UNIVERZITA KARLOVA

PRÁVNICKÁ FAKULTA

Mgr. Ing. Vojtěch KMENT

Elektronické právní jednání

Srovnávací analýza s důrazem na využití elektronického podpisu podle práva EU, České republiky a Německa

Disertační práce

Školitel: doc. JUDr. Karel Beran, Ph.D.
Studijní program: Teoretické právní vědy
Datum vypracování práce: (uzavření rukopisu) 18. května 2018

Prohlašuji, že jsem předkládanou disertační práci vypracoval samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 1 095 789 znaků včetně mezer.[‡]

V Praze dne: *25. května 2018* Podpis: ……..

Mgr. Ing. Vojtěch Kment

[‡] Počet uvedených znaků byl shodně zjištěn softwarem Microsoft® Word 2000 (9.0.6926 SP-3) a softwarem Microsoft® Office Word 2007 (12.0.6787.5000) SP3 MSO (12.0.6785.5000) tak, že z konečné verze práce v elektronickém dokumentu formátu *.doc* (Word 97–2003) byl vytvořen zvláštní účelový soubor, který sestává výlučně z textu kapitol 1 až 11 této práce, bez využití funkcí revizí, změn a komentářů. V prohlášení uvedená hodnota odpovídá údaji pro tento soubor:
- „Characters (with spaces)“ při aktivaci „Include footnotes and endnotes“ resp.
- „Znaky (včetně mezer)“ při aktivaci „Včetně textových polí, poznámek pod čarou a vysvětlivek“.

Vzor citace dle ČSN ISO 960:

KMENT, Vojtěch. *Elektronické právní jednání: Srovnávací analýza s důrazem na využití elektronického podpisu podle práva EU, České republiky a Německa*. Praha: Univerzita Karlova, 2018. 495 s. Vedoucí práce Karel Beran.

KMENT, Vojtěch. *Elektronické právní jednání: Srovnávací analýza s důrazem na využití elektronického podpisu podle práva EU, České republiky a Německa [Electronic Legal Transaction: Comparative analysis with emphasis on the use of electronic signature under the EU law and laws of the Czech Republic and Germany]*. Prague: Charles University, 2018. 495 p. Supervisor Karel Beran.

Tato disertační práce vznikla za částečné finanční podpory Grantové agentury České republiky v rámci řešení grantového projektu GA ČR reg. č. 16-22016S „Právní jednání a odpovědnost právnických osob.“

Obsah

Tato strana je záměrně ponechána prázdná.

Předmluva

Není posláním předmluv podat obsah či akademický abstrakt[1] textu, ale spíše vyjádřit autorovo subjektivní hledisko a osobní vztah k tématu díla, nebo ozřejmit historii vývoje. Základní meze této práce byly vytyčeny rámcovým tématem *elektronického právního jednání* v disertačním projektu. Samotný projekt již však předpokládal, že v rámci tématu dojde k soustředění na některou dílčí problematiku, u které bude moci dojít ke zkoumání právně čerstvých nebo nových jevů.

Zaměřením této práce je srovnávací analýza elektronického právního jednání podle práva EU, ČR a Německa, s důrazem na využití vyšších verzí elektronického podpisu, jejichž úprava vyplývá především z nedávno účinného evropského nařízení (EU) č. 910/2014 Sb., označovaného zkratkou eIDAS, a jejíž vrchol představuje takzvaný *kvalifikovaný elektronický podpis*. Faktická koncepce kvalifikovaného elektronického podpisu ovšem nová není, byla založena již dřívější směrnicí 1999/93/ES (v práci označovanou DirES). Je to právě jeho koncepční základ takzvané infrastruktury veřejného klíče, který představuje komplexní výzvu. Ta spočívá v tom, zda lze splnit nejen abstraktní kryptografické modely, jež jsou považovány za silnou kryptografii a samy o sobě za teoreticky odolné, ale i jejich předpoklady. Ty zahrnují jednak bezchybnou a nesnadno prolomitelnou implementaci v elektronických zařízeních informační technologie, tak i organizační a právní navázání na fyzické osoby takovým způsobem, aby vzniklé digitální záznamy, zajištěné digitálním podpisem, bylo možné právně spolehlivě přičítat určité osobě jako výsledek její záměrné činnosti, tj. i jako její právní jednání. Celý tento koncepční základ se za účinnosti DirES vhodně označoval jako *rámec [framework] elektronického podpisu*, zatímco v novém nařízení eIDAS jako *služby vytvářející důvěru*.

Podstatným požadavkem DirES na zaručený (*advanced*) a potažmo i na kvalifikovaný elektronický podpis bylo, že musel být *vytvořen s využitím prostředků, které podepisující osoba mohla mít plně pod svou kontrolou (means ... under ... sole control)*. Transpozice DirES v právně a technicky rozvinutých státech jako Německo pak směřovala ke dvěma cílům. Prvním bylo, aby rámec elektronického podpisu zajišťoval podepisujícím osobám skutečný *trh* různých produktů, prostředků a služeb, ze kterých by si podepisující osoba mohla svobodně vybrat. Druhým cílem bylo, aby

[1] Pro rychlé zjištění právně akademického obsahu práce doporučuji samotný *abstrakt* (s. 475), popř. jeho sekci *závěrů* (s. 480) či určení *původních poznatků* (s. 481).

uvedené produkty, prostředky a služby všechny prošly nezávislou *předchozí kontrolou* ohledně toho, zda skutečně plní právní a v posledku všechny technické požadavky implementace kryptografie. Nejen oči a slib výrobce, ale i další nezávislé oči technické zkušebny, bezpečnostního auditora nebo dohledového úřadu byly předpokladem *kvalifikace* pro finální použití.

Tvorba systémů informačních technologii představuje výzvu již sama o sobě, rychlost inovací oboru pak i pro právo IT. Při návrhu a tvorbě prostředků IT, které implementují silnou kryptografii, se požadavky ale kvalitativně gradují. Již vůbec nedostačuje jakkoli rozsáhlé funkční testování, které si běžně může zajistit samotný uživatel u demoverze nebo v pilotním projektu. Je třeba zjišťovat, zda produkty neobsahují navíc žádnou skrytou funkcionalitu (tzv. zadní vrátka), ať úmyslnou nebo nedbalostní, a do jaké míry jsou odolné proti úmyslným útokům na své ochranné funkce. Ověřování vyžaduje specializované kryptoanalytiky, provádí se až v rovině nízkoúrovňového návrhu integrovaných obvodů, kontrolují se varianty útoků různými fyzikálními metodami a je naprosto mimo možnosti uživatelů.

Silná kryptografie bývá státy považována, přiznaně či mlčky, za *technologii dvojího užití*. Legislativa států se proto chová ke kryptografii běžně macešsky. Někdy kryptografii zakazuje vůbec, pravidlem bývá, že jejímu šíření nepomáhá. Tržní mechanismus sám pak tlačí jen na nižší cenu, což se zpravidla odrazí v nižší než potřebné péči výrobce a může usnadnit prolomení. Za nejvýznamnější výjimku ze státní disloajality ke kryptografii pro masy považuji právě metodologii *rámce elektronického podpisu* používanou Evropskou unií. Užití kryptografie pro podpis státy neohrožuje. Podpis slouží k autentizaci obsahu a podepsané osoby, nikoli k šifrování obsahu.

Fyzická osoba si může být dostatečně jista bezpečností prostředků a služeb, které rámec nabízí. Spolu s akcentem na výhradní kontrolu prostředků (*sole control*) celý scénář pak skutečně ústil k zajišťování *autonomie* jednající osoby v maximální možné míře a to v tom smyslu, jak autonomii tradičně chápe soukromé právo.

Podepisující osoba stále spoléhá na technické prostředky a služby. Již z principu tomu nemůže být jinak, neboť digitální svět je běžně přístupný pouze zprostředkovaně. Legislativa však zajišťuje předchozí kontrolu i vytvoření trhu prostředků a služeb. Trh se nejen diverzifikuje dle potřeb, stlačuje cenu, ale brání i vzniku bezpečnostně nežádoucí monokultury technických zařízení. Nejen právní předpisy, ale i všechny

relevantní technické normy a specifikace jsou zde k dispozici pro kontrolu veřejností. Legislativa se asi všemi myslitelnými způsoby snaží zaručit, že činnost technického zařízení je zcela a výlučně subjugována vůli osoby, která zařízení drží a ovládá. Je to zajištění tohoto podřízení techniky, které zpětně ztěžuje popření pravosti podpisu i jím podepsaného obsahu. Takový elektronický podpis je pak využitelný nejen v právu soukromém, ale i v právu veřejném, jakož i pro vnitřní komunikaci úřadů a společností.

Ze všech výše uvedených důvodů je institut kvalifikovaného elektronického podpisu hodný pozornosti, a právě proto je na něj zaměřena tato práce.

Současně je nutné připustit, že za více než 15 let si vyšší verze elektronického podpisu populace nijak zvlášť neoblíbila a míra penetrace činí cca 3–4 % obyvatelstva ČR v ekonomicky aktivním věku. Důvodů je zřejmě řada. Vyžaduje určité počáteční náklady podepisující osoby, péči o techniku, a to i v době, kdy se podpisy nevytváří. U tradičního vlastnoručního podpisu tato zátěž nemá obdobu. Schopnost se podepsat si nosí lidé bez jakékoli námahy v sobě, v rámci své neuromotorické paměti a systému. Svoji roli určitě hraje i rozpačité přijímání elektronicky podepsaných dokumentů nebo dat, nedostatek technického zázemí na straně příjemců. Zdá se, že na straně podepisující, ale i spoléhající osoby, je výhodnější disponovat stacionárním prostředím, jako je budova úřadu, kancelář společnosti, nebo byt. Existuje též určité zbytkové riziko ztráty kontroly navzdory výše popsané péči legislativy, výrobců, zkušeben, auditorů, dohledového orgánu. Je třeba určitá sebedisciplína při užívání.

Vyšší verze elektronických podpisů (zaručený, kvalifikovaný) se od počátku prosazují spíše tam, kde je zapotřebí ochrana vyšších hodnot. Ze soukromého práva se jedná o oblast internetového bankovnictví v širokém slova smyslu, ve veřejném právu o takzvaný e-government. V druhém případě je chráněnou hodnotou zákonné využívání veřejné moci a její kontrola až po potenciální soudní přezkum.

Nejpopulárnějším a velmi častým případem užití elektronického právního jednání se za poslední dekádu však zřejmě staly nákupy v elektronických obchodech, oblast označovaná jako e-commerce.

V okamžiku, kdy jsme konfrontováni s naznačenými problémy, je přirozené obrátit se k právu a hledat odpovědi i v něm. Lze se jednak soustředit na analýzu samotné úpravy (zejména kap. 6, 7 a 8), zároveň však rozšířit pozornost na téma *elektronického právního jednání* obecně nebo na některá jiná provedení. Právě kontrasty

komparací vnáší poznání do toho, co je pro který právní institut nebo způsob jeho faktického provedení charakteristické. Na jaře 2017 jsem proto uvažoval až o podrobné komparaci právního jednání elektronickými obchody vůči právnímu jednání s kvalifikovanými elektronickými podpisy. To se ukázalo časově i rozsahem práce neúnosné. Přesto na základě těchto směrů rešerší vznikla kapitola 10, která mimo jiné pojednává o právním jednání právnických osob elektronickými agenty, jakým je i elektronický obchod. Téma pak zpětně ovlivnilo a posílilo můj náhled na nový institut *zaručené* a *kvalifikované elektronické pečeti* ze samotného nařízení eIDAS, podávám výklad, který se částečně liší od dosud v ČR zastávaného.

Vysvětlující význam poskytuje i předřazená teoretická část (kap. 2 až 5), která se zabývá *právním jednáním* popř. *elektronickým právním jednáním* obecně, zejména srovnáním nauky a relevantních částí soukromého práva Německa a ČR. Obecně teoretický vrchol této práce v kapitole 4 pak rozebírá funkce podpisu, zejména vlastnoručního, částečně i elektronického. Výsledky této kapitoly umožňují kvalitnější rozvahy o podpisech v právních i faktických kontextech.

Ze získaných poznatků se zdá, že se praxe vždy sama snaží nalézt takový způsob realizace právního jednání, který je pro účastníky nejsnadnější a ještě vyhovující z hlediska pokrytí rizik, a to i rizik právních. Obdobně i původní vlastnoruční podpis je institut povstalý z obyčejů. Ujal se dlouho před vznikem prvních kodexů z počátků 19. století a ani v průběhu pozdějších dob zákonodárci neměli potřebu jeho znaky a funkce nadměrně právně normovat. Na způsobu jeho vytvoření, ale i případech použití, se společnost dokázala ustálit zdola skoro sama. V kontrastu s tím právní úprava elektronického podpisu je „oktrojovaná“ do vztahu mezi podepisující a spoléhající osobou shora právním řádem, byť s nejlepší možnou snahou napodobit co nejvěrněji funkce vlastnoručního podpisu.

Vyvstávají ale i jiná právní hlediska. Právní jednání elektronickými obchody strany provádí ve fázi realizace práva, kdy obě jednající strany mají zájem na uzavření dohody a uskutečnění obchodu a plně spolu spolupracují. Využívá se vícekrokový proces, v nichž na podpisovou složku právního jednání není kladen zvláštní důraz a je na straně kupujícího nahrazen především jím provedenou platbou, což odpovídá i reálnému způsobu anonymního maloobchodního prodeje v kamenných prodejnách.

Oproti tomu hlavní funkcí kupříkladu datových schránek je potvrzené doručování, tedy nucený příjem datové zprávy, jejímuž přijetí by se adresát často raději vyhnul. Zpravidla se jedná o úkon některého správního řízení, obecně o výkon veřejné moci, včetně moci soudní. Takové systémy proto bude nutné z podstaty věci navrhovat i zavádět jinak, než systémy, k nimž mají uživatelé přirozeně vstřícný vztah.

V právní praxi slouží podpis pro stvrzení důležitých právních jednání, pro možnost pozdějšího dokladování nebo dokazování. Buď jej vyžaduje právní předpis, ať již soukromoprávní nebo veřejnoprávní, nebo protistrana jednání. Podepisující osoba jej zpravidla vytváří v době své relativní vstřícnosti, náročnost provedení by ji neměla odradit od provedení jednání. Účel podpisu ale v posledku bývá v důkazním zajištění o provedení právního jednání a o jeho obsahu, tedy možnosti vymáhání právní odpovědnosti. Ze střetu těchto dvou cílů, tj. snadnosti použití a důkazní hodnoty, bude vyplývat to, s jakými technikami provedení elektronického podpisu se v praxi spokojí spoléhající osoby nebo platné právo. Plyne z toho i to, že osud kvalifikovaného elektronického podpisu, ale i jiných druhů technik podpisu, ještě vůbec není u konce.

Sepisovatelé nařízení eIDAS si nízké penetrace vyšších verzí elektronického podpisu byli vědomi. Rozhodli se umožnit vytvářet kvalifikované elektronické podpisy i na dálku, zřejmě s pomocí chytrých telefonů. Tím by se podpisy mohly více rozšířit do masy populace, vznikla by možnost jejich mobilního a nikoli spíše jen stacionárního použití. Právě za tímto účelem byl požadavek výhradní kontroly prostředků z DirES v eIDAS nahrazen výhradní kontrolou dat pro vytváření podpisu. Mé hodnocení této inovace je zdrženlivé. Vítal bych ji, kdyby současně existoval mechanismus omezení výše rizik osob nebo jiný právně bezpečnostní mechanismus, které navrhuji i v závěru[2].

Ještě radikálnější byli sepisovatelé českého adaptačního zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, kteří pro písemnou formu soukromého právního jednání dovolili jen elektronický podpis prostý. Ten nemá vůbec žádné důkazní vlastnosti a ty budou muset být všechny zajištěny jinými metodami, zřejmě pravidelností provozu a autentizací na počátku sezení nebo provádění právního jednání. Tyto metody mohou být pohodlnější pro „podepisující“ osobu, neposkytují jí však již autonomii tak, jako to činil kvalifikovaný elektronický podpis. Rozhodující nakonec zřejmě bude opět praxe. Oblast e-commerce si však dosud vystačila bez

[2] Srov. 11.3 a 11.4.

formality písemné formy s podpisem, faktická důkazní přesvědčivost zůstává zatím[3] stejná.

S nařízením eIDAS přichází konečně i do České republiky *kvalifikovaný elektronický podpis*, který dosud nebyl českým právním řádem vyžadován. Na druhé straně práce ústí v poznatek, že právní úprava nařízení není úplná. Některé otázky subjugace činnosti techniky pod vůli fyzické osoby nejsou vyjádřeny, strany si je musí zajistit dobrovolně samy, v rámci smluvní svobody nebo dle vnitřních předpisů, jinak mohou zůstat sporné. Podepisující fyzické osoby resp. pečetící právnické osoby však získávají možnost těžit z prostředků a služeb, které jsou nově poskytovány v rámci ustanovení o *službách vytvářejících důvěru*. Tato oblast je nařízením upravena sjednocujícím způsobem, což vytváří dobrý předpoklad toho, že v EU vznikne trh s navzájem se podporujícími řešeními, na němž se již v roce 2017 vyskytovalo téměř dvěstě kvalifikovaných poskytovatelů. Je možné, že evropský zákonodárce zůstal v některých obtížných otázkách zdrženlivý i proto, jelikož jen kusá úprava se mu osvědčila v oblasti e-commerce. Spoléhá na dotvoření samotnými soukromými subjekty, kterým poskytuje značný prostor. I když samo nařízení stanoví pro kvalifikovaný elektronický podpis právní účinek rovnocenný vlastnoručnímu podpisu, neznamená to ještě stanovení stejných důkazních účinků. Upozorňuji pak, že zmíněnému dotvoření je třeba věnovat pozornost nejen technicky, ale i právně.

Hledá-li někdo jednotné řešení elektronické podoby právního jednání v písemné formě, u nějž lze nejspíše očekávat, že bude právně přípustné ve všech odvětvích práva, v rámci právních řádů všech členských států EU a bude dobře právně i technicky využitelné i přeshraničně, bude jím zřejmě stále především řešení využívající kvalifikovaný elektronický podpis. U veřejnoprávních podepisujících český právní řád připustil používat pouze[4] kvalifikovaný elektronický podpis. Jak je uvedeno výše, ten navíc představuje současný technicko právní vrchol počítačové bezpečnosti pro tento účel, dostupný běžné soukromé osobě. Pokud lze nalézat právní nedostatky či technické slabiny v jeho rámci, tím spíše budou existovat hlubší či širší, ale zamlčované, potíže u řešení jiných.

[3] V ČR bude praxe jasnější poté, když v červenci 2018 nabude účinnosti zákon č. 250/2017 Sb., o elektronické identifikaci, a až se stanou funkční technické systémy, které na něm budou založeny. Technické inovace jsou nepřetržité, jakož i jejich právní hodnocení.

[4] Výjimka je dovolena přechodnými ustanoveními, jejichž účinnost končí v září 2018.

Elektronické transakce příležitostně potřebují i jiné bezpečnostní mechanismy, než je samotný elektronický podpis. Nařízení eIDAS upravuje i od elektronického podpisu odvozené digitální objekty a takzvané služby vytvářející důvěru. Ty plní další funkce ověřování pravosti informací v jinak inertním digitálním kyberprostoru. Vznikají pak otázky o jejich podstatě, vlastnostech a právním významu. Novinkou jsou elektronické pečeti, včetně právních požadavků na ně a jejich účinků. Nalézání odpovědí na výše uvedené otázky je též ambicí tohoto textu.

Posoudit výhody či nevýhody jakékoliv právní úpravy lze nejen jejím hodnocením z pohledů praxe, ale i na základě srovnání nebo abstraktnějšími či systematickými úvahami v rámci úpravy samotné. Z těchto důvodů obsahuje tento text jak exkurz do teorie právního jednání, tak různá srovnání teorie i platné úpravy mezi právními řády ČR a Německa.

Práce vznikala následovně. Zárodek textu byl sepsán již na podzim 2013 a na jaře 2014, kdy byl ještě soustředěn na vývoj práva EU a Německa od roku 1997, kdy byl v Německu přijat vůbec první zákon o digitálním podpisu, přes rok 2001 a transpozici směrnice DirES, až do tehdy platného stavu práva. Německo je považováno za všestranně vyspělý stát, který je silný ekonomicky, technologicky, početností populace a pochopitelně i právně. Právní řád ČR náleží do stejné středoevropské právní kultury, což činí srovnávání i více schůdné. Zejména mne zajímalo, zda německá úprava obsahovala přiměřené požadavky na všechny součásti rámce elektronického podpisu, včetně potřeby jejich nezávislých kontrol. Též jsem zkoumal problematiku vztahu technické normalizace k právu, jak se nyní používá ve státech EU obecně a pro oblast informačních technologií zvlášť.

Krátce předtím (r. 2012) již ale došlo k vydání návrhu nařízení Komisí a návrh procházel zákonodárným procesem, završeným publikací nařízení v srpnu 2014. V důsledku přijetí nařízení eIDAS se dalo očekávat, že německé předpisy budou derogovány a mé pojednání o nich zastará, což posléze i nastalo. Z pojednání o právu let 2000 až 2016 jsou v této práci ponechány jen velmi dílčí vysvětlující nebo komparativní fragmenty zejména tam, kde dřívější německá úprava předčila stávající unijní, nebo německá judikatura řešila problematiku, kterou stávající nařízení opomíjí.

Brzy poté vznikly pasáže textu o nové definici elektronického podpisu prostého. Další dva roky trvaly do nabytí účinnosti patřičných částí nařízení. Během stejné doby

byly Komisí postupně vydávány prováděcí implementační akty, které vyhlašovaly čísla různých nových technických norem, na jejichž obsah bylo třeba počkat. Legislativní metoda použitá u eIDAS je totiž založena na kombinaci základní a velmi obecné právní úpravy, jako shora zastřešující právní regulaci, a současného vydání několika desítek technických norem, které částečně v návaznosti na právo, ale částečně i nezávisle na něm regulují materii technicky zdola. V oblasti překryvů zde těžím nejen ze své právní kvalifikace, ale i z kompetence počítačového inženýra, dlouhodobě se zabývajícího počítačovou bezpečností.

Poslední nutné prováděcí rozhodnutí bylo vydáno až na jaře 2016, pouhé dva měsíce před účinností částí eIDAS týkajících se služeb vytvářejících důvěru. K tvorbě textu jsem se tak vrátil na podzim 2016, pracoval na něm průběžně a prakticky celou druhou polovinu roku 2017, dopracování pak proběhlo počátkem roku 2018. Až teprve během léta 2017 byl vydán německý implementační zákon k nařízení, což teprve umožnilo novou smysluplnou komparaci platného práva. Z konečné verze práce byly kvůli již tak značnému rozsahu vyňaty obecné analýzy o vztahu unijního a obecného vnitrostátního práva v případě evropského nařízení. Jsou však ponechány závěry o možnostech implementace nařízení obecně, jakož i mnohá konkrétní implementační doporučení.

Vedle nadčasové právní teorie je nyní obsah textu soustředěn výlučně na právní stav po přijetí nařízení eIDAS. Čtenář dostává do rukou zpracování tématiky zcela aktuální. Vzhledem k dlouhým periodám novelizací unijního práva lze předpokládat, že nejen právní teorie, ale i významná část ostatního textu rychle nezastará. Jednotlivým novým právním konceptům byla věnována intenzivní pozornost. Do značné míry se však jedná o právní úpravu zcela novou, jíž se zatím věnuje jen omezené množství právní literatury. Některé výklady institutů nařízení eIDAS jsou mnou provedeny zřejmě vůbec poprvé, v jiných předkládám někdy i názory odlišné od dosud vyjadřovaných. Měly by sloužit pro rozvoj dalšího diskursu. Nemohu vyloučit, že vzniknou i jiné přístupy či názory, než které zde zastávám. Text by proto neměl být chápán jako kanonický zdroj právní jistoty, ale jako zdroj jisté argumentace a poznání, které je vhodné vzít na zřetel, popřípadě se s nimi vypořádat, pokud možno vlídně.

Poděkování

Rád bych předně poděkoval své manželce Ing. Markétě Kmentové, Ph.D., a dále i všem jiným členům své užší i širší rodiny. Především díky jejich podpoře bylo vytvoření tohoto textu možné.

Vřele děkuji i svému školiteli doc. JUDr. Karlu Beranovi, Ph.D., za zajištění základních možností činnosti, za jeho připomínky a za trpělivost, kterou si vyžádalo vytvoření díla rozsáhlejšího, než bylo původně zamýšleno.

Dovolím si vzpomenout i již zesnulého prof. Ing. Jana Hlavičku, DrSc., děkana FEL ČVUT v letech 1990–1994, který u mne krátce již před těmito roky položil jisté základy vědecké a systematické práce.

Děkuji též všem osobám, které se zasloužily a starají o studijně vlídné prostředí knihovny Právnické fakulty Univerzity Karlovy, včetně zajištění elektronických zdrojů zahraničních odborných periodik a publikací.

Tato strana je záměrně ponechána prázdná.

1. Úvod a předmět práce

Předmětem této práce je srovnávací analýza elektronického právního jednání podle práva EU, ČR a Německa, s důrazem na využití elektronického podpisu, jehož úprava vyplývá především z nedávno účinného evropského nařízení (EU) č. 910/2014 Sb., označovaného zkratkou eIDAS. V rámci této analýzy je věnována zvýšená pozornost i zcela novému institutu elektronické pečeti, jehož rozvinutější verze jsou určeny výhradně pro právnické osoby.

Této srovnávací analýze je předřazena teoretická část (kap. 2 až 5), která se zabývá právním jednáním, ale i institutem tradičního (vlastnoručního) podpisu obecněji. Tato teoretická část je předpokladem pro lepší pochopení vnitřní struktury dále používaných pojmů, ale i naopak externích souvislostí, možných či vhodných kontextů nebo omezení použití. Obecnější poznatky mohou poskytnout nadčasový základ orientace pro oblast, která se neustále rozvíjí a mění technologicky a následně i právně. Zjištění širšího kontextu může být užitečné i pro toho čtenáře, kterého původně zajímá jen některý úzký právní problém.

Z důvodu rozsahu je hlavní pozornost této práce zaměřena zejména na ty pojmy z nařízení eIDAS, jejichž využití vrcholí v *kvalifikovaném elektronickém podpisu*, který má dle nařízení právní účinek rovnocenný vlastnoručnímu podpisu. V novém nařízení jsou tyto pojmy shrnovány pod názvem *služby vytvářející důvěru*.

Cíl dosažení ekvivalence je sice snadno pochopitelný, v praxi je však poměrně obtížně realizovatelný. Vyžaduje totiž souhru několik vědních disciplín, především kryptologie, počítačové bezpečnosti a konečně i práva. Primárním posláním této práce je řešení právních otázek. Pouze tehdy, když si právo či jeho teorie nevystačí, provádíme v nejmenším možném rozsahu exkurze do navazující technické normalizace, v jejímž rámci autor využívá svou druhou plnou kvalifikaci v oblasti počítačové bezpečnosti, je schopen rozhraní oborů prostupovat a spojovat.

Kvalifikované elektronické podpisy představují jednu z právně i fakticky nejjistějších možností, jak implementovat právní jednání s podpisem v elektronickém prostředí. Organizační rámec podepisující osobě umožňuje vybavit si zcela své vlastní technické prostředí, čímž se zajišťuje její nezávislost a autonomie. Kvalifikované elektronické podpisy jsou proto vhodné pro právní jednání v rámci soukromého práva,

které ze zásady autonomie vychází. Je však možné jejich univerzální využití napříč celým právním řádem, k čemuž i dochází. Autor si je pochopitelně vědom, že prakticky se kvalifikované elektronické podpisy prosadily zejména v oblasti elektronického bankovnictví *(internet banking)* a v takzvaném *e-governmentu*, čímž je třeba rozumět zejména činnost a úkony úřadů veřejné správy a vůči nim.[1] Obecně lze říci, že se dnes jedná o takové oblasti, ve kterých se chrání vyšší hodnoty buď finanční, nebo společensko-mocenské.[2]

Cílem textu jako celku je se kriticky vypořádat s otázkou, zda zaručené a kvalifikované elektronické podpisy a jimi potvrzované právní jednání skutečně v elektronickém prostředí dosahují věrnosti a spolehlivosti a zda poskytují srovnatelnou právní jistotu, jako kdyby v tradiční podobě byly vyjádřeny písemně a vlastnoručně podepsány. Nejjobecněji se jedná o výzvu, zda zaručený nebo kvalifikovaný elektronický podpis splňuje požadavky na obdobně přijatelné rozdělení přínosů a rizik mezi podepisující a spoléhající se osobu. Navazujícím nosným dilematem textu je, v čí neprospěch bude řešen spor, pokud údajně podepsaná osoba svůj podpis popře. Rozbor těchto otázek[3] se vzhledem k již zmíněné složitosti rozpadá na velmi mnoho dílčích témat a otázek v mnoha různých kontextech a úrovních přiblížení.

Přestože je kvalifikovaný elektronický podpis velmi jistou formou, jak lze elektronické právní jednání podepsat, z kvantitativního hlediska se jedná o způsob, který není převažující. V této souvislosti je třeba uvést, že čistě kvantitativně se valná část elektronicky podepisovaného právního jednání v současnosti realizuje s využitím elektronického podpisu prostého. Této formě podpisu však není věnována v této práci hlavní pozornost. Kromě rozsahu textu je důvodem i to, že taková orientace by vedla na právní oblast, která se tradičně označuje jako *e-commerce* a zahrnuje především uzavírání smluv na dálku prostřednictvím elektronických obchodů, ale i další navazující témata práva v prostředí sítě internet. Tyto zejména tzv. klikací smlouvy[4] sice mají právem předepsány určité náležitosti, dodržení písemné formy mezi ně ale zpravidla nenáleží. Jejich použití z důkazního hlediska o skutkovém stavu pak nepřináší rovněž

[1] Autor doporučuje, aby se pojem *e-government* vykládal a zajišťoval včetně technických návazností na technické zařízení a vybavení soudů, což nevylučuje udržení ústavního oddělení moci soudní.

[2] Jedná se zejména o zajištění zákonnosti veřejné moci, o dokumentaci jejího výkonu, o dohled či dozor nad ní, ale i o následnou možnost jejího soudního přezkumu, což vše směřuje k zajišťování právního státu, součásti materiálního ohniska ústavy České republiky.

[3] Stejnou či blízce analogickou jsou tytéž otázky ve vztahu k zaručeným nebo kvalifikovaným elektronickým pečetím, proto text do značné míry současně odpovídá i na ně.

[4] V textu níže označované zejména jako technika *click-wrap* podpisu, srov. část 4.5.

nic nového. Autor se proto nedomnívá, že by změna definice prostého elektronického podpisu způsobila v této oblasti přelom praxe. Ta je opřena spíše o vícekrokové procesy, v nichž na podpisovou složku právního jednání není kladen zvláštní důraz, a je na straně kupujícího nahrazen především jím provedenou platbou, což odpovídá i reálnému způsobu maloobchodního prodeje v kamenných prodejnách, často zcela anonymnímu.

Provozovatelé elektronických obchodů, pokud mají zvláštní požadavky na bezpečnost svých postupů, mohou fakultativně spíše těžit z nových bezpečnostních služeb vytvářejících důvěru, které nařízení eIDAS poskytuje. Jednou z takových možností je i v textu probírané využití zaručené elektronické pečeti pro fakultativní pečetění povinně poskytovaných informací právnickou osobou (kap. 10).

Tento text se též nezabývá elektronickou identifikací a kapitolou II. nařízení eIDAS. Tato problematika musí být upravena převážně na vnitrostátní úrovni,[5] bude představovat významnou, ale též do značné míry právně samostatně upravenou oblast. Mechanismus identifikace (autentizace) může sloužit pro počáteční ověření totožnosti vzdáleného uživatele informačního systému, kterým v současnosti typicky bude webový server. V rámci následného používání systému (serveru) pak uživatel může i provést právní jednání, typicky pouze s prostým elektronickým podpisem. Vnitrostátní úprava a dle ní realizovaný státní identitní systém budou jistě využívány správnímy úřady pro poskytování služeb e-governmentu.

1.1 K obsahu textu

Kromě předmluvy a úvodu se text systematicky člení do kapitol. Z toho tvoří obecnou teoretičtější část kapitoly 2 až 5. První zvláštní částí je kapitola 6, soustředěná pouze na nařízení eIDAS (části služby vytvářající důvěru) a jeho výklad v kontextu práva EU. Další zvláštní části v kapitolách 7 až 10 pojednávají o vnitrostátních implementacích nařízení eIDAS, popř. o právním jednání po implementaci nařízení eIDAS. Závěrečná kapitola 11 obsahuje souhrny a závěry. Níže je vysvětlena struktura celého textu, obsah kapitol a smysl jejich zařazení.

1. Úvod a předmět práce

Tato kapitola popisuje zaměření a obsah textu.

[5] Zákon č. 250/2017 Sb., o elektronické identifikaci. Účinnost nabývá 1. července 2018.

2. Právní jednání jako pojem práva ČR

Cílem této kapitoly je odpovědět na otázku, jak se pojem *právní jednání* chápe v českém právu a jeho teorii. Je popsán širší smysl právního jednání (2.1), který teorie práva používá v kontextu celého právního řádu, tedy i správního práva. Užší smysl (2.2) je soustředěn na soukromé právo. Je zde poskytnut stručný průřezový pohled české civilistiky. Kapitola je zakončena historickým exkurzem do obecného zákoníku občanského (2.3), který v českých zemích platil od roku 1811 a dal tak vzniknout tradičnímu pojetí, jež česká civilistika dnes zaujímá. V něm použitá německá právní terminologie má důležitý význam i pro pochopení vývoje pojmů, popisovaného v další kapitole, nejen z historického, nýbrž i z věcného hlediska.

3. Právní jednání v soukromém německém právu

V německém právu se za právní jednání běžně považuje pojem *das Rechtsgeschäft*, ale spadá pod něj i *die Willenserklärung*. S oběma pojmy se setkáme pouze v civilním právu. Kapitola obsahuje objasnění pojmů třemi způsoby. Nejprve tak, jak byly objasněny v důvodové zprávě německého občanského zákoníku BGB zvané Motive (3.1) z r. 1888, poté jak bývá problematika podávána v běžné soudobé německé nauce (3.2) a nakonec jak se jí podrobně zabývá především právní teoretik Flume (3.3), který reflektuje vývoj německé teorie a různá pojetí německých teoretiků za více než dvě století. Kapitola je rozsáhlejší než jí předcházející, neboť českému právní prostředí jsou tyto informace běžně méně dostupné a současně představují vydatný zdroj o možných právních přístupech k právnímu jednání, množství teoretických poznatků o nahlížení na vůli, na projev vůle a na jejich vzájemný vztah.

Za pozornosti hodný přínos této kapitoly autor spatřuje zkoumání alternativ, jak právně řešit nesoulad mezi vůlí a projevem vůle, tedy otázku, zda především omyl má být přiřknut v neprospěch právně jednající osoby, anebo v neprospěch adresáta právního jednání. S tím souvisí i pozornost věnovaná rozporovatelnosti[6] právního jednání. Omyl je totiž často morálně indiferentní a zákonodárce v rámci soukromého práva nemá žádný důvod stranit jedné nebo druhé straně. Jedná se tak o zpracovanou, obtížnou a zřejmě právně nejpodobnější otázku dilematu tohoto textu. Tímto podobným dilematem je již v úvodu zmíněná otázka, v čí neprospěch bude řešen spor, pokud

[6] V Němčině pojem *die Anfechtbarkeit*. Pro odlišení od konceptu *odporování* právním jednáním v právním řádu ČR je v tomto textu termín překládán jako *rozporovatelnost*.

údajně podepsaná osoba svůj podpis popře. Německá systematika pojmů se navíc od české částečně liší. Zařazení kapitoly pomáhá lépe chápat jak německé platné právo, tak způsob uvažování německých právníků.

4. Podpis a jeho funkce z pohledu práva

Kapitola se zabývá prvkem podpisu z právně teoretického hlediska. Přirozeně se zde vychází z tradice provádění vlastnoručního podpisu, v druhé polovině kapitoly jsou však zkoumány i některé náhledy na podpis, které přináší až užívané techniky elektronických podpisů. Po základním zkoumání vlastnoručního podpisu (4.1) jsou analyzovány zejména funkce podpisu, z nichž autor považuje nakonec za velmi pregnantní německou systematiku funkcí (4.2). Funkční analýza umožňuje jednak orientaci v obecně nejednotné terminologii, jednak vytváří určitý srovnávací etalon. Jednotlivé užívané techniky elektronického podpisu je pak možné hodnotit i podle toho, které funkce splňují, popřípadě zda dokonce nepředstavují takzvaný funkční ekvivalent. Vzhledem k technologické dominanci Spojených států je dále pozornost věnována i formám podpisů (4.3) v common law, jakož i v něm rozvinuté teorii funkcí podpisu (4.4). Teoretici common law přistupovali k funkcím odlišně, nicméně vesměs lze nalézt korespondenci s německou systematikou. Pro orientaci je pak uvedeno základních osm druhů techniky elektronického podpisu (4.5), které se dnes ve světě používají. V dalším textu zkoumané právní úpravy je tak možné hodnotit nejen vůči systematice funkcí vlastnoručního podpisu, ale i z hlediska toho, které techniky elektronického podpisu je budou způsobilé realizovat. V kapitole je stručně probrán i kryptologický pohled na podpis (4.6), neboť právě digitální podpisy jsou očekávanou technikou zaručeného a kvalifikovaného elektronického podpisu. Na závěr byla doplněna i problematika komitmentů podpisu (4.7), která vyvstává do pozornosti právě až v rámci implementací elektronických podpisů.

5. Elektronické právní jednání

Tato kapitola představuje přechod od zcela obecné teoretické průpravy (kapitoly 2 až 4) k elektronickému právnímu jednání, byť jej stále analyzuje v relativně obecné rovině. Z toho část 5.1 se zabývá právním jednáním v soukromém právu ČR a část 5.2 v soukromém právu Německa. Část 5.3 obsahuje srovnávací shrnutí.

Elektronické právní jednání lze obecně provádět bez ohledu na formu (5.1.1, 5.1.2). Pro právní jednání v písemné formě je pak třeba písemnost (5.1.3), pro platnost

pak typicky doplněná podpisem (5.1.5). Písemnost i podpis mohou být i v elektronické podobě, resp. být prováděny právním jednáním učiněném elektronickými prostředky, přičemž způsob elektronického podepsání stanoví jiný právní předpis.

Německé právo též vychází z bezformálnosti právního jednání. Po vyjasnění teoretických nuancí a přístupů (5.2.1 až 5.2.4) se dochází k některým zvláštním formám, a to sice písemné (5.2.5.1), elektronické (5.2.5.2) a textové (5.2.5.3). Odlišností systematiky oproti české je, že písemná forma právního jednání se dosahuje prvotně výlučně v listinné podobě s vlastnoručním podpisem, zatímco elektronická vyžaduje elektronický dokument podepsaný kvalifikovaným elektronickým podpisem. Za stanovených podmínek pak elektronická forma může nahrazovat či splňovat požadavek na písemnou formu.

6. Nařízení eIDAS (elektronické podpisy)

V této kapitole jsou předkládány detailní analýzy pojmů a institutů souvisejících s elektronickým podpisem tak, jak jsou nově upraveny evropským nařízením eIDAS, v jeho části označované jako služby vytvářející důvěru. Výklady dotyčných pojmů vycházejí zejména ze samotného nařízení eIDAS a zůstávají v úrovni práva Evropské unie, tedy bez ohledu na to, jak by byla provedena implementace do některého z právních řádů států EU. Ačkoli tento text jako celek není zamýšlen být právním komentářem, úrovní a podrobností výkladu se mu v této kapitole přibližuje. Autor se přitom rozhodně nesnaží probírat nařízení lineárním způsobem, rozsah zpracování a detailnost rozborů je spíš nechtěným důsledkem snahy nevynechat žádnou právní otázku, která při používání vyšších verzí elektronického podpisu může vzniknout na straně podepisující (ev. pečetící) osoby, nebo na straně spoléhající osoby (strany).

Úvodní část 6.1 poskytuje několik metod pro prvotní přiblížení struktury nařízení a orientaci se čtenáře v něm. Ačkoli se do značné míry jedná o analytické závěry, jsou v části 6.2 popsány základní koncepty nařízení, které mohou čtenáři též usnadnit pochopení tohoto nařízení jako celku.

V části 6.3 se analyzuje předmět a oblast působnosti nařízení, které stanoví některá nesamozřejmá omezení jeho použitelnosti nebo mají zásadní dopad na jeho výklad. Část 6.4 se zabývá novou definicí elektronického podpisu prostého a hledáním smyslu jejího významu. Navazující část 6.5 probírá autentizační elektronické podpisy, změny jejich pojetí. V eIDAS mezi ně náleží zaručený (6.5.1) a zejména pak

kvalifikovaný (6.5.3) elektronický podpis. Část 6.6 se věnuje elektronickým pečetím, zejména zaručené elektronické pečeti a zjišťování jejího významu či smyslu zavedení v nařízení (6.6.4). Je zde představen autorův nový, byť zatím minoritní výklad, který dochází k tomu, že účelem zaručené a kvalifikované elektronické pečeti je blížit se elektronickém podpisu přímo právnické osoby samotné, aniž by to bylo výslovně stanoveno. Část 6.7 stručně probírá elektronické časové razítko. Část 6.8 se zabývá novým zastřešujícím pojmem služeb vytvářejících důvěru, jakož i subjekty jejich poskytovatelů. V části 6.9 se probírají otázky spojené s důvěryhodnými seznamy, které právně i technicky patří mezi zdařilejší součásti nařízení. Část 6.10 se zabývá kvalifikovanými prostředky pro vytváření elektronického podpisu. V části 6.11 je probírán postup a problematika ověřování (technické) platnosti kvalifikovaného elektronického podpisu, řešící některé dřívější závažné nedostatky. V části 6.12 se řeší otázky odpovědnosti poskytovatele služeb vytvářejících důvěru a v části 6.13 odpovědnost členského státu. V části 6.14 se řeší, zda adresát elektronické transakce musí souhlasit s jejím přijetím v elektronické podobě s elektronickým podpisem. Část 6.15 probírá důkazní účinky digitálních objektů z nařízení eIDAS, jak jsou vyjádřeny nařízením. Kritické náhledy autora na nařízení jsou soustředěny do části 6.16. Poukazuje se zde na 15 dílčích problémů, které jsou považovány za neřešené buď vůbec, nedostatečně nebo nejasně. V části 6.17 je zmíněna možná hypotéza tohoto stavu, totiž možnost, že předkladatel návrhu nařízení byl významně ovlivněn francouzským pojetím z *Code civil*. Koncepce založená na francouzském právním řádu pak mohla být příčinou v návrhu nevyřčeného předpokladu, že značná část problematiky bude vyřešena až technickými normami, přičemž z těchto technických norem budou vyplývat i právní povinnosti. Taková konstrukce přináší pro implementaci v právu ČR některé nečekané následky.

7. Implementace nařízení eIDAS v právu Německa

Kapitola stručně popisuje implementaci v textu zkoumaných částí nařízení eIDAS v Německu. Účelem je především poskytnout přehled upravených záležitostí pro případné srovnání s implementací českou. Některé německé zdroje vypracované k účelu implementace však již byly využity i pro výklad nařízení eIDAS v předchozí kapitole. Implementace vždy aspoň nepřímo indikuje, jak je chápáno a vykládáno samotné nařízení. Německo reagovalo s implementací zpožděně zákonem *eIDAS-Durchführungsgesetz* (7.1 a 7.2). V jeho rámci hlavní podrobnosti jsou obsaženy

v *Vertrauensdienstegesetz* (7.3), mírně novelizován byl i německý *Zivilprozessordnung* (7.4). Německo zde neplní roli předpokládaného vzoru vůbec ideálně, do dokončení textu nebyla přijata prováděcí vyhláška.

8. Implementace nařízení eIDAS v ČR

Kapitola obsahuje přehled implementace v textu zkoumaných částí nařízení eIDAS v ČR, jak byla provedena zejména adaptačním zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce. Nejčastěji bude pozornost věnována zřejmě adaptivně-recepčním ustanovení (8.2). Obsažen je i rozbor konkretizačních a doplňovacích ustanovení (8.3), ale i institucionálně-kompetenčních (8.4) a sankčních (8.5). Adaptačním zákonem recipované pojmy se následně využívají (8.6) desítkami novelizací napříč právním řádem. Adaptační zákon neprovádí žádné změny v důkazních (8.7) pravidlech.Chyba: zdroj odkazu nenalezen Kapitola je završena přehledem témat, jejichž úpravu autor považuje za v implementaci opomenutou (8.8) a ustanovení, která byla derogována (8.9) bez výslovné náhrady, tj. dochází v nich k menší či větší změně v právním řádu ČR. Důsledky, které přinášejí změny uvedené v 8.8 a 8.9, by zřejmě měli reflektovat jak praktikující právníci, tak je případně může zvážit i zákonodárce.

9. Právní jednání s elektronickým podpisem v ČR

Zatímco v kapitole 8 se probírá samotná implementace nařízení eIDAS v právu ČR, v této kapitole se pojednává o některých možnostech právního jednání s elektronickým podpisem dle právního řádu ČR, ve stavu po účinnosti adaptačního a změnového zákona k eIDAS. V části 9.1 jsou soustředěny některé legislativní připomínky. V části 9.2 je probíráno pozadí zpracování listin u veřejnoprávních původců, jakožto důležitého předpokladu presumpce správnosti veřejných listin. V části 9.3 jsou zmíněny možnosti elektronického podání[7] a splnění náležitostí podpisu při něm. V části 9.4 je stručně probrána možnost soukromého právního jednání, včetně zhuštěného konceptu nahlížení autora na důkazní účinky kvalifikovaného elektronického podpisu.

10. Elektronické právní jednání právnických osob (ČR)

Účelem kapitoly je podat základní souhrn možností soukromého elektronického právního jednání právnickou osobou v právním řádu ČR. Po přijetí nového občanského

[7] Text by si zde svou strukturou poté zasloužil obdobné pojednání i opačné činnosti, tj. o vytváření rozhodnutí a o doručování.

zákoníku právní řád ČR vychází z teorie fikce. Právní úpravu nutí, aby za právnickou osobu jednali její zástupci (10.1). To sice je dobře možné v tradiční praxi, při automatickém provozu se však stále častěji používá právní jednání elektronickým agentem. Jsou zjištěny základní teoretické možnosti pojetí (10.2) elektronických agentů. Další část 10.3 je soustředěna na to, jaké právní požadavky dopadají na právnickou osobu, pokud právně jedná svým elektronickým obchodem. Východiskem této právní úpravy je právo EU (10.3.1). Ze souhrnu plyne, že právnická osoba může provozovat elektronický obchod stejně snadno jako osoba fyzická a že při svých činnostech nemusí určovat fyzickou osobu jako za sebe jednajícího zástupce. Unijní právo je v této oblasti do právního řádu ČR (10.3.2) transponováno poměrně přesně v § 1811 an. obč. zák., pro provádění právního jednání dostačuje pak takzvaná textová podoba. Další rozbor (10.3.3) ukazuje, že tak jako pro provoz není přikázáno používání takzvaných serverových certifikátů,[8] stejně dobře je možné zmíněnou textovou podobu, v unijním právu nazývanou jako trvalý nosič *(durable medium)*, fakultativně zajišťovat zaručenými elektronickými pečetěmi, provozuje-li internetový obchod právnická osoba. V případě jiných elektronických agentů (10.3.4) může být použití zaručených nebo kvalifikovaných elektronických pečetí sice možné, ale nemusí dostačovat. V závěrečné části 10.4 se probírá splnění náležitostí písemné formy právního jednání při použití elektronických prostředků právnickou osobou.

11. Souhrn a závěr

Závěrečná kapitola shrnuje nejdůležitější poznatky z této práce. Vrací se k ústřední otázce tohoto textu, totiž k čí tíži připsat elektronické právní jednání potvrzené kvalifikovaným elektronickým podpisem, jehož (technická) platnost je úspěšně ověřena, ale jehož provedení údajná podepisující osoba následně přesto popírá. Toto dilema má zřejmě jiné řešení ve veřejném právu (11.1) a v soukromém právu (11.2). Autor dále navrhuje odlišné možnosti technického a právního rozvoje, které by umožnily se dilematu vyhnout, nebo jej vyřešit jinak. Takovou možností jsou například apriorní omezení použitelnosti (11.3) nebo převod jednání na rozporovatelný proces (11.4). Další části shrnutí charakterizují nařízení eIDAS (11.5) a právní možnosti pro i proti vyšší míře doplnění a konkretizace nařízení vnitrostátní implementací v ČR (11.6). V části 11.7 je obsaženo pět hlavních bodů závěru.

[8] V terminologii nařízení eIDAS se jedná o (kvalifikované) certifikáty pro autentizaci internetových stránek.

Dílčí souhrny teoretického i praktického charakteru jsou však také uváděny průběžně, zejména v závěrech kapitol 7 až 10.

1.1.1 Negativní vymezení předmětu práce

Jak již bylo uvedeno, téma práce a prozkoumávání dílčích otázek a témat bylo nutné po dosažení určitého rozsahu omezit a uzavřít. Některým dalším otázkám se autor hodlá brzy věnovat v rámci navazujících časopiseckých publikací,[9] další budou rozvíjeny jistě i jinými autory, možná i v reakci na tento text nebo potřeby praxe.

Některá další témata pak autor jako primární zaměření textu nezamýšlel. Tento text se nezabývá otázkami volby rozhodného práva, kolizními pravidly a většinou ani jinými aspekty vymáhání práva při obecném právním jednání v prostředí internetu. Zájemcům o toto pojetí či témata lze doporučit například přehledovou publikaci Wanga, aktualizovanou[10] v roce 2014. V tuzemsku je takovou prací dílo Koščíka[11] z roku 2011, které je dodnes do značné míry použitelné. Téma pokrývá Härting.[12] Pro výklad platného evropského práva pro *e-commerce* je k dispozici čerstvý komentář.[13] Poslední dvě zmíněné publikace se částečně využívají i v tomto textu.

Je-li v tomto textu brán na zřetel větší horizont geografie nebo jurisdikce, než je ČR nebo Německo, pak je jím především území EU a právo EU. Z unijního práva je pak probíráno spíše hmotné právo, nikoli procesní aspekty jeho vymáhání.

Text se primárně nezabývá ani právním jednáním prováděném s pomocí elektronických obchodů (jen částečně v kap. 10, zejména část 10.3). Toto téma je v tuzemsku bohužel na úrovni právních monografií opomíjené a existuje asi jen letitá

[9] Autor by se časopisecky brzy rád věnoval podrobně důkazním účinkům kvalifikovaného elektronického podpisu v právním řádu ČR. V tomto textu k těmto důkazním účinkům srov. 9.4.1.

[10] WANG, F. F. *Law of Electronic Commercial Transactions : contemporary issues in the EU, US and China*. New York: Routledge, 2014.
Wang se snaží zodpovědět sedm otázek: 1. Co je to elekronická kontraktace? 2. Kdo kontrahuje? 3. Kdy je smlouva uzavřena? 4. Jak lze zahrnout obecné smluvní podmínky? 5. Jak napravit komunikační chyby? 6. Kde je elektronická smlouva uzavřena? 7. Jak lze řešit elektronickou bitvu formulářů? Wang pro tyto otázky vyhledává a srovnává řešení z různých právních úprav (zejména na úrovni práva EU, USA a Číny), včetně úprav z modelových návrhů zákonů, dosud neratifikovaných mezinárodních smluv atp.

[11] KOŠČÍK, M. Pojem a obsah právních úkonů na internetu. *Revue pro právo a technologie* [online]. 2011, roč. 2, č. 4, s. 30–75. [cit. 2017-12-07]. Dostupné z: <https://journals.muni.cz/revue/article/view/4089>. Nastaly ovšem právní změny. Je účinný nový občanský zákoník v ČR, jakož i nový zákon o mezinárodním právu soukromém, došlo k přijetí a nabytí účinnosti evropské směrnice 2011/83/EU o právech spotřebitelů a nařízení EU 1215/2012 (Brusel I bis). Nic z uvedeného přesto nepředstavuje dramatické koncepční změny z hlediska pojetí práce Koščíka, ale je třeba o nich vědět.

[12] HÄRTING, N. *Internetrecht*. Köln: Verlag Dr. Otto Schmidt KG, 2014.

[13] LODDER, A. R., MURRAY, A. D. (eds). *EU regulation of e-commerce : a commentary*. Cheltenham: Edward Elgar Publishing, 2017.

publikace Frimmela.[14] Doporučit lze již výše zmíněný čerstvý komentářChyba: zdroj odkazu nenalezen evropského práva v oblasti *e-commerce*, byť ani ten nepokrývá veškerou problematiku.[15] K elektronickým obchodům je dostatek zahraniční literatury,Chyba: zdroj odkazu nenalezen která ovšem zpravidla akcentuje domovský právní řád autorů.

V textu (s výjimkou části kap. 2) se též nenachází podrobná teorie *právního jednání* ve veřejném právu ČR nebo Německa. Zejména oblasti správního práva jsou značně fragmentované a využívají i odlišnou terminologii. Některé kapitoly textu s výklady práva jsou však někdy využitelné i ve veřejném právu. V textu, včetně některých souhrnů či závěrů, se upozorňuje i na dopady pro veřejné právo.

1.1.2 Důvody pro volbu práva Německa pro právní srovnávání

Právo Německa bylo v tomto textu pro srovnání zvoleno z několika právních i mimoprávních důvodů. Německý kodex soukromého práva (BGB) je dostatečně věkovitý (platí nepřetržitě od roku 1900), ale přitom je již dostatečně moderní. Je tak zajištěna kontinuita v judikatuře soudů. Německo je velký stát s řádově osmdesáti miliony obyvatel, což se příznivě odráží na množství jeho právního provozu, na objemu judikatury, ale i na množství činných právníků, kteří právo rozvíjejí a vykládají. Němci i v právu jsou považováni za perfekcionisty s tendencí podrobného plánování, v jejich právu či právní literatuře by měly být nalezeny odpovědi či preventivní řešení mnoha potenciálních právních problémů.

ČR a její právní řád právně náleží do oblasti středoevropského práva, jehož hlavním představitelem je dnes Německo. Samotná ČR historicky byla ovlivněna rakouskou podobou civilního práva v ABGB. Nový občanský zákoník (zákon č. 89/2012 Sb., občanský zákoník) se snaží vybrat to modernější z právních předloh více států, na ABGB se již výlučně neváže, ale bezesporu usiluje zůstat v rámci dlouhodobější tradice středoevropské civilistiky ČR.

Mimoprávním důvodem je, že Německo je v současnosti jedním z technologicky nejrozvinutějších států v Evropě. Vedle Francie a Spojeného království je právě Německo státem, v němž jsou obchodní společnosti schopny samostatně vyvinout a testovat pokročilá kryptografická zařízení, potřebná pro vyšší formy elektronického podpisu. Konsekventně lze očekávat, že v právu Německa by měly být nalezitelné

[14] FRIMMEL, M. *Elektronický obchod: právní úprava*. Praha: Prospektrum, 2002.
[15] Například nakládání s obalovými odpady, popř. zvláštními druhy odpadů.

vhodné právní úpravy, jako projev zájmu jeho domácích subjektů. Důvodem je i komerční význam Německa v obchodní výměně s ČR, která dosahuje téměř čtyřicet procent importu i exportu ČR vůči celé Evropské unii.

Ze všech uvedených důvodů výchozí hypotézou autora bylo, že Německo bude představovat ideální komparativní právní etalon.

1.1.3 Poznámky k terminologii a zavedeným zkratkám

Autor původně usiloval o formulaci textu bez používání zkratek, jako jsou QES[16] nebo $AdES_{QC}$[17] apod., protože si je vědom, že ryze právním čtenářům nebudou bezprostředně srozumitelné a nejsou ideální ani z hlediska (české) jazykové kultury. V kapitolách vycházejících pojmově z nařízení eIDAS však některé věty začaly nabývat takové délky, že nakonec usoudil, že občasné použití zkratek povede nejen k potřebnému zkrácení, ale snad i ke snadnějšímu pochopení. V tomto textu jsou zkratky používány vždy jako zkratky pojmů právních, neplyne-li výslovně jinak. Z důvodu snadného přechodu k jiné literatuře byly užity anglické akronymy, které jsou v související právní i technické literatuře poměrně běžné, na rozdíl od českých.

V rámci srovnávacích činností se bylo třeba vypořádat i s tím, jak překládat zejména některé právní odborné pojmy z němčiny. Byly zvoleny určité výrazy, které jsou v právní češtině neobsazené a které text poté konzistentně dodržuje. Nemusí se jednat vždy o překlady optimální (např. *vyjádření vůle* pro *Willenserklärung*) nebo zažité, ale umožňují autorovi a následně i čtenáři snadno rozlišovat kontext právního řádu v diskursu celého textu.

