný názor, i když se znění zákona změnilo. Judikatura k současnému občanskému zákoníku dospěla k závěru, že „*je třeba za podstatné považovat spolehlivé zjištění toho, že podpis na závěti pochází od zůstavitele a že je dán v takové formě, aby nebylo pochybností o totožnosti zůstavitele*“; že „*jde zejména o to, aby pisatel závěti byl zcela jednoznačně určen*“[72] a že „*podepsal-li zůstavitel závěť alespoň svým příjmením, je tím splněna náležitost podpisu závěti, pokud o totožnosti podpisu zůstavitele nejsou žádné pochybnosti*“[73].

Dle názoru autora je tato situace nepřijatelná, pokud nemá oporu v zákoně. S požadavky judikatury lze sice souhlasit, ale nelze si představit situaci, kdy vlastnoruční podpis písemného právního úkonu je v jednom případě v zásadě akceptovatelný a v druhém nikoliv, a to na základě shodného znění dotčených ustanovení.

2.3.3 Funkce podpisu

Vlastnoruční podpis naplňuje řadu funkcí. Těmi nejčastěji uváděnými jsou následující[74]:

---

[71] Civ. rozh. č. 51/1984. Cit. dle: ELIÁŠ, K. Právní úkony na soukromých listinách se zvláštním zřetelem k jejich podepisování. *Ad Notam.* 1996, 3, 56 s.

[72] Rozhodnutí Nejvyššího soudu ČSR ze dne 27.1.1983, sp. zn. 4 Cz 82/82, uveřejněné ve Sbírce soudních rozhodnutí a stanovisek pod č. 51/1984.

[73] Tamtéž.

[74] ČERMÁK, K. Elektronický podpis - pohled soukromoprávní. *Bulletin advokacie*. 2002, 11, 67-68 s.

- označení toho, kdo učinil právní úkon (z tohoto hlediska jde o součást projevu vůle, jelikož v sobě zahrnuje informaci o tom, kdo má být považován za autora úkonu) (označovací funkce);
- potvrzení, že ten kdo, učinil právní úkon, tak skutečně učinit chtěl a že se jedná o jeho vlastní projev vůle (z tohoto hlediska jako součást obsahu samotné vůle, jelikož krom pouhé identifikace osoby deklaruje obsah právního úkonu) (deklarační funkce);
- ověření totožnosti jednajícího (z tohoto hlediska není součástí vůle, ani jejího projevu, ale důkazem o tom, kdo podepsal právní úkon) (důkazní funkce).

Označovací funkci plní vlastnoruční podpis do jisté míry velmi omezeně, jelikož v mnoha případech je jeho čitelnost velmi omezena nebo naprosto nulová. V takovém případě lze tvrdit, že označovací funkci plní spíše jiná část projevu vůle, kde je strojově vytištěno jméno.[75] Na jednu stranu se každá osoba svobodně rozhoduje, jakým způsobem uvede své jméno pod text, na druhou stranu je však rukopis natolik unikátní vlastností každé osoby, že je možné říci, která osoba dokument skutečně podepsala. Z tohoto důvodu podpis plní stejně dobře označovací funkci jako tu důkazní.[76]

Ovšem výše uvedené platí pouze u obvyklých podob podpisu. Je možné si představit případ, kdy se osoba z nějakého důvodu podepíše druhou rukou, než se obvykle podepisuje, nebo se podepíše tiskacím písmem. V takovém případě je důkazní funkce omezená, resp. žádná u druhého případu. Avšak jednoznačně lze dovodit, že se jedná o vlastnoruční podpis. V takovém případě je lichá domněnka, že je možné posuzovat, zda se jedná o podpis či nikoliv, podle toho, jak plní výše uvedené funkce.[77]

Deklarační funkce podpisu osoby, která nejedná v zastoupení, osvědčuje vůli a záměr osoby být vázán právním úkonem (animus signandi). Podpisem osoba vyjadřuje svůj souhlas s obsahem dokumentu. Proto například pokud dokument neobsahuje přesná prohlášení smluvní strany nebo dokument nereprodukuje věrně znění dohody smluvních

[75] SOKOL, T. Podpis, jeho podstata a role při právních úkonech. *Právní rádce*. 2004, 12, 4 s.

[76] LABORDE, C. M. *Electronic Signatures in International Contracts*. Frankfurt am Main : Peter Lang, 2010. 27 s.

[77] K opačnému názoru srov. REED, Ch. *Internet Law: Text and Materials*. Second Edition. Cambridge : Cambridge University Press, 2004. 182 s.

stran, tak podepisující osoba odmítne úkon podepsat. Pokud by podpis učinila, byl by ve vztahu k dalším osobám dán souhlas s obsahem úkonu.[78]

Termíny užívané v různých jazycích pro institut podpisu vyjadřují různé vlastnosti podpisu. V anglickém a francouzském jazyce je používané slovo „signature".[79] Pochází z latinského „signum", což v překladu znamená důkaz, znamení. Ve španělském jazyce slovo „firma" je odvozeno od slova „firmar" s významem potvrzovat. Německé „Unterschrift", stejně jako české podpis, je odvozeno od „níže napsané", což odkazuje na funkci ověření integrity listiny. Podpis v tomto případě slouží jako prostředek k zamezení a zjištění pozdějších změn listiny. Tato funkce čerpá z obvyklého připojení podpisu na samotný konec listiny a obsah, který je uveden pod podpisem, nemá obvykle žádný právní význam, jelikož mohl být přidán kdykoli po podepsání listiny.[80] Podobně parafy na jednotlivých stranách listiny značí, že strany nebyly vyměněny, a tak osvědčují integritu listiny, avšak samy o sobě neplní roli podpisu.[81]

Funkce ověřující integritu listiny souvisí s funkcí vyjadřující úplnost listiny. Podpis dle této funkce deklaruje úplný projev vůle a nikoliv pouze návrh, kterým strana nezamýšlí být vázána.[82]

Jednou z posledních funkcí podpisu je upozornění podepisující osoby na právní následky, které jsou s takovým jednání spojeny. Jak již bylo uvedeno, písemná forma právního úkonu je pávem vyžadována zejména u úkonů, které jsou pokládány za důležité. Podpis listiny na konci tak upozorňuje podepisující osobu, aby se více zabývala obsahem listiny, kterou podepisuje.[83]

---

[78] LABORDE, C. M. *Electronic Signatures in International Contracts*. Frankfurt am Main : Peter Lang, 2010. 28 s.

[79] Shodně psáno, avšak jinak vyslovováno.

[80] Což nelze brát bezvýhradně. Rozdílně k tomu např. Cohen v. Roche, 1 KB 169 (1927); Kilday v Schancupp 91 Conn 29 (1916); McNear v Petroleum Export Corp 280 P 684.

[81] LABORDE, C. M. *Electronic Signatures in International Contracts*. Frankfurt am Main : Peter Lang, 2010. 28 s.

[82] Německy nazýváno jako „Abchlußfunktion". *Christopher Kuner, Attorney-at-Law* [online]. c2005 [cit. 2011-11-16]. Written Signature Requirements and Electronic Authentication: A Comparative Perspective. Dostupné z WWW: <http://www.kuner.com/data/articles/signature_perspective.html>.

[83] LABORDE, C. M. *Electronic Signatures in International Contracts*. Frankfurt am Main : Peter Lang, 2010. 29 s. V německé literatuře označováno jako Warnfunktion. KUNER, Ch.; MIEDBRODT, A. *Christopher Kuner, Attorney-at-Law* [online]. c2005 [cit. 2011-11-16]. Written Signature Requirements and Electronic Authentication: A Comparative Perspective. Dostupné z WWW: <http://www.kuner.com/data/articles/signature_perspective.html>.

2.4 Elektronický podpis

Právní úprava elektronického podpisu je v českém právním řádu soustředěna v Zákoně. Další významné normy týkající se elektronického podpisu jsou obsaženy v ustanoveních § 2 odst. 3 a § 40 odst. 3 občanského zákoníku. První zmíněné ustanovení umožňovalo elektronické podepisování ještě před tím, než byl přijat Zákon, a pouze pokud bylo toto stranami dohodnuto. Druhé ustanovení dnes vytváří rámec pro elektronické podepisování písemných právních úkonů, když odkazuje na zvláštní právní předpis, který stanovuje konkrétní úpravu a kterým je Zákon.

Zákon je provádějícím předpisem směrnice Evropského parlamentu a Rady 1999/93/ES, o zásadách Společenství pro elektronické podpisy, ze dne 13. prosince 1999 (dále jen „Směrnice“). Směrnice členské státy zavazuje, aby zajistily, že elektronické podpisy založené na kvalifikovaných osvědčeních a vytvořené pomocí prostředků pro bezpečné vytváření podpisu budou splňovat právní požadavky na podpis ve vztahu k datům v elektronické podobě, stejně jako vlastnoruční podpisy splňují tyto požadavky ve vztahu k údajům vlastnoručně psaným nebo vytištěným na papíře, a dále, že budou připuštěny jako důkazy v soudním řízení.[84]

Dalším předpisem, který zasahuje do oblasti použití elektronických podpisů, je směrnice Evropského parlamentu a Rady č. 2000/31/ES, o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu, ze dne z 8. června 2000 (dále jen „Směrnice o elektronickém obchodu“). Členské státy musí zajistit, aby právní řád umožňoval uzavírání smluv elektronickou cestou.[85] Tím však není vyloučena možnost vyžadovat kvalifikovanou formu elektronického podpisu - což vyplývá z bodu 35 recitálu Směrnice o elektronickém obchodu. Směrnice o elektronickém obchodu v čl. 9 odst. 2 dává členským státům právo vyloučit uzavírání některých smluv v elektronické formě. Konkrétně se jedná o smlouvy zakládající nebo převádějící práva k nemovitostem s výjimkou práv z nájmů, smlouvy, při nichž se vyžaduje zásah orgánů veřejné moci nebo osob vykonávajících veřejnou moc, smlouvy o zajištění, které osoby uzavírají mimo svoji obchodní nebo profesní činnost, a smlouvy z oblasti rodinného a dědického práva. K těmto výjimkám dochází v českém právním

[84] Ustanovení článku 5 odst. 1 Směrnice.

[85] Ustanovení článku 9 odst. 1 Směrnice o elektronickém obchodu.

řádu zejména rozlišováním požadavku na formu podpisu - podpisu a vlastnoruční ho podpisu.

Zákon stejně jako Směrnice rozlišuje 4 základní druhy elektronického podpisu. Avšak na rozdíl od Směrnice je u Zákona vyzdvihována jeho technologická neutralita, když právní důsledky spojuje s jakýmkoliv elektronickým podpisem.[86] Vychází tak částečně z článku 5 odst. 2 Směrnice, který stanoví zákaz diskriminace elektronických podpisů pouze z důvodu, že:

- mají elektronickou podobu, nebo
- se nezakládají na kvalifikovaném osvědčení, nebo
- se nezakládají na kvalifikovaném osvědčení vydaném akreditovaným ověřovatelem, nebo
- nejsou vytvořeny prostředkem pro bezpečné vytváření podpisu.

Pro další výklad je nutné se stručně seznámit s jednotlivými formami elektronického podpisu tak, jak je stanovuje Zákon, a také s některými dalšími formami.

2.4.1 Formy elektronického podpisu

2.4.1.1 Prostý elektronický podpis

Legální definice elektronického podpisu na rozdíl od běžného podpisu v českém právním řádu nechybí. Je obsažena v ustanovení § 2 písm. a) Zákona, které říká, že jde o údaje:

- v elektronické podobě,
- které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a
- které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě.

Právní veřejnost dříve vedla diskuzi ohledně povahy jména připojeného za textem elektronické pošty a dalších podobných metod, které dle názoru některých odborníků byly považovány za elektronický podpis.[87] Jak bylo výše uvedeno, pokud se nejedná o podpis v případě jména připsaného psacím strojem, nelze analogicky uvažovat ani o jméně připsaném za textem elektronické pošty jako o prostém elektronickém podpisu.[88]

---

[86] HULMÁK, M. Elektronický právní styk. *Právní rozhledy*. 2005, 7, 229 s.

[87] MATEJKA, J.; CHUM, V. K právní úpravě elektronického podpisu. *Bulletin advokacie*. 2002, 3, 31 s.

[88] Stejný názor zastává HULMÁK, M. Elektronický právní styk. *Právní rozhledy*. 2005, 7, 231 s.

Tento nesoulad odstranil zákon č. 440/2004 Sb., který novelizoval Zákon, když připojil k definici elektronického podpisu požadavek „*jednoznačného*“ ověření.

Z praktického hlediska lze za prostý elektronický podpis považovat dle názoru autora této práce například běžně dohodnuté heslo ve smluvním vztahu (za předpokladu, že se ho třetí osoba nemá možnost dovědět) sloužící k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě. Takový požadavek může naplnit i jméno, ale pouze spolu s dalšími údaji, které nejsou třetím osobám veřejně přístupné, jelikož například jméno s datem narození není schopné jednoznačně identifikovat podepisující osobu, protože s takovými údaji může disponovat kterákoli osoba. Takový podpis by nenaplňoval zákonný požadavek jednoznačné identifikace.

Je možné uvažovat nejen o osobních údajích podepisující strany, ale o jakékoli frázi, která se sama o sobě běžně neužívá ve smluvních vztazích v místech obvyklých pro podpis. Nejvhodnější formou by byl patrně volně smyšlený bezvýznamový řetězec znaků, který by střídal více znakových řad (malých a velkých písmen, číslic, ostatních znaků). Prostý elektronický podpis v této formě by bylo možné dohodnout v písemné rámcové smlouvě, která by stanovovala pravidla pro další smlouvy a která by byla podepsána vlastnoručně nebo například některou z vyšších forem elektronického podpisu. Příklad této rámcové smlouvy je uveden v Příloze č. 1 této práce. Tento přístup byl s ohledem na ustanovení § 2 odst. 3 občanského zákoníku možný již před přijetím Zákona.

Podobně by tomu bylo v případě, kdy jedna ze smluvních stran osobně předala pro komunikaci svou adresu elektronické pošty. V tomto případě je patrně oslabena označovací funkce pro třetí osoby, ale pro samotné smluvní strany je dostatečně patrná již od samotného ověření identity osoby, a to díky osobnímu kontaktu obou stran a za předpokladu, že přístup k předaným schránkám elektronické pošty mají pouze smluvní strany. Důkazní funkce by v takovém případě také nebyla omezena pod únosnou míru. V tomto případě by bylo však nutné za textem zprávy znovu připojit vlastní adresu elektronické pošty, jelikož pouhé uvedení adresy odesílatele v hlavičce přijaté zprávy není možné posuzovat jako projevení vůle být vázán zprávou z důvodu automatizovaného připojení této informace ke každé zprávě elektronické pošty.[89] Opět

[89] Shodně k tomu i LENG, T. K. Have you signed your electronic contract? *Computer Law & Security Review*. 2011, 27, 79 s. a také rozhodnutí Rosenfeld v Zerneck 776 NYS2d 458. Tento názor lze vzhledem k dalším úvahám o vůli přijmout i pro český právní řád. Opačně McGuven v Simpson NSWSC 35 (2004).

se ale dostáváme k závěru, že charakteristickým prvkem podpisu rozhodně není naplnění všech základních funkcí podpisu v plném rozsahu.

Pokud bychom srovnali český právní řád se zahraničími, tak bychom došli ke zcela odlišným závěrům. Tyto rozpory jsou způsobeny zejména jinými legislativními přístupy zahraničních právních řádů, což vede k řadě problémů na poli mezinárodní kontraktace (k tomu více v podkapitole o legislativních přístupech).

V angloamerické právní kultuře je kladen důraz více na elektronický podpis jako součást projevu vůle být vázán úkonem než na formu elektronického podpisu. Proto je například za elektronický podpis považováno i prosté uvedení jména za textem elektronické pošty, což je analogické k angloamerickému pojetí psaného podpisu. Dokonce ani nezáleží, zda jméno bylo skutečně do zprávy dopsáno či bylo automaticky připojeno k textu. Podobně je tomu u tzv. „click-wrap" smluv, kde se pouze vyplní základní údaje v internetovém formuláři a poté se obvykle odešle potvrzení stisknutím tlačítka „Souhlasím" nebo „I accept". Důkazem mohou být i četná soudní rozhodnutí o tomto pojetí elektronického podpisu ve Velké Británii[90], Spojených státech amerických[91] a Singapuru[92].

2.4.1.2 Zaručený elektronický podpis

Zaručeným elektronickým podpisem se dle ustanovení § 2 písm. b) Zákona rozumí elektronický podpis, který splňuje následující požadavky:

- je jednoznačně spojen s podepisující osobou,
- umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
- byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
- je k datové zprávě připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.

Tento podpis na rozdíl od prostého elektronického podpisu poskytuje řadu záruk, které vyplývají ze zákonných požadavků. Jednou z těchto záruk je tzv. jednoznačnost,

[90] Především Hall v. Cognos Limited, Hull Industrial Tribunal Case No. 1803325/97.

[91] Shattuck v. Klotzbach, 14 Mass. L. Rptr. 360 (Mass. Super. Ct. 2001); Sea-Land Serv., Inc. v. Lozen Int'l, LLC., 285 F.3d 808 (9th Cir. 2002); Cloud Corp. v. Hasbro, Inc., 314 F.3d 289 (7th Cir. 2002); Roger Edwards, LLC. v. Fiddes & Son Ltd., 245 F. Supp. 2d 251 (D. Me. 2003); On Line Power Tech., Inc. v. Squared D Company, 2004 WL 1171405 (S.D.N.Y.).

[92] SM Integrated Transware Pte Ltd. v. Schenker Singapore (Pte) Ltd., [2005] SGHC 58.

která spočívá ve zvýšené ochraně příjemce datové zprávy ve vztahu k elektronickému podpisu, jelikož elektronický podpis je jednoznačně spojen s podepisující osobou. Dále se jedná o tzv. identifikaci a autentizaci, která umožňuje identifikovat podepsanou osobu ve vztahu k datové zprávě. Nakonec se jedná o možnost ověření integrity datové zprávy, která umožňuje rozpoznat jakékoli změny po podepsání datové zprávy.[93]

Tato forma elektronického podpisu však nepředstavuje ekvivalent ověřeného podpisu, jak nesprávně uvádí důvodová zpráva.[94] Lze tak dovodit i z výše uvedeného. Pokud by tato forma měla být rovna ověřenému podpisu, musel by tak stanovit zákonodárce. Dokonce lze tvrdit, že vlastnoruční podpis je vyšší formou než jakákoli z forem zaručeného podpisu.

S důvodovou zprávou lze částečně souhlasit, když tvrdí, že návrh zákona je zaměřen především na tuto formu podpisu[95], avšak nejen tato forma poskytuje dostatečnou právní platnost.[96] Tu poskytují všechny formy elektronického podpisu upravené Zákonem.

Důvodová zpráva dále vyzdvihuje technologickou neutralitu Zákona, když v rámci zaručeného podpisu se neváže pouze na technologii asymetrické kryptografie, ale umožnuje použití i dalších technologií (zejména těch biometrických, např. identifikace pomocí DNA, otisku prstu atd.).[97] Zde je ovšem nutné poznamenat, že elektronický podpis založený na těchto technologiích také využívá metody asymetrické kryptografie, avšak k tomuto tématu až dále.

Zejména v právních řádech angloamerického kultury se lze setkat také s označením digitální podpis, které označuje formy založené na asymetrické kryptografii.

2.4.1.2.1 Public Key Infrastructure

[93] Zvláštní část k § 2, Důvodová zpráva k návrhu zákona o elektronickém podpisu a o změně některých dalších zákonů. MATEJKA, J.; CHUM, V. K právní úpravě elektronického podpisu. Bulletin advokacie. 2002, 3, 31 s.

[94] Zvláštní část k § 2, Důvodová zpráva k návrhu zákona o elektronickém podpisu a o změně některých dalších zákonů.

[95] Tamtéž.

[96] MATEJKA, J.; CHUM, V. K právní úpravě elektronického podpisu. Bulletin advokacie. 2002, 3, 32 s.

[97] Zvláštní část k § 2, Důvodová zpráva k návrhu zákona o elektronickém podpisu a o změně některých dalších zákonů.

Zaručený elektronickým podpis funguje na základě tzv. asymetrické kryptografie využívající dvojici klíčů, které fungují pouze v páru a z nichž jeden je veřejně přístupný (označováno jako PKI – Public Key Infrastructure). Jeden klíč (tzv. soukromý) je výhradně v držení podepisující osoby a slouží k tvorbě samotného elektronického podpisu, který je unikátní pro každý podepisovaný elektronický dokument[98]. Takto vzniklý elektronický podpis může existovat pouze ve vazbě na podepisovaný dokument a je výsledkem složitého výpočtu z tzv. hashe dokumentu (čili kontrolního součtu souboru, který slouží jako zkrácené unikátní označení pro každý soubor). Druhý klíč (tzv. veřejný), který je přístupný veřejnosti, slouží k ověření, zda podepsaný dokument byl opravdu podepsán příslušným soukromým klíčem. [99]

Držitel soukromého klíče s ním musí zacházet s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití. V případě hrozícího nebezpečí zneužití soukromého klíče je povinen uvědomit poskytovatele certifikačních služeb, který vydal certifikát spojující soukromý klíč s podepisující osobou (revokace nebo také zneplatnění).[100] Další bezpečnostní pojistkou je nemožnost odvodit soukromý klíč z veřejného klíče.

Z PKI technologie tedy plyne řada výhod ve srovnání s vlastnoručním podpisem. Vlastnoručně podepsat lze jakoukoli i prázdnou listinu. V případě doplnění či změny textu se toto neprojeví na samotné podobě podpisu. Naproti tomu elektronický podpis je vždy závislý na konkrétním podepsaném dokumentu a nemůže existovat sám o sobě. Jakákoliv následná změna se tedy okamžitě projeví a elektronický podpis je vyhodnocen jako neplatný. S tím souvisí další výhoda, kdy vlastnoruční podpis je vyhodnocován na základě podobnosti s jiným podpisem případně obvyklým psaným projevem podepsané osoby, avšak vyhodnocení elektronického podpisu je výsledkem mimo jiné matematického výpočtu, který je nesrovnatelně přesnější. Lze tedy konstatovat, že podpis byl vytvořen za použití konkrétního soukromého klíče, což je

[98] Prakticky lze podepsat téměř každý elektronický soubor. Autor pro lepší názornost zvolil elektronický dokument, který bude patrně nejčastěji podepisován.