[16] Qualified Electronic Signature.
[17] Advanced Electronic Signature based on a Qualified Certificate.

2. Právní jednání jako pojem práva ČR

Než v této práci přistoupíme ke zkoumání jejího předmětu, tj. elektronického právního jednání, je užitečné si přiblížit způsob používání obratu *právní jednání*, jak je užíván v nauce českého práva, popř. v českém platném právu.

2.1 Právní jednání (širší smysl)

V české teorii práva se pojem právní jednání předně používá pro popis jedné ze čtyř druhů právních skutečností. **Právní skutečností** se přitom dle Gerlocha rozumí „okolnost, s níž právní norma spojuje vznik, změnu nebo zánik právního vztahu, tj. subjektivních práv a právních povinností.“[1] Mírně podrobněji dle Harvánka právní skutečnosti jsou „v hypotéze normy předvídané (přírodní nebo společenské) podmínky**,** okolnosti, za nichž dochází ke vzniku (změně, zániku) právníhu vztahu.“[2] Zmínka o hypotéze potřebuje rozbor. Samotná hypotéza obecné právní normy není schopna založit normativní charakter právní normy, neumožňuje ani rozhodnout o tom, zda je právní norma plněna, anebo nikoli. Normativní účinek se dosahuje až v okamžiku spojení s dispozicí. Harvánkovu definici by proto bylo zřejmě potřeba chápat tak, že zmíněná hypotéza již potenciálně obsahuje i výsledek hodnocení jiných právních norem (vč. jejich dispozic), resp. se jedná o přeformulaci existujících právních norem tak, aby jejich dispozicí následně byl právě vznik (změna, zánik) právníhu vztahu. Podle obecné české civilistiky právní skutečnost je „objektivní skutečnost, kterou objektivní právo, tj. právo v objektivním smyslu, jednak bere na zřetel (a tudíž je schopno ní pracovat), jednak s ní spojuje právní následky.“[3] Definice může reflektovat, že se pojem (právního) následku nově objevuje v § 545 a § 500 obč. zák. Pojem sice není definován, ale lze souhlasit, že se „právními následky zpravidla rozumí ... vznik nebo změna, anebo zánik subjektivních práv a/nebo povinností.“[4]

Primárním kritériem dělení právních skutečností v nauce pak je soulad s objektivním právem, resp. s jeho právními normami.[5] Druhým kritériem je, zda jsou „projevem vůle, nebo nastávají mimovolně“,[6] resp. zda se jedná o „jednání jakožto

[1] GERLOCH, A. *Teorie práva.* 3. vydání. Plzeň: Aleš Čeněk, 2004, s. 161.
[2] HARVÁNEK, J. et al. *Právní teorie*. Plzeň: Aleš Čeněk, 2013, s. 265.
[3] DVOŘÁK, J. – ŠVESTKA, J. – ZUKLÍNOVÁ, M. *Občanské právo hmotné*. *Svazek I. Díl první: Obecná část.* Praha: Wolters Kluwer ČR, 2013, s. 154.
[4] DVOŘÁK, J. – ŠVESTKA, J. – ZUKLÍNOVÁ, M., cit. dílo, s. 154.
[5] GERLOCH, A., cit. dílo, s. 161.
[6] GERLOCH, A., cit. dílo, s. 161.

vědomé a volní lidské chování".[7] V závislosti na naplnění těchto kritérií dostáváme klasické čtyři druhy právních skutečností:[8]

1. Právní jednání – projev vůle souladný s normami práva.
2. Protiprávní jednání – delikt, projev vůle v rozporu s normami práva.
3. Právní událost – mimovolní skutečnost v souladu s normami práva.
4. Protiprávní událost – mimovolní skutečnost v rozporu s normami práva.

Z uvedených druhů nás pak zajímá první druh. Dle Boguszaka podstatná kritéria pro další třídění právního jednání „se kryjí s hledisky, podle nichž dělíme právo jednak na *soukromé* a *veřejné*, jednak na *hmotné* a *procesní*." Hlavní dělení pak podle něj je:[9]

I. *Soukromoprávní jednání*, což jsou projevy vůle soukromoprávní povahy, které směřují k vzniku, změně nebo zániku subjektivních práv a povinností hmotněprávní povahy, jež právní normy s těmito projevy spojují.

II. *Veřejnoprávní jednání* v rámci aplikace práva státními orgány či orgány územní samosprávy.

V rámci veřejnoprávních jednání pak nejdůležitějšími případy jsou *individuální právní akty*, kterými jsou správní nebo soudní rozhodnutí, vydávána ve správním nebo soudním řízení. Nejvýznamnějšími rozhodnutími jsou *rozhodnutí ve věci samé*, zejména pokud mají *konstitutivní účinky* (hmotněprávní). Taková rozhodnutí zakládají, mění nebo ruší subjektivní práva a povinnosti hmotněprávní povahy. Současně mají i procesněprávní účinky, tj. zakládají, mění nebo ruší procesní práva a povinnosti. Dalšími jsou *rozhodnutí procesněprávní*, bez rozhodnutí ve věci samé, pouze s procesněprávními účinky. Pro takové se též někdy používá označení *procesní úkony*. Je však třeba rozlišit, zda se jedná o procesní úkon orgánu, který má rozhodovací pravomoc v daném stadiu řízení, a jsou rozhodnutím, mají tedy plně veřejnoprávní povahu (včetně presumpce správnosti). Na druhé straně jsou procesní úkony účastníků (stran) řízení, které mají pouze procesněprávní účinky.

Rozhodnutí ve věci samé s *deklaratorními účinky* nemění hmotněprávní práva a povinnosti, vykazuje však účinky procesněprávně. Taxonomii Boguszaka zde uvádíme zejména proto, jelikož provádí asi nejúplnější výčet výskytu pojmu

[7] Boguszak in BOGUSZAK, J. – ČAPEK, J. – GERLOCH, A. *Teorie práva*. 2. vydání, Praha: ASPI Publishing, 2004, s. 127.
[8] Parafráze z GERLOCH, A., cit. dílo, s. 161.
[9] Boguszak in BOGUSZAK, J. – ČAPEK, J. – GERLOCH, A., cit. dílo, s. 128–131.

právního jednání, jak mu lze v právním řádu ČR rozumět. Budeme-li se zabývat elektronizací právního jednání, uvidíme později, že k ní dochází ve všech uvedených případech. Pro jednoznačnost uveďme, že se zde stále vyjadřujeme v pojmech analýzy a taxonomie právní nauky, platné právo může příležitostně používat odlišné obraty, které nicméně lze pod některý zde uvedený teoretický pojem podřadit.[10]

Česká teorie práva za účinnosti zák. č. 40/1964 Sb. často využívala toho, že soukromoprávní jednání (soukromé právní jednání) bylo platným právem označováno jako tzv. *právní úkon*, zatímco nový občanský zákoník používá pojem *právní jednání*. V dělení právního jednání na dva poddruhy proto dříve nevznikal pojmový zmatek výskytu stejného obratu v pojmu i v jeho členění. Nově nauka hovoří o právním jednání v *largo sensu* (jak o něm vykládá i tato část textu) a ve *stricto sensu* (soukromé právní jednání). Teorie práva též někdy zhušťuje veřejnoprávní jednání na nejvýznamnější případ s dopadem do hmotného práva. Výsledkem může být vyjádření, že jedním ze čtyř druhů právních skutečností je „právní jednání *largo sensu*, které je projevem vůle souladným s normami práva a které dělíme na právní jednání *(stricto sensu)* fyzických a právnických osob a individuální právní akty orgánů veřejné moci."[11] Tento výklad je pro prvotní přiblížení pojmu adekvátní. Není nijak v rozporu s výše uvedenou bohatší taxonomií Boguszaka, která je pro účel tohoto textu vhodnější.

Autor na tomto místě upozorňuje, že existuje znatelný rozdíl kvality vůle i projevu vůle v rámci právního jednání soukromoprávního a veřejnoprávního.[12] Vůle se autonomně uplatňuje pouze v rámci soukromého práva. V rámci veřejného práva je zejména vůle osob na straně orgánů veřejné moci podřízena zásadě vlády právy,[13] tj. že dle čl. 2 odst. 2 Listiny *„Státní moc lze uplatňovat jen v případech a v mezích stanovených zákonem, a to způsobem, který zákon stanoví."* Vůle i projevy vůle osob orgánů veřejné moci se proto musí dobrovolně podřizovat ustanovením zákonů. Přesto je činnost těchto osob v důležité části nenahraditelná a neautomatizovatelná, neboť jejich aplikace práva předpokládá jak kognitivní lidské schopnosti vůči právu i vůči skutkovým stavům, tak lidské schopnosti pro zvažování aplikace práva, zasažených hodnot, přiměřenosti, uvážení (diskrece). V právní nauce pak pochopitelně vznikají

[10] Autor nevylučuje možnost, že se v platném právu ČR vyskytnou obraty o právním jednání, které do zde uvedené taxonomie teorie podřaditelné nejsou, budou však výjimečné.

[11] GERLOCH, A. *Teorie práva.* 7. vydání. Plzeň: Aleš Čeněk, 2017, s. 157.

[12] Přesto jak teorie práva, tak příležitostně i platné právo přisuzuje veřejnoprávním aktům, byť i jen procesním, náležitost vůle nebo projevu vůle. Jsou shodně přítomné, ale v rozdílné kvalitě.

[13] Autor si je vědom, že v české nauce se hovoří o právním státu. Přibližně analogický pojem z práva common law však dle něj lépe ilustruje vztah bezprostřední podřízenosti osobní vůle vůči právu.

spory o to, do jaké míry jsou uvážení a vůle rozhodovatelů zasaženy jejich subjektivitou, a do jaké míry se drží objektivní litery zákona. Autor zde nechce tuto debatu rozvíjet, ale domnívá se, že bez objektivity zákona by právo jako systém ztrácelo smysl, bez lidského vkladu do pochopení a výkladu práva by se však právo nedalo zjistit a být vůči lidem, jako konečným adresátům práva, vůbec použitelné.

Dalším rozdílem je, že veřejné právo je zhusta formálnější (písemná forma apod.) než právo soukromé. Důvodem bývá požadavek na vyšší určitost veřejnoprávního jednání, ale i na vznik záznamů, které lze nezávisle přezkoumávat vyššími instancemi správních úřadů, popř. i soudně.[14] S jistou mírou zjednodušení lze říci, že v soukromém právu se akcentuje svoboda a autonomie účastníků jednat mezi sebou v co nejvyšší míře tak, jak sami chtějí, včetně maximální efektivnosti možnosti provedení jednání, zatímco ve veřejném právu se zajišťuje ochrana jedince před veřejnou mocí, jakož i prosazování určitých hodnot, které se při tom osvědčily, a to i na úkor případné efektivnosti provedení jednání. Dalším důvodem rozdílnosti může být, že ne ve všech případech účastník veřejnoprávního jednání poskytuje součinnost v rámci procesních úkonů. Ty pak proto musí být upraveny dostatečně určitě, zachovat ochranu účastníka, přesto však umožnit prosazení aplikaci práva, popř. později i jeho výkon.

K soukromému právu lze uvést, že i zde jsou adresáti práva poutáni jeho kogentními ustanoveními. Míra volnosti a autonomie je však mnohonásobně vyšší než ve veřejném právu. Ačkoli tedy teorie práva slučuje pod právní jednání *(largo sensu)* soukromé právní jednání *(stricto sensu)* a veřejnoprávní jednání, právní úpravy, kvalita vůle, projevy vůle i provedení jednání obou druhů se budou značně lišit. Více rozmanitosti pak zřejmě poskytuje soukromé právní jednání, tj. právní jednání v užším smyslu, kterému se věnujeme níže.

2.2 Právní jednání (užší smysl)

Druhý význam pojmu *právní jednání* je shodný s výše uvedeným soukromým právním jednáním, jedná se o užší význam pojmu, který je omezen na soukromé právo. Dle české civilistiky se jím obecně rozumí „všechno, co právní subjekt – osoba činí objektivně seznatelně (tj. pro smysly třetích osob zřejmým způsobem) s úmyslem vyvolat právní následky“[15] a spadá pod právní skutečnosti, pro které je charakteristická existence vůle. Civilní nauka upozorňuje, že systematiku porušuje *vytvoření věci* nebo

[14] Článek 36 odst. 2 Listiny.
[15] DVOŘÁK, J. – ŠVESTKA, J. – ZUKLÍNOVÁ, M., cit. dílo, s. 154.

vytvoření díla (autorského), protože tyto činnosti nejsou dle ní nezbytně na vůli[16] závislé, může je provést i malé dítě nebo osoba nesvéprávná. Při těchto jednáních rovněž nemusí vždy vůbec existovat cíl vytvoření právních následků. Teorie civilní[17] i obecná[18] tato vytvoření přesto řadí mezi právní jednání, jelikož je to patrně jednodušší řešení, než je zařazovat mezi jiné právní skutečnosti. Navíc zde aspoň jistá psychologická vůle, s výsledkem souladná, je přítomna, byť nikoli v právní kvalitě smyslu pojmu.

Nauka zjišťuje, že pojem není v platném právu definován, a vyvozuje, že „právním jednáním se rozumí takové chování osoby, subjektu práva, které je schopno – podle ustanovení objektivního práva – vyvolat právní následky.“[19] Za právní následky považuje vznik, změnu nebo zánik práv a/nebo povinností. Podle § 545 obč. zák.: *„Právní jednání vyvolává **právní následky**, které jsou*

- *v něm **vyjádřeny**, jakož i právní následky plynoucí ze*
- ***zákona,***
- ***dobrých mravů,***
- ***zvyklostí***
- *a **zavedené praxe stran**.* “[20]

Z negativních (§ 551–553 obč. zák.) i pozitivních (§ 546 obč. zák.) náležitostí právního jednání či jeho výkladu (§ 556–568 obč. zák.) lze vyvodit, že základem právního jednání je vůle projevená navenek (projev neboli prohlášení vůle).[21] Pojem právního jednání se velmi blíží pojmu *právní úkon*, který byl používán v zák. č. 40/1964 Sb. Ačkoli pojmy nejsou shodné, civilisté se domnívají, že „svou podstatou jsou si velmi blízké, ... při práci s právními předpisy a v aplikační praxi je lze zásadně zaměňovat.“[22] Celkově lze shrnout, že k právnímu jednání je zapotřebí:[23] (i) *vůle*, (ii) *navenek projevená*, (iii) která *má právní následky*.

Vezmou-li se v potaz uvedené tři faktory, je zřejmé, že k vůli musí existovat *subjekt*, o jehož vůli se jedná, ať již se jedná o osobu fyzickou, anebo o osobu

[16] Dobře ilustruje, že vůli právníci zpravidla redukují do kontextu práva a nemíní jí obecnou psychologickou vůli.
[17] DVOŘÁK, J. – ŠVESTKA, J. – ZUKLÍNOVÁ, M., cit. dílo, s. 155.
[18] BOGUSZAK, J. – ČAPEK, J. – GERLOCH, A., cit. dílo, s. 129.
[19] DVOŘÁK, J. – ŠVESTKA, J. – ZUKLÍNOVÁ, M., cit. dílo, s. 156.
[20] Rozčlenil a zvýraznil autor.
[21] DVOŘÁK, J. – ŠVESTKA, J. – ZUKLÍNOVÁ, M., cit. dílo, s. 156.
[22] DVOŘÁK, J. – ŠVESTKA, J. – ZUKLÍNOVÁ, M., cit. dílo, s. 156.
[23] DVOŘÁK, J. – ŠVESTKA, J. – ZUKLÍNOVÁ, M., cit. dílo, s. 156.

právnickou, které se vůle přičítá. Srov. níže náležitosti subjektu. Právní následky se projevují změnou práv a povinností, tedy obecně požadavky na chování subjektů práva, ale mohou se týkat též dalších předmětů, kterých se právní jednání týká. Srov. níže náležitosti předmětu.

V § 546 obč. zák. se upřesňuje, že právně lze jednat *„konáním nebo opomenutím"*. Nauka doplňuje z tradičního římského práva, že pod konání spadá dání *(dare)* nebo činění *(facere)*, zatímco pod opomenutí patří prosté nekonání povinnosti *(non facit)* a v případě práva zdržení se *(omittere)* jeho využití nebo strpění *(pati)* jeho omezování bez obrany prostřednictvím právních prostředků.

Právní jednání, tj. konání nebo opomenutí, může dle § 546 obč. zák. nastat *„výslovně nebo jiným způsobem nevzbuzujícím pochybnost o tom, co jednající osoba chtěla projevit"*. První možnost znamená jednání slovy. Druhou možnost nauka vykládá jako tzv. *konkludentní* právní jednání, přičemž etymologický význam slova má znamenat „ten, jenž je v něčem obsažen".[24] Osoba jedná bez použití slov, ale přesto je navenek objektivně zřejmé, jakou vůli chce projevit. Projev vůle může být zjevný z kontextu jednání, např. nákup v samoobsluze potravin, anebo objektivněji, například zničením listiny závěti. Srov. též níže. Mlčení nebo nekonání samo o sobě ale nejsou považovány za projev vůle. Proto není třeba nijak reagovat například na (nevyžádané) nabídky, aniž by to mohlo mít právní význam ve smyslu souhlasu s nabídkou, a to i kdyby nabídka takovou klauzuli výkladu mlčení obsahovala.[25]

2.2.1 Náležitosti právního jednání

Teorie občanského práva tradičně rozlišuje různé náležitosti právního jednání, a to i) subjektu, ii) vůle, iii) projevu vůle, iv) předmětu. Ty mají s ohledem na náš zájem (elektronické právní jednání) různé stupně důležitosti. Zde je probereme jen stručně.

Mezi náležitosti *subjektu* patří, že právně jednající musí mít právní osobnost i dostatečnou míru svéprávnosti. Pro právní jednání je třeba buď plná svéprávnost,[26] nebo přiměřenost rozumové a volní vyspělosti nezletilých,[27] popř. způsobilost k danému jednání v případě částečné svéprávnosti.[28] Právně jednat mohou i osoby právnické, zejména prostřednictvím svých zástupců (§ 151 an. a § 161 an. obč. zák.).

[24] ZUKLÍNOVÁ, M. Právní jednání podle občanského zákoníku č. 89/2012 Sb. Praha: Linde, 2013, s. 40.
[25] DVOŘÁK, J. – ŠVESTKA, J. – ZUKLÍNOVÁ, M., cit. dílo, s. 157.
[26] Ustanovení § 15 odst. 2 obč. zák.
[27] Ustanovení § 31 an. obč. zák.
[28] Ustanovení § 581 obč. zák.

Předmětem právního jednání je to, čeho se týká, popř. to, čeho se týkají práva a povinnosti právním jednáním založené. Náležitostmi předmětu podle teorie jsou dovolenost a možnost předmětu. Dovolenost se rozumí ve smyslu právním. Je třeba odlišovat nedovolenost předmětu od nedovolenosti samotného jednání, např. pro rozpor se zákonem nebo dobrými mravy, tj. např. podle § 580 obč. zák. O nedovolenost předmětu by se jednalo například v případě komerčního nakládání s částí lidského těla, která je v rozporu s § 112 obč. zák. Obecná teorie práva zde hovoří o primárním a sekundárním objektu právního vztahu, kde primárním je samotné chování, sekundárním je objekt, který se k chování váže.[29] Možností se rozumí, že to, čeho se právní jednání týká, je fyzicky, tj. objektivně možné, za současných vědeckých poznatků a technologických možností. Má-li být *„plněno něco nemožného"*, je takové právní jednání podle § 580 odst. 2 obč. zák. neplatné.[30]

Těžištěm pojmu *právní jednání* jsou vůle a projev vůle, popř. vztah mezi nimi. *Vůle* je „psychický (vnitřní) vztah jednajícího k zamýšlenému následku"; též „chtění, zájem na dosažení nějakého výsledku nebo následku."[31] Výjimkami jsou již výše zmíněné vytvoření díla nebo věci. Není nutné, aby si osoba byla vědoma, že jedná právně, tj. nemusí si být vědoma, že právo provedené jednání považuje za jednání právní. Typicky však právní jednání řídí vůle jednajícího, který chce vyvolat právní následky, a to zpravidla právě ty, které jsou v právním jednání samy vyjádřeny.[32] Zákonné znění je volnější. Umožňuje například, aby strany vyjádřily jen základní ujednání, a zbytek plní buď dle obsahu zákona pro daný typ jednání, nebo podle zvyklostí, které si mezi sebou zavedly dříve.

Dle civilistiky se drtivá většina teoretiků kloní k tomu, že *bez vůle* nejde o právní jednání, shodně stanoví § 551 obč. zák. Na existenci vůle se přitom usuzuje z vnějšího projevu. Při vytváření projevu se zřejmě uplatní právní domněnka *„rozumu průměrného člověka"* a *„schopnosti jej užívat s běžnou péčí a opatrností"* podle § 4 odst. 1 obč. zák., vyjadřující má rovněž povinnost jednat poctivě a v dobré víře (§ 6 a § 7 obč. zák.). Náležitostmi vůle jsou *svoboda* vůle (bez donucení fyzického nebo psychického), *vážnost* vůle (ne předstírání žertem nebo hrou), nepřítomnost právně významného

[29] GERLOCH, A., cit. dílo, 2017, s. 169–170.
[30] DVOŘÁK, J. – ŠVESTKA, J. – ZUKLÍNOVÁ, M., cit. dílo, s. 164.
[31] DVOŘÁK, J. – ŠVESTKA, J. – ZUKLÍNOVÁ, M., cit. dílo, s. 158.
[32] DVOŘÁK, J. – ŠVESTKA, J. – ZUKLÍNOVÁ, M., cit. dílo, s. 159.

omylu a obecněji i nezneužití stavu *tísně* (§ 1796 obč. zák.). Vnitřní pohnutka nebo motiv vůle jsou však právně nerozhodné, proto i omyl o nich.[33]

Na *projev vůle* se kladou náležitosti určitosti, srozumitelnosti a případně formy. *Určitostí* je míněna jednoznačnost. Neurčité je takové jednání, jehož význam nelze zjistit ani výkladem (§ 553 obč. zák.). *Srozumitelnost* dostačuje relativní, tj. mezi stranami jednání. Absolutní neurčitost nebo nesrozumitelnost způsobuje zdánlivost, tj. neexistenci jednání, nicméně dle české úpravy ji lze dodatečně zhojit (§ 553 odst. 2 obč. zák.). Ve *formě* jednání platí zásada bezformálnosti (§ 559 obč. zák.), resp. svobody volby formy, v čemž ale jednající může být omezen ujednáním nebo zákonem. Teorie tradičně dělí právní jednání na výslovné a konkludentní, přičemž výslovné se člení na ústní a písemné. Zákon příležitostně předepisuje jako povinnou i ústní formu, např. pro prohlášení o uzavření manželství. Častěji zákon předepisuje písemnou formu, popř. se na písemné formě ujednají strany jednání. Písemné jednání vyžaduje pro perfekci podpis (§ 561 odst. 1 věta první obč. zák.). K nahrazování písemné formy právním jednání učiněném elektronickými prostředky srov. níže (5.1). Někdy zákon předepisuje přítomnost všech podpisů jednajících osob na téže listině, čemuž vyhovuje i spojený svazek listů. Zákon může pro právní jednání předepsat i tzv. přísnou písemnou formu, tj. formu veřejné listiny, typicky notářský zápis.[34]

2.2.2 Členění právních jednání

Právní teorie používá členění na základě mnoha kritérií. Z hlediska elektronického právního jednání největší smysl má členit dle subjektů a dle adresování.

Podle subjektů se právní jednání rozlišují na *jednostranné* a *dvou-* či *vícestranné*. O stranách se zde hovoří z toho důvodu, že obecně je možné, aby na každé straně byla více než jedna osoba. Hovoří se pak o pluralitě subjektů. Kromě případných rozdílů požadavků na technické zajištění styku mezi stranami rozdíl spočívá i v okamžiku perfekce. U jednostranného vzniká právní jednání jeho učiněním, ale může též někdy být třeba, aby došlo jiné osobě. V případě vícestranného právního jednání vzniká nejdříve v okamžiku, kdy právní jednání učinila poslední ze stran, ale může též ještě vyžadovat dojití protější straně či stranám.[35]

[33] DVOŘÁK, J. – ŠVESTKA, J. – ZUKLÍNOVÁ, M., cit. dílo, s. 158–161.
[34] DVOŘÁK, J. – ŠVESTKA, J. – ZUKLÍNOVÁ, M., cit. dílo, s. 161–163.
[35] DVOŘÁK, J. – ŠVESTKA, J. – ZUKLÍNOVÁ, M., cit. dílo, s. 165.

V případě jednání mezi nepřítomnými osobami[36] dle § 570 obč. zák. je totiž třeba rozlišovat mezi právním jednáním *adresovaným* a neadresovaným. Adresovaná právní jednání působí vůči *„nepřítomné osobě [až] od okamžiku, kdy jí projev vůle dojde"*. Dojitím či doručením se rozumí, že se projev vůle dostal do *dispoziční sféry adresáta*. Dostačuje tedy, aby měl možnost se s ním seznámit, není nutné, aby tak skutečně učinil, ať již nevybírá klasickou poštovní schránku, nebo schránku elektronické pošty. Až dojité právní jednání se těší své perfekci, tedy hotovosti právního jednání.[37] Z hlediska technického provedení je pochopitelně pak vhodné volit taková, která v případě sporu jsou schopna prokázat, že k dojití došlo.

Běžně kupř. u dvoustranné smlouvy dochází ke smluvnímu procesu mezi oferentem a adresátem, přičemž oferta i akceptace jsou adresovaným právním jednáním, takže každé musí protistraně dojít. Mezi nepřítomnými stranami k uzavření smlouvy proto dojde až dojitím akceptace do dispoziční sféry oferenta (§ 1745 obč. zák.). Výjimkou je jednání za podmínek podle § 1744 obč. zák., kdy adresát tzv. *konkludentně akceptuje* tím, že začne se začne chovat, typicky plnit, podle oferty.[38]

2.2.3 Obsah právního jednání

V teorii se za obsah právního jednání tradičně považují složky právního jednání. Ty se následně člení na podstatné, pravidelné a nahodilé. Je potřeba si zde uvědomit, že na obsah v tomto smyslu se nahlíží spíše materiálně než formálně. Formální pojetí obsahu právního jednání vyvstává spíše v rámci formálního provedení právního jednání, tedy při písemném právním jednání. Obsahem pak formálně je písemnost, kterou jednající osoba podepisuje, do materiální roviny se však dostane až svým výkladem.

Kritická je přítomnost *podstatných složek (essentialia negotii)* právního jednání, jimiž jsou ty, „bez kterých by právní jednání nebylo tím, o které má jít".[39] Absence složky má za následek zdánlivost (tj. právní neexistenci) jednání. Obsah takového právního jednání by neodpovídal zákonu (§ 547 obč. zák.). Občanský zákoník u typových obligací (§ 2055–2893) podstatné složky vždy uvádí v prvním paragrafu daného druhu právního jednání, ad rubrica *„Základní ujednání"*. Pokud se jedná o atypický závazek, v občanském zákoníku výslovně neupravený, je třeba podstatné

[36] V případě jednání mezi osobami přítomnými pravidlo platí shodně, ale vzhledem k okamžité komunikaci jej nemá smysl zmiňovat.
[37] DVOŘÁK, J. – ŠVESTKA, J. – ZUKLÍNOVÁ, M., cit. dílo, s. 165, 185.
[38] DVOŘÁK, J. – ŠVESTKA, J. – ZUKLÍNOVÁ, M., cit. dílo, s. 175–176.
[39] DVOŘÁK, J. – ŠVESTKA, J. – ZUKLÍNOVÁ, M., cit. dílo, s. 182.

složky „dovodit z obsahu jednání nebo z vůle stran: je tím to, o čem strany daly najevo, anebo je z okolností zřejmé, že bez dohody právě o této otázce by strana smlouvu neuzavřela“.[40] Podstatné složky se však vyskytují a bývá třeba je určit i v případě jednostranných právních jednání. Je nutné je vyvodit ze zákonných ustanovení. V případě oferty tato musí obsahovat nezbytné složky smlouvy.

Pravidelné složky (naturalia negotii) se v právním jednání vyskytují zpravidla. Nemusí se však vyskytovat nutně. Jejich absence nemá dopad na platnost právního jednání, doplňuje a nahrazuje je zákon z těch ustanovení, která náleží k danému typu právního jednání, určeného z podstatných složek.

Nahodilé složky (accidentalia negotii) se v právním jednání vyskytují jen příležitostně. Zákon je nenahrazuje, musí být součástí jednání explicitně. Mezi nahodilé složky se řadí podmínky *(conditione)*, doložení času *(dies)* a příkaz *(modus)*, je-li dovolený.[41]

Odlišný právně teoretický názor má Flume. Dle něj[42] jsou obsahem právního jednání pouze *essentialia negotii* a *accidentalia negotii*, neboť jen ty jsou původním výsledkem vůle právně jednající osoby (nebo osob). Oproti tomu *naturalia negotii* jsou výsledkem právní úpravy obsažené v legislativě a jednající osoba si často není jejich existence vůbec vědoma. Pokud *accidentalia negotii* odporují kogentním ustanovením z *naturalia negotii*, nebudou vůbec platné. Flume hledí na obsah právního jednání[43] jako na akt v průběhu vytváření a jako na regulaci poté, co je dosaženo perfekce daného právního jednání. Tím je u něj dán akcent na normativní význam obsahu právního jednání, který je založen soukromými osobami.

2.2.3.1 Podmínky

Vedlejší složkou právního jednání mohou být i podmínky, které činí jeho právní následky (vznik, změnu nebo zánik práv) závislé na skutečnostech, které nejsou v okamžiku jednání známy. Skutečnost pro podmínku nemusí být právní skutečností ve smyslu práva, ale jde o „nějakou součást objektivní reality“,[44] tj. vnějšího světa. Neznalost se může týkat toho, zda nastane, kdy nastane anebo zda již nastala, ale zatím

[40] DVOŘÁK, J. – ŠVESTKA, J. – ZUKLÍNOVÁ, M., cit. dílo, s. 182.
[41] DVOŘÁK, J. – ŠVESTKA, J. – ZUKLÍNOVÁ, M., cit. dílo, s. 181–184.
[42] FLUME, W. *Allgemeiner Teil des Bürgerlichen Rechts. Band 2, Das Rechtsgeschäft*. Berlin: Springer, 1992, s. 80–81.
[43] Přinejmenším v kontextu německého práva.
[44] DVOŘÁK, J. – ŠVESTKA, J. – ZUKLÍNOVÁ, M., cit. dílo, s. 183.

není známa. Občanský zákoník dělí podmínky předně na odkládací a rozvazovací (§ 548 odst. 2 obč. zák.). Splnění odkládací podmínky má důsledek, že *„právní následky jednání nastanou"*. Splnění rozvazovací podmínky má za důsledek, že *„právní následky již nastalé pominou"*.

Z hlediska splnění podmínek je obsaženo několik omezení. K nemožným podmínkám se nepřihlíží. Je-li splnění, resp. nesplnění podmínky v prospěch nějaké osoby, pak by běžně tato osoba neměla záměrně způsobit splnění podmínky, resp. zaměrně zmařit její splnění (§ 549 obč. zák.). Sankcí je nepřihlížení k takto splněné podmínce, resp. považování podmínky za splněnou v případě zmaření. Výjimkou ze sankcí je, pokud je osoba k záměrnému působení na splnění, resp. nesplnění podmínky oprávněna. Bez újmy charakteristiky podmínek jako odkládacích a rozvazovacích lze podmínky dále členit či formulovat jako pozitivní (bude pršet) i negativní (nebude pršet). Vznikne-li pochybnost o charakteru podmínky, pak podle § 548 odst. 3 obč. zák. se presumuje, že podmínka je odkládací. Jelikož podmínky jsou součástí právního jednání, platí i o nich, že obsahem a účelem musí odpovídat zákonu i dobrým mravům (§ 547 obč. zák.).

2.3 Právní jednání v Obecném zákoníku občanském – retrospekce

Poslední část této kapitoly je zařazena, jelikož Obecný zákoník občanský platil na území českých zemí téměř 140 let a byl i podkladem, na jehož základě se zde vytvářela civilní právní nauka, jakož i obecnější teorie práva. V tomto textu poslouží i jako časový a terminologický most k německé úpravě v BGB, probírané níže.

Podíváme-li se na první velký právní kodex na území českých zemí v moderní době, tj. na *Obecný zákonník občanský císařství rakouského*[45] (dále jen „o. z. o."), vydaný roku 1811 s účinností od 1. ledna 1812,[46] obrat právní jednání v něm nalezneme pouze zcela okrajově, např. v § 34 *„Zdali cizinec některé* ***jednání právní*** *osobně*

[45] Pracujeme zde se zřejmě nejstarším zněním obecného zákoníku občanského v českém jazyce, veřejně dostupném v knihovnách na území ČR: *Obecný zákonník občanský císařství rakouského*, vytištěn v C. K. tiskárně dvorské a státní, ve Vídni, 1862. Sken vydání je dostupný z: <http://lib.wikipravo.cz/libro/BookExplorer?akce=7&abbr=ozo&aktPage=1>.

[46] Německy *Allgemeines bürgerliches Gesetzbuch für die gesammten Deutschen Erbländer der Österreichischen Monarchie*, zkratka ABGB, 946. Patent vom 1ten Junius 1811. Justizgesetzsammlung. Sken sbírky Justizgesetzsammlung z roku 1811 je dostupný z: <http://alex.onb.ac.at/cgi-content/alex?apm=0&aid=jgs&datum=10120003&zoom=2&seite=00000275>.
Neúřední německý text ABGB ve formátu HTML je k dispozici na: <http://www.koeblergerhard.de/Fontes/ABGB1811.htm>.

předsevzíti může, uvažováno budiž vůbec dle zákonů místních, ...“[47] Zákoník jinak s tímto termínem explicitně vůbec nepracuje. Zákoník sice je vystavěn modulárně podle systému římského soukromého práva, tak jako tomu bylo i jinde na kontinentu, ale nemá ještě systematicky zcela tu terminologickou výstavbu, na kterou jsme v ČR dnes zvyklí.

Současně však úvodní vyhlašovací patent císaře nám dává najevo, že pojem právního jednání již byl v právní komunitě znám: *„diese Handlungen mögen in **zweyseitig verbindlichen Rechtsgeschäften**, oder in solchen **Willenserklärungen** bestehen, die von dem Erklärenden noch eigenmächtig abgeändert...“*[48]. Právníci té doby tedy již znali závazné právní jednání dvoustranné *(das Rechtsgeschäft)*, zatímco pro jednostranné se používal spíše pojem *die Willenserklärung*. Ten se ale použil v obecném zákoníku občanském jen pro termín poslední vůle *(die letze Willenserklärung)*, např. v § 480 o. z. o. Mnoho desítek výskytů má v Obecném zákoníku občanském ale zkrácený pojem *die Erklärung*, překládaný většinou pravidelně jako prohlášení, např. v § 49 se zmiňuje prohlášení zákonného zástupce za nezletilého, tj. právní jednání za něj.

K platnosti manželství je podle § 69 zapotřebí *„das Aufgeboth und die feyerliche **Erklärung** der Einwilligung“*, tj. *„ohlášek a slavného **pronešení**, že k manželství se přivoluje.*“ Z § 75 zjistíme, že *„Die feyerliche **Erklärung** der Einwilligung zur Ehe*“ , v češtině *„Slavné **prohlášení**, že se k manželství přivoluje“*, se činí za přítomnosti dvou svědků před řádným duchovním správcem, tedy jedná se o sňatečné prohlášení obou snoubenců, vlastní uzavření sňatku. Český překladatel se zde dopustil pojmové nekonzistence *pronešení* vs. *prohlášení*.

V § 566 o. z. o. je pro nás zajímavé kazuistické ustanovení[49] *„Dokáželi se, že někdo poslední **vůli** pronesl v zuřivosti, v šílenosti, v blbosti aneb v opilství, jest neplatná.“* Všechny vyjmenované stavy nepříznivě ovlivňují rozum, a potažmo i vůli osoby.

Dalšími pro nás relevantním pojmy jsou učinění slibu, přijetí slibu a smlouva. Podle § 861 o. z. o.: *„Kdo **se pronese**, že chce na někoho právo své převésti, totiž*

[47] Německý originál: „§. 34. Die persönliche Fähigkeit der Fremden zu Rechtsgeschäften ist insgemein nach den Gesetzen des Orts, ... zu beurtheilen;“. Zvýraznění v citacích o. z. o. provedl autor.

[48] V českém znění z roku 1862: „...nechať to bylo nějaké **jednání právní** oboji stranu zavazující, nebo **pronešení vůle**, kteréž by ten, kdo ji pronesl, o své ujmě posud mohl změniti...“

[49] „§. 566. Wird bewiesen, daß die **Erklärung** im Zustande der Raserey, des Wahnsinnes, Blödsinnes, oder der Trunkenheit geschehen sey, so ist sie ungültig.“

něčeho dopustiti, něco mu dáti, k jeho dobrému něco učinit, anebo jemu k vůli něco opominout, ten ***činí slib****; a když druhý platným způsobem* ***slib přijme****, stane se srovnalou vůlí obou stran* ***smlouva****. Pokud strany se smlouvají, a slib ještě není učiněn, nebo ani napřed, ani potomně přijat, smlouva nevzchází.“*[50] Mezníky zde jsou tedy učinění slibu (zřejmě má i význam oferty) a jeho přijetí (akceptace) při srovnalé vůli obou stran. Předchozím vyjednáváním o podmínkách smlouva ještě nevzniká. Ustanovení uvádí, vyjádření jakého obsahu představují právní učinění slibu.

V § 862 o. z. o. se stanoví lhůty pro přijetí slibu. Není-li domluveno jinak, *„budiž slib ústní přijat bez průtahu“*. Při písemném slibu má přijetí běžně následovat do 24 hodin. Dle § 865 nemůže ale slib dát ani přijmout ten, *„kdo nemá zdravého rozumu, též i dítě...“*, přičemž dětmi byly osoby mladší sedmi let.

Z § 863 o. z. o. plyne, že za pronesením (tj. vyjádřením) slibu stojí vůle, že však vyjádření může mít různé formy, včetně formy tzv. konkludentní: *„Vůli pronésti lze nejen výslovně slovy a znameními vůbec obyčejnými, ale i mlčky takovými činy, dle kterých, uvážíme-li všechny okolnosti, není důvodné příčiny, abychom o tom pochybovali.“* Smlouva může mít různé ceremoniální formy podle § 883: *„Smlouva činiti se může ústně nebo písemně; před soudem nebo mimo soud; u přítomnosti svědků nebo bez svědků.“*

I další ustanovení obecného zákoníku občanského se stáčí k pojmu smlouvy. Dle § 869 *„****Přivolení*** *ke smlouvě pronešeno budiž bez nucení, vážně, určitě a srozumitedlně.“* Též však ustanovení o lsti *„Kdo by, chtěje jiného podskočiti, slov nejasných užil, nebo něco jen na oko předsevzal, práv z toho bude.“* Tj. bude za to nést odpovědnost. Například podle § 871 *„Byla-li strana jedna stranou druhou křivým předstíráním v omyl uvedena, a týčeli se omyl hlavní věci, ..., kdo byl v omyl uveden, závazku nevzchází.“* Konečně, dle § 881 *„Kromě případností v zákoně jmenovaných nemůže nikdo za jiného slibu činit, ani přijímati...“*

Kromě uvedených soukromoprávních jednání obsahuje obecný zákoník občanský slovo *die Erklärung* i pro právní akty úřední, např. prohlášení za zletilého *(die Erklärung der Volljährigkeit)* nebo pro prohlášení za mrtvého *(die Todeserklärung)*.

[50] „§. 861. Wer **sich erkläret**, daß er jemanden sein Recht übertragen, daß heißt, daß er ihm etwas gestatten, etwas geben, daß er für ihn etwas thun, oder seinetwegen etwas unterlassen wolle, **macht ein Versprechen**; **nimmt** aber der Andere **das Versprechen** gültig **an**, so kommt durch den übereinstimmenden Willen beyder Theile **ein Vertrag** zu Stande. So lange die Unterhandlungen dauern, und das Versprechen noch nicht gemacht, oder weder zum voraus, noch nachher angenommen ist, entsteht kein Vertrag.“

Dalším pojmem, kterým je obecný zákoník občanský zaplaven, je *das Geschäft*, s více než stovkou výskytů. Obrat lze někdy vyložit jako *záležitost*, většinou však má význam nějaké záležitosti s potřebou aktivního jednání v právním smyslu, tedy *právní jednání*. Často by významu odpovídalo i české slangové *kšeft*, které se však pro spisovný jazyk nevžilo. Pozoruhodné je, že v řadě případů je slovo použito i pro označení druhu smlouvy *(das Abhandlungsgeschäft, Handlungsgeschäft, Borggeschäft...)*. Český překladatel r. 1862 nakonec rezignoval na odlišování termínů *das Geschäft* a *der Vertrag* a kupř. *das Kaufgeschäft* přeložil jako *smlouvu trhovou*, což by dnes byla kupní smlouva. Autor má však dojem, že německé termíny obecného zákoníku občanského se více vztahují ke kauze právního jednání, k její záležitosti *(das Geschäft)*, zatímco pojem smlouva *(der Vertrag)* je již právní pojem, který se odvolává na formu vzniklého právního vztahu, který se zakládá právním jednáním.

Příležitostně obecný zákoník občanský používá jednostranné vazby jako *„vejití v práva“* nebo *„vstupování do závazků“*. Kromě výše uvedených postižení vůle může být soudně ze správy svého jmění vyloučen podle § 21 i marnotratník.

2.3.1 Abstrakce právního jednání z obecného zákoníku občanského

Celkově lze shrnout, že obecný zákoník občanský používá zejména pojmy *die Erklärung* (prohlášení), *das Geschäft* (~[právní] záležitost), *ein Versprechen machen* (učinit slib), *ein Versprechen annahmen* (přijmout slib), *der Vertrag* (smlouva), *die Einwilligung in einen Vertrag* (přivolení ke smlouvě) a jen výjimečně *das Rechtsgeschäft* nebo *die Willenserklärung*.

Všechny tyto pojmy v sobě obsahují prvek lidské vůle a jejího projevu. V různých místech zákoníku se pak nachází ustanovení o vůli a jejích náležitostech, o jejím projevu a náležitostech projevu. V zákoníku jsou řazena tam, kde byl tehdy zákonodárce nejvíce přesvědčen o příhodnosti jejich přítomnosti.

Odhlédněme nyní od různě rozptýleného umístění. O náležitosti vůle pak lze říci, že se má jednat o svobodnou vůli rozumného člověka, tj. s rozumem, kterým disponuje běžně osoba zletilá (v omezené míře i osoba nezletilá, ne však dítě) a současně nepostižená např. šíleností (či zuřivostí, blbostí, opilstvím) nebo soudně prohlášením za marnotratníka. Tvorba vůle má proběhnout bez omylu či lsti. Projev vůle pak musí být též svobodný (bez nucení), vážný (ne naoko), srozumitelný (pochopitelný) a určitý (pochopitelný jednoznačně).

Všechny uvedené pojmy s daným vlastnostmi v zákoníku pak existují proto, aby jejich spojením s odpovídajícím jednáním subjektu či subjektů vzniklo právní vázání jednoho nebo více subjektů.

Uvedené jsou podstatné znaky právního jednání, jak je v různých místech vyjadřuje obecný zákoník občanský. Na území ČR byl Obecný zákoník občanský účinný až do 31. prosince 1950, byť v mezidobí prodělal určité novelizace. Na území Rakouska je nepřetržitě účinný dodnes, jedná se o druhý nejstarší občanskoprávní kodex v Evropě vůbec.

Tato strana je záměrně ponechána prázdná.

3. Právní jednání v soukromém německém právu

V této kapitole probíráme pojetí pojmu *právní jednání*, jak se užívá v německém soukromém právu. Základní úprava je obsažena v německém občanském zákoníku BGB *(Bürgerliches Gesetzbuch)*. Tento kodex vznikl řádově jedno století po výše probíraném rakouském Obecném zákoníku občanském. V BGB je již systematika spojená s právním jednáním, ve srovnání s Obecným zákoníkem občanským, přerovnaná. V úvodu této kapitoly stručně popíšeme situaci.

Vlastnosti právního jednání, jak je pojem chápán ve středoevropské tradici, si s sebou do značné míry nese již pojem *die Willenserklärung*, který tvoří i nadpis titulu 2 pro § 116–144 BGB. Právě pro *vyjádření vůle*[1] *(die Willenserklärung)* reglementuje BGB obdobné náležitosti, jaké jsme pro právní jednání odvodili výše z Obecného zákoníku občanského, např. mentální výhrada (§ 116 BGB), zdánlivé a předstírané jednání (§ 117 BGB), vada vážnosti (§ 118 BGB), omyl (§ 119 BGB), klam a hrozba (§ 123 BGB), různé požadavky na formu atp. Novinkou oproti Obecnému zákoníku občanskému je např. špatný přenos vyjádření vůle (§ 120 BGB).

Slovo *die Erklärung* se v BGB používá buď jako zkrácená forma od *die Willenserklärung* (a má pak i stejný právní význam), což někdy snadno plyne z kontextu použití např. ve stejné větě, stejném odstavci či paragrafu, někdy se však určuje obtížněji. Řídčeji má jazykový význam slova *prohlášení*, tedy formálnějšího projevu. Druhým použitým výrazem pro *právní jednání* je v BGB pojem *das Rechtsgeschäft*. Popis jeho vlastností se někdy mísí s požadavky na vyjádření vůle v rámci ustanovení § 116–144 BGB.

Oba pojmy nejsou v BGB definovány. Nauka pak význam prvního pojmu zjišťuje či definuje například tak, že *vyjádření vůle (eine Willenserklärung)* „je projevení vůle zaměřené na vyvolání právních následků. Vyjevuje vůli k právním následkům, tj vůli, která směřuje na založení, obsahovou změnu nebo zánik soukromého právního vztahu.“[2] Výklad BGB a nauka vyžadují, aby nezbytnou částí vyjádření vůle byl objektivní skutkový znak *(objektiver Tatbestand)*.

---

[1] V tomto textu budeme *die Willenserklärung* z BGB důsledně překládat jako *vyjádření vůle*, abychom jej odlišili od situací, kdy hovoříme o projevu vůle v kontextu jiného právního řádu, nebo obecněji.

[2] „Eine Willenserklärung ist die Äußerung eines auf die Herbeiführung eines Rechtsfolges gerichteten Willens. Sie bringt einen Rechtsfolgewillen zum Ausdruck und somit einen Willen, der auf die Begründung, inhaltliche Änderung oder Beendigung eines privaten Rechtsverhältnisses abzielt.“ In HÄRTING, N. *Internetrecht*. Köln: Verlag Dr. Otto Schmidt KG, 2014, s. 102.

Pojem *právní transakce*[3] *(das Rechtsgeschäft)* je pak německou doktrínou vykládán tak, že se jedná o[4] „skutkový znak *[Tatbestand]*, s nímž právní řád spojuje chtěné právní následky“. Předpokladem právního jednání *(Rechtsgeschäft)* přitom je aspoň jedno vyjádření vůle, u vícestranných právních jednání může být zapotřebí více vyjádření vůle. Při vyjádření vůle *(Willenserklärung)* se vždy jedná o jednání pouze jediné osoby. Na potřebném naplnění znaků právního jednání *(das Rechtsgeschäft)* se může podílet jak vyjádření vůle jen jedné osoby (např. při výpovědi, při rozporování), ale i více osob (smlouva). Předpokladem právního jednání mohou být i další skutkové znaky, např. sjednocení vůlí *(die Willenseinigung)* při uzavření smlouvy.

3.1 Pojmy „die Willenserklärung“ a „das Rechtsgeschäft“ v Motive

V předmětu našeho zájmu, tj. právního jednání, používá BGB dva pojmy. Prvním je *die Willenserklärung*, překládaný jako projev vůle.[5] Z důvodů zvýraznění pojmu a rozlišení, že hovoříme o pojmu z BGB a v kontextu německého soukromého práva, ho v této práci budeme však překládat jako ***vyjádření vůle***. Druhým pojmem je *das Rechtsgeschäft*, který bývá překládán právě jako právní jednání.[6] Po určitém váhání se autor rozhodl, ze stejných důvodů jako u prvního pojmu, že pro překlad *das Rechtsgeschäft* z německého práva se v této práci bude používat ***právní transakce***.[7] Pojem má v Německu poměrně ostře vymezený doktrinární význam.

Předně je třeba si uvědomit, že oba pojmy jsou abstraktními právními pojmy, které se v BGB vyskytují jako součást mnoha právních norem. Ani jeden není v BGB definován. Pro aplikaci práva je tedy třeba se ptát, jaká skutková podstata jednání osoby může tyto pojmy naplnit.

V německé právní literatuře se pravidelně vyskytují popisy těchto pojmů zhruba trojího druhu. První druh popisu se citačně odvolává na první důvodovou zprávu návrhu

---

[3] V tomto textu budeme *das Rechtsgeschäft* z BGB důsledně překládat jako *právní transakce*, abychom jej odlišili od situací, kdy hovoříme o právním jednání jako o zastřešujícím pojmu pro *das Rechtsgeschäft* i *die Willenserklärung*, obecně nebo v jiném kontextu. Pojem právní transakce v této kapitole se nesmí směšovat nebo zaměňovat s pojmem právní transakce z níže probíraného evropského nařízení eIDAS v dalších kapitolách.

[4] „Der Tatbestand, an den die Rechtsordnung den Eintritt einer gewollten Rechtsfolge knüpft.“

[5] HORÁLKOVÁ, M. *Německo-český právnický slovník*. Voznice: LEDA, 2010.

[6] V HORÁLKOVÁ, M., cit. dílo, je das Rechtsgeschäft překládán jako právní úkon, vzhledem k nabytí účinnosti občanského zákoníku by však zcela zjevně pojem byl nově překládán jako právní jednání.

[7] Stejné pojetí překladu das Rechtsgeschäft, tj. *legal transaction*, je použito ve velmi kvalitním překladu BGB do angličtiny, který pochází od Langenscheidt Translation Service, je aktualizován od Neil Mussetta nejčerstvěji od Samson Übersetzungen GmbH a Dr. Carmen v. Schöning. Dostupné z: <https://www.gesetze-im-internet.de/englisch_bgb/>.

zákona BGB zvanou *Motive*,[8] která byl zveřejněna již roku 1888. Konkrétně se odvolává na *Motive I*,[9] kde římská číslice značí první svazek (Band I). Druhý popis používá běžná didaktická právnická literatura občanského práva. Třetí se nachází v hluboce teoretických rozpravách, ze které je níže podáván výklad Flumeho.

Ohledně historického výkladu předkladatelé BGB v *Motive I* především vysvětlují, proč nepodávají definice: *„Pokus o definice pojmů v § 88 saského občanského zákoníku je jen málo povzbudivý pro následování. Nebezpečí, že jakkoli uzpůsobené znění způsobí zmatky, je mnohem větší než protichůdné nebezpečí, že se rozkymácí soudnictví a aplikuje rozhodné zásady právních transakcí na jednání, které přirozenost právních transakcí nemají, anebo že skutečné právní transakce neocení."* [10] Právníci mají na jejich vlastnosti usuzovat z jednotlivých ustanovení, které byly voleny tak, aby v podstatě odpovídaly v té době panující nauce.

Ve své zprávě pak uvádí tento popis: *„**Právní transakce** [das Rechtsgeschäft] ve smyslu návrhu je soukromé vyjádření vůle, směřující k vytvoření právního následku, který vzniká podle právního řádu z toho důvodu, že je chtěný. Podstata právní transakce spočívá v tom, že na vytvoření právních účinků se podílí k nim směřující vůle, a že výrok právního řádu v uznání této vůle uskutečňuje chtěný právní výtvor v právním světě."* [11] Do právního řádu však takovou či podobnou definici vložit nechtějí, jelikož si nejsou jisti tím, zda by obstála za všech okolností a nevyvolávala nejasnosti.

Druhý pojem definují stručněji: *„Pod **vyjádřením vůle** [die Willenserklärung] se rozumí právně transakční vyjádření vůle."*[12] Je to tedy takové vyjádření vůle, které směřuje k vytvoření právního následku z toho důvodu, že je chtěný tím, kdo danou vůli vyjadřuje, přičemž právní řád daný projev vůle uznává, a tak vzniká právní následek. Právní řád však nemusí uznat projev vůle jakéhokoli obsahu. Musí tedy dojít k souběhu toho, že osoba vyjadřuje vůli a obsah této vůle je právním řádem uznatelný.

Není divu, že předkladatelé sami napsali: *„Pojmy vyjádření vůle a právní transakce se pravidelně používají jako stejné. První pojem se volí především tehdy, když vyjádření vůle jako takové vystupuje v popředí, nebo když současně nastává případ, že*

[8] Motive zu dem Entwurfe eines Bürgerlichen Gesetzbuches für das Deutsche Reich. 5 Bände. Verlag von J. Guttentag (D. Collin): Berlin/Leipzig, 1888.

[9] Motive zu dem Entwurfe eines Bürgerlichen Gesetzbuches für das Deutsche Reich. Band I. Verlag von J. Guttentag (D. Collin): Berlin/Leipzig, 1888. 395 s. Digitalizováno na: <https://ia902605.us.archive.org/4/items/motivezudementw01germgoog/motivezudementw01germgoog.pdf>.

[10] Motive ..., cit. dílo, Band I, s. 126.

[11] Motive ..., cit. dílo, Band I, s. 126. Zvýraznil autor.

[12] Motive ..., cit. dílo, Band I, s. 126. Zvýraznil autor.

vyjádření vůle je jen součástí právně transakční skutkové podstaty, která přichází do úvahy."[13] Pojmy tedy často splývají, v právu však bude vhodnější hovořit o právní transakci třeba u kupní smlouvy, zatímco v případě závěti o vyjádření vůle, kde by zejména německé *das Geschäft* neznělo vůbec vhodně. Druhý zmíněný případ rozchodu používání pojmů však budeme muset prozkoumat podrobněji.

3.2 Pojmy „Willenserklärung" a „Rechtsgeschäft" v běžné nauce

V této části popíšeme pojmy *die Willenserklärung* a *das Rechtsgeschäft* stručně a včetně kontextu dalších úzce navazujících pojmů tak, jak je jejich popis běžně nalezitelný v německé právní literatuře, tedy druhým výše avizovaným způsobem. Jedná se o běžně dostupný výklad v rámci teoretického popisu pojmů. Můžeme se s nimi setkat zejména v popisech a výkladech obecné části BGB,[14, 15] anebo v komentářové literatuře,[16, 17] ve které příležitostně bývá shrnující výklad pojmů na počátku jednotlivých částí zákoníku BGB. Účelem zde je poznat i aparát souvisejících pojmů, vůči nimž nebo s jejichž pomocí se námi zkoumané pojmy vymezují, nezacházet však do podrobností.

Právní teorie soukromého práva Německa používá pro všechna lidská chování s právním následkem zastřešující pojem *právní chování (rechtliches Verhalten)*.[18] Ta zahrnují na jedné straně *vyjádření vůle (die Willenserklärung)* a *právní transakce (die Rechtsgeschäfte)*, na straně druhé kategorii tzv. označovanou jako *právní konání (die Rechtshandlungen)*. Užitečnější než druhou kategorii definovat je uvést, že zahrnuje *jednání podobná právním transakcím (geschäftsähnliche Handlungen)* a *reálné akty (die Realakte, též faktická jednání – Tathandlungen)*.

Dle první definice: „„*Vyjádření vůle" (Willenserklärung)* je (soukromé) vyjevení vůle jedince, které má přivodit právní následek (např. uzavření smlouvy)."[19] Uvedené vyjádření vůle tedy musí směřovat k právnímu následku, jinak by vyjádření nemělo žádný právní účinek, resp. přinejmenším žádný účinek v rámci institutu vyjádření vůle.

---

13 *Motive ...,* cit. dílo, Band I, s. 126.

14 REICH, D. O. – SCHMITZ, P. *Einführung in das Bürgerliche Recht : Grundlagen des BGB – Allgemeiner Teil – Allgemeines Schuldrecht – Besonderes Schuldrecht – Sachenrecht*. Wiesbaden: Gabler, 2000.

15 KÖHLER, H. *BGB, Allgemeiner Teil : ein Studienbuch*. München: C. H. Beck, 1996.

16 SÄCKER, J. (ed.) *Münchener Kommentar zum Bürgerlichen Gesetzbuch: BGB Band 1: Allgemeiner Teil §§ 1–240, ProstG, AGG.* 7. Auflage. München: C. H. Beck, 2015.

17 PALANDT, O. *Bürgerliches Gesetzbuch*. 69. neubearb. Aufl. München: C. H. Beck, 2010.

18 REICH, D. O. – SCHMITZ, P., cit. dílo, s. 8.

19 REICH, D. O. – SCHMITZ, P., cit. dílo, s. 11.

Jako „vůle k právnímu následku“ přitom platí každá vůle, která cílí k založení, změně nebo ukončení soukromého právního vztahu.

Složitějším případem abstrakce je další definovaný pojem: „‚*Právní transakce*‘ *(ein Rechtsgeschäft)* sestává z jednoho nebo více vyjádření vůle, které samy nebo ve spojení s jinými znaky skutkové podstaty vyvolávají právní následek, protože je chtěný.“[20] Právní transakce je tedy složený pojem, sloužící pro možnost zachycení více náležitostí právního vztahu současně, resp. jeho potřebných složek, jak se v právním řádu používají pro popis dané právní transakce. Podstatné je, že vždy musí obsahovat aspoň jedno vyjádření vůle, jímž vyjadřující vyjevuje jím chtěnou změnu právního vztahu. Jiné znaky skutkové podstaty přitom mohou být představovány provedením *reálných aktů* (*die Realakten*, též faktické jednání – *tatsächliche Handlung*) a *jednání podobných právním transakcím (geschäftsähnlichen Handlungen)*.

Typicky uváděným příkladem právní transakce je kupní smlouva. Ta ve smyslu § 433 BGB musí zahrnovat dvě souhlasná vyjádření vůle (prodávajícího a kupujícího) o uzavření kupní smlouvy, přičemž její náležitostí jsou ale navíc i reálné akty předání a převzetí kupované věci a zaplacení kupní ceny. Teprve předáním věci resp. zaplacením dochází k převodu vlastnictví věci, resp. peněz.

Dle další definice teorie „‚*jednání podobné právním transakcím*‘ (*geschäftsähnlichen Handlungen*) jsou vyjádření zaměřená na věcný následek“.[21] Náleží mezi ně pravidelně výzvy a sdělení, např. ve formě upomínek (§ 284 BGB), výzev (§ 108 odst. 2, § 177 odst. 2 BGB), stanovení lhůty (§ 326 odst. 1 věta 1 BGB).

Z uvedeného plyne, že německá systematika používá *jednání podobné právním transakcím* k tomu, aby se používala v rámci vedlejších procesních jednání realizace práva, která jsou právem předepsána, ovšem nepředstavují základní vznik, změnu nebo zánik právních vztahů, tj. nejedná se o jednání v kvalitě právní transakce.

Zákonná ustanovení o vyjádření vůle se pak pro jednání podobné právním transakcím aplikují pouze přiměřeně. Jedná se např.[22] o způsobilost k právním transakcím (§ 104 an. BGB), nabytí účinnosti (§ 130 an. BGB), zastupování (§ 164 an. BGB) nebo vady vůle (§ 116 an. BGB).

[20] REICH, D. O. – SCHMITZ, P., cit. dílo, s. 9.
[21] REICH, D. O. – SCHMITZ, P., cit. dílo, s. 15.
[22] REICH, D. O. – SCHMITZ, P., cit. dílo, s. 15.

Konečně, „*reálné akty*' (*die Realakte*, též *faktická jednání – die Tatshandulungen*) jsou na faktický výsledek zaměřené *činnosti vůle (Willensbetätigungen)*, které z moci zákona vyvolávají právní následky".[23]

Na rozdíl od vyjádření vůle u reálných aktů nastává právní následek bez ohledu na to, zda vůle zamýšlela vyvolání právních následku, nebo nikoli. Předpokladem pro provedení reálného aktu proto není způsobilost k právním transakcím u jednající osoby.

Reálné akty zahrnují jak jednání, které není v rozporu s právem, tak jednání protiprávní. V tomto smyslu se jedná o kategorii konání, která nezapadá do používané české právní teorie, neboť sdružuje jednání právní i protiprávní pod jedním označením. Při reálném aktu se proto nikdy nehodnotí způsobilost k právním transakcím, ale někdy se hodnotí deliktní způsobilost, popř. právní způsobilost (k právům a povinnostem).

Příkladem dovoleného reálného aktu je předání písemné objednávky obchodníkovi od dětského poslíčka, který ji nese od objednatele. Není zde na závadu, že poslíček nemá způsobilost k právním transakcím, pokud ji má samotný objednatel. Právem nedovoleným, nicméně přesto reálným aktem je kupř. nedbalé najetí řidičem řízeného vozidla do jiných zaparkovaných vozidel. Právním následkem zde je vznik práva na náhradu škody (podle § 823 odst. 1 BGB) vůči nepozornému řidiči. Souhrnně německá civilistika dělí lidské právní právní chování zhruba takto:

Právní chování (rechtliches Verhalten).

- Vyjádření vůle (die Willenserklärung).
- Právní transakce (die Rechtsgeschäfte).

+

Právní konání (die Rechtshandlungen).

- Jednání podobná právním transakcím (geschäftsähnliche Handlungen).
- Reálné akty (die Realakte) nebo faktická jednání (Tathandlungen).

3.2.1 Pojem „vyjádření vůle" (die Willenserklärung)

Vyjádření vůle má vnitřní a vnější složku: „Vyjádření vůle sestává současně z:

- vnitřní vůle (vnitřní skutková podstata), a
- vnějšího projevu této vůle (vnější skutková podstata) ".[24]

V rámci vnitřní skutkové podstaty právní teorie zjišťuje „tři prvky:

[23] REICH, D. O. – SCHMITZ, P., cit. dílo, s. 16.
[24] REICH, D. O. – SCHMITZ, P., cit. dílo, s. 12.

1. *‚vůle k jednání' [der Handlungswille]*, která zahrnuje vědomí, obecně k jednání; nemají ji například lidé v bezvědomí,
2. *‚vůle k vyjádření' [der Erklärungswille]* nebo *‚vědomí k vyjádření' [die Erklärungsbewußtsein]* znamená znalosti jednajícího o tom, že jeho jednání představuje něco právně významného,
3. *‚vůle k transakci' [der Geschäftswille]* obsahuje vůli vyvolat projevem zcela určité právní následky.“[25]

Ohledně vnitřní vůle a jejího vnějšího vyjádření však platí, že „za obsah (výklad) vyjádření vůle se nepovažuje vnitřní *‚vůle k transakci' [Geschäftswillen]*, nýbrž to, jak by projevu rozuměl neutrální pozorovatel, tzv. *‚horizont objektivního příjemce' [objektiver Empfängerhorizont]*.“[26] Účelem pravidla (§ 133, § 157 BGB) je chránit právní jistotu příjemce vyjádření vůle. Jako příklady objektivního horizontu příjemce se uvádí, že podle okolností může zdvihnutí ruky znamenat nejen hlášení se o možnost dotazu jako ve škole, ale též objednání mázu piva (v pivnici) nebo aukční příhoz.

Očekávané právní následky mohou být postiženy nepřítomností některých ze tří výše uvedených prvků vůle.

V případě chybějící vůle k jednání *(der Handlungswille)*, například kdyby během procesu omdlévání osoba ještě během aukce zdvihla ruku, by se nejednalo o žádné vyjádření vůle ani o právní jednání. Pokud by naivní osoba zdvihla ruku při dražbě, ačkoli by neměla vědomí k vyjádření *(die Erklärungsbewußtsein)*, pravidelně by se k tomu nehledělo, neboť „běžně se při vynaložení potřebné pečlivosti lze seznámit a vyhnout ve styku takovým vyjádřením, které by na základě zásady dobré víry *[Treu und Glauben]* a provozních zvyklostí byly považovány za vyjádření vůle.“[27] Výjimkou by byly pouze případy, pokud by za normálních okolností naivní osoba nemohla znát význam svého jednání, tj. pokud by k tomu neměla rozumný způsob předchozího zjištění. Ve zbylém případu chybějící vůle k transakci *(der Geschäftswille)* vyjadřujícímu se nezbývá než dle § 119, § 121 a § 143 BGB své vyjádření rozporovat.

[25] REICH, D. O. – SCHMITZ, P., cit. dílo, s. 12.
[26] REICH, D. O. – SCHMITZ, P., cit. dílo, s. 14.
[27] REICH, D. O. – SCHMITZ, P., cit. dílo, s. 14.

3.2.2 Vyjádření vůle mezi přítomnými a mezi nepřítomnými

Účinnost vyjádření vůle, které je činěno vůči někomu jinému, závisí v německém právu na tom, zda se děje mezi přítomnými, anebo nepřítomnými. Podle § 130 odst. 1 BGB: *„Vyjádření vůle, které je poskytnuto vůči jinému v jeho nepřítomnosti, bude účinné v okamžiku, kdy mu dojde. Nebude účinné, pokud jinému předtím nebo ve stejném čase dojde odvolání."*

Judikatura vykládá, že „vyjádření je došlé příjemci, když dorazí do jeho okruhu moci tak, že za normálních okolností má možnost se s vyjádřením seznámit a s takovým seznámením se se rovněž počítá."[28] V případě dopisu doručeného do poštovní schránky je tomu například tehdy, když se do schránky obvykle nahlíží. V případě převzetí členem rodiny nebo spolupracovníkem v čase převzetí.

V případě styku mezi přítomnými je tomu v zásadě shodně, nicméně nestačí samotná přítomnost. V případě vtěleného vyjádření (např. listinou) je podmínka přístupu k vyjádření splněna okamžikem, kdy se předáním dostane do obvodu moci (der Herrschaftsbereich) příjemce. V případě nevtěleného vyjádření (ústního, konkludentního) tehdy, když jej příjemce vezme na vědomí. V tomto případě je naopak chráněn vyjadřující se v tom ohledu, že dostačuje, aby dle jím rozeznaných okolností mohl předpokládat, že mu je správně a úplně rozuměno.[29]

Vyjádření se po telefonu náleží k vyjádřením se mezi přítomnými (analogický výklad § 147 odst. 1 BGB).

3.2.3 Nicotnost (Nichtigkeit) vyjádření vůle

Při práci a výkladu s německým BGB vzniká otázka, jak překládat pojmy *die Nichtigkeit* nebo *nichtig*. V české civilistice je zastáván názor, že v oblasti občanského, resp. soukromého práva se má používat pouze pojem neplatnosti a že nicotnost je pojem výlučně správního práva. Pojem se však užívá i v kontextu § 105 odst. 2 BGB: *„Nicotné je také vyjádření vůle, které bylo vydáno za stavu ztráty vědomí nebo přechodné poruchy duševní činnosti."*[30]

Zejména při bezvědomí lze těžko hovořit o existenci vůle nebo právního jednání v jakémkoli smyslu. Pro tento kontext by nejpřípadnější bylo hovořit o neexistenci

[28] REICH, D. O. – SCHMITZ, P., cit. dílo, s. 27.
[29] REICH, D. O. – SCHMITZ, P., cit. dílo, s. 27–28.
[30] „(2) Nichtig ist auch eine Willenserklärung, die im Zustand der Bewusstlosigkeit oder vorübergehender Störung der Geistestätigkeit abgegeben wird."

právního jedání. Tato situace vyžaduje silnější a odlišný výraz, než je i absolutní neplatnost. V kontextu s občanským zákoníkem ČR se pro tyto situace používá pojem *zdánlivé právní jednání*, tj. jednání, které se jeví jako právní jednání, ale není jím, jako právní jednání je z hlediska práva neexistentní. Současně se ale stav *nichtig* vyslovuje i v § 134 BGB: *„Právní jednání, které porušuje zákaz zákona, je nicotné, pokud ze zákona nevyplývá něco jiného."*[31] Právní jednání porušující zákon by však v případě českého právního řádu bylo podle § 588 obč. zák. absolutně neplatné. Konečně např. i v § 125 BGB: *„Právní jednání, které nedosahuje formy předepsané zákonem, je nicotné. Nedostatek formy určené právním jednáním má v případě pochyb za následek rovněž nicotnost."*[32] V případě stejné vady se již v právním řádu ČR bude jednat také již jen o neplatnost, a to buď absolutní, nebo dokonce již jen relativní.[33] O absolutní neplatnost by se mělo jednat tehdy, pokud zákon stanoví formu právního jednání s ohledem na veřejný pořádek, v ostatních případech jen o neplatnost relativní.

Je tedy patrné, že pod význam německého *nichtig* a *die Nichtigkeit*, v kontextu právního jednání dle BGB, by v češtině a českém právním řádu právně spadaly stavy od zdánlivosti až po jen relativní neplatnost. S ohledem na udržení konzistence výkladu německého BGB a související německé civilní nauky se autor v tomto textu nakonec rozhodl pojem *nichtig* (resp. *Nichtigkeit*) překládat jako nicotný (nicotnost). Čtenář by ovšem měl vzít na vědomí, že ve většině případů bude významem pojmu jen neplatnost. *Nichtigkeit* (nicotnost) v BGB zásadně znamená neplatnost *ex tunc*. Velmi vzácně je zhojitelná. Většinou má charakter dále již nezhojitelné neúčinnosti. V případě rozporovatelnosti (srov. níže) se naopak platné právní jednání stane nicotným. V případě pochyb autor doporučuje, aby si čtenář dohledal význam nicotnosti v kontextu k relevantnímu ustanovení BGB v některém komentáři BGB, zmíněném na počátku této kapitoly.

3.2.4 Rozporovatelnost (Anfechtbarkeit) vyjádření vůle

Německý BGB umožňuje vyjadřujícímu, aby své vlastní vyjádření dodatečně rozporoval. Autor zde opět čelí překladové potíži, protože pojmy *Anftechtung*, s ním složené či od něj odvozené, se nejčastěji překládají jako odpor, odporování,

[31] „Ein Rechtsgeschäft, das gegen ein gesetzliches Verbot verstößt, ist nichtig, wenn sich nicht aus dem Gesetz ein anderes ergibt."

[32] „Ein Rechtsgeschäft, welches der durch Gesetz vorgeschriebenen Form ermangelt, ist nichtig. Der Mangel der durch Rechtsgeschäft bestimmten Form hat im Zweifel gleichfalls Nichtigkeit zur Folge."

[33] DVOŘÁK, J. – ŠVESTKA, J. – ZUKLÍNOVÁ, M., cit. dílo, s. 192.

odporovatelnost. V české civilistice je však pojem odporování vyhrazen pro napadnutí právního jednání, jímž dlužník krátí věřitele. Dle německého BGB však lze rozporovat takové své vyjádření, které trpělo nedostatkem vůle nebo vyjádření, a to pro nevážnost, omyl, špatný přenos, klam nebo hrozbu. V českém právu by takové jednání spadalo vesměs pod stav relativní neplatnosti a bylo by možné vůči jeho platnosti vznést námitku (§ 586 obč. zák.) nebo podat vlastní žalobu na neplatnost.[34]

Rozporování je jednostranné vyjádření vůle. Následkem rozporování je nicotnost (neplatnost) od počátku (§ 142 odst. 1 BGB).

Rozporování se vyjadřuje vůči jiné smluvní straně nebo v případě jednostranného právního jednání vůči tomu, komu bylo vyjádření vůle poskytnuto (§ 143 BGB). BGB v zásadě rozlišuje dvě situace. Do první spadají rozporovatelnost pro lstivý klam nebo bezprávnou hrozbu podle § 123 BGB. V těchto případech protistraně nevzniká nárok na škodu.

V případech rozporování podle § 118–120 BGB je rozporující však podle § 122 odst. 1 BGB povinen *„nahradit škody, které jiný nebo třetí utrpěli tím, že na vyjádření spoléhali, ale nikoli přes výši částky zájmu, kterou jiný nebo třetí na platnosti vyjádření měli"*. Tato povinnost ale dle § 122 odst. 2 BGB nevzniká, *„pokud poškozený důvod nicotnosti znal [věděl] nebo neznal v důsledku nedbalosti (musel znát [musel vědět])."*

Z hlediska předmětu našeho zájmu je v BGB prvně zajímavá úprava týkající se rozporovatelnosti pro *omyl* nebo *špatný přenos*:

§ 119
Rozporovatelnost pro omyl

(1) Kdo při poskytnutí vyjádření vůle byl v omylu nebo kdo vyjádření daného obsahu celkově nechtěl poskytnout, může vyjádření rozporovat, pokud lze přijmout, že při znalosti stavu věci a při rozumném posouzení případu by jej neposkytl.

(2) Jako omyl o obsahu vyjádření platí také omyl o takových vlastnostech osoby nebo věci, které by při styku byly nahlíženy jako podstatné.

§ 120
Rozporovatelnost pro špatný přenos

Vyjádření vůle, které je kvůli pro přenos použité osobě nebo zařízení nesprávně přeneseno, lze rozporovat za stejných předpokladů jako vyjádření vůle poskytnutému v omylu dle § 119.

[34] DVOŘÁK, J. – ŠVESTKA, J. – ZUKLÍNOVÁ, M., cit. dílo, s. 189.

Nauka následně rozlišuje několik druhů a kategorií omylů.[35] Do první kategorie patří nevědomé *odchylky mezi vůlí a vyjádřením*.

Omyl vyjádření (§ 119 odst. 1, 2 BGB). Vyjadřující objektivně vyjádřil něco jiného, než vyjádřit chtěl. Příkladem jsou přepsání se nebo přeřeknutí se, například v množství.

Omyl obsahu (§ 119 odst. 1 BGB). Vyjadřující se domnívá, že jeho vyjádření má jiný obsah, ale objektivně se mýlí o obsahu svého vyjádření. Situaci lze popsat, že vyjadřující se neví, co říká, resp. vyjadřuje. Pod slovem tucet si může představovat jen desítku kusů apod.

Falešný přenos (§ 120). Vyjádření vůle je prostřednictvím osoby, instituce nebo prostředku, použité pro přenos, nesprávně přeneseno. Vyjádření ale platí tak, jak bylo příjemci dodáno. Vyjádření nicméně lze rozporovat.

Do druhé kategorie spadají chyby a omyly při *tvorbě vůle*. Tyto omyly se berou v potaz jen někdy. Obecně se nebere v potaz omyl v motivu, pohnutce. Uvedenou výjimkou jsou však i zde omyly podle § 119 odst. 2 BGB.

Omyl motivu (§ 119 odst. 2 BGB). Bere se v potaz pouze tehdy, pokud se jedná o omyl, který se týká ve styku podstatné vlastnosti *(verkehrswesentliche Eigenschaft)* týkající se osoby nebo věci. Jinak se k omylu motivu nepřihlíží.

Omyl ohledně vlastnosti podstatné ve styku (§ 119 odst. 2 BGB). Jedná se o omyl o vlastnosti věci nebo osoby, které by v právním styky byly nahlíženy jako podstatné. Vlastností věci jsou „všechny faktory ovlivňující hodnotu, které plynou z povahy věci nebo ze skutkových či právních okolností". Podstatnými vlastnostmi osoby nebo věci podstatnými ve styku jsou pak „jen takové, které se skutečně a bezprostředně mohou nacházet ve vztahu k obsahu jednání a být považovány za podstatné ve styku". Příkladem vlastnosti osoby je barvoslepost, podstatnou ve styku bude ale jen někdy. Bude podstatným omylem v případě zaměstnání nočního hlídače nebo pilota, nikoli však sekretářky. Věc nebo osoba může mít i právní vlastnosti, např. kvalifikace osoby nebo stavební režim pozemku, které podle okolností mohou být ve styku podstatné. Vlastností, ani tedy podstatnou vlastností, ale není hodnota nebo cena. Omyl o ní není důvodem rozporovatelnosti. Jakékoli jiné omyly vůle nejsou důvodem

[35] Výklad níže je parafrázován dle REICH, D. O. – SCHMITZ, P., cit. dílo, s. 49–53.

rozporovatelnosti. Eventuální nevýhodnost obchodu, nepoužitelnost daru pro nezájem obdarovaného apod. nejsou důvodem rozporovatelnosti.

Výše uvedené možnosti omylu při vyjádření, obsahu, přenosu, vlastnosti je možné rozporovat jen tehdy, jsou-li splněny podmínky závěru § 119 odst. 1 BGB, tj. *„pokud lze přijmout, že při znalosti stavu věci a při rozumném posouzení případu by [vyjadřující vyjádření vůle] neposkytl"*. Jinak řečeno, pokud by vyjadřující o omylu věděl, vyjádření by v daném výsledku nepodal.

Pro náš předmět zájmu je z BGB zajímavá i úprava týkající se rozporovatelnosti pro *lstivý klam*:

§ 123
Rozporovatelnost pro klam nebo hrozbu

(1) Kdo byl k poskytnutí vyjádření vůle přiměn lstivým klamem, nebo protiprávní hrozbou, může vyjádření rozporovat.

(2) Pokud byl klam spáchán třetím, je vyjádření, které bylo poskytnuto jinému rozporovatelné, když o tomto klamu věděl nebo musel vědět. Pokud někdo jiný než ten, vůči němuž bylo vyjádření poskytnuto, bezprostředně nabyl z vyjádření právo, je vůči němu vyjádření rozporovatelné, když o tomto klamu věděl nebo musel vědět.

Takové situace mohou zahrnout i situace útoku na obsah právního jednání. Právní úprava brání tomu, aby ze situace měl prospěch nejen ten, kdo lstivý klam způsobil, ale i kdokoli jiný, pokud o tomto klamu věděl nebo musel vědět, a to bez ohledu na to, zda je tím, vůči komu byl právní jednání poskytnuto, anebo někým třetím, kdo z něj bezprostředně nabyl právo.[36]

Klam je „vyvolání, posílení nebo udržení omylu u vyjadřujícího ohledně objektivních okolností. Klamné počínání přitom musí být původem omylu, je však lhostejné, o jaký druh omylu se jedná." Týká se i případů zamlčených skutečností v případě povinnosti informování, např. požadavek poctivosti a dobré víry *(„Treu und Glauben")* podle § 242 BGB. Klam musí být vyvolán *lstivě*, tj. klamající svým klamavým jednáním vyvolává u potenciální oběti omyl směřující ke vznícení zájmu poskytnout žádoucí vyjádření vůle. Znaky obohacení se klamajícího nebo majetkové poškození vyjadřujícího nejsou nutné, resp. není nutné je dokladovat či dokazovat. V případě klamu se hledí i na hodnotu, která je klamavými skutkovými okolnostmi ovlivněna. Bude-li někdo nabízet odkup zlatých hodinek za desetinu prodejní ceny,

[36] Výklad níže je parafrázován dle REICH, D. O. – SCHMITZ, P., cit. dílo, s. 53–54.

bude takové právní jednání rozporovatelné. Pokud však samotný kupující neví, že hodnota je mnohem vyšší, chybí v jednání aspekt lstivosti.

3.3 Teorie právní transakce (das Rechtsgeschäft) u Flumeho

Pojmu *das Rechtsgeschäft* věnoval objemnou monografii[37] Flume. Považuje jej za velmi důležitý právní pojem, a právě proto o něm podává velmi podrobný rozbor, včetně všech hlavních souvislostí.

Flume nejprve opakuje Julliota de la Morandiere, že „neexistuje žádná právní transakce sama o sobě, ale pouze ty právním řádem uznané a v něm existující prostřednictvím druhů aktů jako kupní smlouva, postoupení pohledávky, převod vlastnictví, zasnoubení, uzavření manželství, závěť, které se považují za spadající pod abstrakci právní transakce.“[38] Svými vlastními slovy pak Flume podává: „Pojem právní transakce je abstrakcí všech v právním řádu vytvořených druhů aktů, které podle svého obsahu, tak jak mu právní řád stanovil, směřují nastavením úpravy ke vzniku, změně nebo zániku právního vztahu pro sebeurčení jedince, tj. k uskutečnění zásady soukromé autonomie.“[39] Toto vztažení se pojmu k obsahu právního řádu je míněno zcela důsledně. Opakuje pohled právníka Lotmara, že „jako ‚nullum crimen sine lege‘, stejně platí i ‚nullum negotium sine lege‘“,[40] přičemž pod *negotium* Flume míní právní transakci (tj. právní jednání v české civilistice).

Druhů právních aktů, kterými se utváří právní vztahy, je přitom v BGB omezený počet *(numerus clausus)*, takže stejně omezen bude i počet druhů právních transakcí. Německé právo poskytuje několik možností vykročení zpoza těchto předem daných mezí. Prvním případem je rozhodnutí judikatury. Jako příklad Flume udává, že zatímco BGB znal jen případ tzv. ruční zástavy, kdy se zastavená movitá věc předává do fyzické dispozice zástavnímu věřiteli, právní praxe nalezla i zástavu bez předání, kdy se k zastavené věci pouze převádí vlastnictví. Jelikož § 930 BGB zná právní převod vlastnictví s ponecháním držby převodci jako zvláštní druh právní transakce, judikatura posléze tuto formu zástavy uznala též jako právně přípustnou. Druhou možností je pro své jednání použít směs různých typů právních aktů a konečně třetí možností je využít obecnou závazkovou smlouvu[41] *(der Schuldvertrag)*. Tu sice BGB výslovně neuvádí,

[37] FLUME, W. Allgemeiner Teil des Bürgerlichen Rechts. Band 2, Das Rechtsgeschäft. Berlin: Springer, 1992.
[38] FLUME, W., cit. dílo, s. 23.
[39] FLUME, W., cit. dílo, s. 23.
[40] FLUME, W., cit. dílo, s. 24.
[41] Flume ji spatřuje ve využití § 305 ve spojení s § 241 BGB, jiní autoři navrhují § 311 odst. 1 ve spojení

například jako smlouvu inominátní, ale jednotlivé druhy závazkových smluv v § 433 a násl. BGB představují pouze exempláře obecného smluvního druhu závazková smlouva.[42] Jak směšování smluvních typů, tak vytváření zcela nových druh smluv nicméně podléhá komplexnímu hodnocení podle pravidel závazkových vztahů, a zcela volné proto není.[43]

Výše uvedené znamená, že soukromá autonomie i smluvní svoboda jsou v principu omezené. Subjekt nemůže volit úpravu obsahu svých vztahů libovolně, ale musí si vybrat z víceméně konečného menu úprav, které mu právní řád předem nabízí! Provede-li svou úpravu v rozporu s právním řádem, pak taková úprava nebude existovat právně, přinejmenším nebude právně vymahatelná. Autonomie přitom bude omezená nejen výčtem druhů aktů, ale i zvláštními a obecnými zákazy, např. zákazem jednat proti dobrým mravům.[44]

Flume to však nepovažuje za apriori omezující. Dle něj soukromá autonomie potřebuje právní řád jako svůj korelát, jehož prostřednictvím se až realizuje.[45] Druhy aktů pro použití soukromou autonomií nevznikají svévolnou sebetvorbou v právu, ale tím, že právní řád uznává a přebírá do sebe ty druhy aktů, které se ve styku mezi lidmi svou pravidelností již dříve samy a úspěšně rozvinuly.

3.3.1 Vymezení právních transakcí (die Rechtsgeschäfte)

Flume uvádí, že výše uvedené pojetí právních transakcí nebylo až zhruba do poloviny 19. století vůbec běžné. Pojem *das Rechtsgeschäft* se sice používal, nikoli však jako indukcí získaná abstrakce právních typů jednání z právního řádu, ale jako pojem získaný dedukcí z vyššího abstraktnějšího pojmu, kterým bylo lidské jednání *(menschlichen Handlungen)*. Typický má být kupř. citát Dabellowa (1794): „Z lidského jednání je jeden obzvlášť důležitý druh, kterému se říká právní jednání [rechtliche Handlungen], nebo právní transakce [rechtliche Geschäfte] *(actus juridici, negotia juridica)*. Rozumí se jimi dovolené lidské jednání, které má za předmět vzájemná práva a povinnosti.“[46] Terminologie nebyla v 18. století jednotná, autoři mísili latinské a německé texty i frazeologii, namísto *das rechtliche Geschäft* se časem ujalo spíše

s § 241 odst. 1 BGB.

42 FLUME, W., cit. dílo, s. 24.

43 Podrobněji kupř. monografie STOFFELS, M. *Gesetzlich nicht geregelte Schuldverträge : Rechtsfindung und Inhaltskontrolle*. Mohr Siebeck, 2001.

44 FLUME, W., cit. dílo, s. 2.

45 FLUME, W., c*it. dílo*, s. 1.

46 FLUME, W., cit. dílo, s. 29.

das Rechtsgeschäft, v rámci 18. století se však jednalo *o právní transakci (das Rechtsgeschäft)* o sobě.

Pro toto pojetí je typické, že se předpokládá, že práva a povinnosti vznikají přímo ze samotného jednání osob, např. ze vzájemné smlouvy, kterou osoby mezi sebou navzájem vytváří své vlastní právo. Jak namítá Flume, při uzavírání například kupní smlouvy ale vůle stran „není materiálně kvalifikovaná k tomu, aby uskutečňovala právní myšlenky" tak, jak to lze očekávat například u zákonodárce, ale „sleduje tím svůj prospěch".[47]

Poznamenejme zde, že v rámci 18. století, kdy vyčerpávající právní kodexy ještě neexistovaly, bylo odlišné uvažování o právních transakcích (právním jednání) obtížně představitelné zřejmě i pro právní nauku. S pojmy v různě psaných verzích zápisu slov se sice pracovalo, ovšem nebyla jim přikládána zvláštní váha. Proto francouzský Code Civil z roku 1804 ani rakouský ABGB z roku 1811 pojem, nebo jeho současnou teorii, nepoužívají. Nauka o právních transakcích *(die Rechtsgeschäfte)* je až hlavním tématem německé právní vědy 19. století, završeným tvorbou zákoníku BGB.

Klademe si nyní otázku, jak můžeme v zákoníku rozeznat ta ustanovení, která pojednávají o právních transakcích. Ve středu pojmu právní transakce se nachází vyjádření vůle. Bez aspoň jednoho vyjádření vůle jedné osoby nemůže právní transakce vzniknout. Právní ustanovení však pro právní transakci mohou vyžadovat vyjádření vůle více osob a dále i vedlejší znaky skutkové podstaty dané právní transakce (např. souhlas vůlí při uzavírání smlouvy). Podstatné zde však je, že obsahem vyjádření vůle je záměr vytvořit, změnit nebo zrušit právní vztah určitým způsobem a že daný obsah vůle právní řád uznává, a proto právě vyjádřené prohlašuje za platné.

Jinak řečeno, původně projevená vůle se stává právem v daném právním vztahu, nikoli však jen proto, že byla projevena jako vážně projevené přání a závazek osoby, ale že ji i právní řád aprobuje. Zvláštní a charakterizující pro právní transakci však je, že právem v právním vztahu se stává to, co bylo původně vyjádřeno.[48]

Tím se situace liší například od pojmu právního jednání pojatého tak, že se jedná o jednání, které je po právu v tom smyslu, že osoba nejedná protiprávně, tedy například že nepoškozuje cizí věc nebo že řádně užívá svou vlastní věc, čímž vykonává své

[47] FLUME, W., cit. dílo, s. 5–6.
[48] Výjimkou je pochopitelně případ, kdy obsah původního vyjádření vůle není právem dovolen.

vlastnické právo k ní. Při takto pojatém právním jednání ale nedochází ke změně právních vztahů.

Právní transakce je ještě kontrastnější s případem, kdy sice dochází ke změně právních vztahů, ovšem jinak, než jak byla vůle vyjádřena, pokud k vědomému vyjádření vůle vůbec došlo. Příkladem může být nedbalostní poškození věci jiné osoby. Jsou-li splněny zákonné předpoklady, vznikne škůdci z tohoto jednání povinnost k náhradě škody. Takové jednání je sice pochopitelně možné odlišit i tím, že se jedná o jednání protiprávní, a nikoli po právu, zde se nám však jedná o nastínění rozdílu mezi počátečním jednáním a výsledným právem.

Chceme-li znovu zdůraznit aprobaci právním řádem, pak lze říci, že právní následek nevzniká primárně proto, že je obsažen v projevu vůle, ale jelikož daný projev vůle lze právně subsumovat pod určitý druh právní transakce, který je obsažen v zákoníku a pro nějž zákon dané právní následky stanoví. Projev vůle tak prochází filtrem zákona jak z hlediska subsumpce, tak z hlediska posouzení obsažených součástí, popř. doplnění o součástí nevyjádřené. Chtějí-li strany uzavřít například kupní smlouvu, tak si musí *sjednat zajištění věci prodávajícím, která je bez věcných a právních vad, její předání, převzetí a převod vlastnictví kupujícímu, za což kupující zaplatí sjednanou cenu*. Zjištění, že se jedná o kupní smlouvu, plyne z toho, že takové ujednání odpovídající § 433 BGB skutečně je obsaženo v projevu vůlí stran, čímž se jednání kvalifikuje jako *právní transakce* a má ty právní následky, které právo explicitně obsahuje, popř. které dovoluje upřesnit v projevu vůle. Jelikož však projev vůle bere existenci zákoníku předem na vědomí, jeho dikci se přizpůsobuje, lze sekundárně přeci jen říci, že právní následky jsou výsledkem projevu vůle, potažmo vůle a potažmo autonomie osoby.

Jelikož pojem právní transakce umožňuje provádět rozsáhlé abstraktní úvahy o velké třídě typů právních vztahů nebo právních typů, které spolu na první pohled nijak zvlášť nesouvisí (např. závěť vs. kupní smlouva), považuje Flume objev právních transakcí za asi největší objev německé právní vědy 19. století vůbec! Právní řešení nalezená pro jeden druh právní transakce, týkají-li se znaků, které mají všechny právní transakce, by totiž následně měla být použitelná i pro všechny ostatní druhy.

Flume ovšem upozorňuje, že některé takové závěry přesto nemusí být zcela správné. Například problémy vad vůle, zejména omyl, je někdy třeba řešit podle

jednotlivých druhů. Připouští také, že jiné právní oblasti německou vědu a zákony a systematiku vycházející z právních transakcí zcela nesledují. Románské právo má problematiku řešit v oblasti závazkového práva (obligace), common law ji řeší ve smluvním právu (law of contracts).[49]

Flume nakonec používá poměrně abstraktní stručný popis, podle nějž lze právní transakce rozeznat: „Právní transakce jsou akty tvořivého tvarování právních vztahů s výsledným vztahováním se aktů na tvarovaný právní vztah.“[50]

Vtažení uznání právním řádem se zde provádí přes použitý pojem právního vztahu. Popis reflektuje, že výsledně vytvarovaný právní vztah nemusí být přesným obsahem aktu, například z důvodu, že zákon k aktu přidá všechna kogentní ustanovení, popř. i nevyloučená dispozitivní ustanovení.

3.3.2 Zásada autonomie a ústavněprávní rovina právních transakcí

Právní transakce spočívají v tvořivé změně právních vztahů ze svobodné vůle osob a v souladu s právním řádem. V jejich rámci proto jednak dochází k uplatňování zásady soukromé autonomie, hlavní vůdčí zásady soukromého práva Německa, jednak se jejich prostřednictvím uskutečňuje sebeurčení jedince.

Soukromou autonomii přitom Flume popisuje jako „princip sebeutváření právních vztahů jednotlivci podle jejich vůle“.[51] Autonomie znamená i to, že vůle jednotlivce nemůže být nahrazena vůlí někoho jiného. Soukromé právo zásadně nepřipouští, aby došlo k utváření právních vztahů bez souhlasu toho, koho se týkají. Pečlivě ošetřenou výjimkou jsou některé situace, kdy se jednostranně poskytuje výhoda někomu třetímu. Nejčastějším případem je oferta k uzavření smlouvy, kterou ovšem lze nepřijmout. Lze odmítnout i jiné výhody, jako dědictví, pochopitelně i darování, řadící se i v Německu mezi smlouvy.

Soukromá autonomie pak „je součástí všeobecného principu sebeurčení *(die Selbstbestimmung)* lidí“.[52] Sebeurčení jednotlivců se odráží ve více základních lidských právech, vyjádřených v čl. 1 až 19 základního zákona (*das Grundgesetz*, dále jen „GG“). Vztahuje se na něj již čl. 1 odst. 1 GG: *„Důstojnost člověka je nedotknulná“*. Za jeho hlavní podporu, zejména ve vztahu k soukromému právu a právním transakcím,

[49] FLUME, W., cit. dílo, s. 30–34.
[50] FLUME, W., cit. dílo, s. 33.
[51] FLUME, W., cit. dílo, s. 1.
[52] FLUME, W., cit. dílo, s. 1.

však Flume považuje článek 2 odst. 1 GG:[53] *„Každý má právo na volný rozvoj své osobnosti, pokud se nedotýká práv jiných a pokud neporušuje ústavní pořádek nebo mravní zákon."*

Flume na jednu stranu zásadu autonomie hájí jako zcela potřebnou pro soukromé právo. Odmítá, že by se jednalo o přežitý relikt individualismu nebo sobectví 19. století, ale že jde o základní předpoklad funkce nejen soukromého práva, ale právního řádu všech současných západních států.[54] Zastává se proto i smluvní svobody, která je podstatnou částí zásady autonomie.

Při ústavněprávním diskursu Flume pak zřejmě správně soudí, že zásada volného rozvoje osobnosti jedince v čl. 2 GG poskytuje silnější ochranu zásadě smluvní svobody, než existovala za Výmarské republiky, ačkoli její ústava zásadu smluvní svobody výslovně zmiňovala, ovšem pod výhradou její omezitelnosti jednoduchým zákonem. Tomuto omezení se však z podstaty nelze vyhnout.[55] Zásada volného rozvoje osobnosti však v sobě smluvní svobodu obsahuje a v GG výhradě omezení jednoduchým zákonem nepodléhá. V ústavněprávní rovině proto v Německu existuje velmi silné zakotvení a ochrana, které nepřímo brání běžným zákonům omezovat smluvní svobodu, pokud by se tím narušoval volný rozvoj osobnosti jedince.

Na druhou stranu ale Flume odmítá přiznat zásadě smluvní svobody, a potažmo i zásadě soukromé autonomie, nejvýsadnější postavení. Prvně již odmítá, že by tvarování právních vztahů plynoucí ze soukromé autonomie bylo zákonodárstvím. Tvrdí: „Tak jako jednotlivci nemohou být soudci ve své věci, nemohou být ani zákonodárci."[56] Flume je skeptický ohledně toho, že by svoboda soukromé autonomie k tvorbě vztahů probíhala v ideální mravní vázanosti. Mnohem spíše ji považuje za určitý projev „sebelásky" (*„die Selbstherrligkeit"*[57]), kterou právo uznává spíše z praktických důvodů života než jako výron ideální spravedlnosti, která by snad hypoteticky byla možná. Uvádí, že zde spíše platí *stat pro ratione voluntas*, tedy že rozum je nahrazen vůlí. Z této opatrnosti pak plyne, proč „zásada soukromé autonomie neposkytuje žádnou legitimitu jednání v ‚sebelásce' za jiné" a proč právo tak často

[53] „Artikel 2 (1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt."

[54] První vydání monografie je z roku 1964, čtvrté z roku 1992.

[55] FLUME, W., cit. dílo, s. 19.

[56] FLUME, W., cit. dílo, s. 5.

[57] Uvozovky používá opakovaně v textu i Flume. Jím užitý pojem, *die Selbstherrligkeit*, lze přeložit i jako aroganci, do sebe zahledění, povýšenost.

stanoví různé omezující podmínky, a to i v případě smluv, kdy přeci jen dochází k určitému vyvažování obsahu vztahu vyjednáváním mezi jeho stranami. Flume je názoru, že i u smluv je třeba výsledné právo poměřovat včetně ustanovení právního řádu, aby o něm bylo možné prohlásit, že je „správné" *(„richtig")*, že jen soukromá vůle stran nemůže založit žádnou právní normu.[58]

Při diskursu o zásadě smluvní svobody v ústavním právu pak odmítá, aby zásada byla automaticky nadřazena zásadám jiným, především pak ve vztahu k zákonodárství. Dle jeho názoru maximou pro tvorbu zákonodárství je již z Říma známá zásada *„ius suum cuique tribuere"*, tj. *„právo má dáti každému to, co mu náleží"*. Této zásadě dle něj jen samotné právo na smluvní svobodu není nadřazeno.[59] V tomto smyslu právo je kolektivním výtvorem společnosti, v jehož rámci se smluvní svoboda, a potažmo i podstatná část sebeurčení jedince i s jeho autonomií, běžně musí realizovat. Právě v tomto důvodu tedy hodnotově tkví počátek podřízení právních transakcí pod uznání právním řádem.

Pro ochranu soukromé autonomie však Flume odmítá podřízení soukromého práva pod přímý účinek ústavních norem stanovících lidská práva, tedy jejich úpravy v čl. 1 až 19 GG. Důvodem mu například je čl. 3 GG, stanovící rovnost před zákonem, obecně pak zásadu stejného zacházení za stejných okolností, předepsanou zde veřejné moci. Dle něj, pokud by se přímý účinek čl. 3 GG měl brát vážně, pak buď vyjde ve střetu se soukromým právem ad absurdum neplatný, anebo naopak zcela zničí soukromou autonomii vůbec. Odmítá proto jak tezi o tzv. nepřímém účinku třetího *(die Drittwirkung)*, tak o absolutní přímé platnosti ústavy.

Dle jeho názoru při ochraně základních lidských práv v ústavě se jedná o ochranu určitých hodnot, ovšem normami, které jsou uzpůsobeny ochraně jedince před státní mocí, zatímco pro ochranu jedinců v rámci soukromých právních vztahů se daná úprava nehodí. Přímá aplikace norem základních práv může způsobit pouze nicotnost právních transakcí, což však dotčeným osobám zpravidla dobře neposlouží. Podporuje proto výrok německého ústavního soudu, že:[60] „Právní obsah základních práv jako objektivních norem se v soukromém právu rozprostírá prostřednictvím předpisů bezprostředně ovládajících tuto právní oblast."

[58] FLUME, W., cit. dílo, s. 6–8.
[59] FLUME, W., cit. dílo, s. 20.
[60] FLUME, W., cit. dílo, s. 22.

Flume je názoru, že stejné hodnoty, které chrání ústava, jsou již přítomny v soukromém právu buď explicitně v důsledku činnosti zákonodárství a judikatury, anebo jsou pokryty pojmem dobrých mravů. Právní transakce, které by porušovaly ústavou chráněné hodnoty, by proto byly vždy nicotné již pro rozpor s dobrými mravy podle § 138 GG. Přímý účinek norem základních práv proto dle něj nemá v oblasti nauky právních transakcí žádný prostor.[61]

Flumeho argumentace se autorovi zdá být právně poměrně přesvědčivá, nicméně některým otázkám se Flume nevěnuje, možná proto, že v praxi Spolkové republiky Německo nebyly aktuální. Flume kupř. uvádí, že v podstatě všechny dříve i nyní[62] existující právní řády zásadu soukromé autonomie uplatňovaly, ovšem ve velmi různé míře a například v socialismu jen velmi omezené. Není zcela zřejmé, zda měl na mysli státy někdejšího východního bloku, nicméně i právo např. ČSSR ponechávalo jedincům autonomii v tom, zda a s kým vstoupí do manželství. Z jakéhokoli dalšího srovnání by vyplynulo, že rozsah a obsah disponibilních právních transakcí byl v ČSSR ale velmi omezený.

Při použití Flumeho tvrzení o nadřazení zákonodárství z důvodu *ius suum cuique tribuere* pak lze argumentovat, že z jistého hodnotového úhlu pohledu, reprezentovaného například režimním etickým heslem „každý dle svých možností, každému dle jeho potřeb," socialistické právo s komunistickými ideály tuto zásadu zajišťovalo a omezení autonomie by tak bylo ospravedlnitelné. Jistě lze namítnout, že právo ČSSR autonomii a následnou iniciativu jedince v soukromoprávní i veřejnoprávní oblasti podvázalo prostředky veřejného práva do takové míry, že vůbec nemohl byť jen vzniknout veřejný diskurs o tom, co má být obsahem zákonodárství, tj. že nebyly naplňovány politické svobody. Takové právně správné hodnocení by však tehdejším občanům východního bloku již nepomohlo a dodnes nepomůže například občanům Severní Koreje, neboť případné řešení je již jen politicko-mocenské.

Podstata této otázky a sporu tedy z právního hlediska leží jinde. Právně užitečná otázka zní, v jaké míře je faktická existence ústavy s liberálně demokratickou podstatou zajištěna nejen dělbou veřejné moci ve státě, ale i zajišťováním soukromé autonomie. Do jaké míry je ještě možné soukromou autonomii omezit, aniž by to způsobilo kolaps společenského uspořádání. Na soukromou autonomii je třeba hledět nejen jako na

[61] FLUME, W., cit. dílo, s. 22.
[62] První vydání monografie bylo roku 1964, čtvrté v roce 1992.

prostředek pro sebeurčení jedince na pozadí existujícího právního řádu, ale i jako na garanci, která jedincům umožňuje mít určitý vliv na zachování právního státu a základních práv, jenž sice rovněž často vykonávají zejména s ohledem na svůj vlastní prospěch, pro zachování sebou nabytých práv, současně však slouží i objektivně žádoucímu cíli, přinejmenším z hlediska liberálně demokratických hodnot. Jakýkoli ranný, a proto ještě účinný politický odpor proti nežádoucímu přetváření veřejné moci je totiž možný jen tehdy, pokud jeho projevení nevede k existenční zkáze jedince, tj. pokud veřejné moci je právně nepřístupný prostor, v němž si jedinec opatřuje prostředky ke svému živobytí. Takovým prostorem je oblast právních vztahů vzniklých na základě soukromé autonomie.

Diskurs tímto směrem překračuje předmět této práce. Flumeho akcent na prioritu zákonodárství je však dle názoru autora třeba tlumit minimálně v tom smyslu, že soukromá autonomie je i prostředkem k ústavní stabilitě, bez níž žádné zákonodárství s Flumeho předpokládanými kvalitami vůbec nemusí existovat.

3.3.3 Úrovně vůle (Handlungs-, Erklärungs-, Geschäftswille)

Jak je uvedeno již výše (srov. 3.2.1), německá teorie v podstatě rozlišuje tři stupňující se úrovně přítomnosti vůle. Přitom se zcela odhlíží od konkrétního obsahu vůle, abstrahuje se od obsahu,[63] pouze se zkoumá kvalita vůle. První úrovní je *vůle k jednání (der Handlungswille)*, která má charakter základního stavu psychického vědomí. Vyšší úrovní vědomí je situace, kdy si osoba je vědoma toho, že její počínání může představovat něco právně významného, je ve stavu *vůle k vyjádření (der Erklärungswille)*, též nazývaném *vědomí k vyjádření (die Erklärungsbewußtsein)*. Konečně nejvyšší úrovní je *vůle k transakci (der Geschäftswille)*, kdy již je záměrem pojato vyvolat zcela určité právní následky.

Dle Flumeho vůle k jednání *(der Handlungswille)* není v případech bezvědomí, hypnózy ani v případě fyzického násilí, kdy někdo vede ruku přemoženého. V posledním případě se jedná o vůli skutečně jednajícího,[64] na přemoženého lze hledět pouze jako na nástroj. Druhou úroveň vůle Tuhr označoval za vůli ke sdělení *(Mitteilungsbewußtsein)* a mínil jí, že vyjadřující je připraven poskytnout sdělení nějakého druhu. Obecně se ale spíše ujal výše uvedený koncept a pojmové označení vůle či vědomí k vyjádření *(Erklärungswille, Erklärungsbewußtsein)*, že „činěné

[63] FLUME, W., cit. dílo, s. 46.
[64] FLUME, W., cit. dílo, s. 46.

chování je právně relevantním vyjádřením".[65] Součástí jeho obsahu tedy již je i to, že vyjádření bude právně relevantní. Flume uvádí příklady z literatury, kdy někdo podepíše a odešle pozvání jinému na oběd, aby následně zjistil, že omylem podepsal a odeslal návrh smlouvy. Vůle k jednání přítomna byla, vůle k vyjádření nikoli. Jiným školním příkladem je zdvižení ruky za účelem pozdravení přítele, které se ovšem mělo odehrát během dražby vín v oblasti Trevíru, což podle místních dražebních pravidel mělo mít významu dražebního příhozu, to ale zdravící nevěděl.[66] Vůle k transakci má několik užívaných definic, například „vůle zaměřená na to, aby svým vyjádřením vyvolala určité právní následky" nebo „záměr směřující k určitému hospodářskému, právně zajištěnému úspěchu". Flume proto shrnuje, že vůli k transakci je tedy třeba chápat jako vůli ve vztahu k obsahu vyjádření. Například při kupní smlouvě bude vůlí k transakci jednajícího to, že chce koupit kupovanou věc za určitou cenu.[67]

Flume shrnuje, že nauka je jednotná ohledně toho, že součástí vůle musí vždy být vůle k jednání. Při hypnóze nebo bezvědomí se tedy o žádné právní vyjádření jednat nebude. Již v druhé úrovni vůle (mylné pozvání na oběd nebo pozdrav rukou) však vzniká zásadní *dilema*, ve prospěch které strany se vyjádření má právně hodnotit. Dle Flumeho je rozbor obsahu a úrovní vůle ale neplodný, neboť v zásadě se vždy jedná o chybné vyjádření vůle. Skutečnými otázkami je určení právní následků. Právních následků, když není přítomna vůle k jednání (př. hypnózy), nebo není vědomí k vyjádření (př. dražba vína), nebo když se vůle k transakci neshoduje s obsahem znaků skutečného vyjádření (přepsání se při objednání 110 kusů místo 100 kusů apod.).[68]

Dle Flumeho je třeba založit argumentaci na tom, jaký je normální vztah mezi vůlí (vědomím) a vyjádřením vůle. Konstatuje, že již von Savigny v rámci svého souborného díla *Systém dnešního římského práva*[69] uvádí, že na vůli a její projev je třeba hledět jako na spolu těsně související: „V podstatě se musí považovat za jedinou důležitou a účinnou vůle o sobě *[der Wille an sich]*. Jelikož to ale je pouze vnitřní neviditelná událost, potřebujeme znaků, aby mohla být jinými pochopena *[erkannt werden]*, a tyto znaky, kterými se zjevuje, jsou právě vyjádření. Z toho ale plyne, že překrývání se vůle s jejím vyjádřením není něco náhodného, nýbrž jejich přirozený

[65] FLUME, W., cit. dílo, s. 46.
[66] FLUME, W., cit. dílo, s. 47.
[67] FLUME, W., cit. dílo, s. 47.
[68] FLUME, W., cit. dílo, s. 48.
[69] VON SAVIGNY, F. C. *System des heutigen Ramischen Rechts*. Band 3. Veit, Berlin, 1840.

stav.“[70] Flume s tímto přirozeným překrýváním vůle a vyjádření souhlasí. Navíc z toho pro něj plyne, že z tohoto přirozeného faktického překryvu musí vycházet i zákonodárství. Kdyby přirozeného překryvu vůle a vyjádření nebylo, nemohlo by zákonodárství vůbec dovolit, aby právními transakcemi vznikaly právní vztahy. Flume zdůrazňuje, že von Savigny nehledí na vůli jako na psychický fenomén, ale jako na: „Vyjevení téhož, čím vnitřní událost vůle vstupuje do viditelného světa jako vnější zjevení.“[71] Nicméně dle Flumeho ještě po vydání BGB například Tuhr zastává názor, že vyjádření z vyjádření vůle je „jednání, které je provedeno za účelem, aby se průběh duševního života stal známým okolním osobám“.[72] Účelem takových definic je oddělit vůli a její vyjádření, zatímco von Savigny vyžaduje o jejich podstatě uvažovat zároveň.

Souhlasněji s von Savignym uvažoval například Windscheid, že: „Vyjádření vůle je spíš výrazem vůle než sdělením vůle. Je to vůle ve svém očividném vnějším zjevení.“[73] Součástí znaků této vůle pak rovněž je vyvolání právních účinků. V podobném smyslu Enneccerus přirovnává vyjádření vůle k publikaci zákona. Dokud zákon nebyl vyhlášen, nejen že je neznámý, ale z hlediska práva neexistuje. Flume shrnuje, že současné obecné mínění německé nauky je, že vyjádření vůle je aktem uplatněním vůle *(ein Akt des Vollzugs des Willens)* a že vychází z právě zmíněných klasiků jurisprudence.

3.3.4 Teorie vyjádření vůle (Willens-, Erklärungs-, Geltungstheorie)

Výše uvedené závěry o vyjádření vůle jako spíše jednoty vůle a vyjádření, o přirozenosti a pravidelnosti jejich překryvu, ještě neodpovídají na výše zmíněná dilemata nesouladu vůle a vyjádření. Paradigmatem nesouladu bývá obecně omyl, byť právo zná i další. Při zodpovězení otázky právních následků pak lze buď stát na straně vyjadřující osoby, anebo na straně příjemce vyjádření vůle.

Ve prospěch vyjadřující se osoby hovoří takzvaná *teorie vůle (Willenstheorie)*, kterou založil již právě výše zmíněný von Savigny (cca 1840). Tato teorie vychází z toho, že důležitá a účinná je právě vůle o sobě. Pokud je, zejména omylem, vyjádřeno něco jiného, než vůle mínila, nemůže toto něco jiného platit. I vyznavači této teorie nicméně připouštěli výjimku neúčinnosti vnitřní výhrady (mentální výhrady), která je

[70] Citace von Savignyho in FLUME, W., cit. dílo, s. 49.
[71] Citace von Savignyho in FLUME, W., cit. dílo, s. 50.
[72] Citace Andrease von Tuhr in FLUME, W., cit. dílo, s. 50.
[73] Citace von Windscheida in FLUME, W., cit. dílo, s. 50.

dnes stanovena v § 116 BGB. Právním následkem případu omylu vůle však obecně měla být nicotnost (tj. neplatnost) vyjádření vůle.[74]

V sedmdesátých letech 19. století vzniká protichůdná *teorie vyjádření (Erklärungstheorie)*. Podle Bähra (1875) vyjadřující „odpovídá za vnější zjevení své vůle tak, jako by jej skutečně chtěl".[75] Bähr se však ještě stále pohyboval v rámci teorie vůle a pouze zavedl v případě omylu fikci vůle na základě vyjádření. K formování teorie vyjádření dochází až tehdy, když se jako protipól vůle za rozhodující prohlásí vyjádření. To dokončil Danz (cca 1897): „Vyjádření vůle, které je skutkovým znakem právní transakce, lze definovat jako chování osoby, které podle pravidel styku při zvážení všech okolností pravidelně dovoluje závěr o určité vůli, bez ohledu na to, zda v jednotlivém případě je tento závěr o vůli správný, tj. zda skutečně taková vnitřní vůle, která vyplývá z vyjeveného vyjádření vůle, byla u osoby přítomna, anebo nikoli."[76]

Zajímavé je, že tento vývoj již byl zachycen při přípravě BGB. První návrh BGB ještě měl stát na teorii vůle a jednání v omylu považovat za nicotné. V rámci diskursu však došlo ke změně a již druhá verze se přiklonila k současné úpravě v § 119 BGB, která v případě omylu umožňuje jen rozporovatelnost. Sepisovatelé BGB se rozhodli, že nebudou stranit ani jedné ze stran teorie, ale ponechají záležitost raději na okolnostech případu. Po přijetí BGB se spor přesunul do otázky, zda je BGB vystavěn spíš na teorii vůle, anebo teorii vyjádření. Zpočátku dokonce převažoval názor o primariátu teorie vůle, byť silně omezené zájmy protějšku. Dnes se dle Flumeho zastává jednoznačně názor, že z pohledů zmíněných dvou teorií BGB zvolil kompromis mezi nimi.

K tomu přispěl i rozvoj další teorie, která je dnes známa jako *teorie platnosti (Geltungstheorie)*. Výše uvedené rozvahy o vztahu vůle a vyjádření odhlíží od obsahu. V tomto kontextu se nejprve etabloval pojem vyjádření platnosti *(Geltungserklärung)*. Podle tohoto přístupu právní transakce je svým obsahem vyjádřením platnosti (prohlášením, projevem platnosti), neboť právně transakčním aktem se stanovuje platnost regulace (eine Regelung), kterou se zakládají, mění či ruší právní vztahy. Podstatu vyjadřuje Hölder (cca 1889): „vůle, o které zde hovoříme, je vždy normativní vůlí, jedná se vždy o ustanovení nějakého mětí nebo dovolení [Sollens oder Dürfens], nějakého nesmětí nebo nedovolení [Nicht-sollens oder Nichtdürfens]. Zcela stejně jako zákon ustanovuje abstraktní normu, ustanovuje právně platné vyjádření vůle soukromé

[74] FLUME, W., cit. dílo, s. 54–55.
[75] FLUME, W., cit. dílo, s. 55.
[76] Citace Ericha Danze in FLUME, W., cit. dílo, s. 55.

vůle nějakou konkrétní normu, ustanovuje tuto normu právě prostřednictvím vyhlášení.“[77] Flume pochopitelně podotýká, že prohlášení platnosti v rámci vyjádření vůle nenastává jen z vůle vyjadřujícího, ale především z vůle zákona. Přesto Flume shrnuje, že svým obsahem není právní transakce nic jiného než prohlášením platnosti. Toto chápání pak vede na výše uvedenou teorii platnosti.