[99] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi*. Olomouc : ANAG, 2008. 30 s. PETERKA, J. *Báječný svět elektronického podpisu* [online]. 2. Vytváření elektronických podpisů. 2010 [cit. 2011-11-19]. Dostupné z WWW: <http://bajecnysvet.cz/obsah/2.php>.

[100] Ustanovení § 3 odst. 1 Zákona.

poslední výhodou, často označovanou jako nepopiratelnost.[101] Nepopiratelnost bývá často nesprávně označována jako vlastnost, na základě které lze říci, že dokument podepsala konkrétní osoba, na jejíž jméno byl vystaven certifikát, který spojuje danou osobu s konkrétním soukromým klíčem.[102] Dle názoru autora je tento výklad zcela chybný alespoň po právní stránce, jelikož nelze jednoznačně tvrdit, zda opravdu osoba uvedená na certifikátu reálně dokument podepsala. Lze však tvrdit, že podpis byl vytvořen pomocí dat pro vytváření elektronických podpisů osoby uvedené na certifikátu.[103] Nepopiratelnost je dále možné v intencích Zákona chápat jako vlastnost vyplývající z povinností vymezených v ustanovení § 3 Zákona a z odpovědnostních vztahů vzniklých z porušení těchto povinností.

Samotná existence dvojice klíčů nespojuje tyto klíče s konkrétní osobou. K tomu slouží tzv. certifikát. Certifikátem se dle Zákona rozumí „*datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování elektronických podpisů s podepisující osobou a umožňuje ověřit její identitu*“[104]. Certifikát tedy vystupuje jako prostředek ověření totožnosti podepsané osoby. Míra spolehlivosti tohoto ověření je závislá na důvěryhodnosti poskytovatele tohoto certifikátu, který v celé struktuře vystupuje jako garant ověření totožnosti. Míra spolehlivosti poskytovatele certifikačních služeb je navenek patrná především jeho certifikační politikou, která by měla být žadateli o certifikát známá předem[105]. Certifikační autorita se dále řídí dalšími dokumenty, které také vyjadřují míru spolehlivosti a které však nemusí být veřejné. Jedná se zejména o:

- certifikační prováděcí směrnice,
- celkovou bezpečnostní politiku,
- systémovou bezpečnostní politiku,
- plán zvládání krizových situací a plán obnovy.[106]

[101] PETERKA, J.; PODANÝ, J. Problematika elektronické podpisu v soudní praxi. *Právní rozhledy*. 2010, 19, 693 s.

[102] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi*. Olomouc : ANAG, 2008. 31 s.

[103] LEKKAS, D.; GRITZALIS, S.; MITROU, L. Withdrawing a declaration of will: Towards a framework for digital signature revocation. *Internet Research*. 2005, 4, 401 s.

[104] Ustanovení § 2 písm. k) Zákona.

[105] Viz ustanovení § 6 odst. 1 písm. f) Zákona.

[106] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi*. Olomouc : ANAG, 2008. 92 s.

Dále je míra spolehlivosti certifikační autority dána celkovou certifikační strukturou zavedenou v daném státě. V zásadě rozlišujeme soukromou certifikační strukturu, za kterou je odpovědná pouze soukromá společnost nebo neveřejný subjekt, a veřejnou strukturu, která je založena zákonem nebo jiným způsobem veřejnoprávní regulace. Kritériem tohoto členění není stanovení, kdo je vydavatelem certifikátů, ale určuje, kdo je oprávněn stanovit pravidla, dle kterých poskytovatel certifikačních služeb uskutečňuje svou činnost.[107] Dále se budeme blíže věnovat veřejné certifikační struktuře, pokud není uvedeno jinak.

Dvojici klíčů a certifikát pro zaručený elektronický podpis si může vygenerovat každý s využitím jednoduchého programu. Avšak takovýto certifikát může znít na jakékoli jméno a proto z definice elektronického podpisu uvedené v Zákoně ho nebude moci považovat za elektronický podpis, jelikož mu bude chybět jednoznačné ověření identity.

V tento okamžik nastávají dvě varianty, jak tento problém zhojit. Jednou je předání našeho veřejného klíče druhé smluvní straně osobně, čímž došlo k jednoznačnému ověření totožnosti. V praxi si lze použití zaručeného elektronického představit například obdobně jako v případě prostého elektronického podpisu, a to na základě analogické dohody dle Přílohy č. 1, kde místo fráze v roli podpisu bude vystupovat zaručený elektronický podpis poskytnutý každou ze smluvních stran. V rámcové smlouvě by byl definován identifikačním číslem či jiným vhodným identifikátorem podpisu.

Druhou možností je přenést ověření identity na třetí dostatečně důvěryhodnou osobu[108], která to provede tak, že ke konkrétnímu páru klíčů vydá pro podepisující osobu certifikát. Touto osobou je právě poskytovatel certifikačních služeb (dále též jako „certifikační autorita“). Pravost, důvěryhodnost a vydavatel certifikátu podepisující osoby jsou poté osvědčeni tak, že poskytovatel certifikát podepíše svým podpisem se svým vlastním certifikátem (kořenový certifikát). Certifikát poskytovatele je vydáván na základě příslušné legislativy buď přímo poskytovatelem (selfsigned certifikát), nebo orgánem veřejné moci, který působí v roli nejvyšší certifikační autority.[109]

---

[107] KOENIG, W. Approaches of Digital Signature Legislation. In LAMERSDORF, W.; MERZ, M. *Trends in Distributed Systems for Electronic Commerce, International IFIP/GI Working Conference TREC'98 Hamburg, Germany, June 3–5, 1998 Proceedings*. Heidelberg : Springer, 2003. s. 41.

[108] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi*. Olomouc : ANAG, 2008. 70 s.

[109] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi*. Olomouc : ANAG, 2008. 45-46 s.

Podobně by bylo možné uvažovat o případě, že třetí důvěryhodná osoba ověří údaje obou stran na certifikátech, který si sami vytvořily ke svým klíčům a skrze tuto osobu si zašlou své veřejné klíče obsahující ověřené certifikáty.

V závislosti na povaze poskytovatelů certifikačních služeb lze rozlišovat další odvozené formy zaručeného elektronického podpisu.

2.4.1.3 Zaručený elektronický podpis založený na kvalifikovaném certifikátu

Zaručený elektronický podpis založený na kvalifikovaném certifikátu není v zákoně explicitně definován. Existence však vyplývá kromě zásady smluvní svobody i z řady ustanovení Zákona.

Tato forma, jak napovídá název, naplňuje všechny znaky zaručeného elektronického podpisu. Navíc je však přidán kvalifikovaný certifikát.

Kvalifikovaným certifikátem je certifikát, který má náležitosti podle ustanovení § 12 Zákona a byl vydán kvalifikovaným poskytovatelem certifikačních služeb, který splňuje podmínky stanovené v ustanovení § 6 Zákona. Z této definice vyplývá, že pojem kvalifikovaného certifikátu je nerozlučně spjat s pojmy certifikát a poskytovatel certifikačních služeb, který vydává certifikáty, příp. kvalifikované certifikáty, pokud splňuje Zákonem stanovené podmínky, a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy. Certifikátům se budeme věnovat dále.

2.4.1.4 Zaručený elektronický podpis založený na kvalifikovaném certifikátu od akreditovaného poskytovatele certifikačních služeb

Zaručený elektronický podpis založený na kvalifikovaném certifikátu od akreditovaného poskytovatele certifikačních služeb (dále jen „uznávaný elektronický podpis“) se od předešlé formy liší pouze v certifikační autoritě, které stejně jako v předchozím případě vydává kvalifikované certifikáty, avšak v tomto případě byla certifikační autoritě udělena akreditace Ministerstvem vnitra. Pro udělení akreditace musí certifikační autorita splňovat podmínky určené ustanovením § 10 Zákona.

Uznávaný elektronický podpis je považován za jednu z nejbezpečnějších forem elektronického podpisu, proto je také možné ho používat dle ustanovení § 11 Zákona v oblasti orgánů veřejné moci, přičemž totéž platí i pro výkon veřejné moci vůči fyzickým a právnickým osobám.

Bezpečnost uznávaného elektronického podpisu je dána především zvýšenou možností identifikace podepsané osoby prostřednictvím kvalifikovaného certifikátu.

Důvěra v tento certifikát je dána zejména důvěrou v samotnou certifikační autoritu, která certifikát vydala, a dále pak spočívá v akreditaci a dozoru, který vykonává Ministerstvo vnitra.[110]

Český právní řád ponechává na certifikačních autoritách, aby si vydávaly své kořenové certifikáty (selfsigned certifikáty) a určovaly svou hierarchii.[111] Oproti tomu Německá úprava deleguje pravomoc kořenové certifikační autority na Spolkovou síťovou agenturu, která spadá pod Spolkové ministerstvo hospodářství a technologie.[112] Taktéž například slovenským zákon o elektronickém podpisu svěřuje tuto kompetenci NBÚ SR.[113] V tomto ohledu je možné vnímat německý nebo slovenský dvoustupňový systém jako dalšího garanta bezpečnosti uznávaných elektronických podpisů, jelikož nejvyšším poskytovatelem certifikátů je orgán veřejné moci.

2.4.1.5 Zaručený elektronický podpis založený na kvalifikovaném certifikátu a vytvořený pomocí prostředku pro bezpečné vytváření podpisu

Tato forma elektronického podpisu není výslovně upravena Zákonem, avšak lze dovodit, že je proveditelná pro každou z výše uvedených forem zaručeného elektronického podpisu. Rozdíl spočívá v použití prostředku pro bezpečné vytváření podpisu. Požadavky na tento prostředek jsou uvedeny v ustanovení § 17 Zákona.

Zákon tuto formu považuje z hlediska důvěry a dokazování za nejdokonalejší, když v ustanovení § 3 odst. 2 Zákona deklaruje, že použití zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu a vytvořeného pomocí prostředku pro bezpečné vytváření podpisu umožňuje ověřit, že datovou zprávu podepsala osoba

---

[110] V současné době jsou akreditovanými certifikačními autoritami První certifikační autorita, a. s., Česká pošta, s. p., a eIdentity a. s.

[111] Více k hierarchii certifikátů v PETERKA, J. *Báječný svět elektronického podpisu* [online]. 2010 [cit. 2011-11-19]. 5.4.2.3 Systémové úložiště certifikátů v MS Windows. Dostupné z WWW: <http://bajecnysvet.cz/obsah/5x4x2x3.php>.

[112] *Bundesnetzagentur* [online]. c2011 [cit. 2011-11-19]. Über die Agentur. Dostupné z WWW: <http://www.bundesnetzagentur.de/cln_1912/DE/DieBundesnetzagentur/UeberDieAgentur/UeberDieAgentur_node.html>. REBEL, T. F.; DARGE, O.; KOENIG, W. Approaches of Digital Signature Legislation. In LAMERSDORF, W.; MERZ, M. *Trends in Distributed Systems for Electronic Commerce, International IFIP/GI Working Conference TREC'98 Hamburg, Germany, June 3–5, 1998 Proceedings*. Heidelberg : Springer, 2003. s. 44.

[113] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi*. Olomouc : ANAG, 2008. 44-45 s.

uvedená na tomto kvalifikovaném certifikátu. Domněnka stanovená v tomto ustanovení však postrádá jakýkoli normativní charakter.

2.4.1.6 Rozšířené elektronické podpisy

Rozšířené elektronické podpisy (AdES - Advanced Electronic Signatures) jsou další formou založenou na zaručeném elektronickém podpisu. Jedná se o celou rodinu podpisů, jejichž náležitosti jsou stanoveny a odlišeny technickými standardy. Tato forma podpisu rozpracovává koncept LTV (Long Term Validation), který má za cíl odstranit problém s dlouhověkostí elektronických podpisů, resp. jejich certifikátů.

Celá tato technologie je založena na přibalení jak samotného elektronického podpisu k dokumentu, tak i všech certifikátů (i těch nadřazených – např. kořenové certifikáty certifikační autority), dále časová razítka[114] a všechny jejich certifikáty a potřebné CRL seznamy[115]. Výsledný balík je nutné dostatečně „zafixovat“ tak, aby

[114] Časové razítko je po technické stránce velmi podobné elektronickému podpisu, avšak s rozdílem, že obsahuje údaj o čase, na který je možné se spolehnout (u tzv. kvalifikovaného časového razítka, kde poskytovatel odpovídá za správnost časového údaje). Časové razítko vzniká tak, že poskytovatel časových razítek „podepíše“, resp. orazítkuje, zaslaný hash dokumentu s uvedením garantovaného času. I když je razítko technicky podobné elektronickému podpisu, tak nepředstavuje žádné právně relevantní jednání. Jedná se pouze o potvrzení, že samotný dokument existoval před tím, než časové razítko vzniklo. PETERKA, J. Proč elektronické podpisy nejsou věčné? e*Archiv.cz* [online]. 10.5.2010 [cit. 2012-02-12]. Dostupné z: <http://www.earchiv.cz/b10/b0510001.php3>.

[115] CRL (Certificate Revocation List) je jedním ze způsobů zveřejňování zneplatněných certifikátů. Certifikační autorita vydává aktualizované seznamy jejích zneplatněných certifikátů, ovšem jednotlivé záznamy bývají z praktických důvodů po určité době odstraněny a nahrazeny jinými. Záznam je poté přesunut do starších verzí CRL seznamů, které má certifikační autorita povinnost archivovat po dobu deseti let. Tyto jsou většinou veřejně přístupné. Problém je však v tom, že nejsou stanoveny standardní postupy, kde a jak se mají tyto starší seznamy zveřejňovat, a každá certifikační autorita používá jiný způsob, na základě čehož nejsou běžné programy pro ověření platnosti podpisu schopny tyto informace nalézt. Druhou metodou, která se však u nás nepoužívá, je využití protokolu OCSP (Online Certificate Status Protocol). Prostřednictvím protokolu použitého v této metodě se program, který ověřuje platnost podpisu, interaktivně zeptá certifikační autority na případnou revokaci konkrétního certifikátu a obratem dostane odpověď. Další nevýhodou CRL seznamů je jejich zveřejňování až po určité době, kdy poskytovateli dojde informace o zneplatnění certifikátu. PETERKA, J. Datové schránky: když už ani časové razítko nepomůže. e*Archiv.cz* [online]. 4.10.2010 [cit. 2012-02-12]. Dostupné z: <http://www.earchiv.cz/ b10/b1004001.php3>.

později nebylo možné informace nahradit padělanými certifikáty, razítky nebo CRL seznamy. [116]

2.4.1.7 Biometrické podpisy

O biometrických podpisech lze především mluvit v rámci zaručených elektronických podpisů, jelikož ve své technologicky nejdokonalejší podobě používají také prvků asymetrické kryptografie. Jsou založené na využití určitých fyziologických nebo behaviorálních vlastností jednotlivce, které jsou pro něj unikátní. Biometrické metody je možné rozdělit na anatomicky-fyziologické (využívající konkrétních charakteristik jednotlivce – tvář, oční sítnice, oční duhovka, otisky prstů, DNA) a behaviorální (využívající určité dynamiky chování jednotlivce, např. mluvený projev – hlasitost, rychlost mluveného projevu, hloubka hlasu; písemný projev – rychlost psaní, náklon pera, míra podobnosti podpisu, dynamika úderů na klávesnici).[117] Biometrie zde slouží pro ověření totožnosti podepisované osoby, proto je nutné, aby určitý důvěryhodný třetí subjekt garantoval toto ověření. Jednou z nevýhod biometrických podpisů je právě skutečnost, že třetí subjekt musí zpracovávat tato důvěrná data, která pochopitelně mohou být zneužita.

Po ověření shodnosti vložených biometrických dat s daty uloženými u ověřovatele je nutné k dokumentu dostatečně pevně připojit biometrický vstup nebo jiná data osvědčující, že byl dokument podepsán. Zafixování dat se provádí opět prostřednictvím asymetrické kryptografie, což může vést k závěru, že využití biometrických metod může být nadbytečné vzhledem k ostatním formám elektronického podpisu dostupných v současnosti. Samozřejmě by bylo možné určité druhy biometrických podpisů vložit přímo do dokumentu, ale to by znamenalo, že podpis by mohl existovat sám o sobě a byl by tedy snadno zneužitelný jednoduchým odejmutím a následným přidáním do jiného dokumentu. Také by nebylo již možné

[116] PETERKA, J. Elektronický podpis na rozcestí. e*Archiv.cz* [online]. 6.6.2011 [cit. 2012-02-12]. Dostupné z: < http://www.earchiv.cz/b11/b0606001.php3>.

[117] RAK, R.; MATYÁŠ, V.; ŘÍHA, Z. a kol. *Biometrie a identita člověka.* Praha : Grada Publishing a.s., 2008. 106 s. KAILASH, N. G.; KAMALESH N. A.; PRATEEK A. A. *Digital Signature: Network Security Practices.* New Delhi : Prentice-Hall of India Pvt. Ltd., 2005. 39 s.

mluvit o jedné ze podforem zaručeného elektronického podpisu, jelikož by neplnil Zákonem stanovené podmínky pro tuto formu.[118]

Další nevýhody mohou vyplývat zejména z pořizovacích nákladů na vstupní zařízení pro biometrická data a také z fyziologických změn souvisejících zejména se stárnutím podepisující osoby, což bude hlavně patrné u behaviorálních biometrických metod.

Pro další rozšiřování použití biometrických podpisů bude nutné zjistit, zda výhody spočívající ve zvýšené schopnosti ověřit identitu podepisující osoby, v menší možnosti zneužití podpisu spolu s vyšší mírou jednoznačného propojením prostředku pro vytváření elektronického podpisu s podepisující osobou skutečně převáží výše uvedené nevýhody.

2.4.2 Legislativní přístupy

2.4.2.1 Obecný rámec

Koncem devadesátých let dvacátého století a na počátku nového milénia byly v mnoha zemích přijímány zákony upravující oblast elektronického podpisu. V rámci jednotlivých právních řádů bylo možné sledovat pouze několik hlavních záměrů, které vedly k přijetí těchto zákonů, byly jimi zejména:

- umožnění dalšího vývoje obchodu pomocí prostředků spolehlivé elektronické komunikace,
- snížení výskytu podvržených elektronických podpisů a podvodů v oblasti e-commerce,
- upevnění důvěry veřejnosti v e-commerce a elektronické podpisy,
- umožnění nástupu e-governmentu. [119]

I když jsou tyto záměry stát od státu téměř totožné, lze při jejich naplňování spatřit odlišné přístupy. Brzo bylo jasné, že pro takový nástroj mezinárodní komunikace, jakým je internet, je existence divergentní legislativy stejně nebezpečná jako její absence.[120] Zatímco v rámci elektronických transakcí je vliv hranic

[118] PETERKA, J. Elektronický podpis na rozcestí. e*Archiv.cz* [online]. 6.6.2011 [cit. 2012-02-12]. Dostupné z: < http://www.earchiv.cz/b11/b0606001.php3>.

[119] KAILASH, N. G.; KAMALESH N. A.; PRATEEK A. A. *Digital Signature: Network Security Practices.* New Delhi : Prentice-Hall of India Pvt. Ltd., 2005. 39 s.

[120] LINCOLN, A. Electronic Signature Laws and the Need for Uniformity in the Global Market. *The Journal of Small and Emerging Business Law.* 2004, 8, 79-84 s.

jednotlivých států rozostřen, tak pro náležitosti elektronického podpisu jsou určující především vnitrostátní právní předpisy. Opět vyvstává téma platnosti elektronického podpisu, nyní již nikoliv na domácí scéně, ale spíše na té mezinárodní. Otázkou je tak, zda elektronický podpis splňující požadavky v jednom státě za něj bude uznán i v jiném.[121] Rozdílnost, s jakou se chopily jednotlivé státy naplnění výše uvedených záměrů, tak vedla k právní nejistotě mezinárodních elektronických obchodů, což je možné označit za nesystémové a kontraproduktivní řešení vzhledem k tomu, že nová legislativa měla přispět k usnadnění elektronických obchodů.

V důsledku těchto rozporů se objevila druhá vlna legislativních snah, tentokráte na nadnárodní úrovni ve snaze harmonizovat jednotlivé právní úpravy. Jelikož nedostatek v jednotnosti právních úprav elektronického podpisu bránil rozvoji mezinárodního obchodu, ujal se jako první tohoto úkolu UNCITRAL a vydal dva vzorové zákony UNCITRAL Model Law on Electronic Commerce (1996) a UNCITRAL Model Law on Electronic Signature (2001). Další pokusy o harmonizaci můžeme sledovat v rámci Evropské unie spolu s přijetím výše uvedených směrnic a v rámci Spojených států amerických spolu s modelovým zákonem UETA[122] a federálním zákonem E-SIGN[123]. UETA a E-SIGN si jsou velmi podobné a do značné míry se překrývají. Jelikož americký kongres si nebyl jistý, kdy budou státy ochotny přijmout modelový zákon UETA, proto byl schválen i zákon E-SIGN, který přímo stanovuje platnost elektronické kontraktace, avšak mnohem obecněji. Dále lze připomenout dokument Mezinárodní obchodní komory (ICC) nazvaný General Usage for International Digitally Ensured Commerce (GUIDEC), který je spíše souhrnem informací a doporučení pro jednotlivé smluvní strany v elektronickém obchodním styku.

[121] LABORDE, C. M. *Electronic Signatures in International Contracts*. Frankfurt am Main : Peter Lang, 2010. 49 s.

[122] Uniform Electronic Transactions Act, 1999 (USA).

[123] Electronic Signatures in Global and National Commerce Act, 2000 (USA).

2.4.2.2 Rozdílné přístupy

Nejčastěji uváděným hlediskem pro členění legislativních přístupů je otevřenost jednotlivých právních řádů k uznávání rozdílných technologií uplatněných v elektronickém podpisu.[124]

2.4.2.2.1 Preskriptivní přístup

Tento přístup je znám také jako mandatorní nebo přístup digitálního podpisu. Definuje pouze elektronické podpisy založené na PKI a také pouze jim přiznává právní účinky. Takový podpis je považován za protějšek vlastnoručního podpisu. Preskriptivní přístup byl uplatněn zejména u prvních států přijímajících legislativu elektronických podpisů.[125] Jeho příkladem může být zákon amerického státu Utah[126] nebo německý zákon o elektronickém podpisu[127].