Podle jejích zastánců, jako byli Enneccerus, Nipperdey, von Larenz nebo Dulckeit, se v rámci vyjádření vůle „nesmí rozštěpit akt vůle, jako psychologická výchozí skutečnost, a od něj oddělený akt vyjádření, který jen sám slouží k vyhlášení vnitřní vůle“.[78] Tato pozice je však víceméně v souladu s východiskem von Savignyho. Není proto divu, že teorie platnosti dobře odpovídá teorii vůle, ovšem s tím, že obsah vyjádření má význam prohlášení platnosti. Do protikladu vůči teorie vůle pak vystupuje pouze tehdy, když se jedná o otázku omylu. Podle teorie platnosti totiž omylem postižené vyjádření vůle je přesto platné. Platnost však lze odstranit následným aktem, totiž rozporováním. Tímto způsobem tedy teorie platnosti překonává dualismus mezi teorií vůle a teorií platnosti. V případě omylu pak teorie platnosti je shodná s teorií vyjádření. Odlišné je však ospravedlnění. Teorie vyjádření vycházela z ochrany dobré víry *(Vertrauensschutz)*. Teorie platnosti pak vychází z toho, že vyjadřující svou vůlí ustavil své vyjádření v platnost. Jelikož však teorie platnosti má již ve svém základu soulad vůle s vyjádřením, nemůže v principu řešit všechny případy nedostatků vůle, když není souladný překryv mezi vůlí a vyjádřením. Nemůže ani řešit výše probíraný případ omylu prakticky, protože v praxi vždy může docházet k přepsáním se v množství apod.[79]

3.3.5 Sebeurčení vs. sebeodpovědnost

Dle Flumeho není žádná z výše uvedených teorií zcela odpovídající. Dle něj všechny tyto teorie uvízly v rámci příliš těsného pojmového rámce, který poskytla pojmová jurisprudence. Souhlasí s tím, že teorie vůle používá správné ospravedlnění, totiž obsahové sebeurčení plynoucí z právní transakce nebo vyjádření vůle. Poukazuje však na to, že sebeurčení není jedinou hodnotou, o kterou se v rámci vyjádření vůle jedná. To se totiž vždy provádí v rámci nějakého sociálního prostředí, vůči jiným osobám, které jsou rovněž zasaženy. Nastupuje pak i sebeodpovědnost,[80] která je

[77] Citace Eduarda Höldera in FLUME, W., cit. dílo, s. 57.
[78] FLUME, W., cit. dílo, s. 58.
[79] FLUME, W., cit. dílo, s. 59.
[80] Německé *Selbstverantwortung*, tj. odpovědnost za sebe, překládáme z důvodu stručnosti takto.

prakticky vždy součástí sebeurčení. Při sebeurčování vždy hrozí i riziko pochybení sebeurčení. Je pak otázkou, kdo má toto riziko nést. Má jím být ten, který realizuje sebeurčení, anebo jeho protějšek, který s ním vstupuje do daného právního vztahu? Podle Flumeho je sebeodpovědnost korelátem sebeurčení. Flumeho ale neuspokojují ani teorie vyjádření nebo teorie platnosti. Teorie vyjádření nereflektuje, že ochrana dobré víry *(Vertrauensschutz)* je v rozporu se sebeurčením a teorie platnosti nerozlišuje rozpor vůle a vyjádření. Dají-li se pak sebeurčení a sebeodpovědnost vedle sebe, dle Flumeho je dost dobře možné, že sebeodpovědnosti náleží přednost vůči nedostatku ospravedlnění sebeurčení ve vyjádření postiženém omylem vůle. Dle něj však v případě přednosti nelze jednoznačně určit, která právní norma je a priori správná. Flume proto zakončuje, že právní řád stanovil, že právně pozitivní regulace musí být chápána a posuzována tak, že podstatou vyjádření vůle je, že to „je akt právního tvarování v rámci sebeurčení, ale rovněž v sebeodpovědnosti".[81]

3.3.6 Vyjádření vůle (Willenserklärung) a právní transakce jako regulace

Flume nepovažuje samotný pojem *Willenserklärung* (vůle-vyjádření) za šťastný z hlediska účelu, pro který se právně používá, který právně má. Především z něj není dostatečně jasné, že se jedná o právní termín, o finální právně tvořivé jednání, jehož nastáním vznikají právní následky, že se jedná o *actus iuridicus*, tj. akt, kterým se něco ustavuje za platné. Jak je uvedeno výše, obsahově pak má vyjádření vůle *(Willenserklärung)* spíše charakter prohlášení platnosti *(Geltungserklärung)*.[82]

Pod *vyjádřením vůle* lze rozumět jednak akt, jednak výsledek aktu. Z hlediska aktu se jedná o jeho průběh, z hlediska výsledku jde o regulaci. Právo může stanovit na průběh aktu určité podmínky, zejména v běžném případě vícestranných právních transakcí (př. smlouva) musí být provedeno více vyjádření vůle. Regulace jako výsledek právní transakce se má k právní transakci jako aktu, tj. k průběhu, zhruba stejně, jako se má zákon k zákonodárnému procesu. Flume upozorňuje, že předpisy o právních transakcích se běžně rozpadají na řadu částí. Jedná se například o předpisy o svéprávnosti (*Geschäftsfähigkeit*, § 104 an. BGB), o nedostatcích vůle (§ 116 an. BGB), o formě právních transakcí (§ 125 an. BGB), o přístupu k vyjádření vůle (§ 130 an. BGB), o uzavírání smlouvy (§ 145 an. BGB). Uvedená ustanovení jsou občas prolínána odlišnou problematikou, například výkladu (§ 133 a § 157 BGB), obecných

[81] FLUME, W., cit. dílo, s. 77–78.
[82] FLUME, W., cit. dílo, s. 78–80.

hranic právně transakční regulace (např. § 134, § 135 an., § 136, § 138), předpisů o nicotnosti a rozporovatelnosti (§ 139 an. BGB), k nimž se však podrobnosti mohou nacházet ve zvláštní části BGB.[83]

Obsahem je vyjádření vůle nebo právní transakce regulace. Obsah se pak tradičně dělí na *essentialia*, *naturalia* a *accidentalia negotii* (shodně jako česká nauka, srov. 2.2.3). Dle Flumeho patří do obsahu právní transakce pouze *essentialia* a *accidentalia*, neboť jen ty bývají skutečně v rámci právní transakce vyjádřeny a určitě vycházejí z vůle jednajících, z jejich soukromé autonomie. Oproti tomu *naturalia* pocházejí z vůle zákonodárce.[84] Vůči tomu lze namítnout, že jednající mohou někdy být srozuměni se zákonnou úpravou, obsahem právního vztahu jsou pak i *naturalia*.

3.4 Souhrn

Německý civilní kodex BGB obsahuje a používá pro pojem soukromého právního jednání dva pojmy, a to *vyjádření vůle*[85] *(die Willenserklärung)* a *právní transakce (das Rechtsgeschäft)*. Pojmy mají podobný až stejný základní právní význam, výše podaný, a blíží se významu pojmu *právní jednání* z právního řádu ČR. Zatímco vyjádření vůle může být vhodnější pro jednostranné projevy vůle, pojem právní transakce bývá zpravidla vhodnější pro vícestranné projevy vůle. Pojem právní transakce se používá též tehdy, pokud náležitostí jsou další skutkové znaky.

Oba pojmy však nejsou definované, což umožňuje drobné odchylnosti v pojetí, ale i ve vývoji chápání pojmů. Flumeho analýza ukazuje, jak se oba pojmy, z nichž se více soustřeďuje na pojem *právní transakce (das Rechtsgeschäft)*, proměnily během let cca 1850 až 1900 do podoby v BGB, ale jak se i poté rozvíjelo či měnilo jejich pochopení. Zajímavý je Flumeho poznatek, že sice valnou část nauky lze sdílet pro všechny druhy právních transakcí, ale některé vady je přesto nutno zkoumat zvlášť. Flumeho koncepce právní transakce jako zákonem nucené formy právního jednání je zajímavá i jím zdůvodněná, zasloužila by si však důkladnější rozbor. Koncepce českého občanského zákoníku se jeví více přirozenoprávní (srov. § 2 odst. 1 a např. § 3 odst. 1 obč. zák.). Dle § 574 obč. zák. je pak třeba na právní jednání *„spíše hledět jako na platné než jako na neplatné"*. Dokonce i případy rozporu se zákonem jsou

[83] FLUME, W., cit. dílo, s. 78–80.
[84] FLUME, W., cit. dílo, s. 80–81.
[85] V tomto textu se *die Willenserklärung* z BGB důsledně překládá jako *vyjádření vůle*, abychom jej odlišili od situací, kdy hovoříme o projevu vůle v jiném kontextu nebo obecněji.

v českém občanském zákoníku zeslabeny, neboť dle § 580 odst. 1 obč. zák. neplatné je právní jednání, které odporuje zákonu, jen *„pokud to smysl a účel zákona vyžaduje"*.

Flume zastává shodně s von Savignym názor, že vůle a vyjádření se pravidelně překrývají, jsou souladné. Právě toto umožňuje, aby právní řád uznával vyjádření vůle nebo právní transakce. Vyjádření je spíše výrazem než sdělením vůle. Flume však odmítá absolutizovat, že by soulad existoval vždy, neboť například praktickým omylům nelze nikdy zcela předejít. Stejně odmítá absolutizovat, že by byla plně uspokojivá kterákoli z užívaných teorií, tedy teorie vůle, teorie vyjádření nebo teorie platnosti. Místo toho požaduje, aby se v rámci vyjádření vůle vždy zvažoval vztah složky sebeurčení a sebeodpovědnosti.

Německá civilistika důrazněji akcentuje kvazi-normativní podstatu vyjádření vůle nebo právní transakce, tedy že obsahově se jedná o regulaci, v níž ovšem běžně chybí jakákoli obecnost.

Německá nauka o složkách či aspektech vůle v poměru k projevu vůle je propracovanější než česká. V souhrnu řeší ale BGB i český občanský zákoník problematiku stejných druhů vad či nedostatků vůle či projevu vůle. Úprava ale není zcela shodná, zejména co se týče právních následků stejných vad. V oblasti dodávání právního jednání nepřítomnému adresátovi jednání se česká úprava zdá být německým BGB inspirována velmi těsně.

Klasifikace v německé civilistice vychází z jiného členění lidského *právního chování (rechtliches Verhalten)*, než se používá v teorii české civilistiky. Německé pojmosloví, zejména u *právních transakcí (die Rechtsgeschäfte)*, dává lépe najevo, že podstatou takového právního jednání je větší „akce", větší komplex vzájemných práv a povinností, které mohou být i časově rozprostřenější. Lépe odpovídá pojmu vztah, resp. právní vztah, jako relaci mezi subjekty práva. Odlišení od jednání podobného právním transakcím *(geschäftsähnliche Handlungen)* nebo od reálných aktů *(die Realakte)*[86] umožňuje lépe rozlišovat kvalitu právních transakcí v právním slova významu. Česká teorie zde trpí nejasností, zda jakýkoli drobný akt subjektu se má rovněž považovat za právní jednání, byť se jedná o akt v rámci předchozího provedeného právního jednání již předvídaný a subjektem jen řádně provedený. Takové analýzy spadají do oboru teorie občanského práva a přesahují účel tohoto textu.

[86] Ev. faktická jednání *(Tathandlungen).*

V této kapitole uvedené chápání základní německé terminologie BGB je nicméně nutným krokem pro porozumění, když budeme níže srovnávat úpravy a využití v tomto textu zkoumaného elektronického právního jednání v rámci obou právních řádů.

Tato strana je záměrně ponechána prázdná.

4. Podpis a jeho funkce z pohledu práva

V této kapitole se provádí právní rozbor vlastnoručního podpisu a jeho alternativních elektronických forem v úrovni teorie. Zjišťuje se, že náležitosti a požadavky na vlastnoruční podpis nejsou výslovně vyjádřeny zřejmě ve vůbec žádném právním řádu, ale mají spíše konvenční či obyčejový charakter. Důsledkem je, že ačkoli se vlastnoruční podpis používá ve všech právních řádech podobně,[1] právně se o něm pojednává i značně rozdílnými termíny a v různé systematice. Tyto rozdílné koncepce právníků nebývají chybné, ale mají různou úroveň přesnosti a především se různí. Nejednotnost pak značně ztěžuje orientaci, neboť někdy se stejná slova používají pro různé záležitosti a jindy rozdílné termíny pro stejné záležitosti. Mnoho slov a pojmů tak nabývá nejednoznačnosti.

První pokusy o funkční ekvivalenci s vlastnoručním podpisem byly založeny zejména na kryptografických metodách takzvaného digitálního podpisu. Do oboru podpisů tím pronikly i pojmy kryptologické, jakož i pojmy technické nebo pojmy z oboru technických norem. Z právního pohledu jsou někdy značně matoucí. Množství pojmů se později ještě více rozšířilo dalšími druhy technik elektronických podpisů, které navíc znejasnily, co a proč se má za podpis vůbec považovat.

Udržet si přehled a jasnost uvažování ve výsledné směsi pojmů různého původu se ve výsledku může ukázat jako poměrně obtížné, zejména když k tomu přistoupí i nutnost vykládat právní předpisy, které se týkají elektronických podpisů, popř. elektronických podpisů ve vztahu k jiným právním předpisům.

Smyslem této kapitoly proto je provést teoretickou analýzu problematiky, uspořádit ji a nastolit v ní určitý řád, který se výše uvedené potíže pokusí odstranit. Teoretické podklady či výsledky této kapitoly, jakož i ustavené pojmy, pak slouží v dalších kapitolách pro odkazy i pro zdůvodňování.

4.1 Vlastnoruční podpis

S vlastnoručním podpisem jsme v kulturním prostředí ČR běžně obeznámeni od dětství. Malé děti si již od 2. třídy základní školy nadepisují samy své pracovní sešity jménem a příjmením. Později tak označují i své písemné testy a začínají si zvykat, že

[1] Podobnost zde však neznamená stejnost. Právní vyžadování přítomnosti podpisu pro písemnou formu se může značně lišit podle právního řádu, různá mohou být i důkazní pravidla.

listiny aj. předměty s uvedením jejich jména k nim nějakým způsobem náleží. I jejich rodiče někdy škole podpisem potvrzují různé zprávy a listiny, jedinec si tak postupně osvojuje zkušenost a zvyklosti předchozích generací, že v některých životních situacích bývá použití podpisu vyžadováno.

S příchodem dospělosti by si již měl být člověk vědom, že jeho podpis může mít i právní význam, že bude vyžadován zejména u významnějších právních jednání a že protistrana může podepsanou listinu později různými způsoby uplatnit a v ní vyjádřené závazky právně vymáhat. Význam podpisu jako rozhodujícího momentu je zachycen i v takových dílech, jako je tragédie Faust od J. W. Goetha, je součástí západní kultury, včetně povědomí odpovědnosti za učinění podpisů.

Podpis se fakticky provádí perem (dříve inkoustovým, dnes častěji kuličkovým, popř. gelovým) na psací materiál, typicky papír. Pero je v zásadě pasivním nástrojem, jehož jediná vlastní vnitřní funkce spočívá v přiměřeném uvolňování inkoustu při dotyku pera s papírem. Podpis je vytvářen aktivně přímo rukou podepisující osoby. Při vytváření podpisu dochází k trvalému vtělení tahu písma buď do psacího materiálu (tlakem kuličkového pera), jindy spíš navrstvením na něj (inkoustová pera). Protože vzniklý záznam tahu na papír může dobře reprezentovat i rychlost, sklon nebo tlak pera, má vlastnoruční podpis charakter mnohorozměrného záznamu, tj. nikoli pouze dvourozměrného obrázku z běžného tisku. Z tohoto důvodu bývá v literatuře označován i jako takzvaný *holografní podpis* a právě tyto vlastnosti jsou i důvodem jeho poměrně obtížného napodobení a tím i obtížné padělatelnosti. Fyzická osoba mívá svůj podpis od určitého věku poměrně ustálený a z dostatečného počtu vzorků lze srovnat, zda podpis odpovídá.

Schopnost provést ustálený podpis spočívá v biomotorické paměti dané fyzické osoby, podpis sám je vytvářen v zásadě podvědomě. Tuto schopnost od osoby nelze oddělit. Podpis proto má charakter určitého biometrického parametru fyzické osoby.

Od jiných biometrických parametrů (např. otisk prstu, sken duhovky...) se však podpis zásadně liší tím, že je vytvářen na základě volního uvážení. Současně během vytvoření podpisu dojde k jeho vtělení na psací materiál listiny. Vtělení podpisu na psací materiál má tedy charakter záznamu o jedinečném projevu vůle, který jistě proběhl a současně není přítomen výsledek stejného projevu vůle nikde jinde. Obě náležitosti, tedy použití vůle i její okamžité a jedinečné vtělení, jsou důležité zároveň,

sama o sobě by žádná nestačila. Tento záznam lze ověřit a důkazně použít. Jestliže je podpis umístěn na vhodném místě písemnosti, lze konvencí (obyčejem) nebo právem stanovit, že se celý nebo nějaká část obsahu písemnosti přičítá dané fyzické osobě jako projev její vůle. Proto se podpis hodí pro potvrzování projevů vůle vyjádřených v listinách a v rámci práva se podpis hodí pro provedení písemného právního jednání. Je nutné odlišit, že zatímco podpis obecně vždy je výsledkem použití vůle v psychologickém slova smyslu, při použití pro právní účel musí být zformována i vůle právně jednat, dochází tedy navíc k použití vůle i v právním smyslu.

Pokud bychom se pokusili zjistit, zda se výše uvedené poznatky o podpisu, požadavky na tvorbu či provedení vlastnoručního podpisu v právním řádu nacházejí, zjistíme, že je právní řád ČR neobsahuje. Právo pouze v řadě případů použití vlastnoručního podpisu předepisuje, jeho náležitosti však opomíjí. Polčák *pravidla vytváření vlastnoručního podpisu* považuje za právní obyčej[2] a navíc uvádí, že obyčejový charakter má podpis nejen v jiných právních řádech, ale i napříč právními kulturami a že „ani při důsledném hledání se nám nedaří nalézt právní řád, který by formální definici listinného podpisu obsahoval".[3]Autor zde může přisvědčit, že přinejmenším v kontextu právního řádu Německa a common law definice též nenalezl.[4]

Hodnocení dostatečnosti podpisu je pak záležitostí soudního rozhodování. V ČR dostačuje uvedení pouhého příjmení a čitelnost podpisu se nevyžaduje.[5] V závislosti na okolnostech může někdy dostačovat i jen parafa.[6] V jiných jurisdikcích mohou být pravidla soudního hodnocení ale odlišná.

Za druhé pravidlo obyčejového práva související s vlastnoručním podpisem pak Polčák považuje *právní domněnku projevu vůle*, tedy obyčejové pravidlo, že „stručně řečeno, to, co osoba podepíše, vyjadřuje její vůli, je do té míry zaužíváno, že není důvod o něm pochybovat."[7] Tuto právní domněnku považuje za velmi silnou, nicméně nikoli absolutní, ale u soudu vyvratitelnou.

---

2 POLČÁK, R. Praxe elektronických dokumentů. *Bulletin advokacie.* 2011, č. 7–8, s. 53–61, s. 55.
3 POLČÁK, R. *Praxe elektronických dokumentů*, cit. dílo, s. 55.
4 Je pochopitelně obtížné být schopen jakkoli rozsáhlou rešerší dokázat nevyskytování se úpravy; nelze vyloučit možnost definice ve zvláštní právní úpravě; součástí hlavních úprav práva, zejména práva soukromého, však takové definice nejsou a nejsou ani v relevantní literatuře zmiňovány.
5 Melzer a Korbel in MELZER, F. – TÉGL, P. a kolektiv. *Občanský zákoník – velký komentář. Svazek III. § 419–654.* 1. vyd. Praha: Leges, 2014. Komentátor, s. 635–636.
6 Melzer a Korbel in cit. dílo, s. 636.
7 POLČÁK, R. *Praxe elektronických dokumentů,* cit. dílo, s. 55.

V případě druhého pravidla již nelze tvrdit, že nikde v právu neexistují vůbec žádné úpravy. Kupříkladu v německém právu ale nejsou součástí práva hmotného, nýbrž procesního. Podle § 440 odst. 2 ZPO[8] platí: *„Je-li pravost podpisu jména jistá ... platí pro psaní nad podpisem ... domněnka pravosti.“* Pravý podpis implikuje domněnku pravosti písemnosti, přičemž o pravosti podpisu může soud rozhodnout třeba na základě znaleckého posudku. Pravost se někdy označuje i jako původnost. Tato domněnka ze ZPO vyjadřuje hlavní účel vlastnoručního podpisu, jak je běžně chápán, totiž *autentizační funkci*. Podle Polčáka je vlastnoruční podpis standardním institutem používaným tisíce let k tomuto autentizačnímu účelu.[9] Podobná, nikoli však totožná úprava se od účinnosti nového občanského zákoníku nachází v jeho § 565.[10]

Od pravosti je poté nutné provést překlenutí k pravdivosti, též označované za správnost (např. právě v § 565 obč. zák.). Pravdivost ovšem má různý význam podle povahy obsahu písemnosti a povahy subjektu. V soukromém právu může spočívat buď v pravdivosti osvědčení o skutkovém stavu, který podepisující stvrzuje, anebo v opravdovosti vůle k právnímu jednání podepisujícího. Druhý případ odpovídá výše zmíněné domněnce projevu vůle, jak by pojem vůle byl vykládán v souvislosti s právním jednáním. Tuto domněnku vůle či správnosti skutečně soudy uplatňují, byť může být případně vhodné provést analýzu jejich judikatury pro podrobnosti.Chyba: zdroj odkazu nenalezen

Pokud původce jedná s písemností podle některé úpravy veřejného práva, i pak se zpravidla uplatní domněnky pravosti či správnosti. Posuzování náležitostí písemnosti však bude záležitostí obecného i zvláštního veřejného práva, které může vyžadovat přítomnost i dalších autentizačních prvků a náležitostí listiny k její platnosti, ale i k uplatňování presumpce správnosti. V závislosti na právní úpravě se může jednat o veřejnou listinu. Vůle původce pak sice bude přítomna ve smyslu psychologického významu pojmu a částečně i ve smyslu vůle zformované právem, což však ale vůbec nebude stejný význam, jaký má vůle z právního hlediska v soukromém právu. V něm je subjekt především nadán autonomií či svobodou ohledně provádění právního jednání. Lidská vůle projevovaná během jednání podle veřejného práva, zejména ze strany orgánů veřejné moci, sice využívá kognitivní lidské schopnosti, podstatou vůle, tj. chtěním, by však měla být podřízena zákonům nebo jejich prováděcím předpisům.

[8] Zivilprozessordnung.
[9] POLČÁK, R. *Praxe elektronických dokumentů,* cit. dílo, s. 55.
[10] Podrobný výklad platného práva zde není podáván, může se však nacházet v textu níže nebo v jiných publikacích autora.

Právě toto podřízení se je podstatou zásady vlády práva.[11] Využití lidské vůle ze strany orgánu veřejné moci zde je zaměřeno spíše jen na pomocné funkce, jako je porozumění skutkovému stavu, zvažování použitelné právní regulace, komunikace, zvažování v rámci diskrece, ale zvažování i v rámci obecné přiměřenosti jednání. Tyto činnosti nelze zpravidla považovat za redukovatelné na činnost automatu, musí být zásadně prováděny v lidské kvalitě činnosti, přesto jak iniciativa, tak jednání samo podléhají hmotnému i procesnímu veřejnému právu. Nuancím uplatňování vůle v rámci veřejného práva by bylo možné se dále věnovat, není to však posláním tohoto textu. Níže i výše se, není-li výslovně zmíněno jinak nebo to neplyne z obsahu textu, věnujeme právnímu jednání, vůli, podpisům v rámci soukromého práva.

O tom, že vlastnoruční podpis slouží v rámci soukromého práva k potvrzení o vyjádření vůle, není třeba mít zvláštní pochybnosti. Svědčí o tom zejména ta ustanovení práva, která představují náhradní možnosti namísto podpisu pro ty osoby, které běžný vlastnoruční podpis vytvořit nemohou. Vytváření vlastnoručního podpisu je kupříkladu podmíněno psací gramotností, jež historicky vůbec nebyla samozřejmá. I nový občanský zákoník v § 563 obsahuje možnost vytvořit namísto podpisu jen vlastní znamení (značku, symbol), svou rukou nebo jinak.[12] Podmínkou je schopnost seznámit se s obsahem právního jednání, např. pomocí pomůcek nebo prostřednictvím jiné osoby, kterou si zvolí. Pro dodržení písemné formy pak vlastní znamení musí být provedeno za přítomnosti dvou svědků, kteří listinu podle § 39 obč. zák. i sami potvrdí.

V Německu jsou požadavky na písemnou formu u osob bez schopnosti podpisu přísnější. Nemůže-li podle § 126 odst. 1 BGB[13] být listina podepsána *vlastnoručním podpisem*, tj. svým jménem a vlastní rukou, musí se v případě negramotných osob namísto podpisu použít *znamení ruky* (Handzeichens), které ale musí být notářsky ověřené. Znamením ruky může být např. symbol, značka, tři křížky. Zákon nepřipouští žádnou další autonomně proveditelnou[14] možnost nahrazení podpisu.

Zde je namístě upozornit, že zákoníky někdy umožňují i jiné formy podpisu, než je vlastnoruční, a to pro jiné účely, než je užití negramotnými nebo invalidními osobami. Tak například podle § 561 obč. zák. *„podpis může být nahrazen*

[11] V naší právní kultuře prosazované v rámci zásady právního státu.

[12] Lze si představit vytvoření znamení perem v ústech, jeho držením nohou nebo ochromenou rukou, popř. i pomocí protetických umělých náhrad paží apod.

[13] Bürgerliches Gesetzbuch.

[14] Není tedy možné se podepsat například inkoustovým otiskem prstu. Jsou ale vždy možné náročnější formy, tj. podpis ověřený notářem podle § 129 BGB nebo notářský zápis podle § 128 BGB.

mechanickými prostředky tam, kde je to obvyklé". Mechanické prostředky zahrnují razítka, popř. samotný tisk obrázku podpisu tiskárnou. Používat by se dle názoru autora měly spíše jen tehdy, když se provádí velké množství jednání hromadně a kdy by podepisující stejně obsahu jednotlivých listin nevěnoval zvláštní pozornost. Obvyklost může být objektivní v odvětví nebo subjektivní ve vztahu stran.[15] Bývá shledávána v bankovnictví a finančnictví.[16]

Dalšími druhy podpisů jsou podpisy elektronické, kterým se věnuje tento text. V českém občanském zákoníku se na formu či formy elektronických podpisů odkazuje v jeho § 561 blanketně. Dle německého občanského zákoníku je možné podle § 126 odst. 4 BGB nahradit písemnou formou elektronickou formou. Její náležitosti jsou uvedeny v § 126a BGB, vystavitel vyjádření musí uvést svá jména a elektronický dokument podepsat kvalifikovaným elektronickým podpisem.

Z uvedeného výčtu je patrné, že i právo samotné pro formu podpisu připouští více možností. Bude tedy existovat něco důležitějšího, než je podoba vlastnoručního podpisu, co má být podpisem naplňováno. Tím něčím jsou zřejmě funkce podpisu, kterým se věnujeme níže.

4.2 Funkce vlastnoručního podpisu podle německé právní nauky

K potřebě zabývat se funkcemi vlastnoručního podpisu docházejí různí autoři z různých právních kultur, ale i z profesí mimo právo. Níže je kupříkladu zmiňována analýza funkcí v rámci common law (srov. 4.4), ale i v oboru kryptologie (4.6).

V ČR se funkcemi podpisu nedávno zabývali Korbel a Melčák, dle nichž má funkce stvrzení konečnosti a vážnosti vůle, identifikace podepsané osoby a autentičnosti (vč. ochrany před zfalšováním),[17] obdobně uvádí i Polčák[18] funkce identifikace osoby, deklarace vůle a fixace obsahu (formální uzavření obsahu). Dle Čermáka ml.[19] má podpis funkce označení toho, kdo učinil právní úkon (označovací funkce), potvrzení, že se jedná o projev jeho vlastní vůle (deklarační funkce), ověření totožnosti jednajícího (důkazní funkce). Provést výčet funkcí vlastnoručního podpisu není samoúčelné.

[15] Melzer a Korbel in MELZER, F. – TÉGL, P. a kolektiv, cit. dílo, s. 643.
[16] ŠVESTKA, J. – DVOŘÁK, J. – FIALA, J. a kol. *Občanský zákoník – komentář. Svazek I. (§ 1–654).* 1. vyd. Praha: Wolters Kluwer ČR, 2014. Komentáře Wolters Kluwer Kodex Rekodifikace, s. 1388.
[17] KORBEL, F. – MELZER, F. Písemnost, elektronický a biometrický podpis v elektronickém právním jednání. *Bulletin advokacie.* 2014, č. 12, s. 31–36, s. 32.
[18] POLČÁK, R., cit. dílo, s. 55.
[19] ČERMÁK, K. ml. Elektronický podpis: pohled soukromoprávní. *Bulletin advokacie.* 2002, č. 11, s. 64–77.

Právníkovi umožňuje orientovat se ve smyslu požadavku na přítomnost podpisu do vyšší hloubky, než je konstatování, že buď se jedná o kogentní požadavek práva, anebo o požadavek protistrany. Znát funkce podpisu umožňuje i racionálně vytvářet jeho technické implementace nebo se v nich orientovat.

Za asi nejúplnější analýzu, navíc pocházející z nám blízké kultury i právního prostředí, považuji níže uvedené funkce podpisu podle německé nauky.[20] V kontextu německého práva se jedná o tyto funkce podpisu vztažené k písemnému vyjádření:[21]

1. „**Ověřovací** (Verifikation). Příjemce má možnost provedení a původnost podpisu ověřit vůči jemu známým vzorům pravého podpisu.

2. **Identifikační** (Identifikation). Vlastnoruční podpis jména umožňuje zjistit vystavitele listiny. Identifikace jednajícího je možná, jelikož stálý podpis se jednoznačně váže k osobě podepsaného.

3. **Pravostní** (Echtheit). Prostorové spojení podpisu s listinou, která obsahuje text vyjádření, vytváří souvislost mezi dokumentem a podpisem. Tím by se mělo zaručit, že vyjádření obsahově pochází od podepsaného.

4. **Uzavírací** (Abschluss). Vlastnoruční podpis je prostorovým uzavřením textu a dává najevo, že vyjádření vůle je jím ukončeno. Současně je odděleno i přípravné stadium pouhých návrhů od právní závaznosti.

5. **Varovací** (Warn). Vědomým aktem podepsání je jednající upozorněn na zvýšenou právní závaznost a osobní přičitatelnost podepsaného vyjádření. Tím je chráněn před ukvapením se v právním jednání.

6. **Zachovávací** (Perpetuirung). Požadavek písemné formy vede k tomu, že podpis a především text jsou trvale a čitelně zachyceny v listině, což umožňuje i jejich trvalé ověřování. Tím se zajistí, že informace o vyjádření není jen povrchní, nýbrž vyjádření je zdokumentováno.

7. **Důkazní** (Beweis). Vlastnoruční podpis pod zachyceným textem slouží potřebě předložení a provedení důkazu o právním jednání a vede k trvalé jasnosti. Písemná forma usnadňuje důkazně povinnému provedení důkazu, pokud odpůrce důkazu nepopře pravost podpisu.“

[20] Drucksache 14/4987, Entwurf eines Gesetzes zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr, Deutscher Bundestag, 14. 12. 2000, s. 16–17.

[21] Z metodických důvodů je pořadí funkcí přeskupeno a jsou očíslovány. Výklad ověřovací funkce je parafrázován. Seznam nevyjadřuje jen funkce vlastnoručního podpisu, ale vlastně funkce celých podepsaných písemností v listinné podobě.

Funkce jsou uvedeny zhruba v tom pořadí, jak by se jimi zabýval velmi pečlivý příjemce listiny. Nejprve by srovnáním s jemu známými podpisy **ověřil**, že přítomný podpis odpovídá jemu známému vzoru. Takové vzory mohou být ve starší korespondenci, v knize podpisových vzorů atp. Toto ověření lze rovněž nazývat *autentizací podpisu*, a jelikož vlastnoruční podpis je přímým projevem člověka, jedná se i o *autentizaci* nějaké *fyzické osoby*. Ze svých záznamů by příjemce následně zkontroloval **identitu** (totožnost) podepsaného vůči totožnosti tvrzené v listině.

Nedisponuje-li příjemce zkontrolovatelnými vzory a záznamy, má dvě hlavní možnosti. První je provést si u příležitosti vytvoření prvního podpisu kontrolu svou vlastní přítomností, včetně případné kontroly osobního průkazu apod. Druhou možností je tvrzenému provedení podpisu i identitě věřit s tím, že v případě pozdějšího sporu se uvedené funkce podpisu mohou zkusit aspoň dodatečně.

Jádrem užitečnosti a efektivnosti podpisu je **pravostní** funkce. Podpis je malý a rychle vytvořitelný prvek, který *autentizuje písemnost* přítomnou na listině. Přes ověřovací a identifikační funkce podpisu je pak písemnost vztažena nejen k podpisu, ale i k totožnosti osoby, která jej provedla. Funkce **uzavírací** znamená, že podpisem v nějakém čase nastala jistá konečnost formování vůle podepsaného, kterou podpis chrání i na listině ohledně neporušenosti obsahu podepsané části nad podpisem, před dodatečným přidáváním textu.

Vůči přijímací osobě se projevuje **varovací** funkce pouze reflektivně, utvrzuje ji o vážnosti vůle podepsaného. **Zachovávací** funkce udržuje projev vůle na listině i značně dlouhou dobu. **Důkazní** funkce se může využít vůči třetím osobám nebo úřadům, v případě sporu i před soudem.

Z hlediska podepisujícího funkce nastupují zhruba v pořadí: varující, uzavírací, pravostní, po vytvoření podpisu se přidají ověřující, identifikační, zachovávací a důkazní.

Pro podepisujícího jsou též německou naukou nezmiňované, ale podle autora důležité **ochranné vlastnosti**. Ty spočívají v tom, že ověřovací funkce vlastnoručního podpisu jej nepřetržitě chrání před zfalšováním, že podpis běžně nelze vytvořit nevědomě a podpis jiné listiny než chtěné je možný jen při hrubé nedbalosti.

Pro obě strany je důležité, že vytvoření podpisu je velmi levné, potřebné prostředky jsou všude přítomné. Více času a nákladů však již vyžaduje ověřování

podpisu, provádí-li se. Před vytvořením podpisu může náklady způsobovat vynaložený čas a zvažování, zda a jakou revizi písemnosti podepsat.

Uvedené funkce podpisu spolu vzájemně souvisí, navazují na sebe, popř. se i vzájemně překrývají. Například pravostní, identifikační ani důkazní funkce by neměly smysl bez funkce ověřovací a je otázkou, zda ověřovací funkce nemá být chápána jako již jejich vlastní pevná součást. Teleologicky je hlavní funkcí funkce *důkazní*, která by ale nebyla možná bez splnění prakticky všech ostatních funkcí. Sloučením některých uvedených funkcí, vypuštěním samozřejmých (zachovávací) nebo jinou terminologií (např. krycí funkce pro pravostní a uzavírací funkci) se lze snadno dostat na kratší seznam či jiné pojmy. Autor proto netvrdí, že jiné, stručnější systematiky nejsou možné. Kupříkladu i německá právní nauka sama příležitostně zmiňuje výčet funkcí vlastnoručního podpisu stručněji,[22] za hlavní pak považuje funkce pravostní, identifikační, důkazní a varovací.

4.3 Formy podpisu v common law

Kontinentální právníci vedou v patrnosti, že pojem podpisu je v anglickém common law podstatně neurčitější, než je tomu na kontinentu. Situaci dokumentuje např. poměrně rozsáhlý přehled případů *(case law)* forem podpisu,[23] soustředěný na případy z Anglie.[24] Případy lze rozdělit do několika hlavních oblastí.

Část případů se soustřeďuje na podpis *značkou (a mark)*. Ta může mít „formu jakéhokoli tvaru, včetně znaku kříže, písmene ‚x', tvar několik čar, které se protínají". Použití značek je charakteristické pro osoby bez znalosti psaní a sahá zpět až do 17. století. Místo podpisu ale někdy dostačuje použití *vytištěného jména*, včetně pouhého *vytištění názvu společnosti*, někdy i ve formě *litografovaného jména*.[25] Poměrně časté je dovolení použití gumového razítka, a to v mnoha oblastech. Případ pečetí je probírán níže (srov. pojem *korporátní pečetě* v části 6.6.4).

Další skupina případů se podle Masona týká nezvyklých modifikací formy nebo obsahu vlastnoručního podpisu, jako jsou nečitelné písmo, asistovaný podpis nebo

---

[22] HOEREN, T. – SIEBER, U. – HOLZNAGEL, B. (eds). *Handbuch Multimedia-Recht, Rechtsfragen des elektronischen Geschäftsverkehrs*, 35. Ergänzslieferung. München: C. H. Beck, 2013. Teil 13.3, R. 205.

[23] MASON, S. *Electronic Signatures in Law.* 3rd edition. Cambridge University Press, New York, 2012, s. 16–86.

[24] Příležitostně odbočuje do práva USA, Jižní Afriky apod., odbočky však nejsou objemově významné.

[25] Zřejmě by pokrylo i případy hlavičkových papírů vytvořených jiným způsobem tisku, než je litografie, například ofsetový tisk apod.

značka, odchylky od jména, použití iniciál, použití samotného příjmení, použití obchodní značky (jména), částečný podpis, slova jiná než jméno (např. „matka“ nebo „otec“), ztotožňující fráze („nejvíce milující z matek“) nebo zkratka jména.

Další část případů je k dispozici i pro podpisy mechanickými prostředky, jako jsou psací stroj, telegram, telex, faksimile, popř. podepisující stroje.

Z představeného nelze ani při podrobném studiu zdroje činit snadno abstrahující závěry. Právní posouzení vždy může záviset na právní oblasti, v níž se podpis vytváří nebo hodnotí. Jiné případy se mohou uvažovat za rozhodné pro různé právní oblasti, jako jsou závěti *(wills)*, směnky *(bills)*, nakládání s nemovitostmi *(interest in real property)*, hlasování *(voting)*, soudní řízení a správa *(judicial use)*, podvody *(Statute of Frauds)*, výkon advokacie *(Solicitors Act 1974)*, použití církevní *(ecclesiastic use)* nebo oblast veřejné správy *(administrative use)*.

Ohledně rozmanitosti forem podpisu Mason dovozuje:[26] „Soudní případy ilustrují, že obecně soudci posuzovali platnost podpisu ve vztahu k funkcím, které podpis vykonával ... což vyžadovalo širší porozumění funkcím vykonávaným podpisem. Ať měl podpis jakoukoli formu, soudce hleděl na záměr [*intent*], který byl za podpisem. Proto je možné rozmezí forem podpisu široké.“

Autor však stejný výčet uvedených případů hodnotí tak, že jakkoli je důraz na záměr podepisujícího *(intent of signatory)* z pravidelnějšího připuštění některých druhů podpisů (např. gumové razítko) soudy patrný, skoro stejně často bývala soudci některá stejná forma a priori odmítána pro obavu z falšování. Spolehnutí se pouze na záměr tedy nepřináší dobrou právní jistotu. Slabší formy podpisu soudy připouští tehdy, jsou-li pro ně rozumné důvody, vhodný kontext použití, popřípadě přídavné ochrany. Připouští se někdy i jen z důvodu efektivnějšího provádění podpisů, např. pro hromadné podepisování. Ochranou může být obsažení jiných autentizačních prvků v listině, zajištění bezpečnosti podpisového procesu nějak jinak přímo (např. přítomnými svědky) nebo nepřímo (součást širšího postupu vedoucího včas k odhalení zneužití).

Srovnáním s oblastmi úpravy, které jsou obsaženy v civil law střední Evropy, nicméně plyne, že fakticky pokrytý rozsah úprav forem podpisů není o tolik větší. Střízlivě hodnoceno je v dnešním common law Anglie a Walesu navíc pouze připuštění

[26] MASON, S. *Electronic Signatures in Law.* 2012, cit. dílo, s. 16.

použití podpisů razítky nebo vytištěním jména, přičemž je ale třeba zkoumat, zda je právní oblast použití připouští.

Tak jako v případě civil law, i v common law se pro možnost připouštění nových forem podpisů považuje za důležité provedení analýzy a porozumění funkcím podpisu.

4.4 Funkce podpisu v common law

V oblasti common law se zkoumáním obecných „funkcí zajišťovaných právními formalitami" *(functions performed by legal formalities)*[27] zabýval Fuller, který nalezl důkazní funkci *(evedentiary)*, varovací funkci *(cautionary)* a formační funkci *(channeling)*.

Význam prvních dvou vysvětluje již název a podrobněji jsou rozvedeny níže. Význam formační *(channeling)* funkce Fuller popisuje analogií: „kdo si přeje komunikovat své myšlenky vůči jiným, musí přetvořit hrubý materiál smyslu do definovaných o rozpoznatelných formací *(channels)*; musí zredukovat prchavé entity bezeslovných myšlenek do vzorců konvenční řeči."[28] Obdobně osoba zamýšlející provést právní jednání se musí soustředit na takovou vyjadřovací formu či kanál, které právo uznává. Zejména je proto potřebné, aby ji uznal a rozuměl potenciální soudce v případě sporu, a to včetně žádoucího způsobu nápravy sporu. V případě obecného písemného právního jednání se zejména musí volit správné právní termíny, obsah podčástí i celku být vnitřně souladný, a to vzhledem k cíli jednání i případnému ohledu na možnost jeho vymáhání před soudy.

Další analýzy od McCullagh et al.,[29] a zejména od Sneddon,[30] jsou již spojeny s érou počátků elektronického podpisu a pokoušejí se určit všechny vlastnosti a funkce vlastnoručních podpisů z důvodu návrhů vhodných implementací elektronických podpisů. Zejména Sneddon pokračuje v rozšiřování výčtu přidáním dalších důkazních *(evidentiary)* funkcí. Funkci varovací *(cautionary)* označuje z pohledu příjemce za ochrannou *(protective)* a přidává funkci uchovávání záznamů *(record-keeping)*.

---

[27] FULLER, L. L. Consideration and Form. *Columbia Law Review.* Vol. 41, No. 5 (May, 1941), s. 799–824.

[28] FULLER, L. L., cit. dílo, s. 802.

[29] MCCULLAGH, A. – LITTLE, P. – CAELLI, W. Electronic Signatures: Understand the Past to Develop the Future. (1998) 21(2), University of New South Wales Law Journal 452. [1. 11. 2016] Dostupné z: <http://www.austlii.edu.au/au/journals/UNSWLawJl/1998/56.html>.

[30] SNEDDON, M. Legislating to Facilitate Electronic Signatures and Records: Exceptions, Standards and the Impact of the Statute Book. (1998) 21(2) *University of New South Wales Law Journal* 334. [1. 11. 2016] Dostupné z: <http://www.austlii.edu.au/au/journals/UNSWLawJl/1998/59.html>.

Mason uvedené funkce vlastnoručního podpisu uspořádal, přičemž zejména důkazní funkce rozdělil na primární a sekundární. V současnosti je shrnuje takto:[31]

1. **Primární důkazní funkce** *(primary evidential function)*. Podpis „poskytuje přípustný a spolehlivý důkaz", že podepisující „schvaluje a přijímá obsah dokumentu, ... souhlasí, že obsah dokumentu je vůči němu závazný a bude mít právní účinek" a že „si je vědom důležitosti aktu a potřeby jednat v souladu s ustanoveními dokumentu".
2. **Sekundární důkazní funkce** *(secondary evidential functions)*. Podpis může rovněž poskytovat další přídavné důkazní schopnosti: může „autentizovat totožnost" podepisujícího; potvrzuje tvrzené „charakteristiky, znaky nebo status" podepisujícího; může prokazovat, že podepisující „potvrzuje, ověřuje nebo osvědčuje záznam, ale není nezbytně vázán obsahem dokumentu"; existence fyzického dokumentu „poskytuje záznam záměru podepisujícího", jakož i důkaz „původnosti a úplnosti samotného dokumentu, včetně času, data a místa vyhotovení podpisu na dokument"; podpis svědka může ověřovat „pravost a dobrovolnost vyhotovení podpisu třetí strany"; že „dokument nebyl změněn"; anebo „podpis může poskytovat důkaz toho, že záznam je věrnou kopií jiného záznamu."
3. **Varovací funkce** *(Cautionary)*. Podepisující je varován, že „by měl vynaložit péči před tím, než se zaváže k obsahu dokumentu", čímž je posílena právní podstata dokumentu.
4. **Ochranná funkce** *(Protective)*. Chrání stranu přijímající dokument. „Jako doplněk k varovací funkci" příjemce rozpoznává, že podepisující strana „stvrzuje obsah dokumentu" a „vynaložila plnou pozornost obsahu dokumentu". Může být rovněž „ubezpečena o totožnosti podepisujícího ... o průkazu zdroje a obsahu dokumentu".
5. **Formační funkce** *(Channelling)*. Vlastnoruční podpis „vyjasňuje okamžik, ve kterém osoba uznává akt za právně významný" a snižuje nejasnost „spojenou s orálními vzpomínkami" ohledně obsahu, smyslu a podstaty závaznosti.
6. **Funkce uchovávání záznamu** *(Record keeping)*. Fyzický dokument poskytuje „trvalý záznam podmínek dohody; rovněž umožňuje vládám na základě dokumentů ukládat daně a povoluje audity".

[31] Parafráze a zestručněná citace podle MASON S. *Electronic Signatures in Law*, cit. dílo, 2012, s. 8–10.

Výčet akcentuje důkazní funkce a snaží se pod ně přímo podřadit všechny právně rozhodné vlastnosti přítomnosti podpisu na listině. Přídavné důkazní funkce *(secondary evidential)* nemusí být nutně vlastností každého podpisu, popř. představují i určitou alternativu primárních důkazních funkcí.

Ve srovnání s německou metodikou se ta z common law jeví jako výrazně kazuističtější, funkce mají být co nejvíce přímo uplatnitelné u soudu. Tím, že primární důkazní funkce je vyjádřena jako vztah mezi vůlí podepsané osoby přímo k obsahu dokumentu, jsou v této systematice do důkazní funkce pohlceny pravostní *(Echtheit)* a ověřovací *(Verifikation)*. Otázka identifikační funkce *(Identifikation)* není akcentována,[32] je přítomna jakoby bokem, resp. až v sekundárních důkazních funkcích.

Jak upozorňuje i Mason, rovněž funkce 3 až 6 souvisí s důkazními funkcemi. Z výčtu lze zjistit, že funkce se vzájemně překrývají, některé se opakují (např. funkce svědka) nebo i vylučují (svědek nechce být vázán ve smyslu primární důkazní funkce).

Oproti tomu německá systematika analyticky dekonstruuje komplexní vztah podepisující osoby a podepsané listiny na co nejmenší a navzájem co nejméně závislé jednotky a až mezi nimi nachází funkce. Německá metodika též spíše abstrahuje od volního či právního významu podpisu, tj. zda je učiněn jako projev vůle jednající osoby, která chce obsah listiny učinit právně relevantním, popř. jde jen o projev svědka apod. Pokud by tyto faktory měly být zahrnuty, pak má německá metodika blíže k primární důkazní funkci, ovšem s tím, že sekundární důkazní funkce mohou vyplynout z podepsaného obsahu.

Po výše provedené dekompozici primární a sekundárních důkazních funkcí lze již mezi uvedenými metodikami funkcí vlastnoručního podpisu v common law a v civil law německé nauky nalézt prakticky úplné vzájemné mapování, a to oběma směry. Formační funkci *(channeling)* odpovídá uzavírací *(Abschluss)* funkce, snad jen s tím rozdílem, že v německé verzi uzavírání zdůrazňuje formální jasnost zachycení obsahu listiny v okamžiku provedení právního jednání, zatímco formační funkce více akcentuje okamžiku podpisu předcházející vnitřní intelektuálně volní úsilí, s reflexí forem a termínů práva podepisující osobou. Funkci zachovávací *(Perpetuirung)* odpovídá funkce uchovávání záznamů *(record keeping)*, též někdy označovaná jako uchovávací *(preservatory function)*.

[32] Zdá se, že právníci z common law netrpí důrazem na identifikaci. Přijde jim přirozené, že spoléhající osoba podepsaného zná, a nepovažují za kriticky důležité, zda přítomný podpis nese jméno Roberta Zimmermana, nebo Boba Dylana, pokud a dokud se jedná o pravý podpis stejné fyzické osoby.

Pouze ochranná funkce *(protective function)* není v německé metodice explicitně zachycena, protože je chápána jako v zásadě důsledek ostatních funkcí. Např. Sneddon považuje ochrannou *(protective)* funkci a varovací *(cautionary)* funkci za zrcadlové funkce, podle pohledu příjemce a podepisujícího. Autor se domnívá, že má-li podepsaná listina důkazní funkci, má pochopitelně i ochrannou funkci, tj. že ochranná funkce je dále přinejmenším i reflexí formační funkce *(channeling)*.

Je třeba též rozlišit, že ochranná funkce *(protective)* je zde odlišná od autorem výše zmíněné ochranné vlastnosti podpisu. Ochranná funkce slouží pro příjemce, ochranná vlastnost pro údajného podepsaného před možností zfalšování jeho podpisu.

4.5 Druhy techniky elektronických podpisů

Zatímco výše jsme se zabývali čistě právní analýzou či teorií vlastnoručního podpisu, zejména jeho funkcemi, v této části uvedeme přehled technických implementací v elektronické podobě, jež se využívají pro provedení podpisu v elektronickém prostředí, které právo některého státu světa za provedení podpisu uznává. Vhodným zpřesněním či vymezením je, že se jedná o podpisy používané v prostředí výpočetní techniky. Nejde tedy například o využití analogových elektronických zařízení apod. Přesto se takové podpisy označují jako elektronické.

Z obsáhlého díla Masona, autora[33] mezinárodního souhrnu legislativy i soudních případů, plyne,[34, 35] že jako technické implementace právně relevantního elektronického podpisu se nyní ve světě vyskytuje osm metod:

i. *Napsání jména v e-mailové zprávě.* Jméno na závěru e-mailu je považováno za podpis.

ii. *Napsání jména v elektronickém dokumentu.* Obdobně jako v e-mailové zprávě, ale v textovém editoru, textovém poli pod formulářem apod.

iii. *Jméno v e-mailové adrese.* Za podpis se považuje již jen adresa odesilatele.

iv. *Osobní identifikační číslo (PIN).* Zadání osobního kódu (PIN) finálně potvrzuje (jako podpis) předchozí jednání.

[33] MASON, S. *Electronic Signatures in Law*, cit. dílo, 2012.

[34] MASON, S. Informal Debate on the Issues Relating to Terminology and Clarification of Concept in Respect of the EU e-Signature Legislation, In: *SCRIPTed* [online], 2012, 9:1, s. 82–103, s. 84 [31. 8. 2016]. Dostupné z: <http://script-ed.org/?p=327>.

[35] MASON, S. Electronic signatures: the essentials. In: *InsideOut Magazine* [online], 15th December 2015 [31. 8. 2016]. Dostupné z: <http://communities.lawsociety.org.uk/in-house/insideout-magazine/electronic-signatures-the-essentials/5052726.fullarticle>.

v. *„Click wrap.“* Na displeji je zobrazen právní text nebo odkaz na něj, uživatel zaškrtne[36] políčko a stiskne tlačítko „*Souhlasím ...*“ (*Přijímám ...*). Jméno se neuvádí vůbec nebo se vyplní do předchozího formuláře.

vi. *Sken vlastnoručního podpisu.* Vzniklý obrázek (faksimile) podpisu je následně vkládán do elektronických dokumentů jako jejich podpis.

vii. *Biodynamická verze vlastnoručního podpisu.* Podpis se vytváří na podpisové plošince *(pad)* technickým perem, plošinka *(pad)* nebo zvláštní tablet *(special tablet)* jsou schopny snímat polohu pera i dynamiku vlastnoručního podpisu (tlak, sklon, rychlost, výška nad plošinkou). Záznam o podpisu se poté připojí k dokumentu.

viii. *Digitální podpis.* Používá asymetrickou kryptografii veřejného klíče. Dokument se podepisuje za pomoci soukromého klíče *(private key)*, kterým na světě disponuje pouze podepisující. Podpis dokumentu ověřuje spoléhající veřejným klíčem *(public key)* podepisujícího.

Výčet neznamená, že v každé jurisdikci a situaci budou metody připuštěny jako náhrada vlastnoručního podpisu. Uvedené možnosti jsou však časté.

Součástí výčtu by možná měla být možnost *ix. naskenování celé listiny s vlastnoručním podpisem*, kdy nejen podpis, ale celá papírová listina i s podpisem jsou naskenovány. Následně bývá sken zaslán elektronickou poštou. Metoda vesměs nahradila dřívější faxování a je v obchodním styku nyní běžná. Mason metodu výslovně neuvádí. Zřejmě dokument považuje za elektronickou kopii celé listiny. Podepisující osoba na listině provádí vlastnoruční podpis, a nikoli elektronický. Data podpisu nejsou předem zcela jednoznačně vymezena od dat zbytku podepsané písemnosti. Je však možné je vymezit a vydělit dodatečně.

Ani pak výčet nemusí být nutně zcela úplný. Například namísto zadání PIN je možné sejmout některé biometrické informace „podepisující“ osoby, např. otisk prstu nebo oční duhovky. Mason ani autor je však nepovažují zatím za často se vyskytující možnosti, popř. je považují spíše za metodu identifikace než za podpis.

Nyní je možné demonstrovat, k čemu jsou užitečné výše uvedené analýzy funkcí podpisu. Umožňují například hodnotit výše uvedené techniky implementace elektronických podpisů. K sedmi funkcím vlastnoručního podpisu podle německé

[36] Zaškrtává se nejen křížkem *(cross)*, ale i odškrtávací „fajfkou“ *(tick)*.

nauky, tedy k takzvané funkční ekvivalenci, se teoreticky dokáží přiblížit jen dvě poslední techniky, tj. digitální podpis a biodynamický podpis. Jejich bezpečnost ale musí být zaručena složitými postupy a technologiemi, nezávisle věrohodně ověřenými. U digitálního podpisu je typicky zajišťuje podepisující, u biodynamických spoléhající.

Ke zde uvedené terminologii technických implementací uveďme, že všechny termíny i) až viii) pochází z oblasti běžného jazyka výpočetní techniky. Nejedná se tedy o pojmy právní, ale ani o pojmy z vědního oboru kryptologie. Jde o pojmy praxe, které se používají pro popis skutkového stavu.

Zejména anglosaští právníci však mají tendenci používat pojem digitální podpis i jako pojem právní. Oproti tomu evropští právníci budou v právním kontextu hovořit o digitálním podpisu (skutkově) jako o elektronickém podpisu (právně), popř. jako o některé pokročilejší verzi elektronického podpisu (zaručený, kvalifikovaný).

Ostatní zmíněné techniky i) až vi) funkční ekvivalenci vlastnoručního podpisu nezajišťují. V praxi technické a případně i právní se však používají. V rámci evropského nařízení eIDAS vesměs spadají pod pojem elektronického podpisu prostého.

Význam těchto právních pojmů v rámci evropského nařízení eIDAS je blíže vykládán v samostatné kapitole níže.

4.6 Podpis podle kryptologie

Kryptologie je tradičně odvětví matematiky, které se zabývá šifrováním, tedy původně především utajováním obsahu přenášených zpráv. V dnešní době jsou její metody důležité zejména pro různé ochranné funkce v prostřední výpočetní a komunikační techniky (ICT). Moderní definice proto mohou být těsněji vztažené k využití v rámci těchto technik. Tak podle Menezes et al. *kryptologie* je „nauka o kryptografii a kryptoanalýze“,[37] sestává tedy z těchto dvou relativně samostatných částí. *Kryptografie* je: „nauka matematických technik, které se týkají aspektů informační bezpečnosti, jako jsou důvěrnost, integrita dat, autentizace entity nebo autentizace původu dat“.[38] *Kryptoanalýza* pak je dle stejného zdroje: „nauka o matematických technikách pro pokusy o prolomení kryptografických metod, obecněji o prolomení informačně bezpečnostních služeb“.[39]

[37] MENEZES, A. – VAN OORSCHOT, P. – VANSTONE, S. *Handbook of Applied Cryptography*. CRC Press, 1996, reprint London: 2001, s. 15.
[38] MENEZES, A. – VAN OORSCHOT, P. – VANSTONE, S., cit. dílo, s. 4.
[39] MENEZES, A. – VAN OORSCHOT, P. – VANSTONE, S., cit. dílo, s. 15.

Autor upozorňuje, že prolamování se v současnosti nemusí provádět, a typicky ani neprovádí, na čistě teoretické matematické úrovni, ale může napadat technické provedení kryptografických metod ve výsledných zařízeních. Je tedy paradoxní, že zatímco kryptografie slouží pro ochranu technologií ICT, kryptoanalýza může využít nejen matematické postupy, ale i chyby v návrhu ochrany v ICT, nebo jakékoli jiné proti-prostředky ICT, zpravidla dobře jednoúčelově uzpůsobené potřebám prolomení. Dokonce lze využívat i metody obecnější elektroniky, fyziky, popř. i jiných věd. Dobrou kryptografií je pak ta, která je odolná nejen ryze teoreticky, ale je odolná i proti použitelným metodám kryptoanalýzy, jež v daném čase existují. Ideálně je odolná i proti metodám nebo posílením výkonu, které jsou očekávatelné v horizontu dalších let. V tomto smyslu i kryptografie musí brát ohled na dobrou a efektivní implementovatelnost a současně na odolnost proti kryptoanalýze. O kryptologii lze proto tedy dnes hovořit jako o multidisciplinárním oboru, který kromě matematiky zahrnuje i počítačové vědy, komunikační vědy a elektronické inženýrství. Perspektivně nelze vyloučit zahrnutí i jiných věd, jakou je například kvantová fyzika. Matematické metody však dosud tvoří jádro kryptologie.

Kryptografické metody lze dělit na slabé a silné. Slabé sice poskytují potřebný druh bezpečnostně ochranné funkce, ale současnými metodami kryptoanalýzy jsou již prolomitelné. Lze je tedy použít pouze tam, kde se nepředpokládá soustředěný úmyslný atak útočníka, ale je potřebná například jen ochrana proti náhodnému rušení, nebo chráněné hodnoty jsou malé či zanedbatelné. Silná kryptografická metoda je pak taková, kterou prolomit za použití současných technologií nelze. Lze připustit, že prolomení je teoreticky možné, ale nutný počet pokusů či výpočetních operací je natolik vysoký, že je nelze v reálném historickém čase provést. Definice odolnosti kryptograficky silných metod proto obsahují podmínku „výpočtové neschůdnosti" prolomení. Metody silných kryptografických metod jsou též předmětem otevřeného akademického výzkumu. Předpokládá se, že je otázkou vědecké prestiže akademické komunity, že slabé metody jsou odhaleny. Odolnost metod silné kryptografie proto nikdy nespočívá na tajnosti metody, ale na tajnosti některých klíčů, které metoda užívá. Rozdíl mezi slabou a silnou metodou může též někdy spočívat v délce používaných klíčů.

Jelikož oblast výpočetní techniky, elektronického inženýrství, ale i dalších věd z kryptologie je předmětem neustálého vývoje kvantitativního (spojitého) a někdy i kvalitativního (tj. skokového), kryptografické metody *zastarávají*. Dnešní prostředky

kryptoanalýzy proto někdy umožňují prolomit kryptografické algoritmy, které před 20 lety byly bezpečné.

Další zvláštností, která vystihuje zvláštní vztah mezi matematickou technikou kryptografie a její technickou implementací, je provádění *hodnocení bezpečnosti (security evaluation)*, typicky nějakého technického prostředku nebo systému ICT.[40] Tyto metody vycházejí z kryptoanalýzy, ale současně se staly předmětem technické normalizace, aby poskytovaly pokud možno srovnatelné výsledky. Hlavní dnes užívaná metodika[41] poskytuje i užitečnou hrubou škálu různých úrovní bezpečnosti, tzv. *míry záruky bezpečnosti (Evaluation Assurance Level)*, v úrovních EAL 1 až EAL 7. Čím vyšší je chráněná hodnota, čím vyšší je riziko ataku, čím vyšší je potenciál útočníka, tím vyšší by měla být i hodnota EAL. Žádné technické zařízení však není schopné odolat atakům samo o sobě. Kromě zmíněné technické bezpečnosti musí uživatelé kryptologie vyžívat i vhodná opatření bezpečnosti fyzické, personální a organizační. Všechna opatření by měla být vůči sobě vzájemně úměrná a současně vhodná pro daný účel použití. Jejich návrh může opět být záležitostí technických norem z oblasti informační bezpečnosti, ale může být i předmětem vhodné právní úpravy.

4.6.1 Digitální podpis

Kryptologická či kryptografická literatura může obsahovat potenciálně mnoho druhů definic pojmu *digitální podpis*, navržených podle potřeb autora. Za jedno z děl, v nichž lze hledat ustálenější terminologii, lze považovat knihu *Handbook of applied cryptography*[42] autorů Menezes, van Oorschot a Vanstone. Jedná se o „bibli“[43] akademické kryptografie z druhé poloviny 90. let 20. století, zaostřenou na oblasti prakticky využitelných oblastí kryptografie. Dodnes může sloužit jako platné východisko a základní orientační pomůcka v oboru kryptografie a potažmo i kryptologie, ovšem s tím, že aktuální pokrok kryptologie je již třeba dosledovat v aktuálních odborných časopisech.

V první, úvodní kapitole autoři orientačně uvádí: „**Účel digitálního podpisu** je poskytnout prostředek entitě, aby mohla svázat svou identitu s kusem informace. Postup podpisu zahrnuje transformaci zprávy a nějaké tajné informace, držené entitou, do

[40] V systematice informační bezpečnosti bývá označován jako tzv. TOE – Target of Evaluation.
[41] Soubor norem ISO 15408; též označovaný jako Common Criteria.
[42] MENEZES, A. – VAN OORSCHOT, P. – VANSTONE, S., cit. dílo.
[43] Některé recenze dílo kvůli pokryté šířce témat označují za encyklopedii kryptografie, hloubka zpracování jednotlivých témat však významně překračuje běžnou úroveň encyklopedického zpracování.

visačky zvané podpis.“[44] Pokračují pak: „Účel digitálního podpisu (nebo jakékoli podpisové metody) je **dovolit řešení sporů**. Například entita A by mohla v určitém okamžiku popřít podpis zprávy, anebo by nějaká jiná entita B mohla falešně tvrdit, že podpis zprávy byl vytvořen A. Za účelem překonání těchto potíží je zapotřebí důvěryhodná třetí strana nebo soudce.“[45]

V 11. kapitole, zabývající se celé pouze digitálními podpisy, se uvádí pracovní definice kapitoly: „Digitální podpis je datový řetězec, který spojuje [asociuje] zprávu (v digitální podobě) s nějakou způvodňující [originating] entitou.“[46]

Digitální podpis v pojetí autorů nepředpokládá tedy nutně použití kryptografie veřejného klíče (PKI), podpis se může týkat obecné entity, která má blíže neurčený vztah původu ke zprávě či kusu informace, který podepsala. Metodika digitálního podpisu ale musí být navržena tak, aby případný spor mohl rozhodnout soudce nebo jiná třetí strana. Možnost řešení sporu třetí stranou je podstatnou náležitostí.

V kontrastu s digitálním podpisem autoři hovoří o jiné kryptografické funkci a účelu, o tzv. autentizaci (entity), kterou definují: „**Autentizace entity** je postup, kterým se jedna strana ujistí (pomocí získání potvrzujícího důkazu) **o identitě druhé strany** zúčastněné v protokolu, a že se druhá strana skutečně zúčastnila (tj. je aktivní v čase, nebo těsně předtím, než je důkaz získán).“[47] Autoři upozorňují, že pojmy *identifikace* a *autentizace entity* používají v knize jako synonyma. V právním pojetí tomu tak být nemusí, neboť entitou může být nějaký technický prostředek, zatímco identifikací buď jednoznačné určení tohoto prostředku,[48] nebo fyzické či právnické osoby, která jej používá.

Autentizace entity tak je především prostředek pro zjištění protějšku v rámci právě probíhajícího počítačového sezení. V rámci takto definované *autentizace entity* je nutné upozornit, že spoléhající strana sice sebe samu získaným důkazem ujistí, že jejím právě komunikujícím protějškem je určitá entita, ale matematické metody a uvedený důkaz samy o sobě nemusí být důvěryhodným důkazem pro nezávislou třetí stranu, že k autentizaci došlo. Hlavním důvodem této nedostatečnosti bývá, že použité metody nevylučují, že si důkaz nevytvořila sama. Spoléhající se strana v sezení tedy bude

[44] MENEZES, A. – VAN OORSCHOT, P. – VANSTONE, S., cit. dílo, s. 22. Zvýraznil autor.
[45] MENEZES, A. – VAN OORSCHOT, P. – VANSTONE, S., cit. dílo, s. 30. Zvýraznil autor.
[46] MENEZES, A. – VAN OORSCHOT, P. – VANSTONE, S., cit. dílo, s. 426. Zvýraznil autor.
[47] MENEZES, A. – VAN OORSCHOT, P. – VANSTONE, S., cit. dílo, s. 386. Zvýraznil autor.
[48] Například jedinečné sériové číslo, identifikátor apod.

bezpečně vědět, zda je autentizace protější entity pravá, ale nemusí být schopna o tom bez dalšího přesvědčit třetí osobu.

Autentizace entity pak sama o sobě rovněž neposkytuje žádný důkaz o tom, co bylo obsahem následné komunikace mezi stranami v počítačovém sezení. Situaci lze přirovnat ke kontrole občanského průkazu na recepci podniku. Taková kontrola a záznam o ní poslouží jako důkaz o vstupu osoby v určitý čas do podniku, ale nedokládají, zda a k jakému (právnímu) jednání dané fyzické osoby potom došlo. Právě v tom pak spočívá kategorický rozdíl oproti metodikám digitálního podpisu. Nedochází k autentizaci původce k žádným trvaleji zachytitelným (podepsaným) datům.

Autoři hovoří o *autentizaci entity* v kontrastu s *digitálním podpisem*, který označují i za *autentizaci zprávy*.

Na druhé straně ani metody digitálního podpisu (ve výše uvedených definicích) nebudou samy o sobě dostatečně průkazné pro třetí stranu či soudce, pokud pro entitu, která vytvořila podpis, nebude existovat nějaký mechanismus, který ji bude dostatečně přesně určovat a vázat ji k určité fyzické osobě. Tyto vazby musí být zabezpečeny technickými a organizačními postupy či obecně opatřeními technické, fyzické, personální a organizační bezpečnosti. Mají-li být realizovány, musí právo všechna tato opatření či postupy nějakým způsobem stanovit. Alternativně právo musí alespoň stanovit kritéria, která umožní uznat, že vhodná opatření nebo postupy byly dodrženy.

Pro případ právního jednání fyzické osoby bude též typické, aby vytvoření digitálního podpisu technickou entitou bylo vázáno na těsně předcházející autentizaci fyzické osoby (zvláštní případ entity) vůči ní, jež zahrnuje i její aktivní projev vůle, který by měl zahrnovat i vůli podepsat předloženou zprávu. Jako základ takové autentizace fyzické osoby jsou stále známy pouze tři druhy metod, spočívající v možnostech:[49] **něco vědět** (heslo, PIN, soukromý nebo tajný klíč), **něco držet** (čipová karta, kalkulátor hesel), **něco inherentního fyzické osobě** (biometrika: vlastnoruční podpis, otisk prstu, hlas, skenování duhovky atd.).

Jak ukazuje i tento text v kapitolách níže, není dosažení dostatečné důkazní úrovně metodou digitálního podpisu pro soud snadné, i když bude právo technické, organizační aj. bezpečnostní postupy stanovovat.

[49] MENEZES, A. – VAN OORSCHOT, P. – VANSTONE, S., cit. dílo, s. 387.

Ačkoli definice digitálního podpisu v kryptologii obecně nevyžaduje použití asymetrické kryptografie, ta se v současné praxi užívá prakticky výlučně. V jejím rámci se používá tzv. klíčová dvojice soukromého a veřejného klíče, která se přiděluje každé podepisující osobě. Při vytváření podpisu podepisující osoba (entita) používá soukromý klíč[50] *(private key)*, který je technicky v držení pouze této osoby (entity). Ověření platnosti podpisu se provádí za pomoci doplňkového veřejného klíče *(public key)*. Ověření může provést kdokoli, kdo má veřejný klíč k dispozici.

Pro srovnání, velmi podobné pojetí a terminologii používá i známý kryptolog Bruce Schneier, když hovoří o *autentizaci*[51] (osob, entit), *autentizaci zpráv*[52] a *digitálních podpisech.*[53] V případě digitálních podpisů jsou pro něj důležitými realizacemi ty, které jsou postavené na PKI, a za důležitou vlastnost u nich považuje i *nepopiratelnost*[54] (non-repudiation), která však v jeho pojetí vzniká až po připojení časového razítka k digitálnímu podpisu.

4.6.2 Vlastnosti vlastnoručního podpisu podle Schneiera

Odhalit funkce či vlastnosti vlastnoručního podpisu se pokoušeli i kryptologové. Analýzu však prováděli ad hoc z jim povědomé osobní praxe, nikoli z právních zdrojů. Například podle známého amerického kryptologa Schneiera má tradiční vlastnoruční podpis pět následujících[55] „vlastností:

- Podpis je **pravý**. Přesvědčuje příjemce dokumentu, že podepisující se záměrně rozhodl dokument podepsat.
- Podpis je **nezfalšovatelný**. Je pro příjemce důkazem, že podepisující, a ne někdo jiný, záměrně podepsal dokument.
- Podpis **není znovu použitelný**. Je součástí dokumentu a bezohledná osoba jej nemůže přenést do jiného dokumentu.
- Podepsaný dokument je **nezměnitelný**. Po podpisu dokument již nemůže být změněn.

---

[50] Jde o termín odlišný od tajného klíče *(secret key)*. Tajný klíč („tajnost“) je sdílen nejméně dvěma entitami (fyzickým osobami). Může tedy být použit pro zašifrování a dešifrování zprávy mezi nimi, ale nemůže vůči třetí straně sloužit k důkazu o tom, která ze stran jej použila.

[51] SCHNEIER, B. *Applied cryptography: protocols, algorithms and source code in C.* 2nd edition, John Wiley & Sons, New York: 1996, s. 52–56.

[52] SCHNEIER, B., cit. dílo, s. 56.

[53] SCHNEIER, B., cit. dílo, s. 37–40.

[54] SCHNEIER, B., cit. dílo, s. 40–41.

[55] SCHNEIER, B., cit. dílo, s. 35. Zvýraznil autor.

- **Podpis nelze popřít.** Podpis a dokument jsou fyzické věci. Podepisující nemůže později popřít, že podpis vytvořil.“

Schneier pochopitelně přiznává, že ani jedno tvrzení nemusí v praxi platit absolutně. Vlastnosti nicméně považuje za typické a jejich překonání představuje pro případného podvodníka vynaložení tolika námahy, že pro mnoho praktických situací jsou příjemci vlastnoručního podpisu ochotni riziko podstoupit.

Schneiera vlastnosti podpisu zajímaly z toho důvodu, aby mohl popsat, které kryptologické algoritmy a postupy vlastnosti podpisu splňují. Schneier si pochopitelně byl vědom, že v počítačové praxi je pro vážnější účely nepoužitelná přímá nápodoba metody formou obrázku podpisu. Pro počítače představuje jakékoli kopírování triviální záležitost, a to včetně obrázků i jinak složitých vlastnoručních podpisů. Uvádí: „prostá přítomnost takového podpisu [obrázku] neznamená vůbec nic“.[56] Počítačové soubory je navíc lehké po takovém podepsání změnit, aniž by se ponechal důkaz o změně.

Schneierem nalezené vlastnosti sice poskytují jakousi reflexi o vlastnostech vlastnoručního podpisu, současně však také vnášejí do uvažování zmatek.

Vlastnost *pravosti* pokrývá funkce uzavírací *(Abschluss)*, zřejmě navíc i ve spojení s funkcí varovací *(Warn)*. Označení vlastnosti za pravost však odvádí pozornost opět spíše k *nezfalšovatelnosti* níže, tj. k ověřovací funkci, anebo k pravostní funkci. Snahy implementátora mohou být odvedeny také někam zcela jinam.

Vlastnost *nezfalšovatelnosti* pokrývá zejména funkce ověřovací *(Verifikation)*. Není příliš jasné, zda je pro tuto vlastnost nutné použít i funkci identifikační *(Identifikation)*. Název je však matoucí tím, že ověřovací funkce pochopitelně může vést k závěru o tom, že podpis je falešný, že se jedná o podvrh.

Nemožnost nového použití podpisu pokrývá pravostní *(Echtheit)* funkce. *Nezměnitelnost dokumentu* rovněž pokrývá pravostní *(Echtheit)* funkce. Snad jen v těchto dvou vlastnostech je Schneierova analýza právně přínosná, neboť pravostní funkci jemněji člení.

Nepopiratelnost je nejspíš jen zopakováním vlastnosti nezfalšovatelnosti. Možná je však též určitým odkazem na funkci důkazní *(Beweis)*. Opět je potíží, že v případě selhání ověření (vlastnoručního podpisu) pochopitelně je u soudu popiratelný podpis, dokument i jakékoli důkazní použití.

[56] SCHNEIER, B., cit. dílo, s. 35.

Asi největším kamenem úrazu je právě nepopiratelnost *(non-repudiation)* podpisu a vyjádření této vlastnosti právě touto formou vyjádření. Použití tohoto pojmu se bohužel v kryptologii stalo běžným pro vyjadřování vlastnosti digitálního podpisu. V kryptologii se tímto označením neníí více, než že daná kryptografická metoda směřuje k danému účelu užití, tedy aby nebylo možné popírat původ určité datové zprávy, určitých dat. Jak je vysvětleno výše, až praktické provedení kryptografické metody však je rozhodné ohledně toho, zda je kryptografická metoda prolomitelná, nebo nikoli.

Označení **nepopiratelnost** pravidelně vede technicky uvažující osoby k dojmu nebo k přesvědčení, že digitální podpis, jehož hodnota byla ověřena jako platná, je z hlediska práva podpisem pravým a že navíc takový podpis nelze popřít, nebo je to právně velmi obtížné. Skutečný právní stav může být ale značně odlišný.

4.7 Komitmenty podpisu

Pojmem komitment podpisu je míněn jeho význam, důvod, smysl, pro který ho podepisující osoba vytvořila a na nějž se poté zrcadlově může spoléhající osoba i spolehnout. V tradiční právní praxi se s pojmem komitmentu prakticky neshledáme, ačkoli je jisté, že význam vlastnoručního podpisu je odlišný v takových případech, jako jsou podpis smlouvy, vystavení objednávky, akceptace objednávky, pokladního dokladu, protokolu o převzetí, účtenky, potvrzení své přítomnosti na prezenční listině schůze, podpisu doručenky, podpisu ověřující osoby při vidimaci nebo legalizaci, podpisu svědka na listině atd. Komitment zpravidla bezprostředně plyne z vlastního obsahu listiny, popř. může být plněji vyplývat z kontextu postupu, v němž bylo takové vytvoření podpisu považováno za běžné a mající určitý účel. Podepisující osoba svůj podpis zpravidla vytváří právě pro účel průběhu daného postupu, popř. se orientačně řídí i informacemi v obsahu listiny, zejména v bezprostředním okolí podpisu, zejména těsně nad podpisem. Komitment pak pravidelně mívá i svou právní složku v rovině objektivního práva, jejíhož obsahu si však podepisující osoba nemusí být nutně plně vědoma, pouze tuší, že existuje.

Právo a jeho teorie si pak zpravidla mohly dovolit komitment zanedbávat, protože zpravidla potřebnou klasifikaci jednání lze provést již na úrovni písmem vyjádřeného obsahu a podpis pak považovat za jeho pouhé stvrzení. V tomto smyslu abstrahuje od komitmentu například německá teorie funkcí vlastnoručního podpisu

(srov. 4.2). Teorie je pak použitelná v podstatě shodně jak pro právní jednání *(Willenserklärung)*, tak pro vyjádření vědomosti *(Wissenserklärung)*. V prvním případě bude důkazní funkce teorie bezprostředně vést k důkazu o právním jednání, v druhém případě k důkazu o skutkovém stavu.

V rámci teorie common law (srov. 4.4) si zejména Mason uvědomuje, že význam podpisu může být různý. Jeho primární důkazní funkce je opět vztažena zejména k právnímu jednání, ke znaku závaznosti pro podepisující osobu. Sekundární důkazní funkce však vyjadřují, že podpis může mít i různé jiné významy. Například podpis svědka jej samotného nezavazuje k obsahu vyjádřenému v listině.

Rozvoj uvažování o komitmentu přinesla až elektronická praxe a její snaha o elektronické podpisy. Důvody potřeby starat se nebo vyjádřit komitment elektronického podpisu jsou zde zřejmě dva.

Prvním důvodem je, že elektronický podpis zpravidla podepisuje celá data. I v případě, když data představují dokument, čímž zde rozumíme lidsky srozumitelný obsah analogický obsahu papírové listiny, nemusí být bez dalšího patrné, v kterém místě jej podepisující osoba jakoby podepsala. Tím se ruší možnost vykládat význam podpisu z textu v bezprostředním okolí podpisu. Ten podepisuje celý dokument.[57] V technické praxi lze pak podepsat jakákoli data, tedy i taková, která nejsou dokumentem, ale představují nějaký konečně dlouhý binární záznam. Elektronicky podepisovat lze například i programy (softwarové kódy) nebo lidsky nesmyslná data. Podpis pak má komitment jejich autentičnosti, v případě programů vyjadřuje například jejich původ. Pojmy autentičnost či původ budou bez dalšího mírně neurčité. Tak podpis nemusí vytvořit skutečný autor programového kódu, těch ostatně může být celá řada současně, ale až organizace, která odpovídá za vydání programu. Přesná znalost komitmentu daného podpisu může tuto neurčitost odstranit.

Druhým důvodem je snaha o automatizaci. Zatímco dřívější papírové listiny byly zpracovávány výhradně lidskými osobami, které jsou schopné pochopit hrubý význam listiny a následně i podpisu ze samotné listiny, popř. z bezprostředního okolí podpisu, v elektronické praxi je snaha podepsané dokumenty či data zpracovávat i bez aktivní lidské účasti. To umožňuje úspory, zvyšuje rychlost nebo nepřetržitost funkce

[57] V moderních formátech dokumentů s elektronickými podpisy může být tato potíž odstraněna. Nauka o komitmentech však vznikala na sklonku 90. let, kdy ještě nebyly rozšířeny. Ani v současnosti ale není určení „mista“ elektronického podpisu uvnitř elektronického dokumentu nijak samozřejmou vlastností.

(24/7) bez ohledu na pracovní dobu. Automatizovaný počítačový systém[58] pak nemusí být schopen vyhodnotit význam připojených elektronických podpisů čistě z podepsaného obsahu nebo kontextu procesu, v němž je nasazen. Může sice být schopen ověřit technickou platnost podpisů, ale potřebuje si být jist i významem jeho připojení. V takovém případě je pak ideální, pokud součástí podpisu[59] je i určitý kód, který vyjadřuje komitment a jehož význam lze i automaticky zkontrolovat. Tak kupř. výsledek ověření podpisu bude zřejmě odlišný, pokud ověřující automat zjistí, že podpis dat je podpisem odesílajícího subjektu, a nikoli podpisem původce (autora) dat.

Oba zmíněné důvody nastávat i současně. Níže je probráno několik případů komitmentů v počítačové praxi.

4.7.1 Důvody podpisu (Signature reasons) ve formátu PDF

Definovat význam připojení podpisu se pokouší různá technická řešení. V produktech americké společnosti Adobe Systems při vytváření digitálního podpisu v elektronických dokumentech formátu PDF se historicky umožňuje uvést tzv. *důvod podpisu (signature reason)*. Implicitně se nabízí seznam možností dle níže uvedené tabulky. V závislosti na jazykové verzi softwaru se použijí i uvedené základní textové možnosti vyjádření důvodu podpisu v odpovídajícím jazyce.[60] Osoba podepisující písemnost právního jednání v dokumentu formátu PDF proto učiní nejlépe, pokud neuvede důvod žádný! To je ostatně i implicitní možnost.

#	Signature reasons (English software version)	Důvody podpisu (česká verze softwaru)
0.	*Default (not entered)*	*Implicitně (nevyplněn)*
1.	I am the author of this document	Jsem autor tohoto dokumentu
2.	I have reviewed this document	Zkontroloval jsem tento dokument
3.	I am approving this document	Schvaluji tento dokument
4.	I attest to the accuracy and integrity of this document	Potvrzuji přesnost a neporušenost tohoto dokumentu
5.	I agree to the terms defined by the placement of my signature on this document	Souhlasím s určenými podmínkami umístěním svého podpisu
6.	I agree to 'specified' portions of this document	Souhlasím s určenými částmi tohoto dokumentu

Tab. 1 – Seznam implicitních důvodů podpisu v software Adobe Acrobat

[58] Uvažujeme běžný počítačový systém bez funkcí tzv. umělé inteligence.

[59] Jako součást podepsaných dat, byť zpravidla formou přídavných dat, tzv. atributů podpisu.

[60] Důvody podpisu zde tedy nejsou uloženy jako předdefinovaný kód, který by bylo možné vyjádřit shodně v libovolném jazyku, ale přímo jako krátká věta (řetězec) v některém jazyku. Automatické překlady jsou možné pak spíše jen hypoteticky.

Letmým pohledem na navrhované důvody podpisu 1 až 6 lze usoudit, že žádný z nich není navržen ideálně z hlediska podpisu právního jednání dle právního řádu ČR.

Důvody 1 až 3 působí jako navržené pro určité kroky postupu prací při vytváření dokumentu uvnitř korporace. Od původního autora (důvod 1) návrhu přes případnou kontrolující osobu (důvod 2) až po finální schvalující osobu (důvod 3). Ani jeden z těchto tří důvodů by nevyjadřoval úmysl provést právní jednání ani být následně právně vázán obsahem dokumentu, byť důvod 3 nebo 1 může toto zdání vyvolávat.

Oproti tomu důvody 4 až 6 se zdají být formulovány tak, jako by určité externí právní účinky vyvolávat měly, ovšem dostatečně určité budou snad jen podle práva některého státu v USA.

Důvod 4 působí dojmem, že podepisující osoba vystavuje dokument jako prohlášení o určitých skutečnostech a potvrzuje jejich přesnost, navíc digitální podpis bude zajišťovat integritu podepsaného dokumentu. Nejedná se však o podpis právního jednání. V praxi může být ovšem diskutabilní, co se míní přesností dokumentu. Pro potvrzování v rámci českého práva se fráze sama jeví málo určitá a její používání nelze doporučit. Chce-li podepisující osoba použít svůj podpis pro nějaký takový účel, měla by jeho význam stanovit doložkou, která bude součástí dokumentu a bude formulována vhodně z pohledu rozhodného práva, tedy například právního řádu ČR.

Vyjádření důvodu 5 *„Souhlasím s určenými podmínkami umístěním svého podpisu"* v českém právu není zcela jednoznačným vyjádřením ohledně vázanosti obsahem dokumentu, tj. ani toho, že souhlas má právní povahu právního jednání. Anglický originál *„I agree to the terms defined by the placement of my signature on this document"* by význam souhlasu s obsahem dokumentu po právní stránce a s jeho závazností, dle práva některého státu USA, mít mohl. Slouží zřejmě pro jednostranně podepisované dokumenty. Pro právní jednání dle českého práva však fráze není dostatečně určitá, a proto není ani vhodná.

Důvod 6 *„Souhlasím s určenými částmi tohoto dokumentu"* v českém právu nevyjadřuje dostatečně právní vázanost. Anglická verze *„I agree to ‚specified' portions of this document"* by snad mohla být použita u takových smluv, v jejichž rámci strany vyjadřují souhlas s jen určitou částí dokumentu. Možnost se ale spíše zdá navazovat na technickou vlastnost formátu PDF, ve kterém digitální podpis může „krýt" jen určitou

část dokumentu, jež je po vytvoření podpisu následně i nezměnitelná. Opět nezbývá než konstatovat neurčitost fráze, a proto její nevhodnost v rámci právního řádu ČR.

Důvody 0 až 6 nejsou možnosti vyčerpány. Uživatel může v políčku důvodu podpisu navíc uvést i libovolný vlastní znakový řetězec. Jakýkoli uvedený vlastní důvod se přidá do seznamu a nabízí se v případě vytváření dalších podpisů. Na internetových diskusních fórech či komunitách lze nalézt i žádosti o radu, jak si vymazat asi 50 zavedených vlastních frází důvodu podpisu, což je pochopitelně nepřehledná situace z hlediska určitosti používání. Je-li software nasazován v korporaci, mohou být důvody nebo další uživatelem definované důvody přednastavené pro jednotlivé uživatele, role a pracovní procesy zvlášť.

Technicky jsou důvody v dokumentu PDF realizovány tak, že jsou v souboru umístěny jako textový řetězec v rámci položek podpisu,[61] který obsahuje danou frázi vypsánu. Nemají tedy například přiřazen žádný jednoznačný identifikátor, který by umožnil jejich automatický překlad nebo automatické zjištění významu apod. Důvod podpisu se rovněž na digitálně podepsaném dokumentu sám běžně nezobrazuje! Použitý důvodový řetězec se zobrazí až po vyvolání okna *Vlastnosti podpisu*, což běžně uživatel neprovádí.

Snadno tak může dojít k situaci, že text dokumentu vyjadřuje určitý význam, který by připojený digitální podpis měl stvrdit, avšak u podpisu uvedený důvod může být s tímto významem v menším či větším rozporu. Za takové situace vzniká neurčitost významu podpisu a potažmo i celého dokumentu, popř. i právního jednání, je-li dokument použit pro vyjádření právního jednání.

Důvod podpisu ve formátu PDF představuje jakousi „doložku" digitálního podpisu, která má šetřit místo a nezobrazovat se v ploše dokumentu. Z výše uvedeného lze ale shrnout, že důvody podpisu, jak byly společností Adoby Systems pro formát PDF navrženy a zavedeny, právně způsobují pouze problémy a nepřináší skoro žádné výhody. Není proto překvapivé, že pravděpodobně u verze *Adobe Acrobat Reader 9* (cca rok 2008) bylo uvádění políčka důvodu podpisu z implicitního dialogu vytváření digitálního podpisu zcela vypuštěno. V konfiguraci, např. i u aktuálního *Adobe Acrobat Reader DC*, však lze zobrazování důvodů podpisu pro dialog vytváření podpisu opět zpětně zapnout, zřejmě pro ty uživatele, kteří si na uvádění důvodu podpisu zvykli nebo

[61] Klíč (Key) *Reason* na str. 728, *Reason array* na str. 698 a *Ff* na str. 699 in PDF Reference – Version 1.7, Adobe Portable Document Format, 6th edition, Adobe Systems Incorporated, November 2006.

je mají zavedeno v korporátní praxi. Důvody podpisu mohou stále obsahovat dialogy jiných programových aplikací jiných výrobců, které pracují s formátem PDF a umožňují v něm vytvářet digitální podpis.

Českým uživatelům, kteří dokument vytvářejí a podepisují v kontextu právního řádu ČR, nelze než doporučit, aby důvod podpisu nechali v implicitním potlačeném stavu. Pokud se již políčko důvodu podpisu v dialogu vytváření podpisu zobrazuje, je běžně doporučitelné ho nechat prázdné. Pro spoléhající osoby může tato vlastnost formátu PDF představovat nepříjemnou zátěž při ověřování platnosti podpisu tím, že by vždy měli zkontrolovat i to, zda v rámci okna *Vlastnosti podpisu (Signature Properties)* není uveden nějaký důvod podpisu, který by negoval význam podpisu a potažmo i dokumentu, což by způsobovalo jeho neurčitost, tedy právní vadu.

4.7.2 Důvody podpisu podle ETSI (commitment-type-indication)

Zajímavá taxonomie důvodů přítomnosti elektronického podpisu byla vytvořena v rámci ETSI.

Rámcovým kontextem této systematiky elektronických podpisů je zjevně vytvoření a doručování podepsaných zpráv.

Druh důkazu	Signature reasons	Vysvětlení významu připojení podpisu
-	*Default (not entered)*	*Implicitně (nevyplněn)*
Proof of origin	... indicates that the signer recognizes to have created, approved, and sent the message.	**Důkaz o původu.** Podepisující uznává, že vytvořil, schválil a odeslal podepsaná data.
Proof of receipt	... indicates that signer recognizes to have received the content of the message.	**Důkaz o příjmu.** Podepisující uznává, že přijal obsah podepsaných dat.
Proof of delivery	... indicates that the TSP providing that indication has delivered a message in a local store accessible to the recipient of the message.	**Důkaz o doručení.** Vykonávající poskytovatel služeb vytvářejících důvěru (TSP) potvrzuje, že podepsaná data doručil do místního úložiště, které je přístupné příjemci podepsaných dat.
Proof of sender	... indicates that the entity providing that indication has sent the message (but not necessarily created it).	**Důkaz o odesilateli.** Vykonávající entita potvrzuje, že odeslala podepsaná data (nicméně je nemusela nezbytně vytvořit).
Proof of approval	... indicates that the signer has approved the content of the message.	**Důkaz o souhlasu.** Podepisující schválil *(has approved)* obsah podepsaných dat.
Proof of creation	... indicates that the signer has created the message (but not necessarily approved, nor sent it).	**Důkaz o tvůrci.** Podepisující vytvořil podepsaná data (nikoli však nutně schválil nebo odeslal).

Tab. 2 – Seznam důvodů podpisu podle ETSI

Vytvoření zprávy může sestávat ze dvou důležitých kroků, a to je vlastní vytvoření obsahu *(creation)* a jeho schválení *(approval)*, které je následně předáno

k odeslání odesilateli *(sender)*. Alternativně jsou všechny tyto tři kroky sloučeny a výsledkem je důkaz o původu *(origin)* ve zprávě. Právně významný je zde zřejmě zejména krok souhlasu *(approval)*, který by nejspíš mohl mít charakter právního jednání. Oproti tomu vytvoření může spočívat jen ve vytvoření návrhu (např. advokátní kanceláří) a odesílání může být již jen čistě technickou záležitostí.

Zpráva může být odeslána přímo, ale i prostřednictvím poskytovatele služeb vytvářejících důvěru *(TSP)*. Zpráva může též být podepsána odesilatem *(sender)* i příjemcem *(receipt)*, ale může též být podepsána uvedeným poskytovatelem služeb vytvářejících důvěru a potvrzovat doručení *(delivery)* do úložiště přístupného příjemci zprávy.

V uvedeném komunikačním rámci může tedy být stejná zpráva postupně opatřena celou řadou elektronických podpisů a každý může mít jen zcela ostře vymezený význam. Na rozdíl od komitmentů pro formát PDF mají tyto komitmenty dodnes docela dobrý význam, a to i po přijetí nařízení eIDAS, jelikož právě v něm jsou upraveny i služby elektronického doporučeného doručování.

Uvedená taxonomie pochází ze specifikace ETSI TS 101 733,[62] ev. je též uvedena v RFC 5126,[63] a je zde označena jako atribut `commitment-type-indication`. Potažmo se mohou nacházet ve všech formátech elektronického podpisu (CAdES, PAdES, XAdES), jejichž technické specifikace byly vyhlášeny Komisí (srov. 6.2.2).

Uvedený atribut je podepisovaný a současně vymezuje význam právě toho elektronického podpisu, který jej podepisuje. Uvedené druhy komitmentů mají předdefinované jednoznačné kódy,[64] takže je automat může rozpoznat bez potíží a vyložit jejich význam zcela nezávisle na jazyku, který používá podepisující nebo spoléhající osoba.

4.7.3 Podpisové politiky

Zatímco výše uvedené komitmenty dle formátu PDF (srov. 4.7.1) nebo ETSI (srov. 4.7.2) představují ve svém úhrnu ještě poměrně konkrétní rámec či scénář, v němž se dané komitmenty mohou vyskytnout, techničtí normalizátoři v ETSI navrhli

[62] ETSI TS 101 733 V2.2.1 (2013-04) Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES).
[63] Request for Comments: 5126 CMS Advanced Electronic Signatures (CAdES).
[64] Ať již ve formátu OID z ASN.1, nebo jednoznačných URI.

ještě mnohem obecnější mechanismus, pojmenovaný jako podpisové politiky. Podpisové politiky jsou částečně zmíněny již ve výše uvedené specifikaci TS 101 733, zejména se jim však věnuje technická zpráva ETSI TR 102 041.[65] Dle definice v této zprávě **podpisová politika** *„je sada pravidel pro vytvoření a ověření elektronických podpisů, podle kterých lze stanovit jejich platnost v kontextu určité transakce"*.[66]

Uvedenými pravidly je třeba zejména rozumět dva požadavky na ně. Jednak to, že jsou formulovatelná ve strojově proveditelné formě. Na základě zápisu pravidel může počítačový automat ideálně binárně rozhodnout, zda určitý elektronický podpis je, anebo není platný. V horším případě může výsledek ověření vést na platnost pouze částečnou, s určitými nesplněnými předpoklady. Současně však musí platit i to, že stejná pravidla jsou vyjádřitelná i v lidsky srozumitelné formě, a to z toho důvodu, aby podepisující osobě při vytváření podpisu mohl být význam sdělen a ona byla schopná jej chápat. Stejná lidsky srozumitelná podoba musí být k dispozici i pro spoléhající se osobu, aby byla schopna znát význam, který mu podepisující osoba přikládala. Potřebu těchto dvou forem současně výslovně stanoví i TR 102 041.[67]

Každá podpisová politika umožňuje vytvořit jeden nebo více scénářů, v nichž mohou existovat specifické komitmenty související s jednotlivými elektronickými podpisy a podle nichž se mohou vytvářet a též ověřovat různé elektronické podpisy.

Z našeho pohledu je pochopitelně důležitá otázka vztahu podpisové politiky a právních následků podpisu. Obecně platí, že podpisové politiky jsou vyjadřovány spíše na úrovni technických norem a používají i jejich terminologii, jako jsou například původce, odesilatel, příjemce atp. Na škále od konkrétnosti k abstraktnosti je třeba zřejmě nalézt takový způsob vyjádření, který pro pokrytí co nejvíce případů užití bude co nejabstraktnější a co nejužitečnější, ale ještě je zcela jednoznačný. Právní význam podpisu je třeba vyložit. Přitom platí, že ačkoli lze jednu podpisovou politiku vyjádřit prakticky shodně v různých jazycích, v různých právních řádech se její význam může mírně či více lišit.[68]

---

[65] ETSI TR 102 041 V1.1.1 (2002-02) Signature Policies Report.

[66] TR 102 041, cit. dílo, s. 6.

[67] TR 102 041, cit. dílo, s. 11.

[68] Není účelem v této části konkrétně diskutovat právní výklady. Pro ilustraci jen uveďme, že úkon učiněný systémem datových schránek vůči orgánům veřejné moci podle § 18 odst. 2 zák. č. 300/2008 Sb., ve znění pozdějších předpisů, má stejné právní účinky jako učiněný písemně a podepsaný. Právní fikce zde *odesilateli* zprávy přisuzuje i její původ. Oproti tomu v systematice nařízení eIDAS u služby elektronického doporučeného doručování zůstává *odesilatel* pouze a jen odesilatelem a pojmy kladou určité nároky na službu, aby fakt odeslání byl dokazatelný.

Podpisové politiky lze vytvářet jako vnitroorganizační, pro členy určité početně uzavřené a koordinované skupiny, ale i pro otevřené vztahy, jejichž účastníci pouze musí určité podpisové politiky uznávat jako základ pro tvorbu a ověřování podpisů. Kromě subjektů, které následně vytváří a ověřují podpisy dle některé podpisové politiky, metodika předpokládá i existenci subjektu, který je vydal (např. průmyslové sdružení), a rovněž toho, který ji technicky vydal. Z hlediska uživatelských subjektů je možné, aby politika připouštěla k jedněm datům vytvoření jednoho nebo více podpisů. Takové požadavky lze formulovat jednak formálně, jednak materiálně. Z formálního hlediska se jedná v zásadě o topologický vztah. Podpisy mohou být na sobě nezávislé, zaobalující nebo kombinace předchozích. U nezávislých podpisy nezávisí na pořadí ani časové souslednosti vytváření. Zaobalující podpisy (též posloupnost podpisů, opouzdřenost nebo kontrasignace) znamenají několik podpisů v pořadí za sebou, přičemž jednou z funkcí zaobalujícího podpisu je osvědčit, že dokument byl již dříve podepsán jinou osobou. Možností takového využití je u notáře, který ověřuje podpis. Jinou možností využití je ale i podpis vedoucího podepisující žádost podřízeného. Více podpisů ale může mít i smysl transakční,[69] tj. zahrnutí podpisů notáře, banky, *clearinghouse*, dopravní transakce s použitím rolí *consigner*, *consignee*, *shipper*, *forwarder* atd. Různé podepisující osoby mohou zastávat různé role, z nichž následně plyne význam každého konkrétního podpisu. Podpisová politika může vznášet i další podmínky, jako jsou například výčet či kritéria subjektů poskytovatelů služeb vytvářejících důvěru nebo jejich dílčích služeb.

Potřeba podpisových politik vyvstává ze stejných důvodů jako vyvstává zájem o komitmenty a jejich taxonomii, tj. potřeba významu při podpisu celku a automatizace. V rámci určité podpisové politiky proto bude mít splnění pravidel na technické ověření elektronického podpisu i zcela konkrétní věcný význam, z něhož následně plyne i právní účinek (následek).

V praxi se podpisové politiky ve výše uvedené, vysoce formalizované podobě téměř neujaly. Vyžadují totiž poměrně značné organizační a institucionální úsilí působící na všechny účastníky shora předem, zatímco nejširší praxe má spíše tendenci k autonomní seberealizaci zdola, ze vzájemných interakcí.

[69] Slovo transakce je zde používáno v technickém slova smyslu, tj. označení série operací, vč. vytvoření více podpisů, které má smysl uvažovat pouze vcelku, tj. po dokončení všech jednotlivých operací.

To však neznamená, že podpisové politiky neexistují. Podepisují-li se dokumenty v rámci vnitroorganizačního toku schvalování, bývají podpisové politiky implementovány softwarem jednoho výrobce, který současně provádí technickou implementaci pravidel i jejich vizuální prezentaci pro různé uživatele. V druhém běžném případě, opakovaného použití ve vztazích, vzniká ustálený způsob provedení i významu elektronického podpisu z implementace, z provedení, smluvních podmínek, popř. další dokumentace či činností, které vytváření podpisů provází. V obou případech by bylo možné výše zmíněné podpisové politiky z reálných implementací extrahovat.

Je třeba též upozornit, že výše popsaný model podpisových politik je proti možné formulářově, vícestránkově orientované, nebo obecné počítačové praxi omezený. Praxe připouští nejen řadit k datům podpisy podle určitých rolí, ale případně i přídávat další datové součásti, které rozšiřují podepisovaný obsah a tím volněji modifikují význam dalších podpisů. I to může být důvodem nepoužívání podpisových politik.

4.7.4 Souhrn o komitmentech

Důvody používání komitmentů spočívají v možnosti automatizace a v určení významu podpisu, pokud se podepisuje jen celek dat. Uvedené příklady komitmentů výše dokládají, že konkrétní znění komitmentu bývá mnohem přesněji či úplněji pochopitelné až ze znalosti celkového rámce či scénáře, resp. z přehledu možných jiných komitmentů, významů podpisů, které by se v daném kontextu mohly vyskytnout.

Vzniká otázka, zda přednostně vzniká komitment (podpisová politika) nebo právní požadavek. Příklad komitmentů v PDF ukazuje, že tyto komitmenty byly zřejmě prvotně odvozeny z práva některého státu v USA, komitmenty dle ETSI naopak zřejmě prvotně vznikly v rovině technické normalizace, která pracovala s určitým modelem vytváření a doručování datových zpráv. Obdobně mohou komitmenty (podpisové politiky) vzniknout i z existující praxe přímou elektronickou nápodobou, popř. více iteracemi autonomní seberealizace mezi různými subjekty. Obecně tedy tuto otázku nelze zodpovědět, vznikat mohou oba základní případy, ale původ může pocházet z praxe samé. Zajímají-li uživatele systémů právní účinky, měli by si však vždy nechat provést právní analýzu výsledného systému a ověřit si, zda provedení systému s danými komitmenty či podpisovou politikou má ty právní účinky, které požadují.

Z právního pohledu může být užívání komitmentů, ev. podpisových politik někdy i komplikující. Pokud výslovně použitý komitment nebo podpisová politika

odporují obsahu, který byl podepsán, může vznikat obsahově neurčité právní jednání, což představuje vážnou právní vadu zřejmě v mnoha právních řádech. Komitmentům je proto vhodnější se nejlépe vyhnout, a to tak, že se používají takové moderní formáty elektronického podpisu nebo podepisovaných dat, které umožňují připojený elektronický podpis propojit a vztáhnout dovnitř elektronických dat (dokumentu) tak, že následně lze určit význam podpis přímo z obsahu, což je stejný způsob, jaký se tradičně používá u papírových listin.

V případě potřeby automatizace nemusí uvedné stačit. Pak je vhodnější volit takové provedení, které komitment přiřazuje zcela jednoznačně, je rozšířené, používané, uznávané. Přídavně je též vhodné, aby použité komitmenty či podpisové politiky byly zakotvené v právních předpisech nebo ve smluvní apod. dokumentaci.

4.8 Souhrn

Čtenář této kapitoly může nabýt dojmu, že výše uvedené podčásti jsou jen jakýmsi přehledem, rešerší různých přístupů a pohledů, akcentujících různé priority, a že nemusí být nutně vzájemně kompatibilní. Autor však tento dojem v zásadě nemá. Ačkoli jsou pohledy někdy neúplné nebo skutečně zaměřené na dílčí prioritu, hledí autor na předložené informace jako na většinově konzistentní. Proto zde v souhrnu vybírá jednak to, co je možné na základě této kapitoly již uspokojivě vysvětlit, a jednak to, co považuje za nosné závěry, které lze z výše uvedených analýz dále užitečně používat v právní teorii vlastnoručního podpisu a popřípadě i provedení elektronických podpisů. Především s těmito závěry se pak pracuje i v dalších částech této práce. Tyto závěry pro právní nauku jsou zejména případné pro středoevropskou právní oblast, dle názoru autora však jsou využitelné dokonce i obecněji, tj. pro civil law i common law.

Za funkce vlastnoručního podpisu se v této práci budou nadále považovat **funkce dle německé metodiky**: ověřovací *(Verifikation)*, identifikační *(Identifikation)*, pravostní *(Echtheit)*, uzavírací *(Abschluss)*, varovací *(Warn)*, zachovávací *(Perpetuirung)* a důkazní *(Beweis)*. Jak je uvedeno výše, tato metodika je vesměs převoditelná na systematiku z common law a v zásadě ji pokrývá. Pokrývá s rezervou i ad hoc zjištěné vlastnosti podpisu u kryptologa Schneiera. Rovněž funkce podpisu nalézané českou právní naukou do ní lze podřadit. Současně je pochopitelně správné upozornit, že metodika se nejvíce hodí právě do německého práva a že právě

v německém (důkazním) právu jsou nalezitelné některé úpravy a ustanovení, které ji i přímo slovně a pojmově podpírají.

K těmto sedmi funkcím autor explicitně přidává *ochrannou vlastnost* (před zfalšováním), byť ji částečně lze implikovat z funkce ověřovací. Německá nauka někdy přídavně hovoří i o funkcí *kontrolní*, tj. aby zachycené právní jednání bylo kontrolovatelné třetím osobami, ať již vnitřním auditem, nebo úřady.

Je třeba zjednat jasno ohledně tzv. **autentizační funkce podpisu**, často v textech zmiňované. Nejčastěji se jí míní pravostní funkce, tedy potvrzení podepsaného obsahu podpisem. Ten ověřuje pravost (původnost) obsahu. Některé texty však autentizační funkcí podpisu míní schopnost zjistit totožnost podepsané osoby, autentizovat ji, což je výše ale zváno jako funkce identifikační. Konečně ještě jiné texty autentizací míní přemostění od identifikované podepsané osoby až k podepsanému obsahu (autenticitu obsahu přímo vůči osobě), čemuž nejvíce odpovídá funkce důkazní. Ta je skutečně finálním účelem přítomnosti tradičního vlastnoruční podpisu, z hlediska analytického rozboru je však zjednodušující soustředit se jen nebo přímo na ni. Čtenář proto musí v textech zmiňujících podpis pečlivě rozlišit, co se autentizací v daném textu přesně míní, popř. zda terminologie dokonce nekolísá. Je-li někde níže použit obrat „autentizační funkce" podpisu přímo autorem a nevyplývá-li z kontxtu něco jiného, je míněna funkce pravostní.

Všech sedm funkcí představuje funkční model vlastnoručního podpisu. Techniky, které se u elektronického podpisu snaží splnit všech sedm funkcí, lze nazvat jako **funkční ekvivalenci**.

Kryptologie se snažila a nalezla kryptografické metody, které se funkční ekvivalenci těsně blíží, a označuje je za *digitální podpis*. Používá však pro takové metody též označení autentizace původce zprávy nebo nepopiratelnost. Metody digitálního podpisu v kryptologii jsou v současnosti prakticky výlučně založeny na asymetrické kryptografii, též nazývané jako kryptografie veřejného klíče, nebo jako spadající do infrastruktury veřejného klíče (PKI[70]).

Pojem digitální podpis se též používá pro odlišení druhu techniky elektronického podpisu v těch případech, které jsou vnitřně založeny na využití kryptografických metod digitálního podpisu. Zde se tedy pojem používá pro vystižení skutkového stavu, kterým

[70] Public Key Infrastructure.

je elektronický podpis proveden. Někteří anglosaští právníci používají pojem digitální podpis i jako právní pojem, tj. ve třetím možném smyslu a významu. Autor pro právní pojem používá zásadně označení elektronický podpis.

Druhy techniky elektronického podpisu se však v praxi naprosto neomezily pouze na metody digitálního podpisu navrženého kryptologií, ale používá se nejméně dalších sedm jiných druhů techniky elektronického podpisu, které právo často, nebo aspoň příležitostně, uznává.

Právně existují v zásadě dva akcenty pohledu na vlastnoruční podpis. První je veden prizmatem pohledu, že vlastnoruční podpis je **autentizační prvek** vůči obsahu listiny. Základem a východiskem zde je pravostní funkce *(Echtheit)*. Tato autentizace je doplněna právní domněnkou o projevu vůle, která projev vůle vytvoření podpisu rozšíří v tom smyslu, že za projev vůle fyzické osoby má i obsah listiny nad podpisem. Tato právní domněnka může být obyčejová, může být součástí procesního (důkazního) práva státu, důkazních pravidel aplikovaných soudy, judikatury.[71] Z funkcí vlastnoručního podpisu se zde nakonec využívá všech sedm, včetně funkce důkazní.

Tato právní domněnka o projevu vůle nemusí být adekvátní pro vůbec žádný druh techniky elektronického podpisu, včetně podpisů digitálních nebo biodynamických. V tradičním světě písemných listin je domněnka dostatečně zajištěna přirozenými vlastnostmi listin ve vztahu k lidským smyslům. V elektronickém prostředí jsou všechny informace vůči lidským smyslům prostředkovány technickými prostředky a k žádnému samozřejmému seznámení se podepisující osoby s podepsaným obsahem nemusí dojít.

Druhé prizma pohledu na (vlastnoruční) podpis jej považuje za **stvrzení konečnosti a vážnosti vlastní vůle ve vztahu k obsahu podepsané písemnosti**.[72] Upozaďuje se nebo se vůbec neobsahuje autentizační funkce. Toto pojetí považuje či vtahuje projev vůle[73] v obsahu písemnosti do úplného popředí a z úkonu podpisu činí jen navenek rozpoznatelný akt, kterým podepisující dává najevo konečnost a vážnost své vůle, jež je vyjádřena v písemnosti. Ze sedmi funkcí tomuto pojetí odpovídají funkce varovací a uzavírací. Toto pojetí se užívá pro prvních šest druhů technik elektronického podpisu (srov. 4.5). Zbytek funkcí může částečně nebo zcela odpadat.

[71] Uvedené prameny nebo zdroje mohou obsahovat i výjimky z této domněnky.
[72] Podrobnosti k tomuto pojetí jsou uvedeny ve výkladu elektronického podpisu prostého v rámci nařízení eIDAS níže (srov. 6.4).
[73] Popř. domněnku o projevu vůle.

Důkazní funkce musí být případně zajištěna nějak zcela jinak, a to případně i ohledně toho, že obsah písemnosti byl podepisujícímu skutečně předložen. Při použití vlastnoručního podpisu by zde do úvahy připadala jen letmá parafa nebo jiný druh velmi prosté čáry, vyjadřující souhlas s listinou.

V technické nebo kryptologické rovině skutkového stavu se někdy hovoří o vlastnosti **nepopiratelnosti** (podpisu). Běžně se jen jedná o označení druhu kryptografické metody, která má technicky vést k zajištění tohoto cíle digitálního podpisu, jenž je vytvořen fyzickou osobou. Toto označení je z právního pohledu matoucí, neboť ani kryptografické ověření platnosti takového podpisu nemusí nutně znamenat, že se jedná o podpis pravý, tedy skutečně učiněný podepisující osobou. Neznamená ani to, že osoba uvedená jako podepsaná vytvoření podpisu právně nepopře. Důkazní pravidla právního řádu nemusí být uvedeným označením vůbec dotčena.

5. Elektronické právní jednání

Tato práce se zabývá *elektronickým právním jednáním*. Účelem této kapitoly je proto vyjasnit význam pojmu, a to především s ohledem na nauku a platné právo užívané v ČR a v Německu.

Předně je třeba upozornit, že nijak samozřejmý není ani obrat sám od sebe. Používají se i obraty *právní jednání učiněné elektronickými prostředky* (např. § 561 odst. 1 obč. zák., § 562 odst. 1 obč. zák.), *právní jednání v elektronické formě* (např. § 126a BGB), ale i *právní jednání elektronicky* (např. odvozeně ze směrnice E-commerce). Použijí-li se tyto pojmy ve svém širokém významu, pak jsou asi všechny vzájemným synonymem, v úzkém významu (jaký je například odkázán v závorkách předchozí věty) se však význam odlišuje. Například stručné vyjádření *elektronicky* v návaznosti směrnice E-commerce je použito proto, aby se vyjádřila nemateriální povaha služeb takto prostředkovaných, přičemž data ale mohou být přenášena i opticky (sic), rádiově nebo jinak elektromagneticky. Úzký výklad *elektronických prostředků* by pak použití optického spojení vyloučil, tj. pravděpodobně je pro ně potřeba použít buď široký, nebo aspoň středně široký výklad. Používají se i pojmy jako *elektronická forma* nebo další užívané obraty jako *elektronickou cestou*, v *elektronické podobě* atd. Mohou odkazovat na obecný široký význam, ale i jen na některý zvláštní, omezený význam.

V této kapitole popisujeme elektronické právní jednání v soukromém právu ČR a Německa, jak jej upravují občanské zákoníky obou států a jak je vykládá související právní nauka.

Na úvod předešleme, že způsoby vyjadřování, a to i v platném právu, nemusí být vůbec jednotné. Tak občanský zákoník pravidelně používá obrat *právní jednání učiněné elektronickými prostředky* (např. § 561 odst. 1 obč. zák.). Velmi často se však hovoří o *elektronické podobě*, např. elektronické podobě písemnosti nebo elektronické podobě úkonu nebo jednání. Jindy se místo slova *podoba* užívá slovo *forma*, které mívá zřejmě stejný význam odlišení, ačkoli podoba je slovo popisující spíše vnějškový projev, zatímco forma uspořádání. I když rozlišení může mít význam, zatím zde vycházíme z toho, že se vesměs jedná o zaměnitelné pojmy a obraty.

5.1 Elektronické právní jednání v soukromém právu ČR

V této kapitole se probírá soukromé právní jednání učiněné elektronickými prostředky, tak jak vyplývá zejména z úpravy v občanském zákoníku.

5.1.1 Obecné požadavky

Právní jednání vč. elektronického má jako nutné znaky svobodnou vůli (§ 551 obč. zák.), zjevný projev vážné vůle (§ 552 obč. zák.), určitost a srozumitelnost obsahu právního jednání aspoň výkladem (§ 553 obč. zák.) a vyvolání právních následků (§ 545 obč. zák.).

V souladu s § 545 obč. zák. i naukou lze právní jednání spočívající v konání dělit na výslovné (slovy) a konkludentní (chováním), tedy *„způsobem nevzbuzujícím pochybnosti“*. Výslovné konání se pak v souladu s naukou[1] děje ústně, anebo písemně. Lze vyjádřit určité pochybnosti o výlučné disjunkci uvedených kategorií nauky. Typicky při ústním výslovném jednání bude přítomen značný prvek mimoslovní komunikace, který bude protistranu utvrzovat o pravosti vůle i o pravdivosti poskytovaných informací. Podle Fukuyamy[2] je možné, že právě lidská schopnost odhalovat lži a klam při spolupráci s jinými byla hlavním evolučním důvodem rychlého zvětšení lidského mozku a následně i intelektové kapacity, nikoli tedy například jen individuální činnost při sběru nebo lovu. Tento poznatek by právní nauka neměla zcela ignorovat. Rovněž při konkludentním jednání občas též padne nějaké vhodné doprovodné slovo.