2.4.2.2.2 Minimalistický přístup

Naproti tomu minimalistický přístup rozeznává všechny formy elektronických podpisů.[128] Tento způsob regulace je velmi flexibilní a koncept elektronického podpisu je pojat široce. Každá forma elektronického podpisu zde nese stejné právní účinky jako vlastnoruční podpis.[129] Především v zemích angloamerické právní kultury je důraz kladen spíše na elektronický podpis jako součást projevu vůle než na jeho formu. Tento

---

[124] SMEDINGHOFF, T. J.; BRO, R. H. *FindLaw* [online]. 1999 [cit. 2011-10-21]. Electronic Signature Legislation. Dostupné z WWW: <http://library.findlaw.com/1999/Jan/1/241481.html>. SCHELLEKENS, M. *Electronic Signatures: Authentication Technology from a Legal Perspective. Information technology & law series.* Haag : T.M.C. Asser Press, 2004. 57 s.

[125] Tamtéž. Dále také LABORDE, C. M. *Electronic Signatures in International Contracts*. Frankfurt am Main : Peter Lang, 2010. 51 s.

[126] Digital Signature Act, 1995 (Utah).

[127] Gesetz über Rahmenbedingungen für elektronische Signaturen (Spolková republika Německo).

[128] SMEDINGHOFF, T. J.; BRO, R. H. *FindLaw* [online]. 1999 [cit. 2011-10-21]. Electronic Signature Legislation. Dostupné z WWW: <http://library.findlaw.com/1999/Jan/1/241481.html>. SCHELLEKENS, M. *Electronic Signatures: Authentication Technology from a Legal Perspective. Information technology & law series.* Haag : T.M.C. Asser Press, 2004. 56-57 s.

[129] LABORDE, C. M. *Electronic Signatures in International Contracts*. Frankfurt am Main : Peter Lang, 2010. 51 s.

legislativní přístup je zastáván zejména zákony UETA a E-SIGN a dále také v Kanadě[130], Austrálii[131] a do jisté míry i ve Velké Británii[132].

2.4.2.2.3 Hybridní přístup

Hybridní nebo dvoustupňový přístup je tak označován, protože kombinuje prvky obou předchozích.[133] Jako ekvivalent vlastnoručního podpisu je zde považován zaručený elektronický podpis, ale na druhou stranu tento přístup přiznává právní účinky i ostatním formám elektronických podpisů.[134] Zaručený elektronický podpis však v tomto případě není svázán čistě s asymetrickou kryptografií.

Za příklad nám mohou posloužit modelové zákony UNCITRAL, Směrnice a také třeba singapurský zákon[135].

Český právní řád se z výše uvedeného dělení spíše vymyká tím, že rozlišuje podpis a vlastnoruční podpis, jak je to naznačeno výše. Právní účinky poskytuje zásadně všem formám elektronického podpisu, avšak elektronicky podepsat lze pouze úkony, které nevyžadují jednu z vyšších forem podpisu (vlastnoruční nebo ověřený podpis).

Podobným příkladem vybočujícím z nastíněného členění může být argentinský zákon o elektronickém podpisu[136], který opět přiznává právní účinky každé z forem elektronického podpisu, avšak preferuje zaručený elektronický podpis založený pouze na PKI (digitální podpis) jako ekvivalent vlastnoručního podpisu.[137]

---

[130] The Uniform Electronic Commerce Act, 1999 (Kanada).

[131] Electronic Transactions Act, 1999, c. 2 (Austrálie).

[132] Electronic Communications Act, 2000 (Velká Británie).

[133] SCHELLEKENS, M. *Electronic Signatures: Authentication Technology from a Legal Perspective. Information technology & law series.* Haag : T.M.C. Asser Press, 2004. 57 s. SMEDINGHOFF, T. J.; BRO, R. H. *FindLaw* [online]. 1999 [cit. 2011-10-21]. Electronic Signature Legislation. Dostupné z WWW: <http://library.findlaw.com/1999/Jan/1/241481.html>.

[134] LABORDE, C. M. *Electronic Signatures in International Contracts*. Frankfurt am Main : Peter Lang, 2010. 52 s.

[135] Electronic Transactions Act, 1998 (Republika Singapur).

[136] Ley De Firma Digital. No. 25.506 (Argentinská republika).

[137] MASON, S. Electronic Signatures in Practice. *Jounal of High Technology Law*. 2006, 2, 151-152s.

2.5 Mechanické prostředky

Podpis písemného právního úkonu může být dle ustanovení § 40 odst. 3 občanského zákoníku nahrazen mechanickými prostředky v případech, kdy je to obvyklé.

Mechanickými prostředky můžeme rozumět například razítko, faksimile nebo reprodukci podpisu.[138] Tento výčet je demonstrativní, jelikož zejména mechanických prostředků sloužících k nahrazení elektronického podpisu může být nepřeberné množství. Jako prostředek nahrazení elektronické podpisu bychom mohli uvést zejména uvedení jména za textem dokumentu, přidání naskenovaného vlastnoručního podpisu, potvrzení click-wrap smlouvy nebo za určitých podmínek elektronickou značku.

Obvyklost případu je nutno posuzovat objektivně vzhledem k charakteru právního jednání a k zavedené praxi stran, nikoliv vzhledem k užitému prostředku komunikace.[139] Proto jako prostředek nahrazení podpisu nemůže sloužit uvedení jména s odkazem, že takto běžně dochází k nahrazení elektronického podpisu v případě elektronické pošty. Obvyklost tak zakládá například obchodní zvyklost mezi dvěma smluvními stranami, která byla prvně založena rámcovou dohodou pro použití konkrétní formy elektronického podpisu při uzavírání dílčích kontraktů. V rámci této dohody by se samozřejmě jednalo stále o elektronický podpis, ale pokud by docházelo k uzavírání dalších kontraktů nad rámec rámcové dohody, jednalo by se již o mechanický prostředek nahrazení elektronického podpisu.

[138] ŠVESTKA, J.; SPÁČIL, J.; ŠKÁROVÁ, M.; HULMÁK, M. a kolektiv. *Občanský zákoník I, II.* 2. vydání. Praha : Nakladatelství C. H. Beck, 2009. 365 s. FIALA, J.; KINDL, M. a kolektiv. *Občanský zákoník. Komentář.* Praha : Wolters Kluwer ČR, 2009. 247 s.

[139] FIALA, J.; KINDL, M. a kolektiv. *Občanský zákoník. Komentář.* Praha : Wolters Kluwer ČR, 2009. 247 s.

3. Vliv elektronického podpisu na některé náležitosti právního úkonu

Jak bylo výše naznačeno, podpis je jednou z nezbytných náležitostí písemných právních úkonů. Jako součást písemného právního úkonu může být právně relevantní i při posuzování jiných náležitostí právních úkonů, zejména nositele vůle, projevu vůle, vůle samotné a existence právní normy. V rámci těchto témat je také nutné posoudit problematiku platnosti samotného podpisu.

3.1 Určení a vlastnosti nositele vůle

3.1.1 Způsobilost k právním úkonům

Předpokladem platnosti právního úkonu je, aby jej učinila osoba způsobilá k právním úkonům a nejednala v duševní poruše, která by ji činila k tomuto právnímu úkonu neschopnou.[140]

Způsobilost fyzické osoby vlastními úkony nabývat práv a povinností, resp. působit jiné právní následky, vzniká postupně podle stavu její psychické vyspělosti. V plném rozsahu vzniká až dosažením zletilosti. Nezletilí mají vzhledem k ustanovení § 9 občanského zákoníku způsobilost jen k takovým právním úkonům, které jsou svou povahou přiměřené rozumové a volní vyspělosti odpovídající jejich věku. Fyzická osoba může být způsobilosti k právním úkonům zbavena nebo jí může být omezena. Rozsah omezení způsobilosti je stanoven jednak zákonem (v případě nezletilých nebo u právního jednání v důsledku duševní poruchy) a jednak v rozhodnutí soudu, kterým se způsobilost fyzické osoby omezuje.[141] Způsobilost právnické osoby může být omezena pouze zákonem.[142]

Charakterem jde tedy o psychickou způsobilost rozpoznávací a určovací, tj. způsobilost rozpoznat charakter vlastního jednání a adekvátnost ve vztahu k zamýšlenému výsledku a také způsobilost své chování určit (ovládnout) podle tohoto poznání. [143]

Způsobilost k právním úkonům není omezena ani nijak závislá na skutečnosti, že k jednání dochází prostřednictvím internetu či jiným způsobem za využití elektronických prostředků. Použití elektronického podpisu však má určitá specifika,

[140] Ustanovení § 38 občanského zákoníku.

[141] Ustanovení § 9 a § 10 občanského zákoníku.

[142] Ustanovení § 19a občanského zákoníku.

[143] ŠVESTKA, J.; DVOŘÁK, J. *Občanské právo hmotné 1*. Praha : Wolters Kluwer Česká republika, 2009. 162 s.

která vyplývají zejména z faktu, že právní úkony jsou většinou činěny distančním způsobem. Nevýhodou při uzavírání smluv tedy může být právní nejistota ohledně druhé smluvní strany a platnosti právního úkonu v důsledku omezení způsobilosti druhé strany. Chování druhé strany může být určitým vodítkem pro rozpoznání omezené způsobilosti nebo jednání v duševní poruše. Jednající strana tak nemá možnost předejít případným škodám vzniklým z neplatnosti smlouvy. V úvahu také přichází prevenční povinnost předcházení škodám. V případném pozdějším sporu by se mohlo stát problematickým například i dokazování krátkodobé přechodné duševní poruchy.

Výše uvedené nevýhody byly patrně příčinou, proč zákonodárce stanovil omezení nebo zbavení způsobilosti jako důvod k zneplatnění kvalifikovaného certifikátu kvalifikovaným poskytovatele certifikačních služeb dle ustanovení § 6a odst. 4 Zákona. Vyvstává tak otázka, jak hodnotit právní úkon učiněný osobou s omezenou způsobilostí opatřený kvalifikovaným certifikátem. V zásadě přicházejí v úvahu dvě situace. Pokud se omezení způsobilosti jednající osoby vztahovalo na učiněný úkon, je tento úkon v souladu s ustanovením § 38 občanského zákoníku absolutně neplatný. Pokud by se však omezení způsobilosti nevztahovalo na učiněný právní úkon, byl by tento úkon jednoznačně platný a to i za předpokladu, že by byl certifikát elektronického podpisu zneplatněn až později.

Z ustanovení § 6a odst. 4 Zákona je možné dovodit, že by kvalifikovaný certifikát nebyl vydán osobě s omezenou způsobilostí, resp. bez způsobilosti, i když tento záměr není výslovně v Zákoně uveden. Platně uzavřít smlouvu o poskytování certifikačních služeb, na základě které je vydáván kvalifikovaný certifikát, nemůže tedy osoba s jakkoli omezenou způsobilostí, i když by se omezení nevztahovalo na uzavření takové smlouvy. Tyto osoby však nejsou omezeny v opatřování svých písemných právních úkonů ostatními formami elektronických podpisů a platnost těchto úkonů bude posuzována podle obecných ustanovení občanského zákoníku.

3.1.2 Specifika přičítání projevu vůle

Implicitním předpokladem platnosti právního úkonu je, že písemný projev vůle lze přičíst konkrétní osobě.[144] Patrně tak vyplývá i z požadavku na určitost právního úkonu. V písemných právních úkonech je pravidlem, že subjekt právního úkonu v něm bývá identifikován. K identifikaci fyzických osob se běžně používá její jméno a

[144] ČERMÁK, K. Elektronický podpis - pohled soukromoprávní. *Bulletin advokacie*. 2002, 11, 69 s.

příjmení a případně také další údaje jako rodné číslo, datum narození nebo adresa trvalého pobytu. Ustanovení § 13a obchodního zákoníku nám poskytuje určitý demonstrativní výčet možných identifikačních údajů podnikatelů. Jedná se o firmu, jméno nebo název, sídlo nebo místo podnikání a identifikační číslo osoby, u osob zapsaných v obchodním rejstříku nebo v jiné evidenci také údaj o tomto zápise. Tyto údaje je podnikatel povinen uvádět na všech objednávkách, obchodních dopisech, fakturách, smlouvách a v rámci informací zpřístupňovaných veřejnosti prostřednictvím internetu.

V internetovém prostředí nebývá pravidlem používání identifikačních údajů z reálného světa. Fyzické osoby často používají smyšlená jména a právnické osoby jiná označení než svou obchodní firmu, jméno či název. Takové identifikační údaje lze označit jako „digitální identitu“. Jejím specifikem je, že v tak svobodném a anonymním médiu jako je internet, nemusí vždy odpovídat identitě z reálného světa, jelikož podobu digitální identity si určuje subjekt práva sám. Digitální identita je charakteristická zejména v prostředí internetu, kde dochází k distanční komunikaci, a může být tvořena různými identifikátory jako například smyšlené nebo skutečné jméno, IP adresa, doménové jméno, adresa elektronické pošty atd. Subjekt práva má však ve většině případů několik digitálních identit, které mezi sebou nemusí být nikterak provázány.

Z výše uvedeného plyne, že digitální identita nemusí mít kvalitativně stejnou povahu jako ta reálná. Právní jednání se současným využitím elektronických prostředků, zejména elektronického podpisu, však může probíhat za fyzické přítomnosti osob, mezi kterými komunikace probíhá. V takovém případě je problém provázanosti digitální identity a té reálné vyřešen, jelikož dochází k jednoznačnému ověření totožnosti. Jak ale vyřešit tento konflikt v internetovém prostředí?

V takovéto situaci je nutné, aby právo reagovalo na pokračující růst elektronizace a zvyšující počet elektronických kontraktů. Pokud nechce rezignovat na využití výhod elektronického světa, přicházejí v úvahu dvě cesty, jak se vypořádat s digitální identitou.

První variantou je přiznání těmto digitálním identitám určitý stupeň subjektivity a způsobilosti k právním úkonům. Tato varianta je zatím spíše určitou futuristickou představou, která dle názoru autora dříve nebo později bude muset přijít v souvislosti s rozvojem umělé inteligence. Pokud si představíme určité inteligentní systémy, jejichž cílem může být například doplňování stavu zásob ve skladech nebo celé řízení provozu, bude jejich jednání (logicky zatím uskutečnitelné pouze distančně, proto jednáme pouze

o digitální identitě) zprvu přičítáno reálné fyzické nebo právnické osobě, jejímž jménem by tento systém jednal. Avšak s dalším rozvojem umělé inteligence by mohla vyvstat potřeba uznat takovou inteligenci jako samostatný subjekt práva (např. určitý druh právnické osoby), který by kompletně spravoval majetek svěřený mu jiným reálným subjektem.

Pokud se vrátíme do současnosti, tak druhým způsobem řešení problematiky digitální identity je určitým prostředkem provázat digitální identitu s tou reálnou. I když bychom nalezli zejména dnes řadu odpůrců regulace internetu, jejichž cílem je uchování svobody a anonymity tohoto média (zejména v souvislosti s Obchodní dohodou proti padělatelství – ACTA), vývoj k regulaci internetu jednoznačně směřuje a jednou z prvních otázek bude pravděpodobně právě provázanost digitální a skutečné identity.

Prostředkem pro toto provázání je již dnes elektronický podpis, pro který je jako náležitost stanoven požadavek jednoznačného ověření identity. Jak k tomuto provázání dochází, jsme si naznačili výše. Pro připomenutí v rámci prostých elektronických podpisů k tomu může dojít určitým jednáním mezi podepisující osobou a adresáty úkony (smluvní ujednání, osobní kontakt atd.) a v rámci zaručených elektronických podpisů je garantem určitý třetí subjekt – poskytovatel certifikačních služeb, který totožnost ověří a na základě ověření vydá certifikát, který je spjat s oběma klíči a který dokládá propojení digitální a skutečné identity. Zůstává otázkou, zda i do budoucna u nás tímto garantem zůstanou soukromé subjekty, nebo si tuto výsadu přivlastní stát, což by bylo logické řešení v případě rostoucí potřeby spolehnout se na toto ověření identity. K tomuto vývoji směruje i postupné zavádění e-governmentu[145], který v dalších fázích bude mít i řadu přeshraničních funkcí[146]. V rámci e-governmentu je důkazem zavádění elektronických občanských průkazů s možností nahrát na ně elektronický podpis či elektronických pasů.

Tyto nástroje prostupně spojují digitální a skutečnou identitu a do budoucna si lze představit i situaci, kdy budeme mít pouze jeden průkaz, který bude díky

[145] Více k e-Governmentu - E-Government. MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Archiv stránek bývalého Ministerstva informatiky* [online]. [cit. 2012-02-19]. Dostupné z: <http://aplikace.mvcr.cz/archiv2008/micr/egovernment/default.htm>.

[146] Elektronické občanské průkazy umožní přístup k online službám v celé EU. NOVÁK, Pavel. MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Ministerstvo vnitra České republiky* [online]. [cit. 2012-02-19]. Dostupné z: <http://www.mvcr.cz/clanek/elektronicke-obcanske-prukazy-umozni-pristup-k-online-sluzbam-v-cele-eu.aspx>.

certifikátům navázán na skutečnou identitu. V rámci takového propojení mohou i nadále fungovat jednotlivé digitální identity, které však budou přímo svázány s konkrétním subjektem práva. Fyzická osoba by pak k samotnému spuštění internetového prohlížeče nebo k použití jiných funkcí využívajících internet potřebovala přihlášení tímto průkazem. Anonymita na internetu, resp. anonymita ve smyslu neprovázanosti s konkrétním subjektem práva, by tak zcela přestala existovat.

V souvislosti s elektronickým podpisem jako prostředkem pro svázání digitální a reálné identity vyvstává otázka, zda samotné připojení elektronického podpisu určité osoby postačuje k tomu, aby byl platně učiněn právní úkon této osoby[147]. Patrně lze říci, že to opravdu postačí[148]. V tomto ohledu tedy není rozhodující, kdo se fakticky podílí na tvorbě dokumentu, kterým se právní úkon činí, a na procesu připojení elektronického podpisu.[149]

Na procesu připojení elektronického podpisu se může podílet sama fyzická osoba, o jejíž podpis se jedná, ale také osoba, která oprávněně disponuje s prostředky pro vytváření elektronického podpisu. Zde lze pozorovat další rozdílnost od běžného podpisu. U běžného podpisu nelze připustit, že platně za jiného podepíše, ten kdo napodobí jeho podpis. Předpokladem platnosti písemného právního úkonu je, že jej podepíše přímo ten, kdo jej činí, případně ten, kdo je oprávněn jednat za právnickou osobu. Podobný požadavek, že by data pro vytváření elektronického podpisu měla použít k elektronickému podpisu sama podepsaná osoba, však Zákon nestanoví. Bylo by to i nadbytečné vzhledem k tomu, že v praxi se většinou jedná o pouhé stisknutí myši nebo potvrzení na jiném ovládacím zařízení. V praxi by také bylo obtížné určit a prokázat, která osoba (případně i více osob) tyto prostředky připojila.[150]

Obecně platí, že určitý právní úkon lze přičíst určité osobě jen tehdy, pokud odpovídá vůli této osoby. Pokud by tomu tak nebylo, bude nutno účinky takového jednání posuzovat podle obecných ustanovení o účincích jednání za jiného bez plné moci, resp. při překročení plné moci.[151]

Další otázkou je, za jakých okolností lze ještě přičítat užití prostředků vytvářejících elektronický podpis určité jednající osobě. Na uskutečnění určitého

[147] Za předpokladu, ze jsou veškeré další náležitosti splněny.

[148] I vzhledem k ustanovení § 40 odst. 3 občanského zákoníku.

[149] ČERMÁK, K. Elektronický podpis - pohled soukromoprávní. *Bulletin advokacie*. 2002, 11, 69 s.

[150] Tamtéž, 69-70 s.

[151] Tamtéž, 70 s.

právního úkonu se v praktickém životě může podílet celá řada osob rozdílných od osoby, na kterou zní konkrétní certifikát. Například obsah smlouvy určuje advokát, formální stránku notář, o zachycení na hmotném substrátu se stará úřednice notářské kanceláře a účastníci smlouvy pouze připojují podpisy. V tomto ohledu se osoba, které bude příslušné jednání přičítáno, určí jednak vzhledem k celému obsahu písemného právního úkonu, jednak vzhledem k podpisům, které byly připojeny, resp. k informacím uvedeným na certifikátu.[152]

Z praktického hlediska je problematika přičítání určitého písemného právního úkonu opatřeného elektronickým podpisem určité osobě mnohem složitější, zejména v souvislosti s určením totožnosti osoby, která je uvedena na certifikátu. V tomto ohledu je nutné zmínit, že kvalifikovaný certifikát zpravidla obsahuje ve vztahu ke konkrétní osobě pouze jméno a příjmení podepisující osoby nebo její pseudonym s příslušným označením, že se jedná o pseudonym.[153] Právnická osoba dále může vydat pro své zaměstnance tzv. zaměstnanecký podpis, kde bude kromě jména podepisující fyzické osoby uvedeno také označení zaměstnavatele a případně pozice zaměstnance u zaměstnavatele.[154] V souvislosti s identifikačními údaji mohou být však další osobní údaje uvedeny na kvalifikovaném certifikátu jen se svolením podepisující osoby.[155]

Pouze na základě samotného jména a příjmení uvedeném na certifikátu se však objektivně nedá určit, na kterou osobu zní certifikát elektronického podpisu písemného právního úkonu. Ve svém důsledku se tedy nedá ani zjistit, zda je takový právní úkon platný, resp. platně podepsán jednající osobou, či jde například o pouhou shodu jmen.

Jednou z možností, jak předejít případným sporům o určení subjektu práva uvedeném na certifikátu a z toho vyplývajících důsledků na platnost úkonu, je dobrovolné uvedení bližších osobních údajů držitelem kvalifikovaného certifikátu. Ovšem zde záleží, zda se daná certifikační autorita při ověřování totožnosti dotáže konkrétní osoby, zda si přeje zveřejnit další údaje. Ani v případě dobrovolného uvedení adresy nemusí být situace zcela jasná, jelikož dva lidé totožného jména mohou bydlet na stejné adrese. V praxi se na certifikátu objevuje také emailová adresa, která může sloužit jako dodatečný identifikátor, ale také nemusí vzhledem k relativní volnosti při

[152] Tamtéž.

[153] Ustanovení § 12 odst. 1 Zákona.

[154] Nemusí se však jednat pouze o pracovní či jiný obdobný poměr.

[155] Ustanovení § 12 odst. 3 Zákona.

tvorbě emailových schránek. Právě z tohoto důvodu není považována za osobní údaj, a proto bývá zveřejňována.

Určitou snahou směřující k vyřešení problému v českém právním řádu může být ustanovení § 11 odst. 1 Zákona, které stanovuje požadavek, aby kvalifikovaný certifikát obsahoval takové údaje, aby „osoba byla jednoznačně identifikovatelná“. Ovšem tento požadavek platí pouze v oblasti orgánů veřejné moci a za použití uznávaného elektronického podpisu. Struktura údajů, na základě kterých je možné osobu jednoznačně identifikovat, má být stanovena prováděcím právním předpisem Ministerstva vnitra. Tímto předpisem je vyhláška č. 496/2004 Sb., o elektronických podatelnách, jejíž požadavky[156] byly patrně zaměřeny na určitý nový národní bezvýznamový identifikátor, ale ten se nepodařilo prosadit. Jelikož stanovené požadavky splňoval také vnitřní identifikátor Ministerstva práce a sociálních věcí, tak plní tuto funkci.[157] Tento identifikátor však není patrný ze samotného certifikátu pro veřejnost, i když certifikační autority s ním operují.[158] Certifikační autority dále používají své interní identifikátory osoby, které přesně spojují certifikáty s konkrétními držiteli, avšak ani na základě tohoto identifikátoru nelze dopátrat konkrétní údaje u certifikační autority, jelikož nejsou a dle zákona ani být nemohou zveřejňovány.

Slovenská úprava elektronického podpisu odkazuje ohledně formátu a obsahu kvalifikovaných certifikátů na zvláštní právní předpis vydaný Národním bezpečnostním úřadem Slovenské republiky.[159] Ten určuje o obsahu identifikačních údajů uvedených na každém kvalifikovaném certifikátu, že kromě jména a příjmení nebo pseudonymu musí obsahovat také doplňující identifikátor zabezpečující jednoznačnost

[156] Těmito požadavky se dle ustanovení § 4 vyhlášky č. 496/2004 Sb., o elektronických podatelnách, rozumí: „*Údaj, na jehož základě je možné osobu jednoznačně identifikovat, se uvádí ve struktuře desetimístného čísla v desítkové soustavě v rozsahu 1 100 100 100 až 4 294 967 295 a je spravován ústředním orgánem státní správy. Jeho hodnota není zaměnitelná s rodným číslem a nesmí být osobním údajem podle zvláštního právního předpisu.*“

[157] PETERKA, J. Datové schránky: komu patří podpis na e-dokumentu? VI. *Lupa.cz* [online]. 15.10.2009 [cit. 2012-02-20]. Dostupné z: <http://www.lupa.cz/clanky/datove-schranky-komu-patri-podpis/>.

[158] Z vlastní zkušenosti autora se tento identifikátor objevil na Protokolu o vydání certifikátu od certifikační autority PostSignum.

[159] Ustanovení § 7 odst. 8 zákona č. 215/2002 Z. z., o elektronickom podpise a o zmene a doplnení niektorých zákonov, ve znění pozdějších předpisů (Slovenská republika).

identifikačních údajů držitele certifikátu.[160] V praxi se využívá rodného čísla, které je však u nás osobním údajem.

Určitým vodítkem pro jednoznačné stanovení identity mohou být výše uvedené zaměstnanecké podpisy, díky jejichž údajům o zaměstnavateli a případné funkci zaměstnance na certifikátu je možné mnohem jednodušeji ověřit identitu.

Situace je však mnohem komplikovanější. Jak je patrné z výše uvedených požadavků na obsah kvalifikovaných certifikátů, certifikát nemusí obsahovat jméno a příjmení držitele vůbec. Tyto údaje mohou být nahrazeny pseudonymem držitele certifikátu s označením, že se jedná o pseudonym. V takovém případě je krajně problematické určit skutečnou identitu osoby, které patří elektronický podpis. Pokud však dle slov zákonodárce zaručený elektronický podpis založený na takovém certifikátu umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě a je jednoznačně spojen s podepisující osobou, tak se stále patrně jedná o elektronický podpis, i když jsou tyto údaje velmi obtížně ověřitelné pro osobu ověřující tento podpis. V praktickém sporu by však byly tyto informace jednoduše zjistitelné soudem, jelikož poskytovatel certifikátu má bližší údaje k dispozici a vždy jednoznačně ví, které osobě patří certifikát elektronického podpisu. Otázkou zůstává, kde je hranice obvyklé obezřetnosti a prevenční povinnosti předcházení škodám osoby ověřující údaje na certifikátu, která tyto údaje k dispozici nemá. Patrně by měla požádat podepsanou osobu o věrohodné vysvětlení, proč používá certifikát na pseudonym, nikoliv na jméno.[161] Kupříkladu v případě známých umělců by toto vysvětlení mohlo být snadno pochopitelné.

Obdobná situace může nastat v případě autorizované konverze. Dle zákona o el. úkonech obsahuje konverzní doložka konverze do dokumentu v listinné podobě údaj o tom, zda byl vstupní dokument podepsán platným uznávaným elektronickým podpisem nebo označen platnou uznávanou elektronickou značkou, číslo kvalifikovaného certifikátu, na němž je uznávaný elektronický podpis založen a obchodní firmu akreditovaného poskytovatele certifikačních služeb, který kvalifikovaný certifikát

[160] Ustanovení § 2 odst. 4 vyhlášky č. 538/2002 Z. z., o formáte a obsahu kvalifikovaného certifikátu, o správe kvalifikovaných certifikátov a o formáte, periodicite a spôsobe vydávania zoznamu zrušených kvalifikovaných certifikátov.

[161] PETERKA, J. Datové schránky: komu patří podpis na e-dokumentu? VI. *Lupa.cz* [online]. 15.10.2009 [cit. 2012-02-20]. Dostupné z: <http://www.lupa.cz/clanky/datove-schranky-komu-patri-podpis/>.

vydal.[162] Konverzní doložka již neobsahuje ani samotné jméno a příjmení držitele certifikátu, resp. pseudonym. Na základě čísla kvalifikovaného certifikátu lze však u příslušného poskytovatele certifikačních služeb, který je také na ověřovací doložce uveden, alespoň základní informace o držiteli a stavu certifikátu – jméno, resp. pseudonym, adresa, e-mailová adresa, stav a doba platnosti certifikátu. Komplikace mohou nastat v případě, že žadatel požádal o tzv. neveřejný certifikát. Jde o certifikát, kde na základě čísla certifikátu lze zjistit u příslušné certifikační autority pouze stav a případně dobu platnosti certifikátu. Údaje o držiteli certifikátu jsou patrné pouze z certifikátu. V případě konvertovaného dokumentu do listinné podoby tedy osoba ověřující platnost úkonu vůbec nemá možnost zjistit jméno držitele certifikátu, jeho další identifikační údaje a už vůbec ne, zda jeho certifikát nezní na pseudonym.[163] Je patrné pouze, že daný certifikát je platný a že integrita dokumentu v době konverze nebyla porušena. V takovém případě nezbývá než opět doporučit osobě ověřující platnost dokumentu se na pravý důvod žádosti o neveřejný certifikát zeptat podepsané osoby.

Závěrem lze konstatovat, že zákonodárce by se měl s těmito problémy ohledně informací zveřejňovaných na certifikátech a ověřovacích doložkách vypořádat tak, aby nebylo důvodných pochybností o identitě podepsané osoby. V této souvislosti je nutné upozornit, že pokud by samotný úkon nebo smlouva dostatečně neoznačovaly účastníky a tento nedostatek by nebylo možné odstranit výkladem obsahu úkonu (například i ověřením údajů uvedených na certifikátu elektronického podpisu nebo prověřením těchto údajů na základě sériového čísla u certifikační autority), lze polemizovat o neplatnosti právního úkonu v důsledku neurčitosti.[164]

3.2 Existence vůle

Vůle je jedním z nezbytných pojmových předpokladů vzniku právního úkonu. Jedná se o psychický vztah jednajícího člověka k zamýšlenému (chtěnému) následku.[165]

---

[162] Ustanovení § 25 odst. 2 zákona o el. úkonech.

[163] PETERKA, J. Datové schránky: komu patří podpis na e-dokumentu? VI. *Lupa.cz* [online]. 15.10.2009 [cit. 2012-02-20]. Dostupné z: <http://www.lupa.cz/clanky/datove-schranky-komu-patri-podpis/>.

[164] ŠVESTKA, J.; SPÁČIL, J.; ŠKÁROVÁ, M.; HULMÁK, M. a kolektiv. *Občanský zákoník I, II*. 2. vydání. Praha : Nakladatelství C. H. Beck, 2009. 339 s.

[165] ŠVESTKA, J.; DVOŘÁK, J. *Občanské právo hmotné 1*. Praha : Wolters Kluwer Česká republika, 2009. 119 s.

Za náležitosti vůle jsou obecně považovány její svoboda a vážnost, jakož i absence omylu.[166]

Zatímco svoboda vůle nebude vyvolávat žádné vážnější otázky v souvislosti s elektronickým podepisováním, tak vážnost vůle písemných právních úkonů může být dotčena. Právní věda rozlišuje tzv. vnitřní vůli a projevovací vůli. Vnitřní vůlí je označována vůle způsobit právní následky, které s určitým projevem zákon spojuje. Projevovací vůle vyjadřuje vůli učinit projev vůle o určitém obsahu. Problém nastává v případě, kdy se z projevu vůle vykládá existence vnitřní vůle, i když ji vůbec neobsahuje.[167] Tehdy je tu právě projevovací vůle, avšak není tu vůle způsobit to, k čemu projev směřuje. Zejména v elektronickém světě je rovněž častý případ, kdy existuje určitý projev vůle, ovšem jednající osoba vůbec vnitřní vůli vyjádřit nechtěla a ani o projevovací vůle zde nemůže být řeč. Jedná se zejména o různé bezpečnostní hrozby v podobě počítačových virů, které mohou nevědomky k předem připravené datové zprávě přidat elektronický podpis a tuto zprávu odeslat na určenou emailovou adresu. V takovém případě je zcela zřejmé, že vůle nebyla vůbec projevena. Ostražitému uživateli lze však doporučit, aby si při jakémkoli vyžádání připojení elektronického podpisu nastavil heslo k použití dat pro vytváření elektronického podpisu.

Pokud se podíváme, kdy projev vůle není vyjádřením vnitřní vůle, jsou to zejména situace kdy:

a) někdo sice chtěl učinit projev, ale ve skutečnosti nechtěl to, co projevil jako svou vnitřní vůli (úkony učiněné žertem, na oko, disimulace, aberace tj. přeřeknutí, přepsání);
b) jednající chtěl učinit projev, kterým i projevil svou vnitřní vůli, ale jeho vůle se vytvářela vadně (bezprávná výhrůžka), nebo vnitřní vůle vznikla následkem omylu[168].[169]

---

[166] ČERMÁK, K. Elektronický podpis - pohled soukromoprávní. *Bulletin advokacie*. 2002, 11, 70 s.

[167] Správně by se vůle měla vykládat i okolností, za nichž byl učiněn projev vůle. K tomu dále viz: Rozhodnutí Nejvyššího soudu ze dne 5. 9. 2000, sp. zn. 30 Cdo 2781/99, uveřejněné ve Sbírce soudních rozhodnutí a stanovisek pod č. 11/2003. HULMÁK, M. *Uzavírání smluv v civilním právu*. 1. vydání. Praha : Nakladatelství C. H. Beck, 2008. 16 s.

[168] Zejména v poslední době se objevuje řada podvodných praktik v prostředí internetu, jedná se zejména o tzv. phising a spoofing.

Jak bylo uvedeno výše, zákonodárce vyžaduje vlastnoruční podpis v případech, kdy je na místě vyšší ostražitost vůči podepisovanému úkonu. Ostražitost může být v tomto případě chápána jako snaha o odstranění výše nastíněné diskrepance mezi vnitřní a projevovací vůlí a jako upozornění, že by tento úkon měl být činěn při plném vědomí závažnosti úkonu a jeho následků.

Právě v případě elektronických podpisů se projev vůle omezuje na pouhé stisknutí tlačítka. Ostražitému uživateli lze opět doporučit nastavení hesla k použití dat pro vytváření elektronického podpisu. V praktickém životě i jednodušší způsob připojení elektronického podpisu bude výsledkem volního jednání, avšak je pravděpodobnější, že takový úkon může být učiněn nechtěně či bez hlubšího rozmyslu, aniž by jednající osoba skutečně chtěla způsobit následky spojované zákonem s takovým projevem. Právě technická stránka, která je důvodem jednoduchého provedení aktu připojení podpisu, je však většině takto jednajících osob známa, k čemuž je nutné při určování nedostatku vážnosti vůle přihlížet.[170]

Ve spojitosti s adresovanými právními úkony činěnými na dálku, kde se elektronického podpisu nejčastěji využívá, lze znovu připomenout, že adresát nemá možnost vnímat sekundární informace (např. okolnosti za kterých je úkon činěn) poskytované jednající osobou, pokud je jednající osoba přímo neuvede. Adresát tak pochopitelně nemá možnost rozpoznat, zda je úkon činěn vážně či nikoliv.

3.3 Projev vůle

Ohledně srozumitelnosti a určitosti jako náležitostí projevu vůle platí i v případě elektronických podpisů obecný výklad o právních úkonech a také to, co již bylo výše uvedeno (zejména ohledně přičítání projevu vůle).

Jistá specifika ohledně srozumitelnosti právního úkonu jsou patrná zejména u zašifrovaného obsahu dokumentu. Zde je nutné rozlišovat zašifrovaný dokument prostřednictvím obecných šifrovacích metod a prostřednictvím elektronického podpisu.

V prvním případě je podmínkou srozumitelnosti a tedy i platnosti právního úkonu, možnost adresáta disponovat s dešifrovacími nástroji takového úkonu. V případě, že adresát těmito prostředky nedisponuje a ani s nimi nemá možnost

[169] SPÁČIL, J. Vážná vůle jako základní náležitost právního úkonu v právní vědě a v judikatuře. *Právní rozhledy*. 2004, 22, 811 s.

[170] ČERMÁK, K. Elektronický podpis - pohled soukromoprávní. *Bulletin advokacie*. 2002, 11, 71 s.

disponovat či to na něm nelze spravedlivě požadovat, je na místě učinit závěr, že takový úkon je neplatný pro nesrozumitelnost. Pokud by dešifrovacími prostředky disponoval v přiměřené době poté, co byl právní úkon učiněn, bylo by patrně možné takový právní úkon považovat za platně učiněný okamžikem, kdy adresát začal disponovat s dešifrovacími prostředky. Přiměřenost této doby by byla závislá na konkrétních okolnostech případu. Za předpokladu, že by dešifrovacími nástroji adresát nedisponoval, ačkoli mu to bylo umožněno a bylo možné to na něm spravedlivě požadovat, byl by takový úkon platný.[171]

Jinak tomu bude při využití elektronického podpisu jako šifrovacího nástroje. Veřejný klíč, tj. data pro ověřování elektronického podpisu, lze využít k zašifrování datové zprávy. K dešifrování následně slouží příslušný párový soukromý klíč. Pokud si tedy budeme přát zašifrovat datovou zprávu, je možné využít dostupný veřejný klíč adresáta.[172] Adresát má vždy k dispozici dešifrovací nástroj – soukromý klíč, a proto je mu datová zpráva spolu s právním úkonem vždy srozumitelná.[173] Neplatnost by mohla nastat za situace, že byl použit veřejný klíč jiné osoby než adresáta a ten

tak nemá možnost dešifrovat zprávu a spolu s ní i právní úkon, jelikož nedisponuje příslušným soukromým klíčem.

Abychom zcela vyčerpali možnosti elektronického podpisu ve vztahu k určitosti právního úkonu, je třeba zmínit, že technologie sloužící pro elektronické podepisování se nevyužívá pouze k podepisování dokumentů a jejich případnému šifrování. Lze ji také využít k „podepisování“ webových portálů. Zde je jejím účelem ověření totožnosti majitele portálu, integrity, nezměnitelnosti a šifrování komunikace mezi serverem a uživatelem tak, aby nemohla být zneužita.

Rozdíl po právní stránce oproti elektronickému podpisu spočívá zejména v typu certifikátu, kde místo kvalifikovaného certifikátu je využíván kvalifikovaný systémový certifikát.

Otázkou zůstává, zda taková webová stránka v rámci portálu využívajícího technologii PKI (v souhrnu nazýváno SSL využívaný v protokolu HTTPS) může být považována za písemný právní úkon. Odpověď nám poskytne právní a technický rozbor této technologie.

---

[171] Tamtéž.

[172] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi*. Olomouc : ANAG, 2008. 32 s.

[173] Alespoň za předpokladu, že nebyla porušena integrita zprávy a nebylo s ní jinak manipulováno.

Po právní stránce slouží certifikát, který je vydán danému subjektu, podobně jako v případě elektronických podpisů – umožňuje ověřit identitu subjektu provozujícího server, slouží jako metoda zabezpečení atd. Dále je nutné rozlišovat dvě situace. Za předpokladu, že takový úkon musí být adresován, by podmínky splněny nebyly, jelikož v rámci internetového prostředí je převažující většina internetových stránek neadresovaná. Ohledně úkonů neadresovaných určitému okruhu subjektů by patrně takové stránky nešlo považovat za elektronicky podepsané vzhledem k technickým specifikacím.

Technologie SSL je zde využívána primárně k zabezpečení přenosu dat (komunikaci) a nerozeznává obsah. V podstatě vytváří ochrannou obálku pro jednotlivá paketová data, která jsou odesílána směrem ke konkrétnímu uživateli a naopak. Takto tedy zabezpečuje vše, co se pohybuje mezi serverem a uživatelem. Je také důležité zmínit, že jsou zabezpečována paketová data, která až po svém složení dávají uživateli zobrazenou stránku, nikoliv zobrazená stránka jako celek. Proto samotný výstup celého procesu, pokud proběhl řádně, nebude rozeznatelný od výstupu nezabezpečeného pomocí technologie SSL.[174] V prohlížeči takto zobrazených stránek však může být patrné, že komunikace probíhá prostřednictvím protokolu HTTPS. Z čehož i vyplývá, že daná technologie ověřuje na základě příslušného certifikátu pouze identitu osoby, se kterou je komunikováno, a nikoliv identitu podepisující osoby, jelikož se nejedná o proces podepisování, ale o proces komunikace.

Stejně jako u elektronické značky, tak také zde nelze jednoznačně říci, zda skutečně existovala vůle k uzavření smlouvy a zda tato vůle byla skutečně projevena. Pokud bychom posuzovali existenci podpisu na dokumentu pouze na základě právního analýzy a bez pohledu na jakýkoliv dokument komunikovaný prostřednictvím SSL, mohly bychom se snadno dopustit omylu a posuzovat tuto metodu například jako mechanický prostředek nahrazení podpisu. Dle technické analýzy SSL technologie a při letmém pohledu na jakýkoli takto komunikovaný výstup bude snadno patrné, že výstup neobsahuje žádný mechanický prostředek, nebo dokonce elektronický podpis.

Aplikovat elektronický podpis na vstupní data zabezpečené komunikace a tím pádem je i rozeznat na jeho výstupu ovšem možné je, ale pouze za předpokladu, že původní data, resp. webová stránka, byla při tvorbě podepsána přímo držitelem dat pro

[174] SCHMEH, K. *Cryptography and Public Key Infrastructure on the Internet.* West Sussex : Wiley, 2003. 343 s.

vytváření elektronického podpisu. Při současném podepsání vstupu ale samotný proces zabezpečení SSL technologií do značné míry ztrácí odůvodnění. Naproti tomu není z praktického hlediska možné použít elektronický podpis jako prostředek zabezpečení u dynamicky generovaných stránek.

3.4 Existence normy

Jakékoliv jednání je způsobilé vyvolat konkrétní právní účinky pouze tehdy, pokud je s tímto jednáním spojuje právní norma. Právní norma tak spojuje s daným projevem vůle vznik, změnu nebo zánik právního vztahu.

Nelze však obecně říci, že na posuzování konkrétního jednání se použije pouze jedna norma konkrétního zákona. V potaz přichází celá řada norem stanovujících skutečnosti zejména ohledně posouzení, zda se skutečné jedná o právní úkon, interpretaci právních úkonů, spojení konkrétních právně relevantních účinků s daným jednáním atd. V rámci jednoho právního řádu můžeme rozlišovat i více norem například pro interpretaci právních úkonů. Je tomu tak i u nás, kdy vedle sebe máme § 35 občanského zákoníku a § 266 obchodního zákoníku.

Pokud se zaměříme čistě na jednání veřejně přístupné v rámci internetu a neadresované určitému okruhu subjektů, dojdeme k závěru, že situace je podstatně složitější. Je nutné najít normu, podle které je možné posoudit, zda konkrétní jednání – zveřejnění určité informace – má náležitosti právního úkonu. V úvahu však nemusí přicházet pouze normy jednoho právního řádu. V souvislosti s tím je možné uvažovat o zemích, odkud je informace přístupná, kde je umístěn server hostující danou internetovou stránku, kde má původce informace svůj domicil, místo registrace domény internetové stránky atd. Podobný výčet nás může čekat v případě emailové komunikace.

Použití norem s působností omezenou na území určitého státu je v rámci internetového prostoru, který se vyznačuje nezávislostí na konkrétních hranicích států, vnímáno jako největší problém.[175] V této souvislosti hovoří teorie o delokalizaci společenský vztahů, když je pro nás irelevantní kudy probíhá komunikační spojení, jakým prostředkem je realizováno a často ani to, kde se fyzicky nachází adresát našeho sdělení.[176] Problém je vnímán zejména v tom, že: „*Faktická delokalizace společenských*

[175] GRAHAM, J. H. S. *Internet Law and Regulation.* London : Sweet & Maxwell, 2007. 451 s. KOHL, U. *Jurisdiction and the Internet: A Study of Regulatory Competence Over Online Activity.* Cambridge : Cambridge University Press, 2007. 24 s.