V elektronické praxi může být zajímavý případ elektronického právního jednání provedeného omylem. Spočívá-li omyl v omluvitelně nechtěném stisknutí kláves, tlačítek myši nebo tlačítek na dotykové obrazovce, nebo snadno stisknutelné sekvenci tlačítek, nejedná se dle názoru autora o omyl ve smyslu § 583 nebo § 584 odst. 1 obč. zák., ale o nedostatek vůle podle § 551 obč. zák. K takové aktivitě zařízení může dnes snadno dojít, když např. dotykový chytrý telefon provede během přítomnosti v kapse uživatele nějakou činnost i sám o sobě, popř. když jej při zpomalení odezev uživatel zoufale mačká, aby vyvolal nějakou odezvu, ty však nastanou se zpožděním. Pokud uživatel nějaké jednání provést chce, ale je mu zobrazen jiný text, než který technicky

[1] DVOŘÁK, J. – ŠVESTKA, J. – ZUKLÍNOVÁ, M. *Občanské právo hmotné. Svazek I. Díl první: Obecná část.* 1. vyd. Praha: Wolters Kluwer ČR, 2013, s. 157, 161, 162.

[2] FUKUYAMA, F. *Velký rozvrat: lidská přirozenost a rekonstrukce společenského řádu*, Praha: Academia, 2006, s. 190–191.

odsouhlasí, opět nepůjde pro nedostatek vůle o právní jednání, jednání bude zdánlivé. Pokud jej přesto někdo bude považovat za existující (rozdíl textů např. jen malý) a byl-li podvrh úmyslný, pak jednání bude podle § 584 odst. 2 obč. zák. neplatné, neboť se jedná o lest. Byl-li podvrh neúmyslným, ale o rozhodující okolnosti, bude jednání podle § 583 obč. zák. opět neplatné. Pouze kdyby se jednalo o neúmyslnou změnu a o vedlejší okolnost v rozdílu odsouhlaseného a zobrazeného textu či jiného obsahu, vznikalo by jen právo na přiměřenou náhradu podle § 584 odst. 1 obč. zák.

K jednání v elektronické formě nemůže být v soukromých vztazích nikdo nucen, neboť každý má právo zvolit si formu, ve které chce jednat (§ 559 obč. zák.). Výjimkou je předchozí vzájemné ujednání na formě nebo požadavek zákona (rovněž § 559 obč. zák.). To se týká nejen vlastního aktivního provádění právního jednání v elektronické formě, ale i při jeho přijímání. Tento základní souhlas obou stran o komunikaci jednáním v elektronické formě považuje autor za přednější než úvahy[3] o tom, zda je příjemce vybaven technologií zpracování daného druhu elektronické formy. I kdyby byl, ale s určitou protější stranou nechce elektronicky právně jednat, nelze mu formu vnucovat. Jde o analogickou situaci k tomu, když se někdo k ústnímu jednání vyjádří ve smyslu „dejte mi to písemně, jinak na to neberu zřetel“. Nicméně i některá dojití jednostranných jednání nedohodnutou právní formou mohou mít někdy právní relevanci, např. mohou asi narušit dobrou víru adresáta ohledně některých skutečností.

5.1.2 Elektronické právní jednání bez požadavku formy

Pro elektronické právní jednání je následně důležité rozlišit, zda se jím chce dosáhnout splnění písemné formy, anebo nikoli. Povinnost písemné formy může být uložena zákonem nebo předchozí vzájemnou dohodou stran (opět § 559 obč. zák.). Není-li požadavek na dosažení formy, pak lze *právní jednání učiněné elektronickými prostředky* provést jakkoli. Může být přítomen jakýkoli druh techniky elektronického podpisu i) až viii), elektronický podpis ale nemusí být přítomen vůbec. Mohou být použity i nepočítačové prostředky, jako např. analogový magnetofon nebo analogová videokamera a jejich záznamy. Lze použít i elektronické prostředky nevytvářející záznam, např. rádiovou vysílačku hlasovou nebo s Morseho kódy.

Pokud vzniká elektronický záznam (digitální, analogový), je třeba odlišit, zda takový elektronický záznam je pouze zachycením jednání, které již proběhlo (např.

[3] ČERMÁK, K. ml., cit. dílo, s. 71–72.

kamerový záznam přebírání zboží dokumentuje jeho převzetí), anebo je prvně prostředkem, kterým se vlastní jednání teprve provádí (např. záznam v hlasové schránce obsahující objednávku) a až sekundárně též důkazem o něm. Pouze v druhém případě lze hovořit o právním jednání učiněném elektronickými prostředky. Elektronický záznam o právním jednání přitom může být autentizován též jinak než elektronickým podpisem.

Zde pak lze souhlasit se Sokolem,[4] že právní zavedení kategorie právního jednání učiněného elektronickými prostředky bez požadavku formy je z hlediska práva v podstatě zbytečné, neboť dovolení formy hmotněprávně vychází již z § 559 obč. zák. a procesně z § 125 o. s. ř. a z doktríny volného hodnocení důkazů. Smysl však může mít pro právní dogmatiku nauky nebo z hlediska právní jistoty právně jednajících subjektů.

5.1.3 Písemnost v elektronické podobě

Je-li potřeba splnit *písemnou formu právního jednání*, naší potíží bude, že institut není v občanském zákoníku přesně definován. Je třeba jej odvozovat z nauky, ze zvyklostí právníků, z jazyka, popř. z kontextů použití pojmu v zákonech. Naši situaci zdánlivě usnadňuje, že občanský zákoník v § 561 odst. 1 věta 3 hovoří o elektronickém podpisu *písemnosti*. Usnadnění je jen zdánlivé, protože ani písemnost není v občanském zákoníku definována a platí pro ni to samé, co je řečeno výše o písemné formě právního jednání.

Podle § 3026 odst. 1 obč. zák.: *„Nevylučuje-li to povaha písemnosti, platí ustanovení tohoto zákona o listině obdobně i pro jinou písemnost bez zřetele na její podobu.“* Uvedené znamená, že listina je písemností, je i demonstrativním příkladem druhu písemnosti. Není ale definicí písemnosti ani nestanoví kritéria, při nichž by písemnost v jiné podobě (např. elektronické) bylo možné považovat za ekvivalent listiny. Dokonce ani ustanovení občanského zákoníku o listině z § 3026 asi nevyužijeme, protože § 561 odst. 1 obč. zák. hovoří o podpisu písemnosti, a nikoli listiny. Dále argument nevede zatím nevede.

Teorie hovoří o písemnosti (písemné formě[5]) a o jejím doplnění podpisem pro platnost formy, o psané formě (písemnosti) pak hovoří jako o „jakékoli psané čili

[4] Vyjádření Sokola se týkalo odpovídajících ustanovení v zákonu č. 40/1964 Sb., občanském zákoníku; in SOKOL, T. Ještě k elektronickému dokumentu. *Bulletin advokacie.* 2002, č. 3, s. 42–46, s. 43.

[5] DVOŘÁK, J. – ŠVESTKA, J. – ZUKLÍNOVÁ, M., cit. dílo, s. 162.

zrakem vnímatelné podobě“.[6] Pojem *písemnosti* má být abstrahující od podoby provedení. Písemnost tedy může být v podobě listinné (tj. zejména papírové) nebo v podobě elektronické (zde rozuměj počítačové, jako soubor, elektronický dokument, elektronický objekt apod.). Papírová listina se pak, chybí-li jasná zákonná ustanovení, „z logiky věci“ typicky podepisuje vlastnoručním podpisem, písemnost v elektronické podobě elektronickým podpisem.

Příklad pojetí právní praxí je u Sokola: „písemná forma je zachována vždy, kdy se projev vůle či jakýkoli jiný text objevuje tak, že je zaznamenán písmem, nezávisle na tom, zda-li písmo ...[je viditelné díky inkoustu na papíře nebo promítnuto na displeji počítače]“.[7] Obdobně pro písemnou formu Hulmák: „obsah právního jednání musí být zachycen způsobem, který představuje grafické znázornění souboru znaků, které jsou v nejširším smyslu slova písmem (tento požadavek nebude splněn např. u zvukové nahrávky nebo filmu)“.[8]

Je patrné, že právníci nauky i praxe za písemnost považují především viditelný text, provedený písmem, a je jim lhostejné, zda je text na papíře nebo na displeji. Současně však používají obraty hovořící o zaznamenání či zachování textu, předpokládají tedy trvalejší existenci písemnosti.

Ze slov *písemná* forma nebo *písemnost* by jazykově bylo možné odvodit, že se má jednat o nějak uspořádaný souhrn písmen, nejspíše o posloupnost písmen.[9] Písmena však mohou být součástí nejen nějaké abecedy přirozeného jazyka, tvořit jeho slova a věty, ale i součástí prakticky libovolného matematického nebo jiného umělého systému, použitelného pro komunikaci sdělení.[10] I znaky jako „+“, „-“ či číslice „1“, „2“ atd. tvoří písmena některého druhu algebry, kterými následně lze vyjadřovat nejen běžné počty, ale popsat i geometrické systémy. Písmeny či kódy (kód je také písmenem) se zapisují i programy v programovacích jazycích, ale i jejich data lze, pokud se chce, považovat za písmena.[11] Mez rozmachu tvoří *zjevnost projevu, vážnost vůle, určitost a srozumitelnost obsahu* právního jednání, jakož i *vyvolání právních následků* (§ 545 obč. zák.).

---

6 DVOŘÁK, J. – ŠVESTKA, J. – ZUKLÍNOVÁ, M., cit. dílo, s. 162.

7 Parafráze autora dle SOKOL, T., cit. dílo, s. 43.

8 Hulmák citován k výkladu § 562 OZ in MELZER, F. – TÉGL, P. a kolektiv., cit. dílo, s. 646.

9 Obecně myslitelné jsou však i stromy z písmen, myšlenkové mapy a možná i jiné útvary, třeba koláž.

10 Obdobně Čermák ml. hovoří o různých sémiotických celcích.

11 Takové programy pak jsou schopné emulovat jiné sdělovací systémy, například vykreslit na displeji avatara jednající osoby, vydávat zvuky řeči, řídit chování humanoidního robota, který vyjadřuje právní jednání konkludentně. Autorovi je nicméně jasné, že proražení některých vrstev abstrakce není účelem požadavků na písemnou formu.

Za definici právního jednání v písemné formě v teleologickém smyslu[12] lze snad považovat § 562 odst. 1 obč. zák., dle nějž: *„písemná forma je zachována“* dojde-li prostředky k *„zachycení obsahu [právního jednání] a určení jednající osoby“*. Protože z funkcí vlastnoručního podpisu víme, že o určení jednající osoby se nám u listiny postará vlastnoruční podpis, na písemnost zůstává zachycení obsahu. O písemnost tedy půjde jen tehdy, když je schopna zachytit obsah právního jednání trvaleji. Tradičně moderně na papírovém nosiči. Historičtěji za antiky třeba na papyru, hliněných nebo voskových destičkách či i vytesáním do kamene. Postmoderně na datových nosičích magnetických, optických, ale i elektromagnetických (např. nové paměti SSD), popř. nosič a jeho podstata ani nemusí být známy (uložení v cloudu).

Z poznatků shora lze uzavřít, že *nejkonzervativnější, současně i nejužší výklad písemnosti* je, že se jedná o vyjádření v přirozeném jazyce, trvaleji zachyceném písmeny jeho abecedy. Přidáme-li z matematických symbolů k písmenům jen číslice pro číslování odstavců a vyjádřování množství či peněžních částek, nebude asi žádný právník nic namítat. Dlužno podotknout, že pro právní jednání s povinnou písemnou formou[13] bude takto úzká definice vesměs dostačovat.

Ne každá taková posloupnost písmen ale bude právním jednáním. Je-li písemně zapsána báseň, ale i novinový článek, nepůjde běžně o písemnost právního jednání. Chybí úmysl právních následků.

Ani pravý vlastnoruční podpis nedokáže vytvořit z takového obsahu právní jednání. Může mít význam, ale jiný. Kupříkladu podpis na obraze bývá signaturou, která rovněž pomáhá určit malíře obraze, obraz je ale uměleckým autorským dílem, a nikoli právním jednáním.

Za přiměřený výklad *písemnosti* autor pokládá, pokud aspoň úvod právního jednání je zapsán v některém přirozeném jazyce,[14] případně s mírným využitím čísel a počtů. Takový úvod musí dostatečně vysvětlit význam dalších částí či příloh, tedy metod, jimiž mají být interpretovány, jinak by tyto další části nebyly srozumitelné nebo určité. Takové další části nebo přílohy mohou obsahovat i různé netriviální záznamy, jako jsou tabulky, vzorce, grafy, obrázky, výkresy apod. Taková technická vyjádření často mohou obsahovat jednodušší a jednoznačnější určení toho, co představuje třeba řádné plnění a co naopak podstatné porušení smlouvy (§ 2002 obč. zák.), než by bylo

[12] O teleologii Čermák ml. hovoří obdobně in ČERMÁK, K. ml., cit. dílo, s. 66.
[13] Například pro souhlas s lékařským pokusem, ručitelské prohlášení, uznání dluhu, zástavní smlouvu...
[14] Obdobně Čermák in ČERMÁK, K. ml., cit. dílo, s. 66–67.

možné vyjádřit jen přirozeným jazykem, a mohou tvořit nedílnou součást právního jednání.

Elektronická podoba písemnosti může jít zřejmě dále než podoba listinná. Lze si představit např. vizualizace věcí ve 3D prostoru (např. kuchyňské linky, stavby apod.), vrstvené technické plány, popř. i podrobné technické parametry např. do stroje pro výrobu věci apod. Všechny části či přílohy písemnosti by ale měly být opouzdřené v tom smyslu, že jejich obsah nebude záviset na vnějších údajích, tedy nacházejících se mimo obsah provedeného právního jednání, a to včetně času. Smyslem zachycení v písemné formě je, aby obsah byl opakovaně reprodukovatelný, a to vždy stejně jako při provedení jednání.

Písemná forma bývá naukou řazena pod výslovnou formu právního jednání. Autor dovozuje, že ani zde se zřejmě nemusí jednat o exkluzivně disjunktní kategorii. Četné technické jazyky budou sdělení spíše poskytovat *„způsobem nevzbuzujícím pochybnosti“* podle § 546 obč. zák., než aby bylo vyslovitelné.

Judikatura Nejvyššího soudu považuje písemnost za nezbytnou součást právního jednání. Dle soudu: „Písemná forma právního úkonu předpokládá existenci dvou náležitostí, a to písemnosti a podpisu. Písemnost spočívá v tom, že projev vůle (právní úkon) jednajícího subjektu zahrnuje všechny podstatné náležitosti zachycené v písemném textu listiny. Písemný projev musí být zároveň podepsán, tj. je platný až po podpisu jednající osoby.“[15] Písemnost přitom dle citovaného judikátu může být v elektronické podobě. Pojem písemnosti je tak dle judikatury spojen s pojmem projev vůle, jenž musí zahrnovat všechny podstatné náležitosti, a ty jsou zachyceny v písemném textu listiny. Uvedené pojetí písemnosti podle čerstvější judikatury „lze aplikovat i na formu právního jednání podle ustanovení § 562 odst. 1 o. z.“[16], tj. při aplikaci nového občanského zákoníku.

Že právě pojem písemnost je doktrinárním pojmem vyjadřujícím zachycení obsahu písemné formy právního jednání, souhlasí konzistentně i nauka.[17]

Na pojem *písemnosti v elektronické podobě* můžeme zřejmě bez obav vztáhnout i hlavní obecné požadavky, které klade německá doktrina na pojem *elektronische Dokument* z elektronické formy právního jednání (srov. 5.2.5.2), tj. požadavky

[15] Rozsudek Nejvyššího soudu ze dne 29. 1. 2009, sp. zn. 30 Cdo 1230/2007.
[16] Rozsudek Nejvyššího soudu ze dne 1. 6. 2017, sp. zn. 20 Cdo 1741/2017.
[17] POLČÁK, R. Elektronické právní jednání – změny, problémy a nové možnosti v zákoně č. 89/2012 Sb. *Bulletin advokacie*. 2013, č. 10, s. 34–40, s. 35–36.

dispozice na trvalém nosiče (i v cloudu), dlouhodobého uchovávání, dlouhodobé reprodukce (čitelnosti), úplnosti obsahu právního jednání. Integrita a autenticita jsou zajišťovány jinými prostředky, například kvalifikovaným elektronickým podpisem. Pro jednoznačný komitment uvedeného elektronického podpisu je dobře, aby z obsahu samotné písemnosti v elektronické podobě jasně plynul její vystavitel (původce), jemuž je obsah písemnosti přičítán jako obsah právního jednání.

Autor by pouze dodal, že v závislosti na předpokládané době možnosti právního uplatňování písemnosti v elektronické podobě je třeba velmi pečlivě volit použitý datový formát. Je třeba jej volit tak, aby reprodukce byla vždy jednoznačná a pokud možno i stejná. Není sice třeba absolutně úplná stejnost grafického zobrazení, ale je nutná taková *stejnost*, která vždy povede na stejný výklad obsahu zachyceného právního jednání. Obecně platí, že čím jednodušší datový formát (např. TXT), tím lépe. Je-li třeba složitější formátování, pak je v současnosti nejvhodnější datový formát PDF/A.

5.1.4 Elektronický dokument?

I když autor dochází k podobným výsledkům jako Korbel s Melzerem,[18] totiž že podepsat v elektronické podobě je nakonec možné mnoho druhů písemností, rozchází se nimi v jejich východisku. Oni konstatují obecnou ekvivalenci listiny s elektronickým dokumentem, k čemuž jim slouží definice dokumentu podle § 2 písm. e) zákona č. 499/2004 Sb., o archivnictví a spisové službě. To je však jednak předpis veřejnoprávní, jednak jeho účelem je vybírat a přebírat od původců archiválie. Podle úvodu § 2 zákona jsou pojmy rovněž definovány pro účely daného zákona. Teleologicky účelem definice dokumentu zde pak je to, aby realita byla obejmuta co možná nejšířeji a umožnila archivaci prakticky libovolné informace v libovolné formě, nejen digitální, ale i analogové. Analogovou formu informace nelze přitom elektronicky podepsat podle českého právního řádu a nařízení eIDAS již vůbec, protože není daty. Archivované dokumenty tedy budou zachycovat jakoukoli informaci, a nikoli jen právní jednání. Mnohé obrazy, zvuky, ale i texty jím nikdy nebyly, přesto budou archivovány.

Z těchto důvodů proto není vůbec přesvědčivé, že by při střetu definice *dokumentu* ze zákona o archivnictví s pojmy *písemnost* a *právní jednání*, jak je používá občanský zákoník, měly být náležitosti právního jednání v písemné formě dovozovány

[18] KORBEL, F. – MELZER, F., cit. dílo, 2014, s. 31–36, s. 31.

z právního předpisu o archivnictví, a nikoli výše uvedenou argumentací nauky soukromého práva a samotného občanského zákoníku, jakkoli je složitá.

Adaptační zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce (dále jen „ZSVD“ nebo „adaptační zákon“), vyžaduje ve svých § 5–7 vždy podpis *dokumentu, kterým se právně jedná*. Systematickým i historickým výkladem zákona ZSVD ZSVD(srov. 8.1) lze vyložit, že pojmem se zde míní elektronický dokument, jak je definován v evropském nařízení eIDAS. V rámci výkladu tohoto pojmu zhruba platí, že se jedná o informace vnímatelné lidskými smysly. Přinejmenším pro soukromé právní jednání v písemné formě je ale nutné význam termínu dokument z adaptačního zákona vyložit tak, že se jedná o písemnost v elektronické podobě a náležitosti písemnosti nepřímo určuje občanský zákoník.

Zajímavé je, že i autoři (Kunt, Lechner) z oblasti spisové služby velmi dbají na rozlišení pojmů *písemnost* a *dokument* s tím, že jsou soustředěni právě na dokument[19] (ve smyslu pojmu dle zákona o archivnictví), zatímco „používání pojmu písemnost v oblasti spisové služby není vhodné z více důvodů“,[20] přičemž hlavním důvodem jim je, že některé dokumenty „ani nelze písmem zaznamenat, a přesto do správy spisové služby jednoznačně patří, např. audiovizuální záznam v soudním spisu.“[21] Zdůrazňují však, že v současnosti je již nutné pojem písemnost chápat nezávisle na nosiči, který může být tradiční (analogový, pojem zákona o archivnictví) nebo elektronický (digitální, pojem zákona o archivnictví).[22]

K terminologickému zmatení může dojít, pokud se přeloží pojem německého práva *„elektronische Dokument"* z § 126a BGB. Německý zákonodárce se rozhodl, že pojem listiny *(Urkunde)* ponechá zřejmě pouze pro papírové listiny, u nichž platí, že dochází ke vtělení textu vyjádření i vlastnoručního podpisu přímo na (do) nosič listiny, který zajišťuje nejen soudržnost, ale i částečnou ochranu před dodatečným vpisováním či přepisováním, zatímco pro elektronické písemnosti toto skutečností běžně není. Ani výtiskem se z elektronické písemnosti nestane listina (Urkunde).[23] Pro pro právní jednání v elektronické formě *(elektronische Form)* německý zákonodárce zavedl uvedený pojem *elektronický dokument* (srov. 5.2.5.2). Jedná se zde ale o překlad pojmu

[19] KUNT, M. – LECHNER, T. *Spisová služba*. 2., aktualizované vydání. Praha: Leges, 2017, s. 73–75.
[20] KUNT, M. – LECHNER, T., cit. dílo, s. 76.
[21] KUNT, M. – LECHNER, T., cit. dílo, s. 77.
[22] KUNT, M. – LECHNER, T., cit. dílo, s. 78.
[23] SPINDLER, G. *BGB § 126a Elektronische Form*. Rn. 15. In: SPINDLER, G. – SCHUSTER, F. *Recht der elektronischen Medien.* 3. Auflage, C. H. Beck, 2015.

německého platného práva, jemuž by v českém právním řádu zřejmě nejvíce odpovídal pojem *písemnost v elektronické podobě*.

Jiné zmatení nastává v oblasti nakládání s dokumenty v širokém významu (tj. zhruba v tom, jaký se v ČR používá u spisové služby a v archivnictví) v tom smyslu, že common law nebo technické normy či specifikace z anglosaské oblasti nazývají takové jednotky informace jako záznam *(record)*. Existují dokonce případy křížového prohození překladů v češtině, kdy anglický pojem *record* je překládán jako dokument a současně anglický pojem *document* jako záznam.[24] Při čtení jakékoli zahraniční literatury, nebo i literatury českých autorů psané v cizím jazyku, je tedy třeba si ujasnit, v jakém smyslu autor slova a pojmy systematicky používá, a až podle toho text vykládat a nepřekládat jej pouze dle běžného jazykového překladu.

Konečně je třeba uvést, že slovo *dokument* má v platném právu ČR značný počet výskytů,[25] ovšem vesměs mimo soukromé právo a soukromé právní jednání, o kterém se v této kapitole pojednává. Význam je zde třeba odvozovat z daného právního předpisu nebo odvětví práva. Některé výskyty jsou i pro praxi soukromého práva významné, například autorizovaná konverze dokumentů podle zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů.

5.1.5 Výklady § 561 a § 562 obč. zák.

Systematický výklad obou paragrafů o tom, jak právní jednání učiněné elektronickými prostředky splňuje požadavky platné písemné formy právního jednání, není bohužel jednoznačný. Uveďme různě zastávané výklady.

První výklad je vzácný, uváděl ho snad pouze Sokol[26] vůči předobrazu obou paragrafů občanského zákoníku v dřívějším zákonu č. 40/1964 Sb., občanském zákoníku, tedy vůči § 40 odst. 3 věta třetí a § 40 odst. 3 zákona č. 40/1964 Sb., občanského zákoníku. Podle něj byla obě ustanovení nadbytečná a matoucí. Požadavek náležitosti písemné formy lze dovodit přímo: „písemná forma je zachována vždy, kdy se projev vůle či jakýkoliv jiný text objevuje tak, že je zaznamenán písmem, nezávisle na tom, zda-li písmo samo je viditelné díky tomu, že je přeneseno inkoustem či jiným barvivem na papír nebo obdobný podklad, vytištěno tepelně na speciální faxový papír, případně promítnuto na obrazovku počítače.“ Stejně podivné by bylo, kdyby existovala

[24] KUNT, M. – LECHNER, T., cit. dílo, s. 74.
[25] LECHNER, T. *Elektronické dokumenty v právní praxi*. Praha: Leges, 2013, s. 18–62.
[26] SOKOL, T., cit. dílo, s. 42–46.

zvláštní právní úprava pro případy, kdy by písemná forma byla zachycena na „plechu, umělohmotné fólii nebo březové kůře“. Sokol se výslovně nevypořádává s požadavkem přítomnosti podpisu pro platnost, který byl uveden i v § 40 odst. 3 zákona č. 40/1964 Sb., občanského zákoníku. Z hlediska praxe je pro něj podstatné, aby obsah byl autentický a aby autentičnost byla prokazatelná při důkazním použití. Pokud vyžaduje podpis, pak je pro něj asi to něco, co tuto autenticitu zajišťuje.

Druhý výklad je asi hlavní zastávaný. Platná písemná forma je splněna, je-li připojen elektronický podpis, na nějž odkazuje blanketní norma ve třetí větě § 561 odst. 1 obč. zák. Tento výklad zastávají i komentátoři Melzer a Korbel[27] i komentář Tichého.[28] Konsekventně § 562 odst. 1 obč. zák. je *lex specialis*, jímž lze elektronickými prostředky rovněž splnit písemnou formu, aniž by nutně byl zahrnut elektronický podpis; ustanovení je zřejmě přítomno zejména s ohledem na historické technologie elektronického přenosu právního jednání, jakým byl třeba dálnopis.

Donedávna byl v § 561 odst. 1 obč. zák. odkazovaným zákonem zákon č. 227/2000 Sb., o elektronickém podpisu (dále jen „ZEP“), nově jím je adaptační zákon[29] odkazující dále na nařízení eIDAS. Zatímco dosud mohly být a byly pochyby o tom, který elektronický podpis ze ZEP je „vhodný“, adaptační zákon gramatickým výkladem vcelku jednoznačně připouští elektronický podpis prostý z eIDAS.

Tento výklad z výše uvedeného výkladu Sokola přebírá to, že písemnost v elektronické podobě je „samozřejmým“ splněním požadavků písemné formy a je nutné mít upravenu pouze přítomnost elektronické podoby podpisu. Důvodem by kromě právní jistoty mohlo být např. i to, že jak udává třeba Čermák ml.[30] „pouhé stisknutí tlačítka [je] oproti klasickému rukopisnému podpisu ... daleko jednodušší“, tedy je i slabším osvědčením vůle jako náležitosti právního jednání. Připuštění elektronického podpisu v občanském zákoníku tedy znamená, že i on může dostačovat k vážnosti vůle.

Třetí výklad zastává Lavický.[31] Dle něj „je nutné konstatovat, že elektronický podpis datové zprávy nesmí u právního jednání chybět“ a že „není … možné považovat [§ 562 odst. 1] za (v tomto směru) *lex specialis* oproti § 561 ObčZ.“ Podrobnější výklad jazykový a subsumpcí chybí, diskurs je však veden na pozadí otázky, zda vůči § 562

[27] MELZER, F. – TÉGL, P. a kolektiv, cit. dílo, s. 637–638.
[28] ŠVESTKA, J. – DVOŘÁK, J. – FIALA, J. a kol., cit. dílo, s. 387–1388.
[29] Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.
[30] ČERMÁK, K. ml., cit. dílo, s. 71.
[31] LAVICKÝ, P. a kol. *Občanský zákoník I. Obecná část (§ 1–654). Komentář.* Praha: C. H. Beck, 2014.

odst. 1 obč. zák. vyhovuje e-mailová zpráva. Komentář dovozuje, že nestačí „jakákoli možnost určení jednající osoby (např. jen podle e-mailové adresy)“, ale že toto určení musí být elektronickým podpisem, právě proto musí být přítomen, a to dokonce nejméně zaručený elektronický podpis. Argumentem k tomu mu je i NS v rozhodnutí 33 Cdo 3210/2007, které pro písemnou formu považuje za nutný zaručený elektronický podpis. Tento výklad vychází z toho, že elektronický podpis představuje vyšší míru jistoty o jednající osobě než § 562 odst. 1 obč. zák., byť ne každý elektronický podpis je ještě dostačující.

Čtvrtý výklad zde nabízí autor jako alternativní, ke zvážení. Dle něj požadavky § 561 odst. 1 a § 562 odst. 1 obč. zák. platí současně a nemají vůči sobě vztah speciality. V § 562 odst. 1 obč. zák. pak můžeme nalézt dovolení písemnosti v elektronické podobě a v § 561 odst. 1 obč. zák. příkaz podpisu v elektronické podobě, obojí jako dvě nutné náležitosti pro platné právní jednání v písemné podobě.

Pak by náležitosti písemnosti v elektronické podobě, tedy pro **zachování písemné formy**, byly splněny jen při takovém jednání, které podle § 562 odst. 1 obč. zák. je učiněno elektronickými *„prostředky umožňujícími zachycení jeho obsahu a určení jednající osoby“*. Platnost písemné formy však není v § 562 obč. zák. stanovena. První věta § 561 odst. 1 obč. zák. stanoví, že k **platnosti** právního jednání **v písemné formě** se vyžaduje podpis jednajícího. Podpis tedy musí být přítomen. Další věty § 561 odst. 1 obč. zák. pak upřesňují nezřejmé případy, jak se takový podpis provádí, ve třetí větě je uveden podpis elektronický.

Tento výklad je obdobný výkladu Lavického až na to, že § 562 odst. 1 obč. zák. představuje konjunkční filtr minimálních požadavků na písemnou formu v elektronické podobě. Poměr mezi požadavky obou paragrafů tedy může být i právě opačný. Obrat *určení jednající osoby* lze vykládat nejen jako obsažené tvrzení o totožnosti, ale i jako autentizaci totožnosti jednající osoby v jisté míře spolehlivosti. Běžně by se dosahovala elektronickým podpisem. Následkem tohoto výkladu by byl závěr, že i když adaptační zákon připouští elektronický podpis prostý z eIDAS dle ustanovení § 561 odst. 1 obč. zák., tento nevyhoví požadavku na určení jednající osoby v § 562 odst. 1 obč. zák., a je proto nutné použít elektronický podpis silnější, tedy takový, který určení jednající osoby zajistí.

Pro prosazení čtvrtého výkladu je dále třeba potřít zejména hlavní výklad druhý. Pro podporu čtvrtého výkladu za prvé uveďme, že druhým výkladem předpokládané splnění požadavků písemné formy nějakou písemností v elektronické podobě „samozřejmé“ vůbec není! Zatímco písmena v písemnosti na listině jsou samotným papírovým médiem pevně spojena do slov a vět, písemnost v elektronické podobě zobrazenou na displeji lze připodobnit k situaci, kdy někdo vezme písmenka ze hry Scrabble a vysází jimi na stůl písemné sdělení. Za další sekundu elektronické prostředky písmenka odnesou pod stůl a je mimo přímou kontrolu, zda nejsou přerovnána, ubrána či jiná přidána. Požadavek § 562 odst. 1 obč. zák. na *zachycení obsahu* tedy stanoví, že použité elektronické prostředky musí nějak zajistit, že k žádným změnám obsahu nedojde, a je i proto vždy potřebný.

Za druhé srovnávacím výkladem uveďme, že jak BGB, tak UETA považují za nutné upravit přípustnost jak písemnosti v elektronické podobě, tak elektronického podpisu zvlášť. V § 126a BGB se hovoří jak o elektronickém dokumentu, tak o kvalifikovaném elektronickém podpisu. V UETA se pak v § 7 (c) hovoří o elektronickém záznamu, který nahrazuje písemnost (writing) a § 7 (d) o elektronickém podpisu, který nahrazuje podpis. Ani v ČR by se tedy samozřejmost písemnosti v elektronické podobě neměla dovozovat jen z § 559 obč. zák.

Za třetí, i když zastánci druhého výkladu mají k dispozici dobré argumenty historického výkladu, právní stav se změnil jak přijetím občanského zákoníku, tak nyní eIDAS a adaptačního zákona a zrušením ZEP. Třetí věta § 40 odst. 3 zákona č. 40/1964 Sb., občanského zákoníku, zněla: *„Je-li právní úkon učiněn elektronickými prostředky, může být podepsán elektronicky podle zvláštních předpisů.“* S jistou mírou výkladové benevolence lze v normě spatřovat připuštění, ve smyslu dovolení, provedení právního úkonu elektronickými prostředky, tak i dovolení („může být“) provést elektronický podpis a tím navíc splnit požadavky na platnou písemnou formu. Oproti tomu třetí věta § 561 odst. 1 obč. zák. zní: *„Jiný právní předpis stanoví, jak lze při právním jednání učiněném elektronickými prostředky písemnost elektronicky podepsat.“* Z normy se ztratilo zejména dovolení právního jednání učiněného elektronickými prostředky pro písemnost za účelem dosažení písemné formy, které je nově již vysloveně nutné hledat v § 562 odst. 1 obč. zák. I upravení podpisu je nově nejasné. Protože ve druhé větě, o použití mechanických prostředků, dovolení „může být“ zůstalo, je jisté, že zvláštností nové formulace („jak lze“) hodlal zákonodárce také něco vyjádřit. Podpis je stále nutný,

a je-li právní jednání učiněné elektronickými prostředky dovolené, pak jiný právní přepis stanoví, jak lze písemnost [v elektronické podobě] podepsat. První možností je delegace dovolení elektronického podpisu do jiného právního předpisu. Delegací se však ztrácí i systematická vazba na obč. zák. a jasnost, která existovala v § 40 odst. 3 zákona č. 40/1964 Sb., občanského zákoníku, ohledně toho, že takové jednání elektronickými prostředky splňuje písemnou formu. Tuto jasnost je třeba něčím nahradit, k čemuž se nabízí § 562 odst. 1 obč. zák. Druhou možností je, že „jak lze“ má význam pouze výčtový. Jiný právní předpis jen určuje, jaké jsou možnosti písemnost podepsat, dovolení si ponechává občanský zákoník pro sebe, a to právě v § 562 odst. 1.

Zrušením ZEP se pak ztrácí základní autentizační vlastnosti prostého elektronického podpisu, což zpětně ovlivňuje i systematicky myslitelné výklady občanského zákoníku, jaké byly myslitelné za jeho účinnosti.

Jiné výklady nejsou vyloučeny. Lze kupř. argumentovat, že i když adaptační zákon ZSVD dovoluje prostý elektronický podpis pro jiná jednání než adaptačním zákonem vyloučená, v případě soukromého práva je pro splnění písemné formy právního jednání vyloučen. Jinou možností je připustit, že § 562 odst. 1 obč. zák. sice je *lex specialis* vůči § 561 odst. 1 obč. zák., ale současně obsahuje i teleologickou definici právního jednání v písemné formě, kterou prostý elektronický podpis nenaplní. Tyto výklady jdou ale proti jazykovému výkladu a mají menší právní jistotou. Zejména při účelových snahách stran ve sporu lze asi nalézt i výklady další. Základní způsoby uvažování však zde zmíněny již jsou.

V praxi bude rozhodující, k jakému výkladu se přikloní soudy a jejich judikatura. Autor se domnívá, že při snaze o vyhovění písemné formě právního jednání by se strany měly v rámci praktických možností spíše snažit o použití takového druhu techniky elektronického podpisu, která nějakou autentizační vlastnost má. Kromě absentující důkazní vlastnosti totiž není vyloučeno to, že soudy mohou vzít v potaz i argumentaci některého výše uvedeného výkladu.

V současné judikatuře se ještě soudní hodnocení vyšších instancí po přijetí adaptačního zákona nestihlo projevit. Předchozí judikatura vyžadovala pro splnění podmínky právního jednání v písemné formě existenci písemnosti a podpisu. Písemnost mohla být v elektronické podobě, ale pro podpis nedostačovala forma odpovídající jen prostému elektronickému podpisu z eIDAS. Tak byla opakovaně zamítána podání, která

se dožadovala uznat za právní jednání v písemné formě zprávu internetové elektronické pošty *(e-mail)*,[32] který nebyl nijak zvlášť elektronicky podepsán. Pokud soudy nově uplatní druhý výše uvedený výklad, znamenalo by to i změnu judikatury, neboť nově by běžná zpráva internetové elektronické pošty, ukončená na svém konci zápisem jen jména a příjmení, byla považována za podepsanou písemnost, a tedy i za právní jednání v písemné formě. To by zasáhlo právní jistotu nejen bezprostředně zúčastněných osob, tedy podepisující osoby a adresáta právního jednání, ale mohou tím být zasaženy i osoby třetí, vůči kterým má být dané právní jednání dokladováno v rámci běžného právního styku při realizaci práva, nikoli až při soudním řízení. V praxi se přitom některé sporyChyba: zdroj odkazu nenalezen vedly například o to, zda prostou elektronickou poštou lze platně provést postoupení pohledávky, někdy i na značné částky, což nebylo shledáváno možným a nově by bylo. Takto podepsané listiny přitom vůči třetím stranám bez dalšího nemají žádný prvek autentizace, ochrany před zfalšováním. Níže k této tématice viz též části 6.4 a 9.4.

5.1.5.1 Podpisy více osob na stejné listině

K výše uvedenému diskursu náleží ještě otázka, zda a jak lze splnit požadavek § 561 odst. 2 obč. zák.: *„Jedná-li více osob, vyžadují se jejich projevy na téže listině při právním jednání, kterým se zřizuje nebo převádí věcné právo k nemovité věci, anebo kterým se takové právo mění nebo ruší."* Polčák zde byl názoru, že již výklad pojmu listina se liší v závislosti na tom, zda se jedná o veřejnou nebo soukromou listinu. Zatímco u veřejné listiny považuje za přípustnou i její elektronickou formu, u soukromé listiny „má pojem listiny stále svůj obecný význam papírové písemnosti",[33] přičemž důvodem mu je právě použití pojmu listiny v případu § 561 odst. 2 obč. zák., kdy nepovažuje elektronickou podobu za možnou.

Autor je názoru, že taková elektronická podoba listiny je obecně přípustná, neboť právě to by mělo být smyslem § 3026 odst. 1 obč. zák. Právě toto ustanovení však obsahuje i výjimku „povahy písemnosti", která vylučuje dovolení nebrat zřetel na její (elektronickou) podobu. Nepoužitelnost elektronické podoby listiny v § 561 odst. 2 obč. zák. autorovi prvotně plyne spíše ze závažnosti právního jednání a z potřeby dlouhodobého uchovávání listiny pro důkazní účely, sekundárně ovšem též z podmínky více podpisů na stejné listině.

[32] Například rozsudek Nejvyššího soudu ze dne 10. 4. 2014, sp. zn. 23 Cdo 1593/2012.
[33] POLČÁK, R. Elektronické právní..., cit. dílo, s. 36.

Z hlediska ryze technického pohledu by se podobného účinku ceremonie, jako je vytvoření podpisů dvou osob na téže (papírové) listině, dalo dosáhnout tím, že by u písemnosti (listiny) v elektronické podobě byly připojeny dvě kontrasignační posloupnosti v opačném pořadí, s využitím například kvalifikovaných elektronických podpisů. Bylo by tak zajištěno, že každá ze stran by si současně byla plně vědoma, že listinu podepsala i strana druhá. Současně však nezvyklost či umělost (čtyři podpisy namísto dvou) tohoto scénáře hovoří proti tomu, aby se bez explicitnějšího zákonného dovolení skutečně používal. V případě podpisu tří osob (šesti kontrasignačních posloupností, osmnáct podpisů namísto tří) a více k téže listině by počet nutných různých kontrasignačních posloupností vzrůstal neúnosně a proces je bez dalšího nezvladatelný. Zvláštní právní úprava zde již je skutečně potřebná.

5.1.5.2 Elektronické podpisy podle katastrálního zákona a vyhlášky

Nový zák. č. 256/2013 Sb., katastrální zákon, účinný od 1. ledna 2014, zavádí pojem *„listiny"* v § 7 odst. 1 jako legislativní zkratku pro *„písemnost v listinné podobě nebo v elektronické podobě"*. Dle § 7 odst. 1 katastrálního zákona musí být listina v elektronické podobě opatřena kvalifikovaným elektronickým časovým razítkem a k podepsání musí být použit uznávaný elektronický podpis. Dle § 7 odst. 2 katastrálního zákona musí být podpisy na soukromé listině buď úředně ověřeny, anebo být prokázána jejich pravost. Prováděcí vyhláška č. 357/2013 Sb., katastrální vyhláška, pak v § 65 obsahuje ustanovení o formátu aj. technických náležitostech *„písemnosti v elektronické podobě určené k zápisu práv do katastru"* a v § 64 podmínky ověření pravosti elektronického podpisu, přičemž k prokázání pravosti dostačuje kvalifikovaný certifikát (pro elektronický podpis), na němž je založen použitý elektronický podpis, a tento *„obsahuje jméno, popřípadě jména, a příjmení podepisující osoby a údaj, který umožňuje jednoznačnou identifikaci podepisující osoby"*. Jednoznačná identifikace obsahuje v poznámce pod čarou odkaz na § 63 odst. 3 zákona č. 117/1995 Sb., o státní sociální podpoře, dle nějž Ministersvo práce a sociálních věcí poskytuje *„orgánům zeměměřickým a katastrálním údaje nezbytné pro ověření totožnosti osoby, která činí podání v elektronické podobě"*. Kvalifikovaný certifikát tedy musí obsahovat tzv. identifikátor MPSV. Podle § 64 odst. 1 písm. b) katastrální vyhlášky č. 357/2013 Sb. může pravost elektronického podpisu podepsaná osoba též uznat před katastrálním úřadem, *„že obsah písemnosti v elektronické podobě je projevem její vůle, a potvrdila,*

že je držitelem kvalifikovaného certifikátu, na kterém je založen uznávaný elektronický podpis".

Katastrální zákon tak připouští možnost existence soukromé listiny v elektronické podobě a dokonce stanoví slabší podmínku pro ověření pravosti elektronického podpisu než v případě vlastnoručního podpisu, protože není třeba úřední ověření podpisu. Ani katastrální zákon ovšem neupravuje podmínku přítomnosti více podpisů na stejné listině.

5.2 Vyjádření vůle a právní transakce (německé právo)

Německé právo pro právní jednání s pomocí elektronických prostředků vyžaduje provedení vyjádření vůle nebo právní transakce, jak je o nich pojednáno již výše (srov. 3.2). Pro jejich platnost se vyžaduje přítomnost objektivních a subjektivních znaků skutkové podstaty.

5.2.1 Objektivní znaky skutkové podstaty

V rámci objektivního znaku skutkové podstaty *(objektiver Tatbestand)* právo nevyžaduje partikulární podobu provedení jednání, ale vyhovění obecným požadavkům. Požadavek objektivního znaku skutkové podstaty je splněn, když „podle vnějškově rozpoznatelného smyslu projevu, anebo zvláštního chování s vyjadřovací hodnotou, tím má být vytvořena právní transakce, která vyvolává ve vyjádření určené záměrné vytvoření přístupných právní následků".[34]

Německá teorie z hlediska objektivních znaků rozlišuje dva hlavní druhy možnosti využití elektronických prostředků.

5.2.1.1 Elektronicky přenášená vyjádření vůle

První kategorií jsou „elektronicky přenášená vyjádření vůle" *(elektronisch übermittelte Willenserklärungen)*. Tato vyjádření vůle se od jiných liší pouze tím, že způsob přenosu *(Übermittlungswege)* spočívá v elektronickém přenosu. Do této kategorie spadá jak objednání zboží kliknutím na objednací tlačítko v elektronickém obchodu on-line, tak poptávka po poradenských službách zaslaná elektronickou poštou. K uzavření smlouvy dochází přes vyjádření vůle, která jsou pouze elektronicky přenášena.[35]

[34] HÄRTING, N., cit. dílo, s. 102.
[35] HÄRTING, N., cit. dílo, s. 102.

V rámci této kategorie se někdy přeci jen rozlišuje první způsob on-line projevených projevů jako tzv. *digitálních* nebo *elektronických* vyjádření vůle, zatímco v druhém případě se jedná o *digitálně přenesená* (v úzkém smyslu) vyjádření vůle.

Pro obecné právní vztahy nemá německé právo žádné zvláštní požadavky na zjevování obsahu vyjádření vůle. Pouze v případě úplatných smluv se spotřebiteli jsou dány určité požadavky na obsah objednacího tlačítka, na kterém by měl být nápis „zahlungspflichtig bestellen" *(úplatně objednat)*, nebo stejného významu. Tato povinnost v § 312g odst. 4 BGB bývá nazývána jako tzv. **„Button-Lösung"**.[36] Požadavek svým původem pochází z legislativních aktů EU na ochranu spotřebitele, a měl by tedy platit obdobně i pro elektronické obchody v ČR a v jiných členských státech EU. Účelem zde je upozornit spotřebitele, že smlouva, kterou stiskem tlačítka uzavírá, na jeho straně vyžaduje povinnost zaplacení. Tím se situace odlišuje od jiných uživatelských smluv ke službám či plněním, které jsou na internetu poskytovány zdarma, jejichž použití ale též vyžaduje odsouhlasení smluvních podmínek. V souvislosti se smlouvami uzavíranými se spotřebiteli pak právní předpisy na ochranu spotřebitele vyžadují při průběhu konkraktace, resp. ještě před jejím započetím, poskytnout spotřebiteli četné další informace, které zde nejsou diskutovány. Nepřítomnost může být spojena se sankcemi, například neupozornění na právo na odstoupení od smlouvy ve lhůtě 14 dnů má za následek prodloužení tohoto práva na dobu 1 roku.

Současně však všechny tyto požadavky spotřebitelských smluv uzavíraných na dálku v sobě neobsahují žádné zvláštní požadavky ohledně toho, jaké náležitosti má mít akt, jímž dochází k provedení vyjádření vůle. Platí pouze již výše uvedené, že se musí jednat o „vnějškově rozpoznatelný smysl projevu, anebo zvláštního chování s vyjadřovací hodnotou", které má za cíl vyvolat právní následky ve vyjádření obsažené. Případné omyly se řeší v rámci subjektivních znaků v rámci zkoumání vědomí k vyjádření *(Erklärungsbewußtsein)*, srov. níže 5.2.2.

Požadavky pro smlouvy se spotřebiteli mají charakter jen povinného přídavného doplnění informací, která někdy též současně mají i právně závaznou povahu (např. právo na odstoupení od smlouvy). Pro uzavírání jiných smluv jsou ale právně irelevantní, byť mohou představovat dobrou praxi.

[36] HÄRTING, N., cit. dílo, s. 117.

5.2.1.2 Elektronicky vytvořená vyjádření vůle (automatizovaně)

Druhou kategorií jsou „elektronicky vytvořená vyjádření vůle" *(elektronisch erzeugte Willenserklärungen)*. Při tvorbě těchto vyjádření vůle není osoba bezprostředně přítomna, vznikají na základě činnosti naprogramovaného softwaru. Ten řídí i obsah a čas vydání vyjádření vůle. Teorie vychází z toho, že na konci řetězce programování a konfigurace softwaru se vždy nachází osoba, která je původcem tohoto elektronického vyjádření vůle. Z toho teorie dovozuje, že i **automatizovaná** vyjádření vůle splňují požadavky na objektivní znaky skutkové podstaty vyjádření vůle.[37] Obdobně jako v common law i německá nauka zde někdy hovoří „uzavírání smluv přes **autonomní elektronické agenty**"[38] *(Vertragsschluss über autonome elektronische Agenten)*.

5.2.2 Subjektivní znaky skutkové podstaty

Jak je uvedeno výše (3.3.3 a 3.2.1), německá nauka rozeznává tři stupňující se úrovně přítomnosti vůle při právním jednání: vůle k jednání *(der Handlungswille)*, vůle k vyjádření *(der Erklärungswille)*, resp. vědomí k vyjádření *(die Erklärungsbewußtsein)* a vůle k transakci *(der Geschäftswille)*. Všechny tři společně tvoří subjektivní znaky skutkové podstaty, což platí i pro všechny druhy elektronického vyjádření vůle.

V rámci běžné teorie při chybějící *vůli k jednání (Handlungswille)*, například při hypnóze či bezvědomí, není vůbec žádného vyjádření vůle. Počítačová praxe situaci zesložiťuje, neboť existují případy, kdy uživatel u počítače usne a nevědomky na klávesnici či myší odešle předvyplněný formulář, který příjemce považuje za bezvadné vyjádření vůle. Německá teorie přesto převážně má za to, že v těchto případech se o vyjádření vůle nejedná. Oproti tomu namítá teorie rozumného hodnocení oprávněných zájmů *(interessengerechter Wertung)*, že příjemce nemá běžně žádnou možnost rozpoznat, že se nejedná o platné vyjádření vůle. Pouze tehdy, pokud by příjemce měl *podložené důvody* pochybovat o chybějící vůli k jednání, např. při nesmyslně vyplněných formulářích nebo množstvích apod., je na něm, aby přítomnost vůle k jednání ověřil.

Tento přístup vychází z nauky objektivního horizontu příjemce.[39] Zde je tedy patrné, jaký zásah do jinak obecné teorie právního jednání přináší jeho prostředkování

[37] HÄRTING, N., cit. dílo, s. 103.
[38] HOEREN, T. *Internetrecht.* Skriptum. Münster: April 2017, s. 319. Zvýraznil autor.
[39] HÄRTING, N., cit. dílo, s. 105.

elektronickými prostředky, které odstiňují osoby jednání. Praxe běžných elektronických obchodů se však těmito případy přesto nezdá být narušena, neboť spící osoba zpravidla není schopna smysluplně vyplnit několik po sobě jdoucích formulářů, včetně čísla své platební karty. Rozšiřující se praxe dotykových zařízení tuto situaci spíše jen dále zhorší, stejně jako snahy o co nejsnazší provedení plateb.

V rámci vad *vědomí k vyjádření (Erklärungsbewußtsein)* z důvodu omylu obecná teorie kolísá, od nicotnosti pro nedostatek přítomnosti vůle až jen po rozporovatelnost. V případě elektronicky prostředkovaného vyjádření vůle příkladem může být, že si jednající on-line chce objednat informační materiál o produktu, ale omylem objedná produkt samotný. Podle judikatury BGH se tyto situace řeší posouzením toho, zda i když vyjadřujícímu chybí vědomí vůle k vyjádření, pokud u příjemce *nedbalostně* vyvolá důvěru v určitý vyjádřený obsah, bude se jednat o vyjádření vůle. Hraničním případem zde je, pokud samotné vyjadřujícím použité internetové stránky[40] svou podobou vyvolávají možnost omylu. Pak se již nejedná o nedbalost vyjadřující osoby. Judikatura BGH zde sahá již do předinternetové éry (1984) a je potvrzena i rozsudkem OLG (2006),[41] dle kterého žalovaný své zmýlení mohl „při použití v provozu potřebné pečlivosti" rozpoznat a vyhnout se mu.[42]

Obdobný závěr poskytuje doktrína objektivního či normativního horizontu příjemce. Ta však nehodnotí nedbalost, ale to, zda si příjemce může být objektivně vědom toho, že vyjádření vůle je postižené omylem. V případě neurčitého uživatelského rozhraní pak nemůže být v dobré víře o tom, že došlé vyjádření není případně postižené omylem.[43]

Při vadě *vůle k transakci (Geschäftswille)* je i v případě elektronického právního jednání korekcí pouze rozporovatelnost podle § 119 an. BGB.[44]

5.2.2.1 Objektivní hodnocení subjektivních znaků skutkové podstaty

Härting výše uvedený diskurs o složkách vůle shrnuje tak, že i když se jedná o vnitřní stavy subjektů, není v běžné praxi, tj. například u takových internetových obchodů, které svým provedením nezavdávají důvody k omylu, možné tyto vnitřní

[40] Tyto internetové stránky může typicky vytvořit samotný příjemce vyjádření vůle. Stejné závěry však platí, pokud využívá internetových stránek jiných původců.
[41] OLG Köln. Urteil vom 8. Dezember 2006. Az. 19 U 109/06. Dostupné z: <https://openjur.de/u/120462.html>.
[42] „Anwendung der im Verkehr erforderlichen Sorgfalt" in OLG Köln, Az. 19 U 109/06, bod 27.
[43] HÄRTING, N., cit. dílo, s. 104–105.
[44] HÄRTING, N., cit. dílo, s. 103–104.

stavy subjektů hodnotit. Zastává proto názor, že přítomnost vyjádření vůle je třeba posuzovat pouze objektivně. Pokud příjemce obdrží vyjádření, které má všechny náležitosti vyjádření vůle, je dle něj oprávněn jej považovat za platné vyjádření vůle.

Pokud přesto vyjádření vůle trpí vadou vůle kteréhokoli druhu, tj. vůle k jednání *(der Handlungswille)*, vědomí k vyjádření *(Erklärungsbewußtsein)* nebo vůle k transakci (*Geschäftswille*), je dle něj přiměřenou ochranou právo rozporovatelnosti podle § 119 an. BGB, které poskytuje přiměřené vyvážení mezi ochranou zájmů odesilatele i příjemce jednání.[45]

5.2.3 Poskytnutí (Abgabe) a přístup (Zugang) k vyjádření vůle

Vyjádření vůle nemá pouze charakter výsledku jednání, ale i procesní aspekty. Vyjadřující osoba jej musí vždy poskytnout *(Abgabe)*, čímž se rozumí vyjevení, vydání, vnější vyjádření. Pro perfekci vyjádření vůle, *„které je poskytnuto vůči jinému v jeho nepřítomnosti, bude účinné v okamžiku, kdy mu dojde"* (§ 130 odst. 1 BGB). Taková vyjádření vůle jsou označovaná, že vyžadují dojití *(empfangsbedürftige)* příjemcem. Citované dojití nastává až okamžikem přístupu *(Zugang)* příjemce k vyjádření vůle, do té doby je neúčinné.

V právním styku s pomocí elektronických prostředků bývají běžná vyjádření vůle vyžadující dojití. Je jimi nabídka (oferta) i přijetí (akceptace). K uzavření smlouvy tedy dochází až tehdy, když dojde k dojití přijetí oferentovi. Na druhu elektronického prostředku pak bude záviset, zda je komunikace s jeho pomocí považována za jednání mezi přítomnými, nebo mezi nepřítomnými. Například on-line komunikace některých systémů EDI je považována za komunikaci mezi přítomnými.[46] Oproti tomu komunikace prostřednictvím internetových elektronických obchodů i pomocí e-mailů je považována za komunikaci mezi nepřítomnými, avšak s rozdílným uplatňováním pravidel dojití a přístupu.

V případě elektronických obchodů bývá běžně obsah stránek považován pouze za *„invitatio ad offerendum"*,[47] tedy za výzvu k podávání nabídek, obdobně jako tomu je třeba u klasických papírových katalogů zasilatelských služeb. Uživatel elektronického obchodu pak svým postupem teprve vytváří nabídku *(Angebot)*. Po jejím dotvoření je odeslána provozovateli elektronického obchodu. Provozovatel typicky reaguje ihned

[45] HÄRTING, N., cit. dílo, s. 105.
[46] HOEREN, T., cit. dílo, s. 321.
[47] HOEREN, T., cit. dílo, s. 319.

tzv. potvrzovacím e-mailem *(Bestätigungsmail)*, který stvrzuje podle § 312i odst. 1 bodu 3 BGB, že provozovatel nabídku obdržel a bude dále zpracována. Doba na přijetí provozovatelem obchodu platí dle § 147 odst. 2 BGB, tj. *„do okamžiku, ve kterém navrhovatel příchod odpovědi může za běžných okolností očekávat"*. Do takové doby by provozovatel měl provést vyjádření vůle spočívající v přijetí *(Annahmeerklärung)* a odeslání přijetí uživateli elektronického obchodu. Po dojití přijetí dochází k uzavření smlouvy.[48]

Z výše uvedeného existují výjimky. Pokud jsou u produktů na internetových stránkách pobídky jako *„Sofort kaufen"* (ihned kupte), je již taková prezentace považována ze strany provozovatele elektronického obchodu za závaznou nabídku. Rovněž některé německé soudy mohou setřít rozdíl mezi potvrzením a přijetím. Text potvrzení *„Mnoho díků za Vaší nabídku, kterou vyřídíme tak rychle, jak je to možné"* mohou považovat za přijetí.[49] Pro zamezení nejasností se doporučuje do potvrzení zřetelně uvést *„Keine Auftragsbestätigung"*, tj. že se nejedná o potvrzení objednávky.[50]

V případě internetové elektronické pošty dojití, resp. přístup *(Zugang)* nastává okamžikem, kdy se vyjádření ocitne v oblasti moci příjemce *(Machtbereich des Empfängers)*. V případě sporu leží důkazní břemeno o dojití na odesilateli. Dosud je jako důkaz *prima facie* užíváno, pokud odesilatel neobdrží žádný „Bounce-Mail" (zpráva o nedoručitelnosti). Nejjistější však je, pokud příjemce na internetovou poštu odpoví a tím potvrdí i dojití.[51] Rozhodovací praxe v Německu přijala, že v případě odesílání elektronické pošty vůči podnikatelům může odesilatel počítat s přístupem ihned, pokud je odeslání provedeno během pracovní doby. Pokud je provedeno mimo pracovní dobu, dochází k němu na počátku pracovní doby nejbližšího pracovního dne. V případě spotřebitele se předpokládá, že k přístupu dochází nejpozději o den později.[52] V případě nepravidelností je třeba na ně brát zvláštní ohled.[53]

Zveřejňování adresy elektronické pošty, a to i například jen vytištěním na vizitce, může dokonce založit určitou odpovědnost za to, že je daná poštovní adresa pravidelně vybírána či kontrolována. V případě, že pak například advokát nereaguje na

[48] HOEREN, T., cit. dílo, s. 319–320.
[49] HOEREN, T., cit. dílo, s. 320.
[50] HOEREN, T., cit. dílo, s. 320.
[51] HÄRTING, N., cit. dílo, s. 113.
[52] HÄRTING, N., cit. dílo, s. 109.
[53] HÄRTING, N., cit. dílo, s. 111.