[176] POLČÁK, R. *Právo a evropská informační společnost*. Brno : Masarykova univerzita, 2009. 55 s.

vztahů je totiž přímo rozporná s jedním z nejtradičnějších konceptů práva a současně s jedním z nejstarších principů mezinárodního práva veřejného, tedy s konceptem místní působnosti ve spojení s principem státní suverenity.“[177]

Otázka výběru rozhodného práva, příslušnosti soudních institucí a unifikace pravidel pro smlouvy s mezinárodním prvkem v prostředí internetu tak nabývá v poslední době značně na významu, zejména na nadnárodní[178] a mezinárodní[179] úrovni.

V souvislosti s elektronickým podpisem jako součástí písemného právního úkonu problém delokalizace společenských vztahů vyvstává zejména s ohledem na roztříštěnost právní úpravy v jednotlivých státech. Jak bylo ukázáno v kapitole o legislativních přístupech, liší se vnímání elektronického podpisu stát od státu. Prostředek, který je jedním právním řádem vnímán jako elektronický podpis, nemusí splňovat požadavky na elektronický podpis v jiném právním řádu. Rozdíly jsou samozřejmě nejmarkantnější mezi angloamerickou a kontinentální právní kulturou a vyplývají již z přístupů ke klasickému psanému podpisu.

V praxi mohou nejčastěji vyvstat problémy u vícestranných písemných právních úkonů, zejména smluv, elektronicky podepsaných stranami z různých států, které se liší přístupem k elektronickému podpisu. Pro názornost si představme případ smlouvy uzavřené mezi společností českou a společností ze Spojených států amerických, kdy česká společnost podepsala smlouvu svým platným uznávaným podpisem a americká společnost pouhým uvedením obchodní firmy a jména osoby jednající za tuto společnost. V rámci amerického práva je forma podpisu americké společnosti považována za platný elektronický podpis, jak bylo výše uvedeno. V rámci českého práva nelze bez dalšího tuto formu považovat za elektronický podpis. V případě obvyklosti by bylo možné uvažovat pouze o mechanickém prostředku nahrazení podpisu.

---

[177] Tamtéž, 57 s.

[178] Důkazem může být i přijetí řady předpisů evropského práva. Zejména nařízení Evropského parlamentu a Rady č. 593/2008 o právu rozhodném pro smluvní závazkové vztahy (Řím I), nařízení Evropského parlamentu a Rady č. 864/2007 o právu rozhodném pro mimosmluvní závazkové vztahy (Řím II), nařízením Rady č. 44/2001 o příslušnosti a uznávání a výkonu soudních rozhodnutí v občanských a obchodních věcech (Brusel I), nařízení Rady č. 1347/2000 o příslušnosti a uznávání a výkonu rozhodnutí ve věcech manželských a ve věcech rodičovské zodpovědnosti obou manželů k dětem (Brusel II).

[179] Úmluva OSN o užití elektronických sdělovacích prostředků v mezinárodním obchodu (ECC)

Při posuzování platnosti takového písemného právního úkonu, resp. neplatnosti v důsledku absentující náležitosti – podpisu, mohou nastat dvě situace v závislosti na určení rozhodného práva. Dle amerického práva by byla smlouva platně uzavřena, jelikož podpis české i americké společnosti splňuje požadavky amerického práva na elektronický podpis. Dle českého práva, které má vyšší požadavky na elektronický podpis, by záleželo na posouzení, zda se nejedná alespoň o mechanický prostředek nahrazení podpisu za podmínky obvyklosti tak, jak to stanoví ustanovení § 40 odst. 3 občanského zákoníku. Odlišná situace by nepochybně nastala za současného využití znění dohody uvedené v Příloze č. 1, která by zejména mohla reflektovat požadavky na elektronický podpis uvedené v Zákoně, zejména pak na jednoznačnost ověření totožnosti. Vzhledem k výše uvedenému lze jen doporučit věnovat zvláštní obezřetnost volbě práva a určení požadavků na elektronický podpis.

Český právní řád se o zahraničních elektronických podpisech, resp. kvalifikovaných certifikátech, zmiňuje pouze v ustanovení § 16 odst. 1 Zákona. Kvalifikovaným certifikátům od poskytovatelů certifikačních služeb usazených v některém z členských států Evropské unie, jiném smluvním státu Dohody o Evropském hospodářském prostoru nebo Švýcarské konfederaci se přiznává stejné postavení jako českým kvalifikovaným certifikátům. Kvalifikované certifikáty z ostatních zemí lze za u nás považovat za kvalifikované pouze za předpokladu, že:

a) poskytovatel certifikačních služeb splňuje podmínky práva Evropských společenství a byl akreditován k působení jako akreditovaný poskytovatel certifikačních služeb v některém z členských států Evropské unie, jiném smluvním státu Dohody o Evropském hospodářském prostoru nebo Švýcarské konfederaci,
b) poskytovatel certifikačních služeb usazený v některém z členských států Evropské unie, jiném smluvním státu Dohody o Evropském hospodářském prostoru nebo Švýcarské konfederaci, který splňuje podmínky práva Evropských společenství, převezme odpovědnost za platnost a správnost certifikátu ve stejném rozsahu jako u svých kvalifikovaných certifikátů, nebo
c) to vyplývá z mezinárodní smlouvy.[180]

[180] Ustanovení § 16 odst. 2 Zákona.

Zejména požadavek písm. a) převzatý z článku 7 Směrnice působí částečně diskriminačně v rámci Evropské unie, jelikož vzhledem k článku 3 odst. 2 Směrnice, jsou akreditační systémy v jednotlivých zemích dobrovolné[181]. Poskytovatel certifikačních služeb, který není usazen v některém z členských států Evropské unie, jiném smluvním státu Dohody o Evropském hospodářském prostoru nebo Švýcarské konfederaci a přesto chce působit na evropském trhu, by tak musel žádat o akreditaci v některém členském státě, který dobrovolně zavedl akreditační systém. Takovému poskytovateli by nestačilo splnit požadavky na kvalifikovaného poskytovatele a takto být veden na výše uvedeném území.

Jak je vidno i v rámci Evropské unie se přístupy k implementaci Směrnice liší. Z technického hlediska může být stávající situace mnohem složitější. Například Polsko integrovalo požadavky na kvalifikované certifikáty, certifikační autority a jejich služby v podzákonném předpisu[182]. V něm jsou obsaženy i technické požadavky, které ovšem vycházejí z již neaktuálního technického standardu RFC 3039[183]. Pokud odhlédneme od komplikací se změnami takové normy, tak toto řešení může vést k řadě omezení v rámci smluv uzavíraných v internetovém prostředí.[184]

3.5 Vliv vlastností certifikátu na platnost písemného právního úkonu

Certifikát zaručeného elektronického podpisu může obsahovat určité vlastnosti, resp. údaje na něm uvedené, které již při samotném vzniku mohou vyvolávat určité otázky ve vztahu k platnosti písemných právních úkonů (například výše diskutovaný pseudonym), a dále některé charakteristiky projevující se až časem, resp. až elektronickým podepsáním – platnost certifikátu a určitá omezení uvedená na certifikátu

3.5.1 Platnost certifikátu elektronického podpisu

Elektronické podpisy bývají využívány nejčastěji ve formě zaručených elektronických podpisů založených na technologii PKI, která využívá certifikáty.

---

[181] Například Polsko, Maďarsko nebo Malta akreditační systém neprovozují.

[182] Rozporządzenie Rada Ministrów z dnia 7 sierpnia 2002, Dz.U.02.128.1094 (Polská republika).

[183] Internet X.509 Public Key Infrastructure Qualified Certificates Profile. *Internet FAQ Archives* [online]. [cit. 2012-03-02]. Dostupné z: <http://www.faqs.org/rfcs/rfc3039.html>.

[184] K těmto omezením dále MOJŽÍŠ, M. S kvalifikovaným certifikátem raději necestujte. *Lupa.cz* [online]. 26.01.2005 [cit. 2012-03-02]. Dostupné z: <http://www.lupa.cz/clanky/s-kvalifikovanym-certifikatem-radeji-necestujte/>.

V rámci certifikátů lze hovořit o tzv. platnosti certifikátu. Zákon na řadě míst platnost certifikátu zmiňuje zejména v souvislosti se zneplatněním. Zejména ustanovení § 6a odst. 3 a 4 Zákona stanovují povinnost poskytovatele certifikačních služeb zneplatnit certifikát, pokud:

a) o to jeho podepisující osoba požádala,
b) podepisující osoba uvědomila poskytovatele dle ustanovení § 5 odst. 1 Zákona, že hrozí nebezpečí zneužití dat pro vytváření elektronický podpisů,
c) byl certifikát vydán na základě nepravdivých nebo chybných údajů,
d) se poskytovatel prokazatelně doví, že podepisující osoba zemřela nebo zanikla nebo ji soud způsobilosti k právním úkonům zbavil nebo omezil, nebo pokud údaje, na jejichž základě byl certifikát vydán pozbyly pravdivosti, nebo
e) Ministerstvo vnitra nařídilo zneplatnění jako předběžné opatření, nebo rozhodlo o zneplatnění na základě ustanovení § 15 Zákona.

Z ustanovení § 12 odst. 1 písm. h) Zákona lze dovodit, že kvalifikované certifikáty jsou vydávány na omezenou dobu, která je na nich vyznačena. Důvod tohoto časového omezení platnosti certifikátů spočívá ve způsobu vytváření elektronických podpisů. Jak bylo výše uvedeno, elektronický podpis je unikátní pro každý podepisovaný dokument a je výsledkem složitého výpočtu. Právě složitost výpočtu, jehož výsledek je odvozen od kontrolního součtu konkrétního dokumentu, zajišťuje nemožnost vytvořit k již existujícímu podpisu dokument rozdílného obsahu, avšak s totožným výsledkem – elektronickým podpisem. Pokud by tomu tak nebylo, bylo by možné již existující elektronický podpis určité osoby od dokumentu oddělit a k tomuto podpisu vygenerovat dokument libovolného obsahu (tzv. kolizní dokument), což by zcela jistě vedlo ke značnému zpochybnění využití elektronických podpisů.[185] Tyto vlastnosti jsou také jednou z charakteristik předvídaných v ustanovení § 2 písm. b) Zákona pro zaručený elektronický podpis.

Naše schopnosti vytvořit kolizní dokument se v čase mění s tím, jak narůstají výpočetní schopnosti počítačů.[186] Lze se proti tomu účinně bránit průběžným

[185] PETERKA, J. Proč elektronické podpisy nejsou věčné? e*Archiv.cz* [online]. 10.5.2010 [cit. 2012-02-12]. Dostupné z: <http://www.earchiv.cz/b10/b0510001.php3>.

[186] Znovu lze připomenout Mooreův zákon z úvodu této práce.

zaváděním složitějších algoritmů a delších klíčů, tak aby výpočet kolizního dokumentu byl stále výrazně nad možnostmi výkonu výpočetní techniky v dané době.[187]

Ze soukromoprávního hlediska vystává otázka, zda neplatnost kvalifikovaného certifikátu má vliv na platnost písemných právních úkonů. V úvahu přicházejí dvě situace v závislosti na tom, zda byl písemný právní úkon podepsán s platným či s již neplatným certifikátem.

3.5.1.1 Dokument opatřený elektronickým podpisem založeným na platném certifikátu a problematika dlouhověkosti

Byl-li písemný právní úkon podepsán spolu s platným certifikátem, je jistě právní úkon platný, tedy alespoň pokud obsahuje veškeré ostatní náležitosti stanovené zákonem. Co se však stane po skončení planosti certifikátu? Rozhodně nelze říci, že by elektronický podpis přestal být platným, a v důsledku tohoto by i právní úkon pozbyl platnosti.

Stejně jako u vlastnoručního podpisu, tak i platnost elektronického podpisu nelze vázat na určitou dobu. Podpis je buď platný, nebo neplatný. Po vypršení platnosti certifikátu nebo jeho zneplatnění po podpisu písemného právního úkonu se oslabuje schopnost ověřit platnost certifikátu v době podpisu. V takovém případě nám program pro vyhodnocení může oznámit, že nelze vyhodnotit platnost elektronického podpisu, resp. že „neví“. Právě tato platnost je důležitá pro určení odpovědnosti, jelikož vzhledem k ustanovení § 5 odst. 2 Zákona se podepisující osoba může zprostit odpovědnosti, „*jestliže prokáže, že ten, komu vznikla škoda, neprovedl úkony potřebné k tomu, aby si ověřil, že zaručený elektronický podpis je platný a jeho kvalifikovaný certifikát nebyl zneplatněn*“. V případě porušení povinnosti zacházet s prostředky pro vytváření elektronického podpisu s náležitou péčí a povinnosti uvědomit neprodleně poskytovatele, že hrozí nebezpečí zneužití dat pro vytváření elektronického podpisu je odpovědná podepisující osoba.

Rozpor nastává právě po skončení platnosti certifikátu, kdy na jedné straně jsme nuceni ověřit platnost certifikátu pod hrozbou odpovědnosti za škodu, ale na druhou stranu je naše schopnost tyto informace ověřit značně snížena. Osobě, která by měla přijmout dokument podepsaný podpisem, u něhož nelze ověřit platnost certifikátu, tak

[187] V ČR jsou certifikáty vystavovány na dobu jednoho roku., v zahraničí se lze setkat až s tříletou platností.

lze doporučit, aby takový dokument nepřijala, jelikož by mohla nést odpovědnost za škodu, která jí vznikla.[188]

Takový stav vyžaduje na jednu stranu náležité schopnosti při vyhodnocování platnosti certifikátu elektronického podpisu a na druhou aktivní péči o naše dokumenty.

Vyhodnocování platnosti se řídí určitými pravidly, která je nutné dodržovat pro učinění správného závěru. Nejprve je nutné disponovat všemi certifikáty (zejména poskytovatele certifikačních služeb) získanými z důvěryhodného úložiště. Poté je nutné ověřit integritu dokumentu. Pokud program, prostřednictvím kterého ověřujeme integritu dokumentu, zjistí, že s dokumentem bylo manipulováno, vyhodnotí elektronický podpis jako neplatný. V opačném případě je možné pokračovat dále, kde je nutné ověřit důvěryhodnost certifikátu, což za nás v praxi ověří opět vyhodnocovací program na základě toho, že osobní certifikát na veřejném klíči byl podepsán certifikační autoritou, kterou považujeme za důvěryhodnou. Dalším krokem je vyhodnocení platnosti certifikátu na veřejném klíči podepsané osoby v době vzniku podpisu dokumentu.[189]

Elektronický podpis v sobě obsahuje údaj o svém vzniku, který je však přebrán z nastavení počítače, a jako takový je tedy nedůvěryhodný, protože s ním může kdokoliv manipulovat. K vyhodnocení podpisu je tedy nutné použít určitý časový okamžik, ke kterému máme jistotu, že dokument spolu s podpisem existoval. Jednak jím může být samotný okamžik ověřování podpisu, což bude zejména v případě doposud platného certifikátu elektronického podpisu na dokumentu. Existenci elektronicky podepsaného dokumentu k určitému okamžiku lze také prokázat elektronickým orazítkováním. Časové razítko funguje na obdobném principu jako elektronický podpis. Kvalifikovaným časovým razítkem[190] se rozumí „*datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem*“[191]. Je nutné poznamenat, že dokument nemusí být nutně orazítkován v čase svého podpisu a časový odstup může být velmi značný.

---

[188] PETERKA, J. Proč elektronické podpisy nejsou věčné? e*Archiv.cz* [online]. 10.5.2010 [cit. 2012-02-12]. Dostupné z: <http://www.earchiv.cz/b10/b0510001.php3>.

[189] Tamtéž.

[190] Pokud dále budeme hovořit o časovém razítku je tím myšleno právě kvalifikované časové raítko.

[191] Ustanovení § 2 písm. r) Zákona.

Nyní se dostáváme k problematice péče o dokumenty. Na základě časového razítka jsme tedy schopni relativně s jistotou tvrdit, že dokument v okamžik orazítkování skutečně existoval a je tedy možné k tomuto okamžiku vyhodnocovat platnost podpisu z CRL seznamů z doby orazítkování.[192] Relativita je dána především faktem, že časová razítka jsou také založena na certifikátech a tedy i je může jednou postihnout problém kolizního dokumentu. Jejich certifikáty mají ovšem delší dobu platnosti, jelikož jsou opatřeny podpisem poskytovatele certifikačních služeb, který je založen na mnohem složitějším algoritmu.

Okamžik vzniku razítka jsme tedy schopni deklarovat pouze, pokud je platný i certifikát tohoto razítka. V případě, že se blíží okamžik exspirace certifikátu časového razítka, je v rámci zachování možnosti ověření podpisu nutné postupně v čase přerazítkovávat dokumenty před vypršením doby platnosti stávajícího časového razítka. Můžeme tak libovolně řetězit časová razítka, aniž bychom v čase ztratili možnost věrohodně tvrdit, že dokument v určitý minulý okamžik skutečně existoval. Zároveň je tím náš dokument chráněn proti kolizním dokumentům, jelikož aktuální časová razítka chrání nezměnitelnost starých podpisů a razítek.

Problém nastává ohledně již zmíněných CRL seznamů, které jsou po určité době nahrazovány aktuálnějšími verzemi, jak již bylo výše uvedeno. Staré CRL seznamy jsou sice stále zveřejněny a archivovány po určitou dobu, ovšem to nám nezajišťuje možnost, že v budoucnu budou tyto seznamy stále k dispozici.[193] Možnosti řešení se nabízejí v zásadě dvě – využití OCSP protokolu[194], který je schopen ověřit platnost certifikátu dotazem u poskytovatele k jakémukoliv datu, nebo podepisování pomocí rozšířených elektronických podpisů, které při podpisu k dokumentu přiloží aktuální CRL seznam a časové razítko[195].

---

[192] PETERKA, J. Proč elektronické podpisy nejsou věčné? e*Archiv.cz* [online]. 10.5.2010 [cit. 2012-02-12]. Dostupné z: <http://www.earchiv.cz/b10/b0510001.php3>.

[193] V současné době ani neexistují standardy, jak tyto archivované CRL seznamy zveřejňovat. Proto stávající ověřovací programy nejsou schopny automaticky ověřit platnost u podpisů kombinovaných s časovým razítkem, kde již CRL seznam není aktuální. Tento předpoklad neplatí při možnosti využití OCSP protokolu k ověření platnosti certifikátu nebo rozšířeného elektronického podpisu.

[194] Tento však u nás nevyužívá žádná z certifikačních autorit a Zákon to sám neukládá.

[195] Avšak již neřeší fakt, že záznamy mohou být v rámci českých certifikačních autorit do CRL seznamů přidány až s 24 hodinovým zpožděním. Například dle Rozporządzenie Rada Ministrów z dnia 7 sierpnia 2002, Dz.U.02.128.1094 (Polská republika), to může být až 48 hodin. Toto je třeba si uvědomit při práci s podpisem a také se podle toho patřičně zachovat.

3.5.1.2 Dokument opatřený elektronickým podpisem založeným na neplatném certifikátu

Žádný právní předpis českého právního řádu nestanoví, že elektronický podpis jako náležitost písemných právních úkonů musí být založen na platném kvalifikovaném certifikátu. Při obvyklém používání elektronického podpisu je patrné, že běžně používané programy sloužící k elektronickému podepisování například neumožňují podepsat dokument podpisem založeným na neplatném certifikátu. Není však vyloučeno, že by to nebylo možné.

Autor této práce však zastává názor, že s ohledem na požadavky stanovené Zákonem a technické řešení konceptu zaručených elektronických podpisů založených na technologii PKI a využívajících certifikáty, nelze platně podepsat písemný právní úkon elektronickým podpisem založeným na neplatném certifikátu, a to i kdyby to programové vybavení umožnovalo.[196]

V případě předčasně zneplatněných certifikátů tyto nemohou sloužit jako metoda k jednoznačnému ověření identity podepsané osoby, podobně jako běžné uvedení jména nemůže naplnit tento požadavek. Data pro vytváření byla již jednou kompromitována a je nerozhodné, zda je může k podepisování použít pouze osoba, která je neoprávněně zcizila, nebo více osob, kterým byly tyto data dále neoprávněně poskytnuty (například zpřístupněním těchto dat na veřejně dostupné internetové stránce). Dále takový podpis nesplňuje požadavek vytvoření a připojení zaručeného podpisu k datové zprávě pomocí, prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou, jelikož tyto prostředky již podepisující samozřejmě neudržela pod svou kontrolou a dále se za to nepochybně také zaručit nemůže.

U certifikátu, kterým vypršela doba platnosti, sice osoba tyto prostředky pod svou výhradní kontrolou udržet může, avšak problematickou se stává opět jednoznačnost ověření identity, kdy bychom vzhledem k výše uvedeným kolizním dokumentům museli posuzovat odstup, s jakým došlo k podepsání po vypršení platnosti certifikátu. Je zřejmé, že například 20 let od vypršení platnosti certifikátu nebude takový podpis sloužit jako metoda k jednoznačnému ověření identity podepsané osoby. Pokud bychom připustili opak, mohl by kdokoliv odejmout od jakéhokoliv dokumentu

[196] Opačný názor zastává například ČERMÁK, K. Elektronický podpis - pohled soukromoprávní. *Bulletin advokacie*. 2002, 11, 72 s.

elektronický podpis, který i mohl být v době svého vytvoření a ve vztahu k určité datové zprávě platně učiněn, a vytvořit k němu odpovídající kolizní dokument libovolného obsahu.

3.5.2 Omezení uvedená na certifikátu

Údaj o omezení platnosti certifikátu v čase není jediným údajem skýtajícím určité omezení. Je to však údaj, který má přímý vliv na platnost certifikátu. Ustanovení § 12 odst. 1 písm. i) a j) Zákona formulují další případná omezení, která však nemají přímý vliv na platnost certifikátu a jsou závislá především na požadavcích žadatele o certifikát. Z údaje o omezení použití kvalifikovaného certifikátu podle povahy a rozsahu jen pro určité použití a o omezení hodnot transakcí, pro něž lze kvalifikovaný certifikát použít, ovšem nevyplývá jakýkoli vliv přímý nebo nepřímý (vyplývající například z technického řešení elektronických podpisů) na platnost elektronického podpisu a písemného právního úkonu. Je tedy možné učinit závěr, že elektronickým podpisem založeným na takto omezeném certifikátu lze platně učinit písemný právní úkon.[197]

Při posuzování takového jednání je nezbytné vzít v úvahu, zda jde o běžný certifikát fyzické osoby, která k odlišení[198] svých certifikátů dle svého uvážení požádala při vydání certifikátu o uvedení omezení na něm, nebo zda jde o zaměstnanecký certifikát, v rámci kterého je nutné nejprve posoudit, zda jeho držitel jedná za právnickou osobu[199] uvedenou na certifikátu či jedná svým jménem bez vztahu k právnické osobě.

V případě fyzické osoby lze s přihlédnutím k existenci vůle, jejímu projevu a jejich výkladu usoudit, že osoba platně učinila písemný právní úkon. V potaz mohou pravděpodobně přicházet otázky týkající se omylu, jelikož osoba, která k jednání užila podpisu, jehož certifikát obsahuje určité údaje o omezení použití, měla k žádosti o zapsání těchto údajů do certifikátu zřejmě relevantní důvod. Ovšem ze samotného uvedení těchto údajů na certifikátu nelze predikovat neplatnost takového právního úkonu. To lze v tomto případě pouze ve vztahu k omylu.

V úvahu přichází ustanovení § 49a občanského zákoníku, z něhož je ovšem patrné, že neplatnost právního úkonu nastává pouze za předpokladu, že omyl spočíval

[197] ČERMÁK, K. Elektronický podpis - pohled soukromoprávní. *Bulletin advokacie*. 2002, 11, 72 s.

[198] Například z důvodů kvality a bezpečnosti jednotlivých klíčů a důvěry v daného poskytovatele.

[199] Tzv. zaměstnanecké certifikáty nemusejí být vázány pouze na pracovní poměr.

ve skutečnosti, jež je pro uskutečnění právního úkonu rozhodujícím a osoba, které byl právní úkon určen, tento omyl vyvolala nebo o něm musela vědět. V našem případě zřejmě nelze ani přepokládat, že by omyl v použití jiného soukromého klíče při vytváření elektronického podpisu byl způsoben adresátem právního úkonu. Možné je polemizovat o tom, zda o tomto omylu musel vědět adresát právního úkonu a vzdor tomu druhou stranu na omyl neupozornil. Tak jako tak je jisté, že takový omyl by nebylo možné považovat za podstatný.[200]

V případě právnické osoby k tomu přistupuje problematika vázanosti právnické osoby jednáním svých členů nebo pracovníků. Elektronické podpisy jsou ve vztahu k vlastnoručním specifické tím, že zaměstnanecký certifikát vždy obsahuje údaj o zaměstnavateli, resp. právnické osobě, avšak fyzická osoba držící data pro vytváření elektronického podpisu náležející k tomuto certifikátu je může používat i pro své soukromé účely.[201]

V rámci písemných úkonů opatřených vlastnoručním podpisem dochází zpravidla k uvedení jména a v případě jednání za právnickou osobu i názvu právnické osoby, resp. obchodní firmy, pod samotným podpisem. Na základě těchto údajů a vzhledem k celkovému výkladu právního úkonu lze následně přičítat určité jednání určité osobě, jak bylo uvedeno výše. Právě díky tomuto je u elektronických podpisů důraz na celkový výklad právních úkonů ve vztahu k přičítání jednání konkrétní osobě o to markantnější, jelikož zaměstnanecký certifikát obsahuje údaj o zaměstnavateli nebo právnické osobě vždy.

Dojdeme-li k závěru, že úkon je nutné přičítat fyzické osobě, nikoliv jako členu nebo zaměstnanci právnické osoby, je situace analogická jako v prvním případě fyzické osoby. Zřejmě zde nebude činit větší obtíže fakt, že na certifikátu jsou uvedená určitá

[200] Shodně k tomu ŠVESTKA, J.; SPÁČIL, J.; ŠKÁROVÁ, M.; HULMÁK, M. a kolektiv. *Občanský zákoník I, II*. 2. vydání. Praha : Nakladatelství C. H. Beck, 2009. 434-435 s.

[201] PETERKA, J. Datové schránky: komu patří podpis na e-dokumentu? VI. *Lupa.cz* [online]. 15.10.2009 [cit. 2012-02-20]. Dostupné z: <http://www.lupa.cz/clanky/datove-schranky-komu-patri-podpis/>. Na druhou stranu je otázkou, zda se nejedná o prostředek právnické osoby poskytnutý fyzické osobě jako členovi nebo zaměstnanci a do jaké míry je tento prostředek oprávněn využívat k soukromým účelům, jelikož smlouvu o poskytování certifikačních služeb s poskytovatelem uzavírá právě právnická osoba. Takové neoprávněné použití by ovšem nemělo vliv na platnost právního úkonu uzavřeného nikoliv ve vztahu k právnické osobě.

omezení, jelikož tyto byly patrně zapsány na základě žádosti právnické osoby, a tudíž se vztahují k jednání za právnickou osobu.

Je-li z výkladu patrné, že jednání nad rámec omezení uvedených na certifikátu bylo činěno za právnickou osobu bez ohledu, zda v zastoupení nebo jednáním jménem této osoby, je nutné použít příslušná ustanovení o přičítání jednání právnickým osobám, resp. podnikatelům dle obchodního zákoníku, a překročení zmocnění při tomto jednání. Ustanovení § 20 odst. 2 občanského zákoníku i ustanovení § 15 odst. 2 obchodního zákoníku stanoví shodně jeden z požadavků, a to že druhá strana nemohla vědět o překročení zmocnění pracovníka či člena právnické osoby, resp. zástupce podnikatele. Smlouvu o poskytování certifikačních služeb uzavírá s poskytovatelem daná právnická osoba, resp. podnikatel, a má tedy i vliv na uvedení případných omezení na certifikátu, které by měly reflektovat[202] omezení daná členovi nebo zaměstnanci při jednání za právnickou osobu, resp. podnikatele. Z předešlého je možné dovodit, že vzhledem k těmto údajům měl adresát úkonu možnost vědět o překročení zmocnění, proto by takové jednání nezavazovalo právnickou osobu, resp. podnikatele.

Opačný případ by mohl nastat v případě, kdy omezení byla na certifikátu uvedena například jen jako rozlišovací prostředek jednotlivých soukromých klíčů. V takovém případě však nelze druhé straně doporučit se na toto výhradně spoléhat.

V rámci soukromoprávního jednání je namístě připomenout, že podobně, jako tomu bylo u podpisů znějících na pseudonym, je i zde nutné dbát zvýšené obezřetnosti ve vztahu k jakýmkoliv omezením uvedeným na certifikátu.

[202] Nejlépe se s nimi přesně shodovat.

4. Možnosti zneužití a odpovědnostní vztahy

V rámci elektronického podepisování zvláště v dnešní době častých elektronických podvodů jsou odpovědnostní vztahy o to důležitější. Právní odpovědnost je jedním z druhů právních vztahů, které vznikají v důsledku porušení primární právní povinnosti. Porušením primární právní povinnosti vzniká nová sekundární povinnost sankční povahy. Je možné rozlišovat odpovědnost ústavněprávní, trestní, správní, disciplinární (veřejnoprávní povahy) a různé druhy soukromoprávní odpovědnosti (za škodu, z bezdůvodného obohacení, z prodlení, za vady atd.). [203]

Celý systém odpovědnostních vztahů je založen na posouzení dané skutové podstaty. Ta je souborem určitých náležitostí, kterými jsou nejobecněji objektivní a subjektivní stránka deliktu, objekt a subjekt. Subjektem je konkrétní osoba, která musí být způsobilá k protiprávnímu jednání a konkrétnímu druhu odpovědnosti. Subjektivní stránkou se rozumí zejména zavinění subjektu, což je psychický vztah subjektu k protiprávnímu jednání a jeho následku ve formě úmyslu nebo nedbalosti. Objektem je zákonem chráněný zájem, na kterém je protiprávním jednáním způsobena újma. Objektivní stránkou se rozumí samotné protiprávní jednání subjektu, které je v příčiné souvislosti se vzniklým škodlivým následkem. Ve vztahu k zavinění je možné rozlišovat subjektivní odpovědnost (za zaviněné protiprávní jednání) a objektivní odpovědnost (za škodlivý následek bez ohledu na zavinění).[204]

Zejména v Internetovém prostředí se pak můžeme setkat s tzv. kaskádovitou odpovědností jednotlivých subjektů. *„V zásadě se jedná o princip tzv. postupné odpovědnosti, kdy nemůže-li být shledán primárně odpovědný subjekt odpovědným (ať již z jakéhokoliv důvodu) hledá se sekundárně odpovědný. Takto bychom mohli horizontálně pokračovat dále a dále.“*[205]

V oblasti písemných právních úkonů podepsaných elektronickým podpisem přichází v úvahu zejména odpovědnost trestní, správní a soukromoprávní odpovědnost za škodu následujících subjektů:

---

[203] HENDRYCH, D. *Právnický slovník* [online]. 3.vydání. Praha : C. H. Beck, 2009 [cit. 2012-03-10]. Dostupné z: Databáze Beck-online.cz.

[204] Tamtéž.

[205] MATEJKA, J. *Právo IT - aktuální problémy a související rizika* [on-line]. [cit. 2012-03-02]. Dostupné z WWW: <http://www.slideshare.net/TUESDAY/matejka-web-reim-kompatibility>.

1) podepsané fyzické osoby (osoby, jejíž podpis je připojen k právnímu úkonu),
2) držitele certifikátu,
3) podepisující, resp. podepsavší, osoby (osoby, která skutečně připojila elektronický podpis k právnímu úkonu),
4) osoby, jejíž právní úkon byl podepsán a která může být rozdílná od předešlých osob;
5) poskytovatele certifikačních služeb,
6) třetí osoby, která není nikterak ve vztahu k výše uvedeným subjektům. [206]

4.1 Odpovědnost podepsané osoby

Podepsanou osobou se myslí podepisující osoba dle zákona, čili „*fyzická osoba, která má prostředek pro vytváření podpisu a jedná jménem svým nebo v zastoupení jiné fyzické či právnické osoby*“[207]. Jak již bylo uvedeno, skutečně podepisující osobou může být i osoba odlišná od podepsané osoby. Zákon pouze umožňuje potvrdit, že datová zpráva byla elektronicky podepsána prostřednictvím dat pro vytváření elektronických podpisů podepisující osoby a nikoli tedy to, že datovou zprávu skutečně podepsala podepisující osoba, o které předpokládáme, že tak učinila. Oproti tomu v případě vlastnoručního podpisu můžeme znalecky dokázat skutečnost, že určitý podpis učinila konkrétní osoba. Nejvýznamnější hrozbou tak pro elektronický podpis je zneužití dat pro vytváření elektronických podpisů.[208]

V rámci odpovědnostních vztahů je nutné rozlišovat mezi podepisující a podepsanou osobou. Pro potřeby této podkapitoly je užíváno terminologie zákona, tzn. podepsaná osoba je označena jako podepisující osoba.

Tato osoba je dle § 5 odst. 1 Zákona zejména povinna:

– „*zacházet s prostředky, jakož i s daty pro vytváření zaručeného elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití,*

[206] ČERMÁK, K. Elektronický podpis - pohled soukromoprávní. *Bulletin advokacie*. 2002, 11, 75 s.

[207] Ustanovení § 2 písm. e) Zákona.

[208] MATEJKA, J. *Elektronický podpis*: *Přednáška povinně volitelného předmětu FPR ZČU Internetové a počítačové právo*. Plzeň, 2009.

– *uvědomit neprodleně poskytovatele certifikačních služeb, který jí vydal kvalifikovaný certifikát, o tom, že hrozí nebezpečí zneužití jejích dat pro vytváření zaručeného elektronického podpisu“.*

Co se týče náležité péče, není příliš jasné, jaký v sobě zahrnuje rozsah ve vztahu k prostředkům[209] a k datům[210] pro vytváření elektronického podpisu. Legální definici neobsahuje žádný zákon, avšak lze se domnívat, že by měla odpovídat výše uvedeným povinnostem i potřebné odborné úrovni.[211]

Oznamovací povinnost k poskytovateli certifikačních služeb vzniká zejména, pokud vyvstane jakákoli byť sebemenší možnost hrozby nebezpečí zneužití dat pro vytváření zaručeného elektronického podpisu. Plnění povinnosti se vztahuje k okamžiku zjištění možnosti takové hrozby, a proto je nutné jej chápat subjektivně.[212]

Za škodu způsobenou porušením těchto povinností odpovídá podepisující osoba podle zvláštních právních předpisů. Těmito zvláštními právními předpisy se zejména myslí obecná ustanovení občanského zákoníku o odpovědnosti za škodu. Podepisující osoba se však může odpovědnosti zprostit, pokud prokáže, že ten komu vznikla škoda, neprovedl všechny úkony potřebné k tomu, aby si ověřil, že zaručený elektronický podpis je platný a jeho kvalifikovaný nebyl zneplatněn.[213]

Tato pravidla byla patrně stanovena na ochranu určité třetí osoby, která bude jednat s důvěrou v platnost právního úkonu, který však bude neplatný, jelikož došlo k použití dat pro vytváření elektronického podpisu proti vůli podepisující osoby. Typicky osobou jednající s důvěrou v platnost právního úkonu bude druhá strana smlouvy v rámci elektronické kontraktace. A právě na této osobě bude, aby prokázala, že podepisující osoba porušila, resp. nesplnila některou z výše uvedených povinností, a že existuje příčinná souvislost mezí porušením výše uvedených povinností a vznikem prokázané škody. Tato příčinná souvislost bude nejčastěji zprostředkována skrze neplatnost právního úkonu (typicky smlouvy) tím, že porušením povinností podepisující osoby byla způsobena neplatnost (např. nezajištěním dat pro vytváření elektronického

[209] Technické i programové vybavení pro vytváření elektronického podpisu.

[210] Jedinečné data přímo vytvářející elektronický podpis – soukromý klíč.

[211] MATEJKA, J. „Krádež“ elektronického podpisu, aneb s čím tvůrci zákona (ne)počítali? VI. *ITprávo* [online]. 15.10.2009 [cit. 2012-03-08]. Dostupné z: <http://www.itpravo.cz/index.shtml?x=49365>.

[212] Tamtéž.

[213] Ustanovení § 5 odst. 2 Zákona.

podpisu a jejich následným zneužitím), z čehož vznikla třetí osobě škoda.[214] V případě prokázání veškerých podstatných náležitostí pro vznik odpovědnosti by již bylo pouze na podepisující osobě, zda se dokáže odpovědnosti zprostit či nikoliv.

Škoda ovšem nemusí vzniknout pouze osobě, která důvěřuje v platnost právního úkonu, ale například i právnické osobě, jejímž jménem byla podepisující osoba oprávněna jednat. K tomu více v další podkapitole.

V rámci obchodního zákoníku přichází také v úvahu odpovědnost za škodu způsobenou neplatností právního úkonu dle § 268 obchodního zákoníku za předpokladu, že osoba, které byl právní úkon určen, o neplatnosti právního úkonu nevěděla. Odpovědnost podle obchodního zákoníku a odpovědnost podle ustanovení § 5 Zákona ve spojení s ustanovením § 420 a násl. občanského zákoníku obstojí vedle sebe, avšak v konkrétním případě mohou být splněny podmínky pro vznik odpovědnosti pouze z jednoho z těchto právních důvodů.[215]

Z trestněprávních odpovědnostních vztahů přichází v úvahu zejména trestný čin podvodu způsobený podepisující osobou s úmyslem obohatit se. Podepisující osoba může zejména:

- tvrdit, že se nepodepsala;
- tvrdit, že text byl zaměněn;
- tvrdit, že dokument, který podepsala dříve, vznikl až po zneplatnění dat pro vytváření elektronického podpisu, podepisující osoba následně odmítne odpovědnost za škodu;
- podepisující osoba zneplatní certifikát a začne plnit dříve, než poskytovatel certifikačních služeb vydá další CRL seznam, následně podepisující osoba odmítne odpovědnost za škodu;
- podepisující osoba na základě domluvy s druhou smluvní stranou zneplatní certifikát a druhá smluvní strana začne plnit dříve, než poskytovatel vydá další CRL seznam, tím je způsobena škoda, kterou strany vymáhají po poskytovateli certifikačních služeb.[216]

[214] ČERMÁK, K. Elektronický podpis - pohled soukromoprávní. *Bulletin advokacie*. 2002, 11, 75 s.

[215] Tamtéž, 76 s.

[216] MATEJKA, J. *Elektronický podpis*: *Přednáška povinně volitelného předmětu FPR ZČU Internetové a počítačové právo*. Plzeň, 2009.

V případě dvoustranných právních úkonů je dále potřeba upozornit na specifické možnosti zneužití druhou stranou, které v některých případech vyplývají ze skutečnosti, že právní úkon již byl podepsán jednou stranou. Druhá strana zejména může:

- tvrdit, že právní úkon podepsal někdo jiný (viz kapitola o přičítání projevu vůle konkrétní osobě);
- zaměnit část podepsaného právního úkonu;
- podepsat právní úkon, zneplatnit certifikát a následně tvrdit, že byl právní úkon podepsán po zneplatnění;
- získat data pro vytváření elektronických podpisů druhé smluvní strany po zneplatnění certifikátu a podepsat se za ní s cílem způsobit škodu tvrzením, že dokument byl podepsán před zneplatněním;
- podepisující osoba na základě domluvy s druhou smluvní stranou zneplatní certifikát a druhá smluvní strana začne plnit dříve, než poskytovatel vydá další CRL seznam, tím je způsobena škoda, kterou strany vymáhají po poskytovateli certifikačních služeb.[217]

4.2 Odpovědnost držitele certifikátu

Držitelem certifikátu je „*fyzická osoba, právnická osoba nebo organizační složka státu, která požádala o vydání kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu pro sebe nebo pro podepisující nebo označující osobu a které byl certifikát vydán*“.[218] Již ze samotného rozlišování mezi držitelem certifikátu a podepisující osobou, jak ji definuje Zákon, je patrné, že se nejedná o jednu a tutéž osobu, i když v praxi se o jednu osobu může jednat a velmi často i jedná. Právní věda tyto dvě osoby směšuje právě díky častému reálnému spojení v jedné osobě. Směšovány jsou následně i povinnosti těchto dvou osob, a tudíž i odpovědnostní vztahy plynoucí z těchto povinností.[219]

---

[217] MATEJKA, J. *Elektronický podpis*: *Přednáška povinně volitelného předmětu FPR ZČU Internetové a počítačové právo*. Plzeň, 2009.

[218] Ustanovení § 2 písm. g) Zákona.

[219] Příkladem může být ČERMÁK, K. Elektronický podpis - pohled soukromoprávní. *Bulletin advokacie*. 2002, 11, 75 s. MATEJKA, J. „Krádež“ elektronického podpisu, aneb s čím tvůrci zákona (ne)počítali? VI. *ITprávo* [online]. 15.10.2009 [cit. 2012-03-08]. Dostupné z: <http://www.itpravo.cz/index.shtml?x=49365>.

Ustanovením § 5b Zákona je dána držiteli certifikátu povinnost „*bez zbytečného odkladu podávat přesné, pravdivé a úplné informace poskytovateli certifikačních služeb ve vztahu ke kvalifikovanému certifikátu*“. Zákonodárce zde určitým způsobem znevýhodňuje nekvalifikované poskytovatele, jelikož tato povinnost se vztahuje pouze ke kvalifikovaným certifikátům.

Vzhledem k velmi široce pojaté odpovědnosti poskytovatele certifikačních služeb stanovené v ustanovení § 7 Zákona by však držitel certifikátu odpovídal za porušení výše uvedené povinnosti až sekundárně prostřednictvím následného postihu dle ustanovení § 440 občanského zákoníku v souvislosti s ustanovením § 420 občanského zákoníku. Odpovědnosti z informační povinnosti dle Zákona, ať již jako sekundární nebo jako chybně uváděné primární, se na rozdíl od povinností dle předchozí podkapitoly nelze zprostit prokázáním, že ten, komu vznikla škoda, neprovedl veškeré úkony k ověření, že elektronický podpis je platný nebo nebyl zneplatněn. V důsledku výše uvedeného chybného směšování je však často chybně uváděn opak.

Přichází zde v úvahu zejména odpovědnost za škodu dle obecného ustanovení § 420 občanského zákoníku, které se lze zprostit prokázáním, že škodu nezavinil držitel certifikátu.

V případě držitele certifikátu, který žádal o vydání tzv. zaměstnaneckého certifikátu, by pak mohl přicházet v úvahu následný postih dle ustanovení § 440 občanského zákoníku proti zaměstnanci nebo členovi právnické osoby, který uvedl nepřesné, nepravdivé nebo neúplné informace zaměstnavateli nebo právnické osobě. Následně lze tedy brát v úvahu i ustanovení o odpovědnosti za škodu v mezích pracovního práva.

4.3 Odpovědnost podepisující (podepsavší) osoby

Při posuzování odpovědnosti osoby, která skutečně právní úkon podepsala, tedy v případě, kdy je skutečně podepisující osoba rozdílná od podepsané osoby, je nutné posuzovat oprávněnost osoby používající data pro vytváření elektronického podpisu.

V případě sice oprávněného používání dat pro vytváření elektronického podpisu, avšak při současném překročení oprávnění jednat, se tato situace bude muset posuzovat jako překročení oprávnění z plné moci nebo jednání bez plné moci dle ustanovení § 33 občanského zákoníku. Může tak nastat trochu paradoxní situace, kdy na právním úkonu je podpis jiné osoby než, která je z jednání zavázána, pokud osoba podepisující

(podepisující ve smyslu Zákona, tj. zmocnitel) překročení neschválí dodatečně. Tehdy může osoba, se kterou bylo jednáno, na zmocněnci požadovat buď splnění závazku, nebo náhradu škody způsobené jeho jednáním.