žádost o právní službu od svého mandanta, může mandantovi vzniknout i nárok na náhradu škody, která mu z nekonání advokáta vznikne.[54]

5.2.4 Jiné náležitosti elektronického právního jednání

Výše podaný výklad opomíjí, že pro smlouvy uzavírané prostřednictvím internetu mohou platit další přídavné požadavky. Pro úplnost jen upozorněme, že takové požadavky se týkají jednak smluv uzavíraných mezi podnikateli a spotřebiteli, z nichž zmíněn byl pouze požadavek na text tlačítka, popř. zahrnutí možností odstoupení od smlouvy. Takové požadavky plynou zpravidla z evropského práva a jsou transponovány do BGB, popř. EGBGB. Další požadavky z evropského práva nemusí být ani nutně soustředěny na ochranu spotřebitele. Zejména pochází z evropské směrnice 2000/31/ES, která bývá nazývána jako směrnice E-Commerce. Provozuje-li jedna strana elektronický obchod, typicky jako *prodávající*, stává se navíc *poskytovatelem* služeb informační společnosti ve smyslu směrnice E-commerce a její smluvní protistrana, typicky kupující zákazník, kromě svého soukromoprávního postavení smluvní strany má i postavení a práva *příjemce služeb* ve smyslu směrnice o E-commerce. Zájemce o uzavírání smluv určitého druhu podle německého práva si proto musí provést příslušnou rešerši, jaké všechny právní náležitosti se jeho případu užití týkají.[55]

5.2.5 Náležitosti formy

BGB je založen na principu bezformálnosti právního jednání.[56] Důvodem podle sepisovatelů BGB byly špatné zkušenosti s dřívějšími zákoníky: „Za čím otravnější budou požadavky nucené formy považovány, tím více se zvyklostí provozu bude stávat neohlížení se na předepsanou formu. Tím se z nucené formy za účelem právní jistoty stává pravý opak, spořádaná a důvěřující osoba je bezbranná proti zneužití své důvěry zneužívající protistranou. V tomto ohledu byly při panství nucené formy učiněny obzvlášť nepříznivé zkušenosti.“[57] Výkladově je volnost formy dovozována mimo jiné *a contrario* z § 125 BGB a z první půlky první věty § 126 odst. 1 BGB.[58]

Stanovení povinné formy je tedy v rámci BGB výjimkou. Následky nedodržení jsou stanoveny v § 125 BGB: *„Právní transakce, která nedosahuje formy předepsané zákonem, je nicotná. Nedostatek formy určené právní transakcí má v případě pochyb za*

[54] HOEREN, T., cit. dílo, s. 321.
[55] HOEREN, T., cit. dílo, s. 326–372.
[56] FLUME, W., cit. dílo, s. 246.
[57] *Motive ...,* cit. dílo, Band I, s. 180.
[58] HOEREN, T., cit. dílo, s. 372.

následek rovněž nicotnost." Forma tedy může být stanovena buď přímo zákonem, anebo předchozí právní transakcí (právním jednáním) stran podle § 127 BGB. Zatímco nedodržení zákonem předepsané písemné formy je stiženo nicotností vždy, v případě nedodržení formy z důvodu předchozího sjednání tomu tak bude jen v případě pochyb, tedy pokud strany zjistí, že písemná forma je pro právní transakci konstitutivní. Nicotnost nenastává, pokud je sjednaná forma potřebná jen pro čistě důkazní funkci.[59]

Podle Flumeho platí § 125 BGB nejen pro výslovně zmíněné právní transakce, ale i pro vyjádření vůle,[60] pokud přichází do úvahy, jako je tomu například u smlouvy v případě nabídky a přijetí.

5.2.5.1 Písemná forma

Ohledně náležitosti písemné formy platí podle § 126 odst. 1 BGB: *„Pokud je zákonem předepsána písemná forma, musí být listina podepsána vystavitelem vlastnoručně prostřednictvím podpisu jména nebo prostřednictvím notářsky ověřeného znamení ruky."* Dle Flumeho platí požadavek přítomnosti vlastnoručního podpisu i pro případ písemné formy, pokud je dohodnuta jen mezi stranami. Požadavek písemné formy je dle něj v podstatě **požadavkem formy podpisu**. Podpis musí být vlastnoruční a musí se jednat o podpis vystavitele listiny, a nikoli třeba toho, kdo obsah listiny sepsal nebo jinak připravil. Podpis musí prostorově ohraničovat spodek textu listiny. Text, který následuje za podpisem, není podpisem kryt. Podpis musí být proveden zapsáním jména a z něj by měla vyplývat totožnost vystavitele. Pouze v případě vlastnoručně psaných listin, jako je závěť, dostačuje místo podpisu *„Váš otec"*, neboť totožnost vyplývá jinak. V případě jiných listin se nedoporučuje, neboť například stejný kvazi podpis nebyl uznán v případě příslibu ručení. Jménem se v § 126 odst. 1 BGB míní označení, pod kterým osoba běžně vystupuje v právním nebo obchodním styku. Běžně dostačuje rodinné jméno (příjmení), křestní navíc je nutné jen tehdy, pokud by hrozilo nebezpečí záměny. V případě osoby, která jedná jménem obchodní společnosti, se obchodník může podepsat firmou. Kdo pravidelně používá pseudonym, může se podepsat tímto pseudonymem. Obdobně, pokud takto známě používá pouze křestní jméno. Zkratky jako podpis nedostačují. Čitelnost podpisu se obecně nevyžaduje. V případě použití více listů se doporučuje je očíslovat a spojit, jakož i podepsat jednotlivě každý list.[61]

[59] HOEREN, T., cit. dílo, s. 373.
[60] FLUME, W., cit. dílo, s. 248.
[61] FLUME, W., cit. dílo, s. 250–251.

Vyžaduje-li zákon písemnou formu pro smlouvu, musí být smlouvy obou stran na stejné listině (§ 126 odst. 2 BGB). Telegram není schopen splnit požadavek písemné formy. Ačkoli se podepisuje jeho podací formulář, není podpis poté telegrafickou zprávou přenesen.

V obchodní praxi mají význam i tzv. blanko listiny *(Blankourkunde)*, tj. podpis na prázdném listu. Podpis kryje požadavky písemné formy vyjádření, pod nímž se podpis případně bude nacházet. Přenechání blanko listiny má zásadně stejné následky jako vystavení plné moci k zastoupení podepsaného. Pro případ zneužití listiny platí stejná pravidla jako pro případ překročení oprávnění k zastoupení. Dle Flumeho: „Rovněž v případě falšování bude v podstatě zákonná písemná forma falšovatelem splněna, takže vzniká jeho odpovědnost podle § 179 [BGB].“[62] Civilní sankce dle § 179 odst. 1 BGB je, že ten, kdo překročil zástupčí oprávnění, je zavázán k náhradě škody. Odlišně platí pro případy směnek, šeků a tzv. blanko cessí.[63]

5.2.5.2 Elektronická forma

Německé soukromé právo zavedlo elektronickou formu *(Elektronische Form)* jako samostatný druh formy v přídavných ustanoveních § 126a BGB. V německém právu je této formě přiznána téměř ekvivalance s písemnou formou. Dle § 126 odst. 3 BGB *„Písemná forma může být nahrazena elektronickou formou, pokud ze zákona nevyplývá jinak."* Elektronická forma tedy může nahradit písemnou formu vždy, pokud zákon nahrazení nevylučuje nebo netrvá výlučně na písemné formě.

Podle § 126a odst. 1 BGB se stanoví náležitostí elektronické formy a nahrazení písemné formy: *„Pokud má být předepsaná písemná forma nahrazena elektronickou formou, musí vystavitel do vyjádření připojit své jméno a elektronický dokument opatřit kvalifikovaným elektronickým podpisem."*[64] V elektronickém dokumentu tedy musí být uvedeno jméno výstavce *(Aussteller)*[65] a musí být opatřen kvalifikovaným elektronickým podpisem, jehož náležitosti byly do léta 2016 upraveny německým zákonem *Signatursgesetz*, od doby účinnosti nařízení eIDAS jsou přednostně upraveny

[62] FLUME, W., cit. dílo, s. 253.
[63] FLUME, W., cit. dílo, s. 254–255.
[64] *„§ 126a Elektronische Form*
(1) Soll die gesetzlich vorgeschriebene schriftliche Form durch die elektronische Form ersetzt werden, so muss der Aussteller der Erklärung dieser seinen Namen hinzufügen und das elektronische Dokument mit einer qualifizierten elektronischen Signatur versehen."
[65] EINSELE, D. *BGB § 126a Elektronische Form*. Rn. 5. In: SÄCKER, J. (ed.) *Münchener Kommentar zum Bürgerlichen Gesetzbuch: BGB Band 1: Allgemeiner Teil §§ 1–240, ProstG, AGG*. 7. Auflage. München: C. H. Beck, 2015.

samotným nařízením. Uvedení jména výstavce bylo přikázáno zjevně proto, aby ze samotného elektronického dokumentu bylo patrné, kdo je jeho původcem. Tuto roli měl v případě tradičních papírových listin samotný vlastnoruční podpis. Zatímco však vlastnoruční podpis se musel striktně nacházet pod psaním, u jména výstavce se připouští libovolné umístění v rámci elektronického dokumentu, je možný tedy i *nade-pis („Oberschrift")*.[66] Důvodem je, že kvalifikovaný elektronický podpis následně uzavírá a zajišťuje před změnou celý elektronický dokument. Pokud by však bylo sporné, jaká část písemnosti je považována za stvrzenou, doporučuje se jméno výstavce umístit tam, kde by se běžně nacházel právě elektronický podpis.[67] Uvedený právní požadavek na jméno výstavce zjevně řeší právně teoretickou potíž určit komitment (srov. 4.7) připojeného elektronického podpisu. Uvedení výstavce v elektronickém dokumentu, který je opatřen kvalifikovaným elektronickým podpisem odstraňuje nejistotu ohledně toho, v jakém vztahu či významu (komitmentu) byl uvedený elektronický podpis k němu připojen. Je postaveno najisto, že se bude (může) jednat o právní jednání výstavce v elektronické formě. Podle Wendtlanda má být výstavce z elektronického dokumentu patrný na první pohled.[68]

V § 126a odst. 1 BGB je vyjádřen pojem *elektronický dokument (elektronische Dokument)*, kterým se v případě elektronické formy stanoví název pro písemnost. Pro samotný elektronický dokument nauka dříve dovozovala, že musí být uložen na technickém nosiči,[69, 70] v současnosti však již autor považuje tento požadavek za překonaný, a to přinejmenším v případě unijního práva pro elektronické obchody (srov. 10.3.1), kdy právo sice hovoří o takzvané trvalém nosiči *(durable medium)*, dle unijní judikatury ale již dostačuje uložení v cloudu v rámci určitého účtu zákazníka. V německém právu uvedené unijní úpravě odpovídají požadavky *dispozice na trvanlivém datovém nosiči (auf einem dauerhaften Datenträger zur Verfügung gestellt werden)* a *čitelnosti (lesbar sein)*.[71]

Elektronický dokument *není čitelný* bez pomocného technického prostředku *(Hilfsmittel)*.[72] Elektronický dokument může být při uložení zašifrován, musí však

[66] EINSELE, D., cit. dílo, Rn. 6.
[67] EINSELE, D., cit. dílo, Rn. 6.
[68] WENDTLAND, H. *BGB § 126a Elektronische Form*. Rn. 4. In: BAMBERGER, H. G. – ROTH, H. – HAU, W. – POSECK, R. (Hrsgb). *BeckOK BGB*. 44. Edition. Stand 01.11.2017. C. H. Beck. 2017.
[69] EINSELE, D., cit. dílo, Rn. 3.
[70] ABEL, S. Urkundenbeweis durch digitale Dokumente. *Multimedia und Recht* (MMR), 1 Jg. (1998), Heft 12, s. 644–650. s. 645.
[71] Článek 246a § 4 odst. 3. EBGBG.
[72] EINSELE, D. Tamtéž.

existovat možnost jej rozšifrovat a zajistit jeho *čitelnost psacími znaky (Schriftzeichen)*.[73] Pro dodržení formy dostačuje *zobrazení na displeji (Bildschirm)*, není nutné zajištění tisknutelnosti,[74] existuje však i menšinový protichůdný právní výklad, že potlačení tisknutelnosti ruší zachování elektronické formy.[75] Trvalý nosič musí být schopen data elektronického dokumentu *uchovávat dlouhodobě* a musí být zajištěna *dlouhodobá reprodukce* vyjádření *(eine dauerhafte Wiedergabemöglichkeit der Erklärung)*, bez čehož by elektronický dokument nebyl použitelný pro jakoukoli důkazní funkci.[76] Wendtland shrnuje zde uvedené požadavky stručně jako *dlouhodobou čitelnost*,[77] na displeji, popř. vytištěním.

Elektronický dokument sám o sobě bez dalšího nezajišťuje integritu (nepozměněnost) ani autenticitu (pravost, původnost). Digitální prostředí umožňuje nezjistitelnou manipulaci obsahu i záměnu identity[78] původce elektronického dokumentu. Integritu i autenticitu elektronického dokumentu při právním jednání v elektronické formě zajišťuje až kvalifikovaný elektronický podpis. Původně panovaly v nauce i určité obavy, zda jeho vytváření bude stejně psychologicky výrazné (varovací funkce podpisu), jako tomu je při vytváření vlastnoručního podpisu, ale zdá se, že přítomnost „čipové karty, čtečky a zadání PINu“[79] se vžily jako dostatečná náhrada. Bettendorf přitom považoval za důležité i poučení[80] o právních následcích kvalifikovaného elektronického podpisu, tj. o zásadní rovnocennosti s vlastnoručním podpisem, které musel provést poskytovatel certifikačních služeb při vydávání kvalifikovaného certifikátu, aby podepisující osoba si skutečně byla plně právně vědoma významu svého jednání a nepovažovala projev jen za běžné odklikávání.

V § 126a odst. 2 BGB se určují pravidla elektronického podpisu v případě smluv. V § 126 odst. 2 BGB se předepisuje přítomnost vlastnoručních podpisů na stejné listině, pokud se však vytváří více *stejnopisů listin (gleichlautende Urkunden)*, dostačuje, aby každá ze stran podepsala stejnopis, který bude předán druhé straně. Obdobně dostačuje v případě elektronické formy: *„V případě smlouvy musí strany*

[73] EINSELE, D. Tamtéž.
[74] EINSELE, D. Tamtéž.
[75] Pozn. pod čarou č. 7 v EINSELE, D. Tamtéž.
[76] EINSELE, D. Tamtéž.
[77] WENDTLAND, H., cit. dílo, Rn. 3.
[78] BETTENDORF, J. Elektronische Dokumente und Formqualität. *Rheinische Notar-Zeitschrift* (RNotZ), 5. Jg. (2005), Heft 6, s. 277–294, s. 278.
[79] BETTENDORF, J., cit. dílo, s. 285.
[80] BETTENDORF, J., cit. dílo, s. 285.

elektronicky podepsat vždy stejnopis dokumentu, způsobem určeným v odstavci 1."[81] Platné je dokonce uzavření smlouvy, u níž jedna strana podepíše elektronickou formu stejnopisu kvalifikovaným elektronickým podpisem, zatímco druhá strana stejnopis ve formě tradiční listiny vlastnoručním podpisem.[82]

Podle Lindner-Figura musí elektronický dokument „obsahovat celé právní jednání v povinné formě, platí pro něj zásada jednotnosti/ucelenosti *[Einheitlichkeit]* listiny".[83] Udává též, že na elektronické formě právního jednání se musí v případě smluv shodnout obě strany, byť dostačuje konkludentní souhlas.[84]

Tradiční listina, která je i s vlastnoručním podpisem naskenovaná a jako elektronický dokument odeslaná například elektronickou poštou, nesplňuje požadavky na písemnou formu podle § 126 odst. 1 BGB, protože nevyhovuje § 126 odst. 3 BGB. Současně nesplňuje ani požadavky na elektronickou formu, protože neobsahuje kvalifikovaný elektronický podpis.

Německá judikatura rozhodla i o nepoužitelnosti biodynamického podpisu smlouvy o spotřebitelské půjčce, kterou žalobce podepsal na elektronickém psacím tabletu elektronickou tužkou. Na závěr jednání byl formulář včetně obrazu podpisu žalobce vytištěn a jeden výtisk mu byl předán. Podle § 492 odst. 1 BGB je pro smlouvu o spotřebitelské půjčce předepsána písemná forma. Dle rozsudku „Písemná listina ve smyslu § 126 BGB vyžaduje trvalé vtělení znaků písma na psací materiál jakéhokoli druhu. K tomu v případě elektronického dokumentu všeobecně nedochází, jak *a contrario* naznačuje § 126 odst. 3 s § 126a BGB a jak tomu je i při zde předloženém případu ručně psaného elektronického podpisu na podpisovací plošinku [Unterschriftenpad]. Toto přehlédl jak zemský soud, který se nevěnoval výkladům práva říšskými soudy (při nápisu křídou na břidlicovou tabuli se ještě jedná o trvalé vtělení na „tělesný" materiál), tak žalovaný. Na vlastnosti listiny se nic nemění, pokud původní listina je po krátkém čase zničena, pokud na každý pád vtělení bylo původně (byť jen na krátký čas) provedeno. V předloženém případě oproti tomu byl dokument elektronicky

---

[81] *„(2) Bei einem Vertrag müssen die Parteien jeweils ein gleichlautendes Dokument in der in Absatz 1 bezeichneten Weise elektronisch signieren."*

[82] WENDTLAND, H. *BGB § 126a Elektronische Form*. Rn. 7. In: BAMBERGER, H. G. – ROTH, H. – HAU, W. – POSECK, R. (Hrsgb). *BeckOK BGB*. C. H. Beck. 44. Edition. Stand 01.11.2017. C. H. Beck. 2017.

[83] LINDNER-FIGURA, J. *Kapitel 6. Form des Mietvertrages*. Rn. 120. In: LINDNER-FIGURA, J. – OPRÉE, F. – STELLMANN, F. (Hrsgb.). *Geschäftsraummiete: Handbuch*. 4. Auflage. C. H. Beck, 2017.

[84] LINDNER-FIGURA, J., cit. dílo, Rn. 120.

uložen, ale v žádném časovém okamžiku neexistoval tělesně.“[85] Soud odmítl i návrh žalovaného o tom, aby údajnou mezeru v právu doplnil analogií: „V rozporu s názorem žalovaného nelze dojít k souhrnné analogii jako výsledku § 126 a § 126a BGB, že by podpis na elektronickém psacím tabletu k předepsané formě přesto dostačoval, jelikož zákonné účely formy, zejména varovací funkce a důkazová funkce, zde byly shodně splněny.“[86] Dle Roßnagela, který případ stručně komentoval,[87] má rozsudek dalekosáhlý význam, jelikož vyslovuje, že „vlastnoruční podpis na tabletovém PC nebo elektronickém psacím tabletu nesplňuje písemnou formu, předepsanou právními předpisy. Soud tak přispěl k právní jistotě o tom, zda tato stále více používaná zařízení splňují písemnou formu nebo elektronickou formu.“[88] Biodynamický podpis tedy nesplňuje požadavky ani písemné formy, ani elektronické formy. Nicméně jej lze využít tehdy, pokud BGB ani dohoda nestanoví povinnost formy.

Na základě rozsudku BGH a později ustanovení § 309 bod 13 písm. b) BGB je zakázáno smluvně vyžadovat písemnou formu pro výpověď vztahu ze strany spotřebitele. Od 1. 10. 2016 smí tedy spotřebitel vypovědět spotřebitelskou smlouvu pouze textovou formou.[89]

5.2.5.3 Textová forma

Kromě elektronické formy stanovil německý zákonodárce i podstatně volnější textovou formu v novém ustanovení § 126b BGB: *„Pokud je zákonem předepsána textová forma, musí vyjádření být představováno v listině nebo v jiném vhodném trvalém provedení písemnými znaky, uvedena osoba vyjadřovatele a závěr vyjádření učiněn rozpoznatelný napodobeninou jména podpisu nebo jinak."*

V praxi vznikla například otázka, zda textovou formu splňuje prostý obsah webové stránky. Podle rozsudku OLG[90] tomu tak není, neboť provozovatel stránek může jejich obsah kdykoli jednostranně změnit. Soud požaduje, aby příjemce informace měl možnost informaci stáhnout a uložit. V současnosti má textová forma význam

[85] OLG München. Urteil vom 4. Juni 2012.·Az. 19 U 771/12. Dostupné z: <http://openjur.de/u/498795.html>.
[86] Az. 19 U 771/12, cit. dílo, Bod 25.
[87] OLG München in ROSSNAGEL A. (ed). *Keine Wahrung der Schriftform bei Unterzeichnung auf einem elektronischen Schreibtablett.* Neue Juristische Wochenschrift (NJW), 65. Jg. (2012), Heft 49, C. H. Beck, 2012, s. 3584–3586.
[88] Obrat *elektronická forma* zde Roßnagel zřejmě používá v striktním právním významu § 126a BGB.
[89] HOEREN, T., cit. dílo, s. 374.
[90] OLG Köln, Urt. v. 24. 8. 2007 – 6 U 60/07.

zejména z hlediska plnění různých poučovacích sdělení, která jsou předepsána ve vztahu vůči spotřebitelům.[91]

5.3 Souhrn

Ze srovnání české a německé právní úpravy v této kapitole plynou určité závěry.

Soukromé právní jednání v obou právních řádech je přednostně bezformální! Členění právního jednání z hlediska formy, používané českou naukou, na výslovné a ostatní nemusí být z hlediska elektronického právního jednání nutně mantinelem, do něhož by se právní jednání muselo chtít vejít. Autor na možnou nedisjunktnost uvedených forem upozorňuje již výše v průběhu této kapitoly. Český občanský zákoník je pak v oblasti pojmu právní jednání formulován natolik obecně, že v případě právního jednání učiněném elektronickými prostředky je představitelné, že bude v jistém smyslu napříč kategoriemi nebo provedení bude odlišné od tradičních forem, aniž by to bylo na újmu nevyhovování pojmu právní jednání.

Stejný závěr plyne ze srovnání s německým pojmem *ausdrücklich*, jehož význam je spíše *důrazně*, popř. *výrazně*. To sice zahrnuje český pojem *výslovně*, ale je širšího významu. Rozeznávání ústní, písemné a konkludentní formy je tak spíše záležitostí jak nauky, tak ale i zvyklostí lidí, které ovšem vznikly v klasickém světě osobního nebo listinného styku. Autor nevylučuje, že v rámci světa elektronického vzniknou jiné způsoby vyjadřování se či projevování se, které budou považovatelné za právní jednání, které nebudou zařaditelné do uvedených kategorií. Přitom ovšem nijak nezpochybňuje, že zejména písemná forma právního jednání má zvláštní právní užitečnost v tom, že nutí vyjadřujícího se k vysoké přesnosti vyjádření obsahu právního jednání. Vzhledem k tradici a metodám práva lze proto předpokládat, že si svůj význam podrží i v případě elektronického provádění právního jednání.

Druhý závěr této kapitoly je, že české soukromé právo se dle názoru autora nedostatečně věnuje náležitostem a dovolenosti elektronické formy písemnosti. To může mít za následek výše v kapitole uvedené výkladové nejasnosti. Dtto se týká pojmu elektronický dokument. Americký předpis UETA i německý BGB se vyrovnávají s dovoleností písemnosti mnohem jasněji.

Třetí závěr je, že elektronický podpis prostý jako požadavek podpisu může být nedostatečný.

[91] HOEREN, T., cit. dílo, s. 374.

Čtvrtý závěr je, že německé právo je zcela kategorické z hlediska dovolenosti používat pro elektronickou formu právního jednání výlučně kvalifikovaný elektronický podpis. Důsledkem je právní ochrana subjektů v případě některých kritických druhů právních jednání.

Tato strana je záměrně ponechána prázdná.

6. Nařízení eIDAS (služby vytvářející důvěru)

V této kapitole se věnujeme výkladu nového Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES[1] (dále jen „eIDAS“). Výklad je soustředěn a omezen zásadně na tu míru, v jaké nařízení ovlivňuje elektronické právní jednání potvrzované pomocí elektronického podpisu nebo jemu podobné elektronické pečetě. Diskurs je zde zásadně veden v rámci unijního práva. Upozorňuje se ale na případná úskalí implementace právem EU i členského státu. Diskursu předchází několik úvodních informací, které mají čtenáři napomoci k pochopení pojetí nařízení, k orientaci se v něm.

6.1 Struktura a orientace v nařízení eIDAS

Název a klauzule
Body odůvodnění 1–77

Kapitola I – Obecná ustanovení
Článek 1. Předmět (Subject matter, Gegenstand)
Článek 2. Oblast působnosti (Scope, Anwendungsbereich)
Článek 3. Definice (Definitions, Begriffsbestimmungen)
Článek 4. Zásada vnitřního trhu (Internal market principle, Binnenmarktgrundsatz)
Článek 5. Zpracování osobních údajů (Data processing and protection, ...)

Kapitola II – Elektronická identifikace (Electronic identification, Elektronische Identifizierung)
Články 6–12

Kapitola III – Služby vytvářející důvěru (Trust Services, Vertraunsdienste)
Články 13–45

Kapitola IV – Elektronické dokumenty
Článek 46

Kapitola V – Přenesení pravomocí a prováděcí ustanovení
Články 47–48

Kapitola VI – Závěrečná ustanovení
Články 49–52
z toho Článek 51. Přechodná ustanovení

Přílohy
Příloha I. Požadavky na kvalifikované certifikáty pro elektronické podpisy
Příloha II. Požadavky na kvalifikované prostředky pro vytváření elektronických podpisů
Příloha III. Požadavky na kvalifikované certifikáty pro elekronické pečetě
Příloha IV. Požadavky na kvalifikované certifikáty pro autentizaci internetových stránek

Struktura nařízení eIDAS pro první přiblížení se k němu je zde výše.

[1] Dostupné z: <http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32014R0910>; navštíveno 28. 8. 2017.

6.1.1 Elektronická identifikace vs. služby vytvářející důvěru

První klíčová informace, kterou by zájemce o nařízení měl vzít na vědomí, je, že *kapitola II* o elektronické identifikaci je v zásadě disjunktní s *kapitolou III* o službách vytvářejících důvěru. Systémy elektronické identifikace jsou v nařízení upraveny nezávisle na službách vytvářejících důvěru a jejich systémech. Ačkoli v technické praxi příležitostně může dojít ke smíšení technických prostředků, v nařízení většinou k žádnému mísení ani k systémovým návaznostem nedochází. Naprostá většina pojmů definovaná v článku 3 eIDAS se používá buď v rámci systémů elektronické identifikace (kapitola II), anebo v rámci služeb vytvářejících důvěru (kapitola III). Dokonce lze říci, že nařízení by bylo možné rozdělit na dvě, přijmout a vydat je samostatně.

Příčinou tohoto oddělení je, že pro uvedené systémy je nařízením zvolena zcela odchylná metoda regulace. Důvodem volby odchylné metody regulace pak je to, že zatímco v oblasti elektronického podpisu (z nějž je odvozena většina služeb vytvářejících důvěru, srov. níže 6.8) došlo v roce 1999 k harmonizaci evropského práva směrnicí 1999/93/ES, o rámci pro elektronické podpisy (dále jen „DirES"), v oblasti elektronické identifikace žádný takový harmonizační předpis EU nevydala. Ačkoli DirES byla velmi stručná, přesto způsobila, že členské státy přistupovaly poté k elektronickým podpisům aspoň koncepčně shodně. Nařízení eIDAS proto volí v této oblasti regulační přístup, který má dotvořit *unifikaci právní i technickou*, což je ale možné jen proto, že se v žádném členském státu nejedná o koncepční zlom. V zásadě se zde jedná o jednoúrovňový přístup k regulaci, kdy vše důležité má být stanoveno v samotném unijním právu, a to jednotně. Níže autor polemizuje s tím, že tento cíl nebyl nařízením v mnohém zcela splněn, zřetelně se však jedná o jeho záměr.

V oblasti elektronické identifikace naopak členské státy postupovaly na sobě zcela nezávisle a v řadě případů si vytvořily svou vlastní legislativu a v návaznosti na ni i své vlastní technické systémy, které v rámci svého vnitrostátního elektronického provozu již využívají (v Německu se např. jedná o elektronickou verzi občanského průkazu – *Personalausweis*). Za tohoto stavu by přikázání jednotné, zcela nové technické implementace z evropské úrovně znamenalo zmaření existujících investic, a to nejen samotného identifikačního systému, ale i mnoha elektronických služeb, které identifikaci uživatelů z něj již využívají. Jen některé členské státy, jako např. ČR, elektronickou identifikaci značně zanedbaly a mohly by začít na zelené louce prakticky s jakýmkoli identifikačním systémem. Někdy se jako důvod pro opomenutí

harmonizace této oblasti uvádí i to, že členské státy ji považují za svou vlastní pravomoc, kterou na EU nepřenesly. Nařízení eIDAS proto v této oblasti zvolilo dvojúrovňovou metodu právní regulace. První úroveň, tj. právní úprava i navazující technické řešení identifikačních systémů, zůstává zcela v působnosti členského státu a jeho vnitrostátního práva. Do působnosti unijního práva se zařazuje pouze druhá úroveň, která zajišťuje vytvoření technické nadstavby (existujících) národních systémů elektronické identifikace a jejich propojení do ostatních členských států, aby se v jiných členských státech daly využívat i přeshraničně. Navíc je stanoven i jejich právní účinek. Převažující metodou právní regulace zde je určení způsobů *koordinace* členských států a jim přikázané provedení *doplnění* (vytvoření nadstavby) sebou oznámených identifikačních systémů pro přeshraniční použití. Samotná EU, její úřady ani instituce na sebe žádné technické funkce nepřebírají, nestávají se provozovatelem žádného technického systému.

6.1.2 Elektronický podpis prostý vs. zaručený a kvalifikovaný

Druhé podstatné dělení v nařízení, které se nachází uvnitř pojmu elektronický podpis, je rozdělení na elektronický podpis (prostý) na jedné straně a na elektronické podpisy zaručené nebo kvalifikované na straně druhé.

Nařízení eIDAS zvolilo novou definici pro elektronický podpis prostý. Kromě samotné definice již nařízení pro elektronický podpis prostý žádné další explicitní požadavky nestanoví. Přesto je tato změna natolik významná, že si zaslouží pojednání v samostatném odstavci (srov. 6.4).

Veškerá jiná ustanovení v nařízení (v částech o službách vytvářejících důvěru) se v případech elektronických podpisů týkají *zaručených* elektronických podpisů nebo *kvalifikovaných* elektronických podpisů. Ustanovení nařízení jsou formulována tak, že těmto pojmům zřejmě technicky (tj. fakticky) vyhoví pouze technologie infrastruktury veřejného klíče (PKI[2]). Kryptologie jako obor matematiky zde promiscue hovoří o kryptografii veřejného klíče nebo o asymetrických šifrách. V technické praxi se nakonec jedná pouze o jádro (byť hlavní) algoritmů vytvoření podpisu, zatímco plné vytvoření takového elektronického podpisu vyžaduje použití hned několika různých kryptografických algoritmů různých druhů. Ty bývají sdružovány do tzv. podpisových sad nebo schémat, jejichž nepřímou součástí bývají i požadavky na náhodnost

[2] Public key infrastructure.

generátorů náhodných čísel. Vytvořit takový podpis pak znamená využít konkrétní kryptografické schéma, sestávající z řady dílčích algoritmů, k němuž existuje odpovídající způsob ověření platnosti takového podpisu. Zejména anglosaští autoři mají tendenci tato technická provedení shrnovat pod označením *digitální podpis* a někdy jimi mínit i právní úpravu. V legislativě řady států se skutečně digitální podpis jako pojem vyskytuje. Protože pojednáváme o úpravě EU, budeme používat pojmy *zaručený* a *kvalifikovaný elektronický podpis* s tím, že technickou implementaci budeme stručně nazývat PKI, byť je to technicky zjednodušující.

Všude níže v této kapitole, nehovoříme-li výslovně o elektronickém podpisu prostém nebo z kontextu neplyne něco jiného, se hovoří nebo se nařízení eIDAS hodnotí z pohledu jeho úpravy zaručeného a kvalifikovaného elektronického podpisu, v něm obsažené. Tato skutečnost není opakovaně zdůrazňována.

6.1.3 O částech nařízení stručně

Ze struktury zde upozorníme nejprve na *body odůvodnění.* Kromě těch, jejichž přítomnost je obligátní, např. zmínka o právním základě nařízení, jakož i o všech dokumentech a unijních aktivitách, které k přijetí vedly, mají body odůvodnění význam přinejmenším ze tří hledisek. Prvním je, že mohou poskytnout pomocné výkladové pozadí či hledisko, je-li část normativního textu nejasná. Za druhé body odůvodnění podávají vysvětlení účelu dílčích částí, větších celků nebo cílů, ke kterým nařízení nebo jeho části směřují. Ty mohou, ale nemusí stejně vyplývat i z normativní části. Neodporuje-li normativní text účelům, které jsou vyjádřeny v bodech odůvodnění, je vhodné normativní text vykládat s přihlédnutím k nim. Konečně třetí způsob využití bodů odůvodnění je orientace z hlediska možností další implementace nařízení, ať již unijní, nebo vnitrostátní.

Kapitola I (Obecná ustanovení) obsahuje předně předmět a oblast působnosti nařízení (články 1, 2, 4; srov. též níže 6.3). Článek 3 obsahuje definice různých pojmů pro celé nařízení a článek 5 vymezuje vztah k ochraně osobních údajů, což je jiná, unijním právem tradičně upravená oblast práva.

Obsah a význam *kapitol II* a *III* je již výše (srov. 6.1.1, částečně též 6.1.2).

Kapitola IV obsahuje jediný článek o elektronickém dokumentu a jeho právních účincích. Samostatně je uveden asi proto, jelikož se jej věcně nehodilo zařadit zcela ani pod kapitolu II, ani III. Ustanovení o něm jsou tedy použitelná obecně.

Kapitola V pojednává v podrobnostech o činnosti Komise a procesech, které musí použít, bude-li implementovat některé části nařízení, k jejichž provedení je na různých místech zařízení zmocněna.

Kapitola VI obsahuje závěrečná ustanovení, včetně ustanovení derogačních a včetně ustanovení o různém nabývání účinnosti. Zvláštní pozornost je zde určitě třeba věnovat článku 51 o přechodných ustanoveních, tj. podmínkách přechodu mezi dřívější regulací podle směrnice DirEC do regulace podle nařízení eIDAS.

Přílohy I. až IV. je třeba považovat za normativní text ve stejném smyslu jako je obsah článků 1 až 52. Účel jejich vynětí spočívá spíše v tom, že obsahují dobře vymezené normativní skupiny požadavků, u nichž se předpokládá dlouhá časová stálost. Jejich zvláštností též je, že přímým úběžníkem nejsou požadavky na jednání subjektů práva, ale je jím vždy buď některý digitální objekt (certifikát podle příloh I, III nebo IV), anebo elektronický prostředek (příloha II). Význam má též jejich samostatné číslování v rámci nařízení, neboť technické normy nebo jiné dokumenty, které se případně někdy budou odkazovat na nařízení, tak budou moci těžit z relativní časové stálosti tohoto nezávislého číslování, které by nemělo být zasaženo ani případnými novelizacemi nařízení. Použití příloh je částečně zděděno i jako legislativní technika ze směrnice DirES. Účelem soustředění pravděpodobně bylo mít vyčerpávající seznam požadavků na určité pojmy. To mělo neprávnickým subjektům umožnit věnovat se pouze požadavkům určité přílohy a pominout zbytek právního textu. Zatímco tato technika mohla být poměrně přijatelná v případě formy směrnice, v případě nařízení se autor nedomnívá, že je možné zúžit zkoumání právního významu pojmů v nadpisech příloh pouze na relevantní seznam požadavků, soustředěný pod nimi v přílohách.

6.1.4 Pojem „elektronická transakce" (elektronické právní jednání...)

Pojem elektronické transakce se objevuje již v samotném názvu nařízení. Podle názvu mají elektronická identifikace i služby vytvářející důvěru sloužit pro elektronické transakce, a to sice elektronické transakce na vnitřním trhu, tedy i přeshraničně.

I v jiných jazykových verzích nařízení se používají doslovné překlady jako *electronic transactions*, *elektronische Transaktionen*, *transactions électroniques*, *transazioni elettroniche*, *elektronikus tranzakciókhoz*, *transacciones electrónicas*...

Jedná se tedy o pojem unijního práva, jehož význam je nutné odvodit zejména systematickým výkladem ze samotného nařízení eIDAS. Autor navrhuje, že přídavné

jméno *elektronické* odkazuje na využití elektronických prostředků pro komunikaci, autentizaci digitálních objektů (např. elektronického dokumentu), anebo subjektu komunikace. Pojem *transakce* pak vystihuje pojem *právní jednání* v širokém slova významu. Zahrnuje tedy jak soukromé právní jednání, tak i individuální veřejnoprávní akty, jakož i různé procesní úkony účastníků správních nebo soudních řízení.

Tak kupř. bod odůvodnění 1 eIDAS hovoří o tom, že *„spotřebitelé, podniky a orgány veřejné moci [se zatím] zdráhají provádět transakce elektronickými prostředky a přijímat nové služby"*. Cílem jsou tedy samotné transakce, elektronické prostředky jsou jen jednou z metod nebo forem, jak je provést. Bod dokládá správnost hypotézy autora o významu adjektiva *elektronické*.

Podle bodu odůvodnění 3 eIDAS dřívější směrnice DirES *„upravovala elektronické podpisy, aniž by poskytovala ucelený přeshraniční a meziodvětvový rámec pro bezpečné, důvěryhodné a snadno použitelné elektronické transakce. Toto nařízení acquis uvedené směrnice posiluje a rozšiřuje."* Přitom jak směrnice DirES (bod odůvodnění 17, článek 1), tak nařízení eIDAS (bodu odůvodnění 21, článek 2 odst. 3) odmítají, že by předpis měl dopad na existující požadavky na uzavírání smluv nebo jiných požadavků na formu, daných unijním nebo vnitrostátním právem. Uvedený *„ucelený přeshraniční a meziodvětvový rámec"*, který má být posílen a rozšířen v nařízení eIDAS a neucelený byl již za DirES, má tedy charakter určitých pomocných metod, postupů, technik, využívajících různé elektronické prostředky, které pomáhají provedení transakce elektronickým způsobem tak, aby byla bezpečná, důvěryhodná a snadno proveditelná.

Nařízení přitom věcně reguluje elektronickou identifikaci (kapitola II), služby vytvářející důvěru (kapitola III) a elektronické dokumenty (kapitola IV), byť rozdílnými způsoby (srov. výše). Z toho elektronický dokument je jednou z metod, jak zachytit obsah elektronické transakce, ostatní úprava slouží pro autentizační metody pro digitální objekty, pro subjekty komunikace v různých možných relacích, pro zachycení času, popř. pro ověřené doručování dokumentů nebo jiných dat mezi subjekty.

Z čl. 1 písm. b) eIDAS, o předmětu regulace, že nařízení *„stanoví pravidla pro služby vytvářející důvěru, zejména u elektronických transakcí"* lze dovodit, že např. služby vytvářející důvěru lze využít i pro činnosti, které povahu elektronických transakcí nemají. Skutečně ne každé jednání nebo činnost musí být právním jednáním

(v širokém slova významu), přesto pro ně lze některou ze služeb vytvářejících důvěru využít. Z nařízení nelze ale přesně dovodit hranici pro jednání, které transakcí je a které již není. Pro některé transakce je navíc použití nařízení vyloučeno, i když se o transakce jedná (srov. oblast působnosti níže 6.3).

K podobném významu pojmu transakce nakonec dojdeme i překladem přes němčinu. Český pojem *právní jednání* (soukromé) se běžně překládá jako *das Rechtsgeschäft*. V německém překladu BGB do angličtiny je pak *Rechtsgeschäft* přeložen jako *legal transaction*.

Jak je uvedeno již výše, pojem elektronické transakce v kontextu nařízení eIDAS není vyčerpán pojmem právní jednání v soukromém právu. Například podle bodu odůvodnění 2 eIDAS: *„Toto nařízení má zvýšit důvěryhodnost elektronických transakcí na vnitřním trhu tím, že poskytne společný základ pro bezpečnou elektronickou komunikaci mezi občany, podniky, orgány veřejné moci, čímž posílí efektivnost veřejných a soukromých on-line služeb, elektronického podnikání a elektronického obchodu v Unii "*.

Mají tedy být zahrnuty i elektronické transakce veřejných on-line služeb, bezpečná komunikace mezi občany nebo podniky vůči orgánům veřejné moci. Nařízení eIDAS pak není napsáno z hlediska dichotomie práva soukromého a veřejného tak, jak by tomu běžně bylo například u právního předpisu v ČR. Pro výklad bodů odůvodnění, ale v normativní části např. čl. 27 nebo čl. 25 eIDAS, je pak třeba brát do úvahy právní základ nařízení, tedy dovolené oblasti a rozsah přenosu pravomocí na EU.

Nařízení eIDAS se ve svém právním základu odvolává na celou SFEU a zejména na její článek 114, jehož podstatou je *„sbližování právních a správních předpisů členských států"* za účelem *„vytvoření a fungování vnitřního trhu"*. K tomuto účelu je EU oprávněná podle čl. 26 SFEU přijímat opatření v souladu se SFEU, jakým jsou i právní akty Unie, jako je i nařízení podle článku 288 SFEU. Vnitřní trh podle čl. 26 odst. 2 SFEU *„zahrnuje prostor bez vnitřních hranic, v němž je zajištěn volný pohyb zboží, osob, služeb a kapitálu v souladu s ustanoveními Smluv"*. Zmíněný volný pohyb zboží, osob, služeb a kapitálu je proto hlavním právním základem nařízení. Tento volný pohyb se ovšem realizuje mimo jiné i na základě „transakcí", jejichž elektronickou verzi upravuje nařízení eIDAS a které typicky probíhají mezi soukromými subjekty.

Částečně však zmíněný volný pohyb může být podmíněn i správními předpisy jednoho nebo více členských států, tj. správními úkony vůči orgánu členského státu, anebo napak od něj směrem k jednomu nebo i k oběma stranám soukromé transakce. Správní činnost pak představuje určitou veřejnoprávní složku zamýšlené transakce, popř. o ní můžeme též hovořit jako o transakci veřejnoprávní, která souvisí s tím, aby mohly probíhat jedna nebo více transakcí souvisejících s volným pohybem zboží, osob, služeb a kapitálu.

Současně je třeba jasně vymezit, že mezi přenesené pravomoci nepatří, až na výjimky, jako je např. soutěžní právo, výkon správního práva ani způsob organizace veřejné správy členského státu.

6.1.5 Používané zkratky v této kapitole

V oboru elektronických podpisů podle směrnice DirES, zejména v rámci technických dokumentů, se používalo a dále používá velké množství různých zkratek, které ve značné míře přešly do používání i v rámci nařízení eIDAS. Jejich použití by sice text i zde zkrátilo, ale laický nebo právní čtenář by poté měl potíže mu rozumět. Pro úvod zde zavedeme pouze tři zkratky, pro velmi často používané pojmy.

QES je z anglického pojmu „qualified electronic signature“, česky „kvalifikovaný elektronický podpis“ (článek 3 bod 12 eIDAS). QES je digitální objekt, tj. má povahu dat. Nauka používala pojem i zkratku QES již v rámci dřívější směrnice DirES, a to sice pro podpisy podle čl. 5 odst. 1 DirES.

QSCD je z anglického pojmu „qualified electronic signature creation device“, česky „kvalifikovaný prostředek pro vytváření elektronických podpisů“ (článek 3 bod 23 a požadavky přílohy II. eIDAS). QSCD je prostředek, tj. podle čl. 3 bodu 22 eIDAS *„konfigurované programové vybavení nebo technické zařízení, které se používá k vytváření elektronických podpisů"* (tj. software, harware nebo kombinace softwaru a hardwaru). Kvalifikovaným je tehdy, když splňuje požadavky přílohy II eIDAS. V rámci směrnice DirES se používal podobný pojem **SSCD**. Podrobněji k pojmu právně i technicky srov. níže v 6.10.

QSealCD je z „qualified electronic seal creation device“, česky „kvalifikovaný prostředek pro vytváření elektronických pečetí“ (článek 3 bod 32 a přiměřeně požadavky přílohy II eIDAS).

6.1.6 Druhy subjektů v nařízení eIDAS

V nařízení eIDAS je obtížné se orientovat i podávat jeho výklady již čistě z toho důvodu, že obsahuje 41 definic právních pojmů (článek 3), z nichž pouhé 4 se využívají výlučně v rámci kapitoly II (elektronická identifikace) a 1 výlučně v rámci kapitoly IV (elektronický dokumentu). Ostatních 36 pojmů se týká služeb vytvářejících důvěru.

Pro orientování se čtenáře následuje výčet druhů subjektů, které se v nařízení vyskytují. Zpravidla se jedná o subjekty v nařízení výslovně uvedené, někdy však uvádíme i subjekty, jejichž existenci lze implikovat, v nařízení ale uvedeny nejsou.

6.1.6.1 Subjekty rámce služeb vytvářejících důvěru

Poskytovatel služeb vytvářejících důvěru (čl. 3 bod 19 eIDAS) je subjekt, který poskytuje jednu či více služeb vytvářejících důvěru. Služby vytvářející důvěru jsou v nařízení eIDAS uvedeny taxativně (čl. 3 bod 16 eIDAS).[3] Subjekty jsou fyzické nebo právnické osoby. Z celé tvorby systému dohledu v nařízení lze dovodit, že nařízení předpokládá, že jimi budou zejména subjekty soukromého práva, které budou své služby provozovat úplatně (čl. 3 bod 16 eIDAS), a typicky tedy za účelem dosažení zisku, nicméně nevylučuje explicitně ani neziskové poskytovatele nebo poskytovatele navázané na stát. Všichni tito poskytovatelé podléhají bezpečnostním požadavkům z čl. 19 eIDAS. Jejich činnost a poskytování služeb nepodléhají předchozímu ohlašování ani povolování, jsou ale povinni hlásit státnímu orgánu dohledu případné bezpečnostní incidenty (čl. 19 odst. 2 eIDAS), popř. i subjektům jimi přímo dotčeným.

Kvalifikovaný poskytovatel služeb vytvářejících důvěru (čl. 3 bod 20 eIDAS) je takový poskytovatel uvedený výše, který poskytuje jednu či více kvalifikovaných služeb vytvářejících důvěru a kterému orgán dohledu udělil status kvalifikovaného poskytovatele. Kvalifikované služby vytvářející důvěru jsou verzí taxativně určených služeb vytvářejících důvěru, které v eIDAS mají stanoveny přídavné požadavky. Navíc eIDAS obsahuje přídavné požadavky i na subjekt a činnost samotného kvalifikovaného poskytovatele, jeho zaměstnance atd. Bezpečnostní kontrola kvalifikovaného poskytovatele je předběžná (apriorní), ještě před zahájením poskytování služeb.

[3] Nařízení však připouští, že členské státy mohou v rámci svých právních řádů definovat i jiné služby vytvářející důvěru, které však nebudou těžit z právního rámce v eIDAS, zejména z přeshraničního uznávání.

Zaměstnanec nebo **subdodavatel** kvalifikovaného poskytovatele. Subjekty nejsou přímo v eIDAS definovány, nařízení však stanoví nebo implikuje určité požadavky nebo náležitosti pro ně [např. čl. 24 odst. 2 písm. b) eIDAS].

Orgán dohledu (čl. 17 eIDAS) je členským státem určený orgán, který odpovídá za plnění úkolů členského státu v oblasti dohledu. Jeho povaha je převážně úřední (uděluje či odnímá status kvalifikovaného poskytovatele), nařízení ale částečně předpokládá i technické znalosti jeho pracovníků (schopnost ověřování plnění požadavků eIDAS poskytovatelem). Je dokonce oprávněn případně sám provést audit kvalifikovaného poskytovatele (čl. 20 odst. 2 eIDAS), může se však spokojit s ověřováním na základě zprávy o posouzení shody, vyhotovené subjektem posuzování shody ať již na žádost poskytovatele (čl. 20 odst. 1 eIDAS), nebo orgánu dohledu (čl. 20 odst. 2 eIDAS).

Subjekt odpovědný za vnitrostátní důvěryhodný seznam (čl. 22 odst. 3 eIDAS) odpovídá za jeho zřízení, udržování, zveřejnění. Určuje jej členský stát. Musí být schopen daných technických činností. Může se jednat o soukromý i veřejný subjekt, může, ale nemusí být shodný s orgánem dohledu. Obsah důvěryhodného seznamu aktualizuje podle rozhodnutí orgánů dohledu o udělení, ukončení nebo odejmutí statutu kvalifikované služby a kvalifikovaného poskytovatele.

Subjekt posuzování shody je subjekt, který vykonává činnosti posuzování shody [ev. včetně kalibrace, zkoušení, certifikace a inspekce] – čl. 2 bod 13 nařízení (ES) č. 765/2008. Tento subjekt je akreditován vnitrostátním akreditačním orgánem pro určité činnosti postupy podle nařízení nařízení (ES) č. 765/2008. Podle čl. 3 bod 18 eIDAS je tento subjekt akreditován pro provádění *„posuzování shody kvalifikovaného poskytovatele a jím poskytovatených kvalifikovaných služeb vytvářejících důvěru"*. V praxi se jedná o odborné soukromé obchodní společnosti. Provádí audit (čl. 20 odst. 1 eIDAS) ohledně toho, že kvalifikovaný poskytovatel a jeho daná kvalifikovaná služba splňují požadavky stanovené eIDAS. Poskytovatel pak předkládá výslednou zprávu o posouzení shody orgánu dohledu. Tento audit se provádí před zahájením poskytování kvalifikované služby a pak nejméně jednou za dva roky.

Vnitrostátní orgán pro bezpečnost informací, kterému se dle čl. 19 odst. 2 eIDAS hlásí bezpečnostní incidenty.

Komise je exekutivní orgán EU. V rámci nařízení eIDAS Komise plní roli koordinátora celého systému dohledu, udržuje přehled o tom, jaké subjekty či orgány byly každým členským státem určeny či uznány pro určité role, které nařízení eIDAS. Nařízením je Komise zmocněna k vydání řady implementačních aktů (srov. 6.2.2). Vedle toho je prakticky nejdůležitějším úkolem Komise vydat seznam důvěryhodných seznamů podle čl. 22 odst. 4 eIDAS.

Členský stát je některý členský stát EU, popř. stát, který má na základě mezinárodních dohod s EU stejné povinnosti jako členský stát při implementaci a uplatňování práva EU. Nařízení stanoví členským státům řadu povinností.

ENISA[4] – Evropská agentura pro bezpečnost sítí a informací – je jedna z agentur EU. V rámci eIDAS existuje povinnost orgánů dohledu podávat jí pravidelné zprávy, popř. i hlášení o některých bezpečnostních incidentech. Měla by být expertním centrem, schopným radit členských státům i Komisi v uvedených záležitostech.

6.1.6.2 Subjekty rámce pro QSCD

Určené subjekty certifikující bezpečnost produktů informačních technologií (dále v textu též jako **„určené zkušebny"** nebo **„zkušebny"**). Jedná se o jeden nebo více veřejných nebo soukromých subjektů, které určují členské státy (čl. 30 odst. 1 eIDAS). Jejich činností je provádět certifikace v souladu s čl. 30 odst. 3 eIDAS, spočívající v posuzování bezpečnosti produktů IT, konkrétně QSCD nebo QSealCD. Komise může[5] akty v přenesené působnosti (čl. 30 odst. 4 eIDAS) stanovit zvláštní kritéria, která mají tyto subjekty splňovat. Komise žádný tento akt zatím nevydala, nicméně nedošlo ani k formálnímu zrušení rozhodnutí Komise 2000/709/ES[6], které stejnou problematiku upravovalo v rámci směrnice DirES. Vzhledem k tomu, že tyto subjekty mají podle eIDAS i DirES velmi podobný charakter, je pravděpodobné, že pro tyto subjekty budou nakonec stanovena i podobná kritéria. Ta by měla být vhodná pro subjekt povahy technických zkušeben či laboratoří. Mělo by se jednat zejména o požadavky na jejich technické vybavení, na kvalifikaci jejich pracovníků v oborech kryptologie a informačních technologií, na jejich organizační zajištění, finanční zázemí, odpovědnost, transparenci postupů a současně důvěrnost ohledně konkrétně získaných informací, nezávislost, zákaz střetu zájmů apod. Pro více srov. 6.10.3.

[4] European Union Agency for Network and Information Security.
[5] Do října 2017 Komise takový akt v přenesené působnosti nevydala.
[6] Rozhodnutí Komise 2000/709/ES ze dne 6. listopadu 2000 o minimálních kritériích, ke kterým by členské státy měly přihlížet při jmenování subjektů uvedených v čl. 3 odst. 4 směrnice 1999/93/ES.

Orgán členského státu určující a oznamující zkušebny. Čl. 30 odst. 1 a 2 eIDAS stanoví možnost určení zkušebny a následně povinnost členského státu určené zkušebny oznámit Komisi. Zjevně však za stát musí existovat orgán nebo úřad, který tyto činnosti bude mít v kompetenci.

Orgán členského státu oznamující certifikace. Podle čl. 31 odst. 1 eIDAS musí členský stát oznamovat vznik nebo zánik certifikací Komisi. Za členský stát zřejmě musí existovat orgán nebo úřad, který bude mít činnosti v kompetenci. Pravděpodobně se bude jednat o stejný orgán jako výše, tj. jeden orgán či úřad bude vykonávat povinnosti členského státu podle čl. 30 i podle čl. 31 eIDAS. Určení orgánu, úřadu, jeho kompetencí, popř. doplnění či provedení nařízení, je záležitostí vnitrostátní implementace. Její součástí by zřejmě měla být povinnost zkušebny nahlašovat orgánu státu provedené certifikace QSCD, popř. případy vypršení platnosti certifikace. Uvedené povinnosti nařízení eIDAS nepodřazuje do povinností orgánu dohledu, takže vnitrostátní implementace může stanovit i jiný subjekt.

Výrobce QSCD. Výrobce není v nařízení eIDAS vůbec zmíněn, ačkoli typicky by subjektem, který žádá o certifikaci u zkušebny měl být právě výrobce. Metodologie sepsání eIDAS nevylučuje zcela úplně (srov. 6.10.2 a 6.10.6), že ve vzácných případech může shodu prostředku s právními požadavky na QSCD potvrzovat sám výrobce.

Dodavatel QSCD. Ani dodavatel není v nařízení eIDAS vůbec zmíněn. I on může někdy být žadatelem o certifikaci u zkušebny, zejména v případě, pokud zastupuje výrobce, který na území EU vůbec nesídlí.

Komise má podle čl. 30 odst. 2 a čl. 31 odst. 2 eIDAS zpracovávat seznamy jí oznámených určených zkušeben a oznámených QSCD (pro více srov. 6.10.3).

6.1.6.3 Subjekty elektronické transakce

Podepisující osoba je podle čl. 3 bod 9 eIDAS *„fyzická osoba, která vytváří elektronický podpis“*. Protože je uvedena jako definiční náležitost elektronického podpisu prostého (čl. 3 bod 10 eIDAS), podle nařízení eIDAS jsou všechny druhy elektronického podpisu vytvořitelné jen a pouze fyzickou osobou.

Pečetící osoba je podle čl. 3 bod 24 eIDAS *„právnická osoba, která vytváří elektronickou pečeť“*. Je zmíněna jako náležitost vytváření zaručených a potažmo i kvalifikovaných elektronických pečetí. Tyto druhy elektronické pečeti nemůže

vytvářet jiný druh subjektu než právnická osoba. Pojem právnické osoby se má vykládat široce. Podle bodu odůvodnění 68 eIDAS se právnickými osobami *„rozumějí všechny subjekty, které byly založeny podle práva některého členského státu nebo se tímto právem řídí, bez ohledu na jejich právní formu"*.