Zákon sám výslovně nazakazuje ani nedefinuje neoprávněné použití dat pro vytváření elektronického podpisu. Lze však z účelu Zákona i v návaznosti na občanský zákoník dovodit, že neoprávněným použitím dat pro vytváření elektronického podpisu je „*jakékoliv takové použití, k němuž dochází buď jinak než se souhlasem podepisující osoby, nebo, byť i se souhlasem podepisující osoby, tak, že použití elektronického podpisu vyvolává omyl, typicky omyl o identitě jednající, případně podepsané osoby*“.[220]

Nejčastěji bude možné aplikovat soukromoprávní odpovědnost za škodu podle ustanovení § 420 občanského zákoníku. V rámci obchodního zákoníku přichází opět v úvahu odpovědnost za škodu způsobenou neplatností právního úkonu dle § 268 obchodního zákoníku. Podobně je stanovena odpovědnost za škodu pro neplatnost právního úkonu v ustanovení § 42 občanského zákoníku.

Z trestněprávní odpovědnosti je opět nasnadě skutková podstata trestného činu podvodu.

4.4 Odpovědnost osoby, jejíž právní úkon byl podepsán

U odpovědnosti osoby, jejíž právní úkon byl podepsán (osoby, za kterou jedná například zmocněnec a podepisuje se svým podpisem) je situace ohledně odpovědnostních vztahů, ať už veřejnoprávních nebo soukromoprávních, obdobná jako v předešlých případech. Přichází zde opět v úvahu obecná odpovědnost za škodu dle občanského zákoníku nebo odpovědnost za škodu způsobenou neplatností právního úkonu[221]. Ve zbylém lze odkázat na podkapitolu o přičítání projevu vůle a části o překročení zmocnění při jednání v zastoupení.

4.5 Odpovědnost poskytovatele certifikačních služeb

Z hlediska odpovědnostních vztahů je největšímu riziku vystaven právě poskytoval certifikačních služeb. Zejména kvalifikovaný poskytovatel certifikačních služeb odpovídá dle ustanovení § 7 odst. 1 Zákona za porušení jakékoliv povinnosti

[220] ČERMÁK, K. Elektronický podpis - pohled soukromoprávní. *Bulletin advokacie*. 2002, 11, 76 s.

[221] Ta působí velmi problematicky a není specifikem pouze právních úkonů činěných elektronicky, proto přesahuje hranice této práce.

stanovené Zákonem podle obecných pravidel občanskoprávních předpisů o odpovědnosti za škodu. Z tohoto ustanovení vzniká odpovědnost nejen za porušení povinností poskytovatelem, ale i za porušení povinností jakoukoli jinou osobou. Výjimku působí ustanovení § 5 odst. 2 Zákona.

Dále dle ustanovení § 7 odst. 2 Zákona poskytovatel neodpovídá za škodu vyplývající z použití kvalifikovaného certifikátu, která vznikla v důsledku nedodržení omezení pro jeho použití. Pravděpodobně se v tomto případě bude jednat o odpovědnost objektivní, kdy důkazní břemeno prokazující skutečnosti uvedené v ustanovení § 7 odst. 2 Zákona bude prokazovat právě poskytovatel certifikačních služeb.[222] Dle názoru autora je odpovědnost poskytovatele za škodu koncipovaná Zákonem příliš široce.

Řada soukromoprávních odpovědnostních vztahů může poskytovateli vyplynout i ze samotné smlouvy o poskytování certifikačních služeb mezi poskytovatelem a konkrétním subjektem. V úvahu přichází zejména odpovědnost za vady, jelikož poskytování certifikačních služeb má charakter plnění (jednorázových i opakujících se – ve vztahu ke konkrétním službám). Vadami plnění může být například vygenerování navzájem si neodpovídajících klíčů, chybné uvedení údajů na certifikátu, chybně uvedený časový údaj na časovém razítku atd. Z takto vadného plnění je poté možné uplatňovat nároky z odpovědnosti za následnou škodu. Při uplatňování nároků z odpovědnostních vztahů je také důležité upozornit na skutečnost, že poskytovatelé uvádějí do svých smluv o poskytování certifikačních služeb doložku o použití obchodního zákoníku ve smyslu ustanovení § 262 obchodního zákoníku.

Na kvalifikovaného poskytovatele certifikačních služeb se vztahuje mnoho povinností stanovených nejen Zákonem, ale i zákonem č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů. Z porušení těchto povinností vyplývá zejména odpovědnost za správní delikty[223] a za různé přestupky[224]. Poskytovatelé jsou také vázáni řadou předpisů upravujících podnikání a poskytování služeb spotřebitelům atd., které však nejsou typické pouze pro ně a za jejichž poručení mohou také nést odpovědnost.

Odpovědnostní vztahy mohou vznikat zejména z následujících možností zneužití nebo pochybení poskytovatele certifikačních služeb:

---

[222] ČERMÁK, K. Elektronický podpis - pohled soukromoprávní. *Bulletin advokacie*. 2002, 11, 76-77 s.

[223] Stanovené zejména v ustanoveních § 45-45a zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.

[224] Stanovené zejména v ustanovení § 18a Zákona.

- bezdůvodně zneplatní certifikát podepisující osoby;
- vytvoří certifikát pro neexistující osobu;
- zamění data uvedená na certifikátu;
- při generaci klíčů si ponechá data pro vytváření elektronických podpisů;
- nedodrží příslušné technické normy (zejména při generování klíčů);
- neuvede zneplatněný certifikát v CRL;
- zneužije osobní údaje podepisujících osob, k jejichž klíčům vystavil certifikát.[225]

Zejména v souvislosti s vytvořením certifikátu pro neexistující osobu plynou pro poskytovatele značná rizika. Přitom takový certifikát nemusí být vytvořen ani úmyslně poskytovatelem. Stačí, že poskytovatel svůj systém dostatečně nezabezpečí, resp. zanedbá požadavky na zabezpečení[226], a případný útočník si může certifikát vydat sám[227]. Následným jednáním by patrně škoda vznikla třetím subjektům spoléhajícím na údaje uvedené na certifikátu a dále také zcela jistě samotnému poskytovateli, který by poté mohl uplatňovat následný postih na případném útočníkovi. Ovšem zjištění totožnosti útočníka (i vzhledem k tomu, co bylo řečeno o digitální identitě) a následné dokazování by bylo zřejmě nemožné. Také by patrně nemohl uplatňovat náhradu jemu způsobené škody v celém rozsahu, jelikož ve většině případů by došlo k porušení povinností i na jeho straně, jelikož takový poskytovatel nezajistil odpovídající bezpečnostní opatření svého systému. Míra vzniklé škody přitom záleží nejen na množství takto vystavených certifikátů a jednotlivých případech použití těchto certifikátů, ale i na rychlosti reakce a přijatých opatřeních poskytovatele certifikačních služeb.

Výše popisované případy nejsou zcela ojedinělé. V roce 2011 se objevily dva konkrétní útoky na certifikační autority COMODO a DigiNotar. V daných případech se ovšem nejednalo o kvalifikované certifikáty, ale o certifikáty pro zabezpečení pomocí SSL technologie – komerční certifikáty pro server. Útočník si pro sebe vydal certifikáty

[225] MATEJKA, J. *Elektronický podpis*: *Přednáška povinně volitelného předmětu FPR ZČU Internetové a počítačové právo*. Plzeň, 2009.

[226] Především tak může porušit povinnost stanovenou v ustanovení § 6 odst. 1 písm. c) Zákona.

[227] Může si jich vydat i libovolné množství na libovolné subjekty, které již svůj certifikát mají, např. s cílem způsobit škodu určitým společnostem nebo konkurenci

internetových serverů společností jako Google, Yahoo, Skype, Microsoft. Primárním cílem útoků bylo získat důvěrná data uživatelů těchto serverů.[228]

Holandský poskytovatel DigiNotar, na rozdíl od COMODO, zareagovala opožděně a nedostatečně. V daném případě nestačí revokovat všechny vydané certifikáty v dostatečně krátké době.[229] Jelikož je řada certifikátů velkých internetových serverů ukládána do důvěryhodných úložišť programů, ve kterých dochází k ověřování totožnosti druhé strany, je nutné přijmout celou řadu dalších opatření, aby podvodné certifikáty nebyly dále zneužívány. DigiNotar ovšem celou situaci podcenil, proto následně přišel o akreditaci, což znamenalo jeho zánik.[230]

Průlom v bezpečnosti zahraničních kvalifikovaných poskytovatelů certifikačních služeb se však může dotýkat i českých subjektů, jelikož dle ustanovení § 16 odst. 1 Zákona se certifikátům od poskytovatelů certifikačních služeb usazených v některém z členských států Evropské unie, jiném smluvním státu Dohody o Evropském hospodářském prostoru nebo Švýcarské konfederaci přiznává stejné postavení jako českým kvalifikovaným certifikátům. Pro certifikáty vydané v jiných státech platí ustanovení § 16 odst. 2 Zákona. Situace může být obdobná i v rámci kvalifikovaných certifikátů.

4.6 Odpovědnost třetí osoby

Třetí osobou je zde míněna osoba odlišná od osoby podepisující ve smyslu Zákona, osoby skutečně připojující podpis, osoby důvěřující v údaje uvedené na certifikátu (typicky adresát právního úkonu), držitele certifikátu nebo certifikační autority.

Třetí osoba zpravidla jedná s cílem způsobit škodu dalším subjektům (například v rámci konkurenčního boje) nebo s cílem obohatit sebe. Zejména se může:

---

[228] PETERKA, J. Kauza DigiNotar, aneb: když certifikační autorita ztratí důvěru. *Lupa.cz* [online]. 20.09.2011 [cit. 2012-03-12]. Dostupné z: <http://www.lupa.cz/clanky/kauza-diginotar-aneb-kdyz-certifikacni-autorita-ztrati-duveru/>.

[229] Pokud je revokace zveřejňována pouze prostřednictvím CRL seznamů, je situace díky časové prodlevě o to horší.

[230] PETERKA, J. Kauza DigiNotar, aneb: když certifikační autorita ztratí důvěru. *Lupa.cz* [online]. 20.09.2011 [cit. 2012-03-12]. Dostupné z: <http://www.lupa.cz/clanky/kauza-diginotar-aneb-kdyz-certifikacni-autorita-ztrati-duveru/>.

- podepsat se za osobu, s jejímiž daty pro vytváření elektronického podpisu neoprávněně disponuje;
- zaměnit část podepsaného právního úkonu;
- získat data pro vytváření elektronického podpisu jiné osoby po zneplatnění certifikátu, podepsat právní úkon a následně tvrdit, že úkon byl podepsán před zneplatněním (s cílem poškodit osobu, na jejíž jméno zní certifikát);
- zneplatnit certifikát jiné osoby u poskytovatele certifikačních služeb;
- zachytit podepsaný dokument a odeslat ho opět později (s cílem poškodit jednající osobu nebo i adresáta)
- vydávat se za jinou osobu s cílem získat certifikát na tuto osobu u poskytovatele certifikačních služeb;
- získat cíleným počítačovým útokem nebo podvodem osobní údaje zákazníků poskytovatele;
- vystavit si prostřednictvím cíleného počítačového útoku libovolné množství certifikátů na existující či neexistující osoby;
- manipulací s daty a prostředky pro ověřování elektronického podpisu v úložišti důvěryhodných identit adresáta právního úkonu se vydávat za jinou osobu.[231]

Nejvýznamněji zde působí opět obecná odpovědnost za škodu a z trestněprávní odpovědnosti je nejčastěji naplněna skutková podstata trestného činu podvodu. Ve vztahu k veřejným listinám je nasnadě také naplnění skutkové podstaty trestného činu padělání a pozměnění veřejné listiny. V potaz také přichází počítačové trestné činy, zejména naplnění skutkové podstaty trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací dle ustanovení § 230 zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů (dále jen „trestní zákoník“), a skutkové podstaty trestného činu opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat dle ustanovení § 231 trestního zákoníku.

4.7 Zhodnocení bezpečnostních rizik a návrhy de lege ferenda

Jak bylo výše nastíněno, možnosti zneužití vlastnoručního i elektronického podpisu jsou závislé na charakteristikách, s jakými jsou vytvářeny.

[231] MATEJKA, J. *Elektronický podpis*: *Přednáška povinně volitelného předmětu FPR ZČU Internetové a počítačové právo*. Plzeň, 2009.

Vlastnoruční podpis je výsledkem určitého individuálního a relativně stálého písemného projevu jedince. Pravost vlastnoručního podpisu lze určit posudkem znalce v oboru písmoznalectví. Vyvstávají však určité problémy:

- osoba je individuálně identifikovatelná až od 13 let věku;
- pro určení pravosti podpisu je zapotřebí alespoň 10 nesporně pravých podpisů;
- písmoznalecké posudky nejsou příliš jednoznačné.[232]

V případě elektronického podpisu tyto problémy do jisté míry odpadají díky technické povaze těchto podpisů. Je však nemožné určit, resp. velmi těžko prokazatelné, že elektronický podpis připojila k právnímu úkonu konkrétní osoba. Ale je možné s relativně velkou jistotou tvrdit, že podpis byl vytvořen pomocí dat pro vytváření elektronického podpisu konkrétní osoby.

Ohledně funkce ověření integrity dokumentu jsou však výhody elektronického podpisu v současné době nesporné. V praxi jsou závislé na výpočetním výkonu dostupné techniky. Nárůst výpočetního výkonu ale přináší určité nevýhody v podobě aktivní péče o elektronicky podepsané dokumenty s cílem zachovat možnost ověření jejich platnosti (tzv. problém dlouhověkosti).

Bezpečnost elektronických podpisů je závislá na chování podepisující osoby (zejména na dispozici s prostředky a daty pro vytváření elektronického podpisu). Oproti tomu míra rizika vlastnoručního podpisu je ve vztahu k chování jeho nositele v zásadě neměnná. [233]

Pokud by elektronická kontraktace za současného využití elektronického podpisu zaznamenala do budoucna rozmach, bude na místě zrevidovat stávající úpravu obsaženou nejen v Zákoně, ale i v souvisejících předpisech. Především odpovědnostní vztahy si zaslouží pozornost. Například v arabském emirátu Dubaj hrozí peněžitý trest nebo trest odnětí svobody za použití certifikátu s vědomím, že obsahuje nepravdivé údaje[234], za uvedení poskytovatele certifikačních služeb v omyl při žádosti o certifikát nebo revokaci[235] nebo za porušení povinnosti mlčenlivosti k údajům svěřeným poskytovateli[236]. Zahraniční právní věda dokonce doporučuje zavedení

[232] Tamtéž.

[233] Tamtéž.

[234] Ustanovení článku 29 Electronic Transactions and Commerce Law No. 2/2002 (Dubai).

[235] Ustanovení článku 30 Electronic Transactions and Commerce Law No. 2/2002 (Dubai).

[236] Ustanovení článku 31 Electronic Transactions and Commerce Law No. 2/2002 (Dubai).

specializovaných soudů nebo rozhodčích orgánů pro řešení sporů z elektronických kontraktů.[237] Například Nepál má přímo ve svém zákonu o elektronických obchodech stanovenu věcnou příslušnost specializovaných IT tribunálů, které se zabývají řešením sporů z elektronických obchodů.[238] Dubajský zákon umožňuje alespoň ustanovit specializovanou rozhodčí komisy pro řešení těchto sporů.[239] Ovšem při současném velmi nízkém množství takto uzavíraných smluv a sporů z nich by působily takové soudy spíše nadbytečně. Otázkou zůstává, zda znalost problematiky v případě českých soudů je dostatečná a plně reflektuje její specifika. Stejně jako řadu sporů o doménová jména řeší Rozhodčí soud při Hospodářské komoře ČR a Agrární komoře ČR, mohl by spory z elektronických smluv fakultativně řešit obdobný rozhodčí orgán specializovaný na IT odvětví. Pochopitelně by svou roli dále hrála i soudní soustava. V případě nárůstu významu elektronických kontraktů by v úvahu mohlo přicházet i přenesení věcné příslušnosti pouze na krajské soudy.

Situace může být do budoucna o to vážnější, že český právní řád neobsahuje zákon o elektronických obchodech, který by odrážel zvláštnosti těchto obchodů, zejména pak problematiku rozhodného práva, kontraktační specifika, využití automatizovaných systémů při uzavírání smluv atd.

[237] BLYTHE, S. E. Fine-Tuning the E-commerce Law of the United Arab Emirates: Achieving the Most Secure Cyber Transactions in the Middle East. *International Journal of Business and Social Science*. 2010, 1, 169 s.

[238] Ustanovení § 60-64 Electronic Transaction Act, 2005 (Federativní demokratická republika Nepál).

[239] Ustanovení článku 37 Electronic Transactions and Commerce Law No. 2/2002 (Dubai).

5. Závěr

Elektronický podpis se za více než deset let vývoje v českém právním řádu stal jeho nepostradatelnou částí, která svoje opodstatnění nachází nejen ve sféře e-governmentu. Pro běžného občana České republiky je institut elektronického podpisu stále známější a právě při styku s veřejnou mocí je jím nejčastěji využíván. Stále však jeho využití nedosahuje takových rozměrů jako v jiných státech, kde není výjimkou i kontraktace pomocí tohoto institutu. Právě množství elektronických kontraktů uzavíraných pomocí elektronického podpisu je u nás zcela mizivé. Nasnadě je hned několik důvodů.

Z pohledu běžného občana je elektronický podpis technickým prostředkem, o kterém i přes určitou technologickou vyspělost smýšlí stále skepticky. Elektronický podpis nemusí být na dokumentu nijak vizuálně seznatelný, a přesto tam může být. Dále tento prostředek není výsledkem projevu individuality jedince, který by spojoval právě konkrétní osobu s daným dokumentem díky jasné stopě, kterou sama osoba svou tvořivou činností zanechala na tomto dokumentu. Východiskem mohou být biometrické podpisy, jejichž nevýhodou oproti běžně používané formě (kvalifikovanému elektronickému podpisu) je však poskytnutí citlivých údajů třetí osobě.

Z technického hlediska jsou elektronické podpisy na jednu stranu vhodné pro využití při distanční kontraktaci, avšak na druhou stranu díky tzv. problematice dlouhověkosti se nehodí pro dlouhodobější smlouvy. Právě časová omezenost certifikátů jako nutné technické omezení přináší požadavek aktivní péče o dokumenty s blížící se exspirací certifikátu. Požadavek aktivní péče pak představuje další náklady, což může být také jednou z nevýhod odůvodňující pomalý nástup využití elektronických podpisů při soukromoprávním jednání. Snahy o vyřešení problémů s dlouhověkostí certifikátů a z toho vyplývající možnost, resp. nemožnost, ověření platnosti podpisu jsou v tuto chvíli na počátku. Jsou definovány nejen nové technické standardy (např. AdES - Advanced Electronic Signatures), ale i právní normy, jejichž primárním cílem je toto negativum redukovat na únosnou míru. Teprve čas ukáže, zda tato opatření byla dostatečně účinná.

Elektronický podpis jako jedna z podstatných náležitostí písemných právních úkonů působí řadu problémů při posuzování platnosti těchto právních úkonů jako celku. Řada sporných otázek vyplývá nejen z výše uvedené problematiky dlouhověkosti, ale i

z tzv. zaměstnaneckých, neveřejných certifikátů nebo certifikátů na pseudonym ve vztahu k přičitatelnosti projevu vůle konkrétní osobě. Tyto certifikáty nelze vyloučit z podepisování písemných právních úkonů pouze na základě jejich výše uvedených odlišností, avšak lze doporučit zvýšenou obezřetnost při setkání s nimi, tedy alespoň s neveřejnými certifikáty nebo certifikáty na pseudonym.

Řada rizik se objevuje zejména při kontraktaci mezi smluvními stranami ze dvou odlišných států. Jsou zapříčiněny odlišnostmi ve zvoleném přístupu k elektronickému podpisu. Obdobná situace však může nastat i při kontraktaci mezi smluvními stranami ze států stejného legislativního přístupu k elektronickému podpisu, jelikož i mezi nimi se mohou objevit určité odlišnosti, zejména v rovnosti vlastnoručního podpisu a toho elektronického.

Odpovědnostní vztahy vyplývající z porušení povinností stanovených Zákonem a případně souvisejících předpisů jsou koncipovány velmi široce zejména ve vztahu ke kvalifikovaným poskytovatelům. Další subjekty, na které mohou dopadat odpovědnostní vztahy, odpovídají primárně za škodu. V potaz přichází také trestní odpovědnost. Bezpečnost celé struktury PKI není ovšem dokonalá, což žádná technologie v podstatě být nemůže, proto tedy primárně závisí na chování podepisující osoby. Oproti tomu míra rizika vlastnoručního podpisu je ve vztahu k chování jeho nositele v zásadě neměnná.

Z možných návrhů de lege ferenda lze mimo řešení výše uvedených otázek, které zatím nejsou nijak zásadně řešena nebo jejich řešení jsou v počátcích, dále zmínit úpravu znění konverzních doložek, zavedení povinného využívání OCSP protokolu[240], prostor v rámci elektronizace notářství[241], zrovnoprávnění elektronického podpisu s vlastnoručním, zavedení speciálního zákona o elektronických transakcích, který by plně reflektoval jejich specifika, a zavedení dalších skutkových podstat trestných činů ve vztahu ke zneužití elektronického podpisu.

Závěrem lze dodat, že i když elektronický podpis ušel již dlouhou cestu od jeho zavedení do různých právních řádů po celém světě, tak ho čeká cesta ještě mnohem delší a klikatější, která teprve ukáže jeho kvality či případné nedostatky, a to zejména v případě písemných soukromoprávních úkonů.

---

[240] Zejména k zamezení možným rizikům v souvislosti s prodlevou zveřejnění revokace poskytovatelem od jejího oznámení podepisující osobou.

[241] Možnost úředního ověřování elektronických podpisů.

Seznam použité literatury a pramenů

Knihy

BÍLEK, P.; DRÁPAL, L.; JINDRŘICH, M.; WAWERKA, K. *Notářský řád a řízení o dědictví.* 4. vydání. Praha : C. H. Beck, 2010. 1118 s.

BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi*. Olomouc : ANAG, 2008. 157 s.

DEFLEUR, M. L.; BALL-ROKEACH, S. *Theories of mass communication*. 5th Edition. New York : Longman, 1989. 368 s.

DRÁPAL, L.; BUREŠ, J. a kol. *Občanský soudní řád I, II. Komentář*. 1. vydání. Praha : Nakladatelství C. H. Beck, 2009. 1600 s.

FIALA, J.; KINDL, M. a kolektiv. *Občanský zákoník. Komentář.* Praha : Wolters Kluwer ČR, 2009. 1692 s.

FORD, W.; BAUM, M. S. *Secure electronic commerce: building the infrastructure for digital signatures and encryption*. New Jersey : Prentice Hall, 1997. 470 s.

GRAHAM, J. H. S. *Internet Law and Regulation.* London : Sweet & Maxwell, 2007. 1296 s.

HULMÁK, M. *Uzavírání smluv v civilním právu*. 1. vydání. Praha : Nakladatelství C. H. Beck, 2008. 2003 s.

KAILASH, N. G.; KAMALESH N. A.; PRATEEK A. A. *Digital Signature: Network Security Practices.* New Delhi : Prentice-Hall of India Pvt. Ltd., 2005. 209 s.

KOHL, U. *Jurisdiction and the Internet: A Study of Regulatory Competence Over Online Activity.* Cambridge : Cambridge University Press, 2007. 323 s.

LABORDE, C. M. *Electronic Signatures in International Contracts*. Frankfurt am Main : Peter Lang, 2010. 249 s.

NICHOLAS, B. *An Introduction to Roman Law*. Oxford : Clarendon Press, 1962. 272 s.

POLČÁK, R. *Právo a evropská informační společnost.* Brno : Masarykova univerzita, 2009. 203 s.

POSTGATE, J. N. *Early Mesopotamia - Society and Economy at the Dawn of History*. New York : Routledge, 1992. 367 s.

RAK, R.; MATYÁŠ, V.; ŘÍHA, Z. a kol. *Biometrie a identita člověka.* Praha : Grada Publishing a.s., 2008. 631 s.

REBEL, T. F.; DARGE, O.; KOENIG, W. Approaches of Digital Signature Legislation. In LAMERSDORF, W.; MERZ, M. *Trends in Distributed Systems for Electronic Commerce, International IFIP/GI Working Conference TREC'98 Hamburg, Germany, June 3–5, 1998 Proceedings*. Heidelberg : Springer, 2003. s. 39-51.

REED, Ch. *Internet Law: Text and Materials*. Second Edition. Cambridge : Cambridge University Press, 2004. 329 s.

SAMPSON, G. *Writing Systems: A Linguistic Introduction*. Stanford : Stanford University Press, 1985. 234 s.

SCHELLEKENS, M. *Electronic Signatures: Authentication Technology from a Legal Perspective. Information technology & law series.* Haag : T.M.C. Asser Press, 2004. 150 s.

SCHMEH, K. *Cryptography and Public Key Infrastructure on the Internet.* West Sussex : Wiley, 2003. 343 s.

ŠVESTKA, J.; DVOŘÁK, J. *Občanské právo hmotné 1.* Praha : Wolters Kluwer Česká republika, 2009. 459 s.

ŠVESTKA, J.; SPÁČIL, J.; ŠKÁROVÁ, M.; HULMÁK, M. a kolektiv. *Občanský zákoník I, II*. 2. vydání. Praha : Nakladatelství C. H. Beck, 2009. 2321 s.

Časopisy

BLYTHE, S. E. Fine-Tuning the E-commerce Law of the United Arab Emirates: Achieving the Most Secure Cyber Transactions in the Middle East. *International Journal of Business and Social Science*. 2010, 1, 163-172 s.

ČERMÁK, K. Elektronický podpis - pohled soukromoprávní. *Bulletin advokacie*. 2002, 11, 64-77 s.

DAVIES, S. Computer Program Claims: The Final Frontier for Software. *European Intellectual Property Review*. 1998, 20, 429-433 s.

ELIÁŠ, K. Právní úkony na soukromých listinách se zvláštním zřetelem k jejich podepisování. *Ad Notam*. 1996, 3, 52-59 s.

HULMÁK, M. Elektronický právní styk. *Právní rozhledy*. 2005, 7, 229-234 s.

LEKKAS, D.; GRITZALIS, S.; MITROU, L. Withdrawing a declaration of will: Towards a framework for digital signature revocation. *Internet Research.* 2005, 4, 400-420 s.

LENG, T. K. Have you signed your electronic contract? *Computer Law & Security Review.* 2011, 27, 75-82 s.

LINCOLN, A. Electronic Signature Laws and the Need for Uniformity in the Global Market. *The Journal of Small and Emerging Business Law.* 2004, 8, 67-86 s.

MASON, S. Electronic Signatures in Practice. *Jounal of High Technology Law*. 2006, 2, 148-163 s.

MATEJKA, J.; CHUM, V. K právní úpravě elektronického podpisu. *Bulletin advokacie*. 2002, 3, 27-41 s.

MOJŽÍŠ, M. S kvalifikovaným certifikátem raději necestujte. *Lupa.cz* [online]. 26.01.2005 [cit. 2012-03-02]. Dostupné z: <http://www.lupa.cz/clanky/s-kvalifikovanym-certifikatem-radeji-necestujte/>.

PETERKA, J.; PODANÝ, J. Problematika elektronické podpisu v soudní praxi. *Právní rozhledy*. 2010, 19, 689-700 s.

SOKOL, T. Ještě k elektronickému dokumentu. *Bulletin advokacie*. 2002, 13, 3, 42-46 s.

SOKOL, T. Podpis, jeho podstata a role při právních úkonech. *Právní rádce*. 2004, 12, 4-8. s.

SPÁČIL, J. Vážná vůle jako základní náležitost právního úkonu v právní vědě a v judikatuře. *Právní rozhledy.* 2004, 22, 811-815 s.

Internetové zdroje

APCS eIdentity a.s. Dostupné z: <http://www.acaeid.cz >.

Bundesnetzagentur. Dostupné z WWW: <http://www.bundesnetzagentur.de>.

Certifikační autorita PostSignum. Dostupné z: <http://www.postsignum.cz>.

HENDRYCH, D. *Právnický slovník* [online]. 3.vydání. Praha : Nakladatelství C. H. Beck, 2009 [cit. 2012-03-10]. Dostupné z: Databáze Beck-online.cz.

I.CA. Dostupné z: <http://www.ica.cz>.

Internet X.509 Public Key Infrastructure Qualified Certificates Profile. *Internet FAQ Archives* [online]. [cit. 2012-03-02]. Dostupné z: <http://www.faqs.org/rfcs/rfc3039.html>.

KUNER, Ch.; MIEDBRODT, A. *Christopher Kuner, Attorney-at-Law* [online]. c2005 [cit. 2011-11-16]. Written Signature Requirements and Electronic Authentication: A Comparative Perspective. Dostupné z WWW: <http://www.kuner.com/data/articles/signature_perspective.html>.

MATEJKA, J. „Krádež“ elektronického podpisu, aneb s čím tvůrci zákona (ne)počítali? VI. *ITprávo* [online]. 15.10.2009 [cit. 2012-03-08]. Dostupné z: <http://www.itpravo.cz/index.shtml?x=49365>.

MATEJKA, J. *Právo IT - aktuální problémy a související rizika* [on-line]. [cit. 2012-03-02]. Dostupné z WWW: <http://www.slideshare.net/TUESDAY/matejka-web-reim-kompatibility>.

Ministerstvo vnitra České republiky. Dostupné z: <http://www.mvcr.cz/ >.

PETERKA, J. *Báječný svět elektronického podpisu* [online]. 2010 [cit. 2011-11-19]. Dostupné z WWW: <http://bajecnysvet.cz/>.

PETERKA, J. Datové schránky: když už ani časové razítko nepomůže. e*Archiv.cz* [online]. 4.10.2010 [cit. 2012-02-12]. Dostupné z: <http://www.earchiv.cz/b10/b1004001.php3>.

PETERKA, J. Datové schránky: komu patří podpis na e-dokumentu? VI. *Lupa.cz* [online]. 15.10.2009 [cit. 2012-02-20]. Dostupné z: <http://www.lupa.cz/clanky/datove-schranky-komu-patri-podpis/>.

PETERKA, J. Elektronický podpis na rozcestí. e*Archiv.cz* [online]. 6.6.2011 [cit. 2012-02-12]. Dostupné z: < http://www.earchiv.cz/b11/b0606001.php3>.

PETERKA, J. Kauza DigiNotar, aneb: když certifikační autorita ztratí důvěru. *Lupa.cz* [online]. 20.09.2011 [cit. 2012-03-12]. Dostupné z: <http://www.lupa.cz/clanky/kauza-diginotar-aneb-kdyz-certifikacni-autorita-ztrati-duveru/>.

PETERKA, J. Proč elektronické podpisy nejsou věčné? e*Archiv.cz* [online]. 10.5.2010 [cit. 2012-02-12]. Dostupné z: <http://www.earchiv.cz/b10/b0510001.php3>.

SMEDINGHOFF, T. J.; BRO, R. H. *FindLaw* [online]. 1999 [cit. 2011-10-21]. Electronic Signature Legislation. Dostupné z WWW: <http://library.findlaw.com/1999/Jan/1/241481.html>.

Soudní rozhodnutí

American Multimedia Inc. v. Dalton Packaging, Inc., 143 Misc. 2d 295 (N.Y. Sup. Ct. 1989).

Baker v. Dening, 8 A&E 94 (1838).

Barrletts de Reya v. Bryne, 127 SJ 69 (1983).

Bazak International Corp. v. Mast Industries, Inc., 535 N.E.2d 633 (N.Y. 1989).

Berdan v Berdan, 39 Cal App 2d 478 (1940).

Brydges v. Dix, 7 TLR 215 (1891); France v. Dutton, 2 Q.B. 208 (1891); Newborne v. Sensolid (Great Britain), Ltd., 1 QB 45 (1954).

Cloud Corp. v. Hasbro, Inc., 314 F.3d 289 (7th Cir. 2002).

Clyburn v. Allstate, 826 F.Supp. 955 (D.S.C. 1993).

Cohen v. Roche, 1 KB 169 (1927).

Ellis Canning Co. v. Bernstein, 348 F. Supp. 1212 (D. Colo. 1972).

Goodman v. J. Eban Ltd., 1 QB 550 (1954).

Hall v. Cognos Limited, Hull Industrial Tribunal Case No. 1803325/97.

Harrison v. Harrison, 8 Ves Jun 185, 32 ER 324 (1803).

Hill v. Hill, Ch 231 (1947).

Howley v. Whipple, 48 N.H. 487 (1869).

Chalcraft v. Giles, P 222 (1948).

Joseph Denunzio Fruit Co. v. Crane, 79 F. Supp. 117.

Kilday v Schancupp 91 Conn 29 (1916).

Lazarus Estates, Ltd. v. Beasley, 1 QB 702 (1956).

Lobb and Knight v. Stanley, 5 QB 574, 114 ER 1366 (1844).

London County Council v. Vitamins, Ltd., London County Council v. Agricultural Food Products, Ltd., 2 QB 218 (1955).

McGuven v Simpson NSWSC 35 (2004).

McNear v Petroleum Export Corp 280 P 684.

Murison v. Cook, 1 All ER 689 (1960).

On Line Power Tech., Inc. v. Squared D Company, 2004 WL 1171405 (S.D.N.Y.).

People v. Avila, 770 P.2d 1330 (Colo. Ct. App. 1988).

Phillimore v. Barry, 1 Camp 512, 170 ER 1040 (1808).

Reddings Goods, 14 Jur 1052, 2 Rob. Ecc. 338 (1850).

Roger Edwards, LLC. v. Fiddes & Son Ltd., 245 F. Supp. 2d 251 (D. Me. 2003).

Roos v. Aloi, 127 Misc. 2d 864 (N.Y. Sup. Ct. 1985).

Rosenfeld v Zerneck 776 NYS2d 458.

Rozhodnutí Nejvyššího soudu ČSR ze dne 27.1.1983, sp. zn. 4 Cz 82/82, uveřejněné ve Sbírce soudních rozhodnutí a stanovisek pod č. 51/1984.

Rozhodnutí Nejvyššího soudu ze dne 17.11.1998, sp.zn. 21 Cdo 586/98, uveřejněné ve Sbírce soudních rozhodnutí a stanovisek pod č. 44/1999.

Rozhodnutí Nejvyššího soudu ze dne 31.03.2009, sp. zn. 21 Cdo 51/2008, uveřejněné ve Sbírce soudních rozhodnutí a stanovisek pod č. 13/2010.

Rozhodnutí Nejvyššího soudu ze dne 5. 9. 2000, sp. zn. 30 Cdo 2781/99, uveřejněné ve Sbírce soudních rozhodnutí a stanovisek pod č. 11/2003.

Rozhodnutí Ústavního soudu ze dne 24.4.2006, sp. zn. IV. ÚS 319/05.

Rozhodnutí Vrchního soudu v Praze ze dne 1011.1994, sp. zn. 5 Cmo 179/94.

Sea-Land Serv., Inc. v. Lozen Int'l, LLC., 285 F.3d 808 (9th Cir. 2002).

Selby v. Selby, 3 Mer 2, 36 ER 1.

Shattuck v. Klotzbach, 14 Mass. L. Rptr. 360 (Mass. Super. Ct. 2001).

SM Integrated Transware Pte Ltd. v. Schenker Singapore (Pte) Ltd., [2005] SGHC 58.

Právní předpisy

Digitaalallkirja seadus, 2000 (Estonská republika).

Digital Signature Act, 1995 (Utah).

Electronic Communications Act, 2000 (Velká Británie).

Electronic Signatures in Global and National Commerce Act, 2000 (USA).

Electronic Transaction Act, 2005 (Federativní demokratická republika Nepál).

Electronic Transactions Act, 1998 (Republika Singapur).

Electronic Transactions Act, 1999, c. 2 (Austrálie).

Electronic Transactions and Commerce Law No. 2/2002 (Dubai).

General Usage for International Digitally Ensured Commerce (GUIDEC).

Gesetz über Rahmenbedingungen für elektronische Signaturen (Spolková republika Německo).

Ley De Firma Digital. No. 25.506 (Argentinská republika).

Nařízení Evropského parlamentu a Rady č. 593/2008 o právu rozhodném pro smluvní závazkové vztahy (Řím I).

Nařízení Evropského parlamentu a Rady č. 864/2007 o právu rozhodném pro mimosmluvní závazkové vztahy (Řím II),

Nařízení Rady č. 1347/2000 o příslušnosti a uznávání a výkonu rozhodnutí ve věcech manželských a ve věcech rodičovské zodpovědnosti obou manželů k dětem (Brusel II).

Nařízením Rady č. 44/2001 o příslušnosti a uznávání a výkonu soudních rozhodnutí v občanských a obchodních věcech (Brusel I).

Návrh občanského zákoníku schválený Poslaneckou sněmovnou Parlamentu ČR.

Obecný zákoník občanský, vyhlášený císařským patentem ze dne 1.6.1811, č. 946 Sb. z. s.

Rozporządzenie Rada Ministrów z dnia 7 sierpnia 2002, Dz.U.02.128.1094 (Polská republika).

Směrnice Evropského parlamentu a Rady 1999/93/ES, o zásadách Společenství pro elektronické podpisy, ze dne 13. prosince 1999.

Směrnice Evropského parlamentu a Rady č. 2000/31/ES, o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu, ze dne z 8. června 2000.

The Uniform Electronic Commerce Act, 1999 (Kanada).

Úmluva OSN o užití elektronických sdělovacích prostředků v mezinárodním obchodu (ECC).

UNCITRAL Model Law on Electronic Commerce (1996).

UNCITRAL Model Law on Electronic Signature (2001).

Uniform Electronic Transactions Act, 1999 (USA).

Usnesení představenstva České advokátní komory č. 4/2006 Věstníku.

Vyhláška č. 496/2004 Sb., o elektronických podatelnách.

Vyhláška č. 538/2002 Z. z., o formáte a obsahu kvalifikovaného certifikátu, o správe kvalifikovaných certifikátov a o formáte, periodicite a spôsobe vydávania zoznamu zrušených kvalifikovaných certifikátov.

Zákon 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů.

Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.

Zákon č. 11/1918 Sb., o zřízení samostatného státu československého.

Zákon č. 141/1950 Sb., občanský zákoník.

Zákon č. 215/2002 Z. z., o elektronickom podpise a o zmene a doplnení niektorých zákonov, ve znění pozdějších předpisů (Slovenská republika).

Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů.

Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů

Zákon č. 352/1992 Sb., o notářích a jejich činnosti, ve znění pozdějších předpisů.

Zákon č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů.

Zákon č. 440/2004 Sb., kterým se mění zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů.

Zákon č. 85/1996 Sb., o advokacii, ve znění pozdějších předpisů.

Ostatní zdroje

Důvodová zpráva k návrhu zákona o elektronickém podpisu a o změně některých dalších zákonů.

MATEJKA, J. Elektronický podpis: Přednáška povinně volitelného předmětu FPR ZČU Internetové a počítačové právo. Plzeň, 2009.

Přílohy

Příloha č. 1: Návrh znění části rámcové smlouvy stanovující pravidla pro uzavírání dílčích smluv.

Smluvní strany si touto Rámcovou smlouvou stanovují ve vztahu k uzavírání Dílčích smluv tyto pravidla:

a) Návrh Dílčí smlouvy (dále jen „Návrh“) musí být odeslán druhé Smluvní straně prostřednictvím elektronické pošty na adresu osoby oprávněné jednat za druhou Smluvní stranu, a to konkrétně osobě a na adresu elektronické pošty uvedenou v záhlaví této Rámcové smlouvy.

b) Jako poslední část návrhu Dílčí smlouvy musí Smluvní strana v pozici navrhovatele uvést následující tučně vyznačenou frázi uvnitř uvozovek a s přesným zachováním malých a velkých písmen: „**7N$D09Gz&nC4m81**“ (dále jen „Podpis“). Smluvní strany ve vztahu k Dílčím smlouvám považují Podpis za elektronický podpis dle zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů.

c) Smluvní strana v pozici adresáta návrhu je povinna oznámit druhé Smluvní straně přijetí Návrhu nejpozději do pěti (5) pracovních dnů od přijetí Návrhu a pod tímto oznámením uvést Podpis (dále jen „Přijetí Návrhu“).

d) Dílčí smlouva je uzavřena okamžikem doručení Přijetí Návrhu do schránky elektronické pošty Smluvní strany v pozici navrhovatele.

e) Smluvní strany jsou povinny zacházet s Podpisem s náležitou péčí, zejména aby nemohlo dojít k jeho neoprávněnému použití, a dále zachovávat mlčenlivost o Podpisu ve vztahu ke třetím osobám (dále jen „Závazek náležité péče“).

f) Smluvní strany jsou povinny bez zbytečného dokladu uvědomit druhou Smluvní stranu (dále jen „Oznámení“) v případě, že byl porušen Závazek náležité péče, nebo v případě, že lze důvodně předpokládat, že se znění Podpisu dověděla třetí osoba.

g) Jakákoli Dílčí smlouva uzavřená poté, co bylo učiněno Oznámení, je považována za neplatnou od počátku. Další Dílčí smlouvy mohou být

platně uzavřeny až poté, co strany nahradí Podpis novým podpisem skládajícím se alespoň z patnácti (15) znaků, které budou obsahovat alespoň jedno velké písmeno, jedno malé písmeno, jednu číslici a jeden jakýkoli symbol jiné znakové sady a budou uspořádány tak, aby v celku nedávaly žádné plnovýznamové slovo z českého ani jiného jazyka (dále jen „Nový podpis“).

h) Závazek náležité péče a další z něj vyplývající povinnosti platí obdobně i pro Nový podpis.

i) Pro uzavírání Dílčích smluv se v případech, kdy tato Rámcová smlouva nestanoví jinak, užijí příslušná ustanovení zákona č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů, a zákona 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů.

Cizojazyčné resumé

The electronic signature has become an essential part of the Czech legal order for more than ten years of its development. It finds legitimation not only in the sphere of e-government. For ordinary citizen of the Czech Republic, institute of electronic signature becomes more and more known and it is used in communication with the public authorities in most cases. Still, its use does not reach such proportions as in the other states, where are no exceptions in contracting with this legal institute. The number of electronic contracts concluded using an electronic signature is infinitesimal in the Czech Republic. The reasons are obvious.

From the perspective of the ordinary citizen, electronic signature is still a technical device, about which the citizen is thinking skeptically despite its technological maturity. The electronic signature may not be visually perceptible on the document and it can be there still. Furthermore, it is not the result of expression of individuality, it is result of technical procedure. The starting point could be a biometric signature, which disadvantage is providing of confidential data to third party.

From a technical point of view, electronic signatures are suitable for distance contracts on one side, but on the other side it is not suitable for long-term contracts thanks to the longevity issue. It is time limitations of certificates, which requires active care of documents with the approaching expiration of the certificate. Therefore, active care requirement represents an additional cost, which could be one of the disadvantages. This disadvantage is justifying slow onset of the use of electronic signatures in contract negotiations. Efforts to resolve problems with longevity of certificates and the consequent possibility or impossibility of verifying the signature are at the beginning at this moment. New technical standards (e.g. Ades - Advanced Electronic Signatures), as well as legal standards, are going through approval procedure, which has primary objective to reduce this negative aspect to a tolerable level. Time will show us, whether these measures were sufficiently effective.

The electronic signature, as one of the essential requirements of legal acts in written form, causes a number of problems with considering the validity of such legal acts as a whole. A number of problems arise from the above-mentioned issues of longevity, but

also from the employee certificates, non-public certificates or the pseudonym certificates in relation to attribution of expression of will to specific person.

Among possible proposals *de lege ferenda*, it can be mentioned the formulation of the authorized conversion clauses, mandatory use of the OCSP protocol, giving ample scope to the e-notary, equalization electronic signature and handwritten signature, passing an act on the electronic transactions and passing new crimes to the Criminal code about unauthorized use of the electronic signature.

Finally, it can be noted that while the electronic signature has gone a long way since it's passing in various jurisdictions around the world, so the journey will be much longer and more tortuous and will show the qualities or potential weaknesses of the electronic signature.