Spoléhající se strana je dle čl. 3 bod 6) eIDAS *„fyzická nebo právnická osoba, která se spoléhá na ... službu vytvářející důvěru"*. Spoléhající se strana je definována jen vymezením se vůči určité službě vytvářející důvěru. Nepřímo pak i k poskytovateli této služby. Jelikož využívání služby vytvářející důvěru je možné i mimo kontext elektronické transakce, je třeba pojem chápat jen, anebo především, jako účastníka určitého právního vztahu k poskytovateli. Ten běžně vzniká po právní stránce bez smlouvy, pouze na základě právních ustanovení, zde podle nařízení eIDAS. Spoléhající se strana má podle čl. 24 odst. 4 eIDAS od kvalifikovaného poskytovatele právo na poskytnutí informace o tom, zda certifikát, na který se spoléhá, je platný, a to *„automatizovaným způsobem, který je spolehlivý, bezplatný a účinný"*. Spoléhající se strana, ale potenciálně i jiné subjekty, mohou těžit z odpovědnosti za škodu poskytovatele podle čl. 13 eIDAS. V článku 32 je význam pojmu spoléhající se strany posunut ve směru k autorem níže definovanému pojmu spoléhající se osoba.

Spoléhající se osoba. Budeme jí rozumět jakoukoli osobu či subjekt, která se spoléhá na elektronický podpis nebo na elektronickou pečeť. Dříve se v nauce pro ni používal pojem spoléhající se strany, který je však nově v nařízení eIDAS vymezen odlišně (srov. těsně výše). Spoléhající se osoba se spoléhá na elektronický podpis (ev. el. pečeť), rozhodující je tedy vztah k němu a k podepsané osobě. Pojem se vztahuje příjmo k digitálnímu objektu a potažmo subjektu dané elektronické transakce, nikoli k jejím zprostředkovatelům a podpůrcům. Spoléhající se osoba bývá často adresátem elektronické transakce. Může jí však být i jakákoli jiná třetí osoba, která se transakce přímo neúčastní, transakce jí je však například dokladována. Spoléhající se osobou může být i soud, který řeší spor mezi stranami transakce. Je velmi pravděpodobné, že v rámci spoléhání se spoléhající se osoby je zahrnuta aspoň jedna, často dvě nebo tři služby vytvářející důvěru, a tak bude spoléhající se osoba i spoléhající se stranou, někdy i vícenásobně. Není to však nutné zcela nezbytně. Pojem spoléhající se strany by rovněž neměl být vykládán v tom smyslu, že spoléhající se osoba musí využít službu vytvářející důvěru spočívající v *„ověřování shody a ověřování platnosti elektronických*

podpisů" (čl. 3 bod 9 eIDAS). Nemusí, uvedené může ověřit vlastními technickými prostředky. I to je dobrý důvod zavedení samostatného pojmu.

Subjekt veřejného sektoru je určen v čl. 3 bodu 7 eIDAS jako: *„státní, regionální nebo místní orgán, veřejnoprávní subjekt, sdružení vytvořené jedním nebo několika takovými orgány nebo jedním nebo několika takovými veřejnoprávními subjekty nebo soukromý subjekt, který byl alespoň jedním z těchto orgánů, subjektů nebo sdružení pověřen poskytovat veřejné služby, jedná-li na základě tohoto pověření"*. Zmíněný pojem veřejnoprávního subjektu se přebírá dle čl. 2 odst. 1 bodu 4 směrnice Evropského parlamentu a Rady 2014/24/EU, o zadávání veřejných zakázek. Rozumějí se jimi subjekty se všemi těmito vlastnostmi (tj. kumulativně):

> *„a) jsou založeny za zvláštním účelem spočívajícím v uspokojování potřeb obecného zájmu, které nemají průmyslovou nebo obchodní povahu;*
>
> *b) mají právní subjektivitu a*
>
> *c) jsou financovány převážně státem, regionálními nebo místními orgány nebo jinými veřejnoprávními subjekty; nebo podléhají řídicímu dohledu těchto orgánů nebo subjektů; nebo je v jejich správním, řídícím nebo dozorčím orgánu více než polovina členů jmenována státem, regionálními nebo místními orgány nebo jinými veřejnoprávními subjekty."*

Pro subjekt veřejného sektoru platí zvláštní povinnosti uznávání určitých druhů, formátů a metod elektronického podpisu, resp. elektronické pečetě podle čl. 27 eIDAS, resp. čl. 37 eIDAS. Tyto povinnosti se jej budou zejména týkat, když v rámci určité on-line služby je spoléhající se osobou (znění čl. 27 připouští i jiné výklady). Povinnost uznávání se však již netýká vlastního obsahu nebo formátů dokumentů.

6.1.6.4 Jiné subjekty

Příležitostně jsou v eIDAS zmíněny jiné druhy subjektů. Například:

Orgány pro ochranu údajů (čl. 17 odst. 4 písm. f eIDAS).

6.2 Hlavní koncepty nařízení eIDAS (elektronický podpis)

V této části kapitoly pojednáme o některých hlavních konceptech, které lze nalézt v nařízení eIDAS v souvislosti s elektronickým podpisem.

6.2.1 Strohost nařízení

Nařízení eIDAS v úpravě svého předmětu není úplné. Důsledkem je existence mnoha mezer, nejasností, ale kupodivu i některých nekonzistencí. S určitým

zjednodušením lze říci, že nařízení sestává jednak z definic mnoha pojmů, poté někdy z několika stručných požadavků na tyto pojmy a je završeno stanovením ne zcela zanedbatelných právních účinků (i důkazních), které některé právní pojmy získávají.

Vyšší podrobnost, nicméně stále nikoli vyčerpávající, má nařízení jen v oblasti služeb vytvářejících důvěru, jejich poskytovatelů a orgánů dohledu nad nimi.

Průběžně se v nařízení nacházejí zmocnění k vydání implementačních opatření Komisí, které však mají vesměs jen charakter technického upřesnění, často spočívají pouze v možnosti vyhlásit referenční čísla technických norem.

Roßnagel jej nejprve charakterizoval: „Nařízení eIDAS se různorodě omezuje stylem směrnice na stanovení cílů, ponechává však neupravených mnoho právních otázek, které jsou pro plnou regulaci ve formě rozhodnutí nezbytné.“ [7] Podle Jandta vedle několika kladných „lze uvést příliš mnoho kritických bodů na to, aby se dalo hovořit o přiměřené, pokrokové a objímající evropské harmonizaci“. [8] Důvodem mu jsou i neodpovídající důkazní účinky vůči příliš stručné obsažené úpravě.

Roßnagel po roce analýz shrnuje:[9] „Ve výsledku se ukazuje, že nařízení eIDAS pokrývá regulační potřebu služeb vytvářejících důvěru neúplně a podsložitě.[10] Nedosahuje vůbec úplnou harmonizaci právních podmínek, nýbrž pouze sjednocení některých rohových pilířů.“ Uvedená metafora s jednotnými pilíři, mezi nimiž se nachází příliš mnoho neupravené materie, je zcela výstižná.

Zajímavé zde ovšem je, že výše uvedená zjištění autora samého i dalších jsou již explicitně vyjádřena v úvodních ustanoveních o rozsahu působnosti. Nebylo třeba je dedukovat z analýz, dostačovalo si pozorně úvod nařízení přečíst a vyložit.

Podle článku 1 (Předmět) eIDAS nařízení, s *„cílem zajistit řádné fungování vnitřního trhu a současně usilovat o odpovídající úroveň bezpečnosti … služeb vytvářejících důvěru,"* jednak podle písm. b) *„**stanoví pravidla** pro služby vytvářející důvěru, zejména u elektronických transakcí;"* a podle písm. c) *„**stanoví právní rámec** pro elektronické podpisy, elektronické pečetě, elektronická časová razítka, elektronické*

---

[7] ROSSNAGEL, A. Neue Regeln für sichere elektronische Transaktionen, *Neue Juristische Wochenschrift.* 2014, s. 3686–3692, s. 3687.

[8] JANDT, S. Beweissicherheit im elektronischen Rechtsverkehr – Folgen der europäischen Harmonisierung. *Neue Juristische Wochenschrift*. 2015, s. 1205–1211, s. 1210.

[9] ROSSNAGEL, A. Der Anwendungsvorrang der eIDAS-Verordnung – Welche Regelungen des deutschen Rechts sind weiterhin für elektronische Signaturen anwendbar? *Multimedia und Recht*. 2015, s. 359–364, s. 364.

[10] V originále *„unterkomplex"*. České slovo *zjednodušeně* zde nevystihuje původní pojem.

dokumenty, služby elektronického doporučeného doručování a certifikační služby pro autentizaci internetových stránek" (zvýraznil autor).

Jinak řečeno, nařízení samo avizuje, že v oblasti služeb vytvářejících důvěru *stanoví pravidla*, zatímco pro ostatní zmíněné bezpečnostní mechanismy stanoví pouze *právní rámec*. Zákonodárce tedy upozorňuje, že zatímco pro jednu oblast vytváří pravidla (poměrně podrobnou úpravu), pro jiné oblasti pouze rámce.

Zde je na místě upozornit, že předchozí směrnice DirES se nazývala *„o rámci Společenství pro elektronické podpisy"* (z anglického *„on a Community framework for electronic signatures"*, pozdější český překlad názvu v úředním věstníku EU je zde nepoužitelný) a podle svého článku 1 (Obsah působnosti) směrnice *„Vytváří právní rámec pro elektronické podpisy a některé certifikační služby za účelem řádného zajištění funkce vnitřního trhu"* (překlad opět z anglického znění). Na základě směrnice vznikly transpozice v právních řádech členských zemí, které byly podstatně rozsáhlejší než sama směrnice.

Jestliže nyní nařízení ve svém předmětu opět vyjadřuje, že stanoví pouze rámec, pak tím nepřímo dává najevo, že by existující národní transpozice v daných záležitostech víceméně měly zůstat zachovány nebo nově vytvořeny, aby stále zaplňovaly „mnoho neupravené materie", která se nachází mezi pilířovými pojmy, resp. v právním rámci oblastí podle čl. 1 písm. c) eIDAS.

Jako správná metoda implementace se pak jeví z existujících národních transpozic pouze vypustit právní pojmy definované nově v nařízení eIDAS s tím, že se jiné regulované mechanismy v národním právu víceméně ponechají, přičemž se jen přizpůsobí jiným novinkám v nařízení. Jen některé úpravy týkající se dohledu poskytovatelů služeb jsou nově pokryty v nařízení poměrně podrobně a míra vypouštění obdobných úprav v národním právu bude poměrně vysoká.

Pochopitelně lze souhlasit s Roßnagelem výše, že zvolená forma nařízení je naprosto nevhodná pro případy pouze rámcové úpravy problematiky. Pro takový způsob úpravy slouží směrnice, které si členské státy transponují na míru a vhodně pro systematiku svého právního řádu. Problematika je pak celá upravena na úrovni národního práva.

Výsledek podle nařízení eIDAS naopak znamená, že na úrovni evropského práva se úpravou z nařízení eIDAS sice vynořují pilíře jednotných pojmů, mezi nimiž by však

prostor mělo zaplňovat právo jednotlivých členských států tak, aby právní regulace oblastí zůstala úplná. Takováto metoda právní regulace je pro adresáta právních norem velmi nepřehledná a nepohodlná na porozumění, protože ho nutí, aby přecházel z unijního práva do práva členského státu a zase nazpět v mnoha otázkách.

Zamýšlel-li evropský zákonodárce skutečně vytvořit tuto prolínací metodiku unijního a národního práva, měl to v nařízení, např. v bodech odůvodnění, dát najevo podstatně explicitněji. Byl by tím znatelně usnadnil aspoň pochopení. Řada vykladatelů nařízení se domnívá, aspoň na první čtení, že v nařízení se nachází úprava úplná.

Obdobné vyznění má i článek 2 (Oblast působnosti) eIDAS, neboť v jeho odst. 1 se stanoví vztahování se *„na poskytovatele služeb vytvářejících důvěru usazené v Unii"*. K úpravě práv a povinností podepisující osoby nebo spoléhající se osoby se nařízení tedy nehlásí ani v tomto článku.

Nakonec lze tento koncept nařízení odvozovat i z jeho samotného názvu, do kterého se dostalo pouze *„o ... službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu"*.

Uvnitř rámce, či přesněji řečeno mezi pilířovitou strukturou izolovaných pojmů unijního práva nebude vznikat tradiční právní mezera, ale celý shluk mezer. Jelikož se unijní právo uplatňuje vždy v rámci práva některého členského státu, může zde vzniknout několik situací. Kromě výše již uvedené situace, že je unijní právo nějak poměrně vhodně doplněno právním řádem členského státu, mohou vzniknout i případy, že členské státy mezery nedoplní v rámci implementace nařízení eIDAS vůbec. V takovém případě se národní soud může pokusit mezery vyplnit.

Zřejmě první možností by mělo být zaplnění mezer na základě unijního práva samotného. Autor shledává, že i když při práci na tomto textu věnoval zcela nadstandardní pozornost zvláštnostem unijního práva, není mu jasné, jak by mezery mohlo unijní právo zaplňovat spolehlivě či předvídatelně. Jen vzácně bude využitelný výklad podle užitečného účinku (srov. důvěryhodné seznamy níže). Určitou zcela specifickou metodou se v kontextu nařízení eIDAS, ale pouze něj, může stát spoléhání na doprovodné technické normy a specifikace, které jsou vyhlašovány Komisí prováděcími akty. Některé tyto specifikace snad budou určovat technické podmínky pro zařízení tak, že jeho uživatel, ať již je osobou podepisující, nebo spoléhající, nemůže za normálních okolností jednat chybně. Je však krajně sporné z partikulárních technických

specifikací a norem zpětně indukční metodou získávat pravidla, která by měla mít charakter závazných právních norem pro subjekty. Odporuje to i unijní zásadě právní jistoty, tj. požadavku na jasné a přesné právo. I kdyby se navzdory tomu tato metoda použila, nebude v řadě případů možné indukovat nebo implikovat práva nebo povinnosti ani pak jistě, neboť technická norma může být nerozhodná ohledně toho, který z více do úvahy připadajících subjektů má požadavky normy zajišťovat.

Druhou možností je zaplnit mezery na základě vnitrostátního práva. Autor zde připouští, že v rámci některých právních řádů (srov. 6.17) se nebude jednat o nijak nepřekonatelný úkol a daným národním soudům nebude zatěžko se jej zhostit. V případě jiných členských států se řešení jistě také najde, ale může být nepředvídatelné, a to i z hlediska očekávání různých stran elektronické transakce. Pravděpodobně by národní zaplňování mezer vedlo i na nejednotný výklad v rámci EU.

Roßnagel se zřejmě proto domnívá, že mezery nařízení bude třeba vyplňovat jednotlivými předběžnými otázkami národních soudů k SDEU, což považuje za metodu velmi pomalou i právně nejistou. Autor je názoru, že touto metodou by se právní pravidla nezískala pro celé nařízení eIDAS vůbec nikdy v reálné historické době a že stupeň právní nejistoty rozsudků od SDEU by byl tak vysoký a ty by byly tak obtížně zdůvodnitelné, že by SDEU učinil lépe, kdyby otázky vracel vesměs zpět národním soudům s tím, že řešení mezer je zde záležitostí národní implementace, a pokud ta chybí, pak metodiky výkladů a řešení takových situací ponechat národním soudům.

Autor je zde též názoru, že některé národní soudy (srov. 6.17) budou mít přirozenou tendenci zaplňovat mezery unijního práva svým vlastním národním právem. Při vzetí do úvahy toho, že právní jistota je stěžejní zásadou unijního práva, a při ohledu na zásadu respektu k národní identitě (čl. 4 odst. 2 SEU), spočívající v základních politických a ústavních systémech členských států, by i jiné členské státy měly mít právo zaplňovat mezery svým výkladem. Nejednotný výklad pilířovitých pojmů unijního práva nebo spíše vztahů vznikajících v oblasti mezer mezi nimi se autorovi jeví jako menší zlo než rezignace na právní jistotu, zejména pokud ta je zajišťována nebo požadavek na ní vyplývá z ústavního systému daného členského státu.

Při zvažování toho, proč uvedená situace vznikla, je třeba vzít v potaz i tu možnost, že se unijní zákonodárce snad snažil zůstat inertní vůči požadavkům jednotlivých právních řádů členských států na způsob provádění právního jednání a jeho

podmínky. Než aby se dostal do kolize a aplikační přednosti vůči nim, což by způsobilo možná i vážné narušení stěžejních oblastí soukromého práva, jako je uzavírání smluv, nechal většinu prostoru neupravenu vůbec. Taková legislativní technika tvorby unijního nařízení by pak byla vhodnou metodou. Body odůvodnění však měly být mnohem explicitnější ohledně toho, do jaké míry má právo členského státu nařízení implementovat ve smyslu doplnění.

Ať již bude výsledný způsob řešení obsažených právních mezer jakýkoli, nebude z hlediska požadavků na právo nikdy ideální. Výše zmíněný přístup autora sice přeci jen snižuje míru právní nejistoty, nemůže ale zamezit nepřehlednosti vznikající z prolínání národní a unijní úpravy. Níže (srov. 6.16) se proto snažíme určit alespoň hlavní problematické oblasti nařízení, které nemusí být ihned zřejmé.

6.2.2 Početnost implementačních opatření (zejména technickými normami)

Podstatným rysem nařízení je, že četné podrobnosti mají být implementovány Komisí. Tabulka níže uvádí zmocnění obsažená v nařízení eIDAS k implementačním opatřením k nařízení, jejichž provedení zákonodárce EU svěřil Komisi.

Ustanovení	Zmocnění Komise stanovit	Implementační opatření Komise
čl. 17 odst. 8	Formáty a postupy pro podávání výročních zpráv orgánem dohledu vůči Komisi (může).	
čl. 19 odst. 4 písm. a)	Upřesnění podmínek vhodných technických a organizačních opatření u PSVD (může).	
čl. 19 odst. 4 písm. b)	Formáty, postupy, lhůty pro ohlašování narušení bezpečnosti (může).	
čl. 20 odst. 4 písm. a)	Referenční čísla norem (může) pro - akreditace subjektů posuzování shody, - zprávy o posouzení shody.	
čl. 20 odst. 4 písm. b)	Referenční čísla norem pro pravidla auditu (může).	
čl. 21 odst. 3	Formáty a postupy pro oznámení a ověření zahájení poskytování SVD (může).	
čl. 22 odst. 5	Technické specifikace a formáty pro důvěryhodné seznamy (do 18. 9. 2015).	Prováděcí rozhodnutí Komise (EU) 2015/1505 ze dne 8. září 2015. Zmiňuje: • ETSI TS 119 612 v2.1.1
čl. 23 odst. 3	Podoba značky důvěry (do 1. 7. 2015).	Prováděcí nařízení Komise (EU) 2015/806 ze dne 22. května 2015.
čl. 24 odst. 5	Referenční čísla norem pro důvěryhodné systémy a produkty pro QPSVD (může).	
čl. 27 odst. 4, čl. 37 odst 4	Referenční čísla norem pro splňování požadavků na zaručené elektronické podpisy, resp. zaručené elektronické pečetě (může).	
čl. 27 odst. 5, čl. 37 odst. 5	Referenční formáty zaručených elektronických podpisů, resp. elektronických pečetí nebo referenční metody, jsou-li používány alternativní formáty, uznávaných subjekty veřejného sektoru (do 18. 9. 2015).	Prováděcí rozhodnutí Komise (EU) 2015/1506 ze dne 8. září 2015. Zahrnuje uznání na úrovni B, T nebo LT • ETSI TS 103171 v.2.1.1 – profil XAdES, • ETSI TS 103173 v.2.2.1 – profil CAdES,

		• ETSI TS 103172 v.2.2.2 – profil PAdES, nebo • ETSI TS 103174 v.2.2.1 – kontejner s přidruženým podpisem
čl. 28 odst. 6, čl. 38 odst. 6	Referenční čísla norem pro splňování požadavků na kvalifikované certifikáty pro elektronický podpis, resp. pro kvalifikované certifikáty pro elektronickou pečeť (může).	
čl. 29 odst. 2, čl. 39 odst. 1	Referenční čísla norem certifikací pro splňování požadavků na QSCD, resp. QSealCD (může).	
čl. 30 odst. 3, čl. 39 odst. 2	Seznam norem pro posuzování bezpečnosti produktů informačních technologií (sestaví).	Prováděcí rozhodnutí Komise (EU) 2016/650 ze dne 25. dubna 2016, kterým se stanoví normy pro posuzování bezpečnosti kvalifikovaných prostředků pro vytváření elektronických podpisů a pečetí podle čl. 30 odst. 3 a čl. 39 odst. 2 eIDAS. Stanoví normy pro obecné metodologické rámce: • ISO/IEC 15408, • ISO/IEC 15408-1:2009, • ISO/IEC 15408-2:2008, • ISO/IEC 15408-3:2008, • ISO/IEC 18045:2008. Dále stanoví profily ochrany (PP): • EN 419 211 • EN 419211-1:2014 • EN 419211-2:2013 • EN 419211-3:2013 • EN 419211-4:2013 Nezávazně (orientačně) zmiňuje profily ochrany zahrnující komunikaci QSCD s aplikací vytvářející elektronický podpis: • EN 419211-5:2013 • EN 419211-6:2014 Zatím chybí: normy pro metodiku posuzování bezpečnosti v případě vzdálených podpisů.
čl. 30 odst. 4	**Delegačními akty:** zvláštní kritéria na subjekty certifikující bezpečnost produktů informačních technologií (může).	
čl. 31 odst. 3, čl. 39 odst. 3	Formáty a postupy použitelné pro oznamování certifikací a ukončení certifikací QSCD, resp. QSealCD členským státem (může).	
čl. 32 odst. 3, čl. 40	Referenční čísla norem pro splňování požadavků na ověřování platnosti QES, resp. QESeal (může).	
čl. 33 odst. 2, čl. 40	Referenční čísla norem pro splňování požadavků činnosti kvalifikované služby vytvářející důvěru ověřování platnosti QES, resp. QESeal (může).	
čl. 34 odst. 2, čl. 40	Referenční čísla norem pro splňování požadavků činnosti kvalifikované služby vytvářející důvěru uchovávání platnosti QES, resp. QESeal (může).	
čl. 42 odst. 2	Referenční čísla norem pro splňování požadavků na kvalifikované elektronické časové razítko (může).	
čl. 44 odst. 2	Referenční čísla norem pro splňování požadavků činnosti kvalifikované služby vytvářející důvěru elektronického doporučeného doručování (může).	
čl. 45 odst. 2	Referenční čísla norem pro splňování	

	požadavků na kvalifikované certifikáty pro autentizaci internetových stránek (může).	

Tab. 3 – Přehled zmocnění Komise k implementačním opatřením pro služby vytvářející důvěru

Není-li v tabulce výslovně uvedeno zmocnění k delegačnímu aktu (pro zmocnění čl. 30 odst. 4 eIDAS), jedná se vždy o zmocnění k prováděcímu aktu.

Tento text se sice podrobně nezabývá kapitolou II nařízení eIDAS o elektronické identifikaci, pro úplnost a přehlednost jsou však v níže uvedené tabulce uvedena i zmocnění Komise k implementaci nařízení v této části.

Ustanovení	Zmocnění Komise stanovit	Implementační opatření Komise
čl. 8 odst. 3	Minimální technické specifikace, normy a postupy, jejichž pomocí jsou vymezeny nízká, značná a vysoká úroveň záruky prostředků pro elektronickou identifikaci (do 18. 9. 2015).	Prováděcí nařízení Komise (EU) 2015/1502 ze dne 8. září 2015.
čl. 9 odst. 5	Okolnosti, formáty a postupy pro oznamování systému identifikace členským státem Komisi (může).	Prováděcí rozhodnutí Komise (EU) 2015/1984 ze dne 3. listopadu 2015.
čl. 12 odst. 7	Procesní opatření pro spolupráci mezi členskými státy v oblasti elektronické identifikace (do 18. 3. 2015).	Prováděcí rozhodnutí Komise (EU) 2015/296 ze dne 24. února 2015.
čl. 12 odst. 8	Rámec interoperability (do 18. 3. 2015).	Prováděcí nařízení Komise (EU) 2015/1501 ze dne 8. září 2015 o rámci interoperability.

Tab. 4 – Přehled zmocnění Komise k implementačním opatřením pro elektronickou identifikaci

U elektronické identifikace se vždy jedná o zmocnění k prováděcímu aktu.

6.2.3 Akcent na služby vytvářející důvěru

Pro nařízení eIDAS je typické, že vyšší míru podrobnosti úpravy má v oblasti poskytování služeb vytvářejících důvěru [čl. 1 písm. b) eIDAS], jejich poskytovatelů a dohledu nad poskytovateli než v oblasti digitálních objektů, jako je příkladmo kvalifikovaný elektronický podpis, které by měly být cílem regulace. Nařízení budí až dojem, že jeho účelem je možnost poskytovat uvedené služby, a nikoli mít úpravu digitálního objektu, s jehož pomocí se stvrzují elektronické transakce.

6.2.4 Relativní zvýšení/snížení požadavků na poskytovatele služeb

Směrnice DirES obsahovala poměrně málo požadavků na poskytovatele certifikačních služeb. Zejména však podle čl. 3 odst. 1 DirES neměla činnost poskytovatelů certifikačních služeb podléhat jakémukoli předběžnému povolení, a to ani v případě poskytovatelů, kteří vydávali kvalifikované certifikáty.

Nařízení eIDAS ve srovnání s DirES podstatně zvyšuje počet i druh požadavků na poskytovatele, kteří se nově označují jako poskytovatelé služeb vytvářejících důvěru. V případě kvalifikovaných poskytovatelů služeb vytvářejících důvěru se poskytovatel musí předem podrobit auditu (čl. 21 odst. 1 eIDAS) a výslednou zprávu o posouzení shody předložit orgánu dohledu společně s oznámením o úmyslu zahájit její poskytování. Orgán dohledu zprávu o posouzení shody vyhodnotí, provede rozhodnutí o udělení statusu kvalifikovaného poskytovatele pro danou kvalifikovanou službu. Teprve po zveřejnění daného poskytovatele a jeho kvalifikované služby v důvěryhodném seznamu (čl. 21 odst. 3 eIDAS) smí daný poskytovatel zahájit poskytování dané kvalifikované služby. Činnost kvalifikovaného poskytovatele tak podléhá předběžnému dohledu. V úrovni unijního práva se proto nařízení eIDAS jeví výrazně přísnější, než byla směrnice DirES.

K jinému výsledku srovnání však dojdeme, pokud porovnáme podmínky nařízení o činnosti poskytovatelů v eIDAS s dosud platným právem členských států v této oblasti, tj. s výslednými transpozicemi DirES. Členské státy totiž běžně využily čl. 3 odst. 7 DirES, který členským státům umožnil *„používání elektronických podpisů ve veřejném sektoru podmínit případnými doplňujícími požadavky"*. Členské státy pak typicky stanovily podmínky akreditace poskytovatele certifikačních služeb, který vydával kvalifikované certifikáty, čímž byla rovněž zajištěna již předběžná kontrola těchto poskytovatelů. Navíc výčet podmínek pro akreditace poskytovatelů byl zpravidla mnohem podrobnější, než stanoví nařízení eIDAS. Lze uzavřít, že ve srovnání s dosud platným právem v členských státech u kvalifikovaných poskytovatelů vesměs nedošlo ke změně ohledně podmínky předběžnosti dohledu. V oblasti množství a úrovně požadavků pak došlo spíše k jejich snížení.

6.2.5 Pokrytí více scénářů PKI a snížení požadavků na QSCD/QES

V době tvorby směrnice DirES nebylo zcela jasné, jaké druhy zařízení budou vyvinuty pro účel tzv. *prostředku pro bezpečné vytváření podpisu* (v angličtině *secure-signature-creation device*, z toho užívaná zkratka SSCD). Ty měly splňovat požadavky podle přílohy III DirES. Ty na první čtení téměř budily dojem, že SSCD by mohlo být čistě jednoúčelovým zařízením, které by data, která mají být podepsána, samostatně i zobrazovalo a poté vytvářelo elektronický podpis úrovně kvalifikovaného elektronického podpisu (QES). Ve skutečnosti k takovému rozvoji nikdy nedošlo. Již německé znění DirES obsahovalo pro SSCD zápis *sichere Signaturerstellungseinheit*, tj.

nikoli prostředek, ale jednotka. Dominantní výpočetní platformou tehdy byly osobní počítače s operačním systémem Microsoft Windows a uživatelé informačních technologií nejevili žádný zájem o pořizování jakéhokoli zcela jednoúčelového zařízení, byť by nabízelo možnost velmi bezpečného vytvoření elektronického podpisu.

Jako SSCD byly nejčastěji vyvinuty kryptografické čipové karty *(cryptographic smartcards)*, jež jsou podobné moderním kreditním kartám, které dnes již též bývají vybaveny čipem[11]. Pro jejich použití však bylo nutné mít jako periferii připojenu k PC čtečku čipových karet, což představovalo z hlediska uživatelů další diskomfort a náklad. Tyto technologie jsou nicméně používány dodnes a představují asi nejbezpečnější běžně používané provedení SSCD pro vytváření QES. Nejbezpečnější čtečky čipových karet obsahují i vlastní klávesnici pro zadávání PIN, popř. i menší displej, na němž lze srovnat kontrolní součty vůči aplikaci vytvářející podpis, která běží na PC. S takovou čtečkou a kvalitní kryptografickou kartou si uživatel může být jist, že nedojde k záznamu jeho PIN skrytým softwarem,[12] i si může být poměrně dostatečně jist, že podepisuje skutečně ten dokument, který na svém displeji vidí zobrazen.

Mírně slabší varianout SSCD byly kryptografické tokeny, které se připojují do portu USB.[13] Zahrnují v sobě funkce čipové karty i čtečky, ovšem s tím, že neumožňují na sobě mít klávesnici ani žádný displej.

Uvedené dvě provedení SSCD byly a jsou dodnes standardní. Jejich nevýhodou nicméně je, že potřebují určitou odbornost při instalaci na počítač, jakož i manipulaci s fyzickými součástmi, jako jsou čipová karta, čtečka nebo token.

Zhruba po roce 2006 se začala na trhu objevovat řešení, která nabízela vzdálenou úschovu dat pro vytváření podpisu i vytváření podpisu. Výhodou bylo, že uživatel nemusel do své výpočetní platformy připojovat vůbec žádná fyzická zařízení. Teoreticky možnou výhodou je i potenciálně vyšší kryptografická kvalita a ochrana zařízení, které uchovává data pro vytváření podpisu u poskytovatele. Nevýhodou je určité snížení bezpečnosti na výpočetní platformě podepisující osoby. Poskytovateli služby, který spravuje vaše data pro vytváření podpisu, musíte též téměř neomezeně důvěřovat, že všechny technologie, organizaci i procesy má zavedeny zcela správně.

[11] Okolo roku 2000 většina bankovních nebo platebních karet čipy vybavena nebyla, mívaly pouze embosované číslice a magnetický proužek.
[12] Zadaný PIN se do PC vůbec nepřenáší, pouze do čipové karty.
[13] Tyto tokeny se navenek podobají pamětím flash pro port USB, jejich funkce je však zcela odlišná.

V některých členských státech (např. v Německu) nebyl tento koncept zařízení jako SSCD nikdy dovolen, v jiných (např. v Rakousku) došlo k jejich certifikaci.

Mezitím se dominantní výpočetní platformou pro osobní používání stávaly stále více tzv. chytré telefony.

Nařízení eIDAS se snaží, zřejmě v reakci na nepříliš úspěšnou penetraci zařízení SSCD v populaci a používání QES, zjednodušit podmínky pro vytvoření a použití QES. Mírně nově formuluje definice a požadavky na QES a QSCD (které nahradilo pojem SSCD) tak, aby pokud možno byly vytvořitelné tyto *formy provedení QSCD*:

1. Osobní počítač s čipovou kartou nebo tokenem (tradiční provedení).
2. Mobilní telefon, který má uložen data pro vytváření podpisu ve svém zvláštním bezpečnostním modulu.
3. Elektronický podpis vytvářený na dálku (ať již je vytvoření iniciované na mobilu, na osobním počítači, či na tabletu).
4. Inovativní řešení, jež dosud mohou být i zcela neznámá.

Třetí provedení explicitně zmiňuje bod odůvodnění 52: *„Vytváření elektronického podpisu na dálku, jehož prostředí spravuje poskytovatel služeb vytvářejících důvěru jménem podepisující osoby, přináší mnohé ekonomické výhody, a bude tedy pravděpodobně stále častější."* Taková řešení a služby bude moci podle stejného bodu odůvodnění poskytovat pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru. Zmiňuje je i bod odůvodnění 55 v rámci proklamace otevření se inovačním řešením a službám, kde zřejmě spadají pod *„podepisování v cloudech"*. V normativní části třetí provedení plyne i z reformulace požadavku na zaručený elektronický podpis podle čl. 26 písm. c) eIDAS: *„je vytvořen pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou."* Dřívější text směrnice DirES vyžadoval *„vytvoření pomocí prostředků, které podepisující může udržet pod svou výhradní kontrolou"* [čl. 2 odst. 2 písm. c) DirES]. Rozdíl představuje **první zásadní snížení úrovně** bezpečnostních požadavků, neboť se odstraňuje výhradní kontrola nad všemi prostředky (nejen tedy QSCD), které podepisující osoba měla používat pro vytvoření zaručeného elektronického podpisu. Navíc se snížila i míra výhradnosti. V normativní části odpovídá novému podepisování na dálku i přidání odstavců 3 a 4 v příloze II eIDAS.

Druhé provedení je výslovně zmíněno v bodu odůvodnění 55 jako *„podepisování prostřednictvím mobilního telefonu"*. Je opět důvodem, proč v tomto smyslu vykládat některé normativní části, zejména snížení požadavku na výhradní kontrolu z článku 26 písm. c), na jen *„s vysokou úrovní důvěry"*. Český překlad eIDAS zde není zcela přesný, anglický text zní *„with a high level of confidence"*, tj. *„s vysokou úrovní přesvědčení"*. Jak bylo kritizováno na jednom z workshopů,[14] není zde z nařízení vůbec jasné, zda se má jednat o objektivizované přesvědčení, nebo o subjektivní přesvědčení, popř. o přesvědčení kterého subjektu se má jednat, popř. jaké odborné znalosti se mají u daného subjektu předpokládat. Vyjádření tehdy poskytnuté pracovníkem Komise bylo, že smyslem mělo být snížit rezolutnost formulace. Tím se tedy zřejmě hodlalo více vyjít vstříc tomu, že u praktických realizací technologiemi může být obtížné zcela rezolutně tvrdit, že nemohou nikdy selhat. Dle názora autora je však podmínku třeba vykládat jako požadavek velmi vysoké úrovně přesvědčení a jako přesvědčení osoby s odbornými znalostmi. K tomuto závěru autor dochází především proto, jelikož jakékoli další snížení by vedlo prakticky ke znehodnocení celého rámce metodik, smyslu a účelu nařízení eIDAS.

Čtvrté provedení plyne z bodu odůvodnění 26, který stanoví, že *„vzhledem k tempu technologických změn by toto nařízení mělo přijmout přístup, který je otevřený inovacím"*. Otevřenost inovacím konkrétněji zmiňuje již citovaný bod odůvodnění 55 ve spojení s podepisováním pomocí mobilních telefonů a v cloudu. Obě oblasti považuje za inovační. Je však důležité zdůraznit, že jednak výčet je pouze demonstrativní, jednak anglické i německé znění hovoří spíše o mobilním podepisování *(mobile signing*, *Mobil-Signierung)*. Jsou tedy představitelná i jiná inovační řešení mobilního podepisování, například podpis elektronickými hodinkami, podpis provedený palubní jednotkou vozidla apod. Myslitelná je doslova jakákoli utopie z dnešního pohledu, dokud technické řešení bude schopné plnit podmínky článku 26 eIDAS o zaručeném elektronickém podpisu, bude realizovatelné a praktické. Pochopitelně je možná i jakákoli kombinace s podepisováním v cloudu, resp. vytvářením elektronického podpisu na dálku. V normativní části je prostor inovativním řešením otevřen v čl. 30 odst. 3 písm. b) eIDAS, kde se ovšem stanoví, že certifikace takového řešení musí dosáhnout srovnatelné úrovně bezpečnosti. Etalonem úrovně bezpečnosti jsou zatím

[14] KMENT, V. Evropské nařízení eIDAS: Impuls pro sjednocení elektronického podpisu a identifikace v EU. *Jurisprudence.* 2014, č. 6, s. 25–35.

pouze řešení pro první provedení, která spadají pod čl. 30 odst. 3 písm. a) eIDAS (více srov. 6.10).

Další snížení požadavků na QES plyne z jedné z mála spojnic, které v nařízení eIDAS existují mezi kapitolami II a III. Podle čl. 24 odst. 1 a jeho písm. b) eIDAS může kvalifikovaný poskytovatel při vydávání kvalifikovaného certifikátu[15] ověřit totožnost a případně zvláštní znaky fyzické nebo právnické osoby, jíž je kvalifikovaný certifikát vydáván nepřímo *„tím, že se v souladu s vnitrostátním právem spolehne na třetí osobu: ... na dálku s využitím prostředku pro elektronickou identifikaci, u něhož byla před vydáním kvalifikovaného certifikátu zajištěna fyzická přítomnost fyzické osoby nebo oprávněného zástupce právnické osoby a jenž splňuje požadavky stanovené v článku 8, pokud jde o značnou nebo vysokou úroveň záruky"*.

Nařízení eIDAS tedy připouští **ověřování totožnosti a znaků osoby na dálku**, tj. bez fyzické přítomnosti fyzické osoby nebo zástupce právnické osoby. A dokonce se smí jednat o identifikační prostředek jen značné úrovně záruky [čl. 8 odst. 2 písm b) eIDAS], tj. který nabízí jen: *„**značnou** míru spolehlivosti u deklarované nebo uváděné totožnosti určité osoby a je charakterizován pomocí ... [opatření] ..., jejichž účelem je **značně snížit** riziko zneužití nebo změny totožnosti"* (zvýraznil autor).

Na druhé straně je vhodné upozornit, že požadavek *„souladu s vnitrostátním právem"* umožňuje členskému státu zde nařízení implementovat tak, že možnost ověřování na dálku efektivně potlačí. Pravděpodobně je též dovolené, aby právem členského státu bylo dovoleno používat jen prostředky vysoké úrovně záruky.

Členský stát ovšem nemůže vyloučit, že u osoby certifikované kvalifikovaným poskytovatelem, který působí podle práva jiného členského státu, byla totožnost aj. znaky osoby ověřeny pouze na dálku a jen s prostředkem značné úrovně záruky. Jeho subjekty veřejného sektoru musí i kvalifikované nebo zaručené elektronické podpisy takové osoby podle čl. 27 eIDAS přeshraničně uznávat.

Uvedené relaxace podmínek mohou vést k vyššímu rozšíření kvalifikovaného a zaručeného elektronického podpisu. Současně bezpochyby znamenají i obecné snížení záruk bezpečnostní úrovně kvalifikovaného elektronického podpisu. V závislosti na předpokládaném případu užití to může být prospěšné, ale i právě naopak.

[15] Do úvahy přicházejí všechny druhy kvalifikovaných certifikátů upravené v eIDAS, tedy pro elektronické pečetě, pro elektronické podpisy, pro autentizaci internetových stránek.

6.2.6 Priorita formy pro automatické zpracování pro ověření platnosti

Ve všech níže uvedených případech, kdy připadá do úvahy více podob určité informace, nařízení eIDAS důsledně vyžaduje přítomnost informace ve formě vhodné pro automatické zpracování. Takovou informaci dokáže přečíst, významově jí porozumět a vyložit i jen technický systém, například programové vybavení. Není nutné, aby na vyhodnocování daných informací byla zúčastněna jakákoli lidská osoba.

Z obsahu kvalifikovaného certifikátu pro elektronické podpisy[16] musí být podle přílohy I eIDAS patrné *„alespoň ve formě vhodné pro automatické zpracování"*, že se certifikát vydává jako kvalifikovaný certifikát pro elektronický podpis (písm. a) a popř. též že data pro vytváření elektronických podpisů jsou obsažena v kvalifikovaném prostředku pro vytváření elektronických podpisů (písm. j). V návaznosti na tento kvalifikovaný certifikát, alespoň na základě takového certifikátu, musí podle čl. 24 odst. 4 eIDAS kvalifikovaný poskytovatel poskytnout *„informace o platnosti nebo o zneplatnění kvalifikovaných certifikátů"*, a to *„kdykoli i po skončení doby platnosti certifikátu, automatizovaným způsobem, který je spolehlivý, bezplatný a účinný"*.

Pro hodnocení stavu kvalifikovanosti poskytovatele a jím poskytovaných služeb vytvářejících důvěru je důležitý takzvaný důvěryhodný seznam. Jeho obsah je upraven v nařízení eIDAS a vydává ho každý členský stát. I důvěryhodný seznam musí být podle čl. 22 odst. 2 eIDAS zřízen, udržován a zveřejňován *„ve formě vhodné pro automatické zpracování"*.

Důsledkem výše uvedených požadavků následně je, že **celý postup ověření platnosti** kvalifikovaného elektronického podpisu podle článku 32 eIDAS je **možné automatizovat** (srov. výklad v 6.11.2). To je téměř jistě i cíl systematického zavedení uvedených dílčích požadavků výše. Právě z hlediska dosažitelnosti tohoto cíle je proto třeba jednotlivé požadavky i hodnotit a vykládat, včetně ustanovení souvisejících.

Nařízení umožňuje provádět ověření platnosti kvalifikované elektronického podpisu nejen přímo postupem podle článku 32 eIDAS, ale tuto operaci poskytovat i jako kvalifikovanou službu vytvářející důvěru podle článku 33 eIDAS. Právě proto, že ověření platnosti podle článku 32 eIDAS je automatizovatelné obecně, automatizovaně jej může provádět i kvalifikovaný poskytovatel takové služby. Je pak logické, že podle

[16] Obdobně platí pro kvalifikovaný certifikát pro elektronickou pečeť dle přílohy III.

čl. 33 odst. 1 písm. b) eIDAS i výsledek ověření platnosti kvalifikovaným poskytovatelem musí být spoléhající se straně poskytnut *„automatizovaným způsobem"*.

Uvedené požadavky na automatizovatelnou formu nebyly obsaženy v DirES ohledně kvalifikovaných certifikátů vůbec, a to ani v případě příznaku, že se vůbec jedná o kvalifikovaný certifikát [příloha I písm. a) DirES]. Ani v případě informací o zneplatnění kvalifikovaného certifikátu nebyla podmínka automatizovaného získávání zmíněna (např. chybí v příloze II DirES), ačkoli fakticky v praxi splňována zřejmě byla.

Důvěryhodné seznamy byly zavedeny rozhodnutím Komise 2009/767/ES, přičemž dle jeho čl. 2 odst. 2 se zřizovala jen verze čitelná okem. Až novelizací prováděcím rozhodnutím Komise 2013/662/EU došlo k zavedení *„důvěryhodného seznamu ve strojově zpracovatelné podobě"* v čl. 3 písm. a) rozhodnutí 2009/767/ES. Nařízení eIDAS zde pokračuje v prosazování této podoby jako hlavní použité.

6.2.7 Regulační koncept nařízení

Právní základ nařízení se odvolává na čl. 114 SFEU, body odůvodnění pak konkrétněji na podporu vnitřního trhu a elektronických transakcí na něm (srov. výše 6.1.4). Podstatou článku 114 SFEU je sbližování nebo-li **harmonizace** právních řádů členských států EU. K tomu uvádí Svoboda, že „v právu EU však nejde o proces postavený na vzájemnosti, ale na jednosměrnosti".[17] Vnitrostátní právní řády se mají přizpůsobit unijnímu právu. Harmonizace se provádí „normotvorným uplatňováním práva", které je členskému státu předepsáno sekundárním aktem práva EU, typicky však směrnicí. Oproti tomu nařízení je podle Svobody metodou právní **integrace**.[18] Svoboda připouští, že se i pro účel harmonizace někdy používala nařízení, ovšem zpravidla se jednalo o tzv. rámcová nařízení, která dovyžadovala rozsáhlá doplnění či konkretizaci národní implementací, jejichž potřebu bohužel nařízení eIDAS výslovně neindikuje.

Srovnat rozpor právního základu a použité formy je dle autora možné tak, že za předmět harmonizace (tedy sbližování) se budou považovat elektronické transakce, pro něž pak nařízení jednotně upravuje různé *elektronické autentizační objekty nebo metody*, jakými jsou například elektronické podpisy, elektronické pečetě, elektronická časová razítka, elektronické dokumenty a dále též služby vytvářející důvěru a systémy elektronické identifikace. Takový přístup k harmonizaci v rámci vnitřního trhu by byl teoreticky možný.

[17] SVOBODA, P. *Úvod do evropského práva*. 5. vyd. Praha: C. H. Beck, 2013, s. 227.
[18] SVOBODA, P., cit. dílo, s. 227.

Podle Svobody se dle rozsahu úpravy může jednat o harmonizaci úplnou, minimální nebo opční.[19] Nejčastější má být úplná neboli maximální harmonizace, kdy unijní opatření zcela pokrývá předmět úpravy a členské státy nesmí mít své vnitrostátní právo ani přísnější, ani mírnější. Bývá to typické pro oblasti, které spadají do výlučné pravomoci EU. V případě minimální harmonizace mohou členské státy přidávat požadavky přísnější. Při opční jsou zachovány vnitrostátní i evropské předpisy vedle sebe a subjekt, typicky výrobce, si mezi nimi může vybrat. Budeme-li za předmět harmonizace považovat elektronické transakce, pak nařízení eIDAS představuje, až na některé výjimky,[20] pouze harmonizaci minimální. Právní úprava transakcí, ať již veřejnoprávních, nebo soukromoprávních, i nároky na její elektronickou podobu zůstávají nařízením v podstatě nedotčena.

Budeme-li za předmět harmonizace považovat elektronické autentizační objekty nebo metody, pak se nařízení na první pohled zřejmě snaží o dosažení harmonizace úplné. Na druhý pohled je již výše patrné (srov 6.2.1 o strohosti), že v oblasti elektronických autentizačních objektů a metod[21] samo indikuje, že je pouze rámcovým nařízením. Z naší analýzy jsme zjistili, že právní úprava má dokonce spíše charakter pilířovitých pojmů (srov 6.2.1), a nikoli rámce. Rámec i pilíře vypadávají z teorií uvažovaných způsobů harmonizace, rozhodně je nelze považovat za úplnou harmonizaci, ale ani za zbylé dva druhy. Teorií nejsou uvažovány zřejmě proto, že takový způsob regulace je nevhodný a neměl by být používán. I Svoboda uvádí, že z textu předpisu „se často nedozvídáme, o jaký model jde; proto také nemusí být jasné, zda a v jakém rozsahu zbývá prostor pro legislativní činnost členských států; tato nejistota bývá příčinou řady sporů".[22] Pokud harmonizace není úplná, členské státy dle Svobody mají možnost zachovat nebo přijmout vnitrostátní pravidla v daném poli působnosti, přičemž samozřejmě ale nesmějí být v rozporu s harmonizačními cíly opatření ani být nástrojem diskriminace nebo skrytého omezování.

Pouze v oblasti poskytovatelů služeb vytvářejících důvěru a dohledu nad nimi se nařízení blíží plné harmonizaci, byť i zde asi lze nalézt prostor přinejmenším pro konkretizaci, možná i doplnění.

---

[19] SVOBODA, P., cit. dílo, s. 231.

[20] Výjimkou je např. ekvivalance kvalifikovaného elektronického podpisu s vlastnoručním podpisem; zákaz přeshraničního využívání elektronických podpisů s vyšší mírou zajištění bezpečnosti, než je kvalifikovaný elektronický podpis pro on-line služby subjektů veřejného sektoru.

[21] Omezujeme se zde na část III a část IV nařízení eIDAS.

[22] SVOBODA, P., cit. dílo, s. 231. V pozn. pod čarou Svoboda odkazuje i na spor 227/82 *Van Bennekom*; C-315/92 *Clinique*.

Z hlediska metody úpravy Svoboda udává druhy harmonizace jako úplnou, alternativní nebo pomocí odkazu na technické normy.[23] Úplná neposkytuje možnost výběru, alternativní dává členským státům volnost vybrat si z více možností v opatření a harmonizace pomocí odkazů na normy je jen velmi obecná a v podrobnostech odkazuje na technické normy. Za předmět harmonizace má opět smysl uvažovat pouze oblast elektronických autentizačních objektů a metod. Z tohoto úhlu pohledu je nařízení eIDAS možné považovat za smíšený žánr druhé a třetí metody úpravy. Nařízení do značné míryChyba: zdroj odkazu nenalezen umožňuje členským státům, aby si z nabízených elektronických autentizačních objektů a metod, jakož i služeb vytvářejících důvěru vybraly ty, které chtějí. Současně však je v řadě záležitostí nařízení skutečně jen obecné a odkazuje na technické normy. V rámci metod odkazování na technické normy zná teorie v zásadě dva modely. Jednak takzvaný starý přístup, spočávající v rigidní a detailní harmonizaci, který se dodnes používá v oblasti vyšších rizik, jako jsou motorová vozidla, potraviny, chemické látky, léčiva. Zde se používají detailní harmonizace sektorovými směrnicemi nebo nařízeními.[24] V kontrastu k tomu se od roku 1985 používá i takzvaný nový přístup[25] *(New Approach)*. Pro jeho podrobný rozbor v textu viz 6.10.2.

V souvislosti s metodou technických norem Svoboda upozorňuje, že unijní právo zde musí řešit dvě záležitosti. První je stanovení technických norem pokud možno jednotně pro celou EU, tj. nahrazení národních technických norem technickými normami harmonizovanými, a to aspoň pro úroveň EU. Druhou otázkou je potvrzení shody, že určitý výrobek splňuje harmonizovanou technickou normu, tento postup se nazývá certifikací. Dle Svobody někdy vzniká potíž s uznáváním certifikace provedené v jiném členském státu, než ve kterém byla provedena.[26]

Z hlediska tohoto hodnocení nařízení eIDAS používá modifikovanou podobu *New Approach*, která je podrobně diskutována níže např. v 6.10.2, 6.10.3 a 6.10.6. Důvodem pravděpodobně je, že ačkoli se jedná o rizikovou oblast z hlediska právních jistot, je současně snaha používat přístup otevřený technickým inovacím. Částečně byl tento přístup i zděděn ze směrnice DirES.

---

[23] SVOBODA, P., cit. dílo, s. 231–232.

[24] SVOBODA, P., cit. dílo, s. 253–254. Citovány jsou: nař. 305/2011 – stavební materiály; směrnice 2009/105 – jednoduché tlakové nádoby; směr. 2009/48 – bezpečnost hraček; směr. 2006/42 – bezpečnost strojů; směr. 95/16 – výtahy; směr. 93/42 – lékařské implantáty; směr. 2004/108 elmag. kompatibilita atd.

[25] SVOBODA, P., cit. dílo, s. 253–254.

[26] SVOBODA, P., cit. dílo, s. 253–254.

Z hlediska obsahu regulace je třeba nařízení považovat za předpis převážně veřejného práva. Obdobně např. hodnotil Čermák ml.[27] i český zákon 227/2000 Sb., o elektronickém podpisu, který byl transpozicí směrnice DirES, tedy unijního předchůdce nařízení eIDAS. Uvedené platí navzdory tomu, že jím upravené elektronické autentizační objekty nebo metody mohou členské státy následně využít i v rámci úpravy soukromého práva, například pro potvrzování soukromého právního jednání. Stejně dobře je mohou využít i v rámci svého práva veřejného. A zatímco použití v rámci soukromého práva závisí v posledku na svobodné vůli jednajících osob, ve veřejném právu může být předepsáno jako povinné nebo jako jedna z alternativ povinného způsobu jednání.

Z hlediska správního dohledu nařízení obsahuje v zásadě 4 okruhy:

1. poskytování služeb vytvářejících důvěru a dohled nad nimi,
2. audit poskytovatele služeb vytvářejících důvěru,
3. certifikaci kvalifikovaných prostředků + důvěryhodných systémů a produktů,
4. oblast elektronická identifikace (kap. II nařízení).

6.3 Předmět a oblast působnosti nařízení

Předmět a oblast působnosti nařízení vymezují především články 1, 2 a 4. Jak jsme již výše uvedli, je vhodné zaznamenat rozdíl, že dle čl. 1 odst. písm. b) eIDAS nařízení **stanoví pravidla** pro *„služby vytvářející důvěru, zejména u elektronických transakcí"*, ovšem čl. 1 odst. písm. c) eIDAS pouze **stanoví právní rámec** pro *„elektronické podpisy, elektronické pečetě..."* aj. digitální objekty.

6.3.1 Oblast působnosti

Podle článku 2 odst. 1 eIDAS: *„Toto nařízení se vztahuje na systémy elektronické identifikace oznámené členskými státy a na poskytovatele služeb vytvářejících důvěru usazené v Unii."* Ze tří odstavců článku 2 se jedná o jediný, který oblast působnosti vymezuje pozitivně. Odhlédneme-li od systémů elektronické identifikace, má se nařízení vztahovat pouze na *poskytovatele služeb vytvářejících důvěru* a *usazených v Unii*. Zde je třeba připustit, že formulace nevystihuje působnost nařízení dostatečně. V nařízení se nachází řada ustanovení, které se vztahují na jiné subjekty (srov. přehled subjektů výše), a to i na takové, které nemusí nutně tvořit ani žádný přímý protějšek v právním vztahu s poskytovatelem služeb. Tento rozpor je

[27] ČERMÁK, K. ml., cit. dílo, s. 64.

možné vyložit pouze tak, že pozitivní vymezení v čl. 2 odst. 1 eIDAS je formulováno jen přibližně.

Pojem *služby vytvářející důvěru* je souborný pojem, který je definován v čl. 3 bodu 16 eIDAS (srov. 6.8), přičemž se jedná o postupy či metody odvozené od elektronického podpisu,[28] z nichž část je skutečně poskytována formou služeb a část může být prováděna i samostatně, na poskytovatelích nezávislými subjekty. Takovými příklady jsou vytvoření kvalifikovaného elektronického podpisu podepisující osobou nebo ověření platnosti kvalifikovaného elektronického podpisu přímo spoléhající osobou.

Zcela striktně neplatí dokonce ani druhé omezení na subjekty usazené v Unii. Článek 14 eIDAS umožňuje EU uzavírat mezinárodní dohody mezi EU a třetí zemí, resp. mezi EU a mezinárodní organizací o uznávání služeb vytvářejících důvěru pocházející ze třetí země, resp. z mezinárodní organizace. V takovém případě musí být mnoho požadavků z eIDAS recipováno do takové dohody. Čl. 14 eIDAS zde kupodivu nestanoví předpoklad zásady reciprocity pro uzavření takové dohody, tj. aby i služby poskytovatelů služeb vytvářejících důvěru usazených v Unii byly naopak uznávány v dané třetí zemi, resp. mezinárodní organizaci.

Cílem nařízení je podle čl. 1 odst. 1 *„zajistit řádné fungování vnitřního trhu"* a současně usilovat o *„odpovídající úroveň bezpečnosti ... služeb vytvářejících důvěru"*. Roßnagel pak tento cíl ve spojení se zásadou vnitřního trhu v čl. 4 odst. 1 eIDAS vykládá tak, že oblast působnosti nařízení je vymezena pouze tak, že „platí pro všechny poskytovatele usazené v Unii, pokud své služby nabízejí přeshraničně".[29] Vůči takovým službám pak dle čl. 4 odst. 1 eIDAS *„nesmějí existovat žádná omezení týkající se [jejich] poskytování ... z důvodů spadajících do oblastí, na něž se [nařízení] vztahuje"* a dle čl. 4 odst. 2 eIDAS se nařízení vyhovující služby a produkty *„mohou volně pohybovat na vnitřním trhu"*.

6.3.2 Vyloučení nařízení pro uzavřené systémy

V článku 2 eIDAS je působnost stanovena nejen pozitivně, ale i negativně. Dle čl. 2 odst. 2 eIDAS se nařízení *„nevztahuje na poskytování služeb vytvářejících důvěru, které jsou používány výhradně v rámci uzavřených systémů vyplývajících*

[28] ROSSNAGEL, A. *Das Recht der Vertrauensdienste : Die eIDAS-Verordnung in der deutschen Rechtsordnung.* 1. Auflage. Baden-Baden: Nomos, 2016, s. 43.
[29] ROSSNAGEL, A. *Das Recht ...,* cit. dílo, s. 44.

z vnitrostátního práva nebo z dohod mezi určeným okruhem účastníků". Předpokladem nevztahování jsou zde služby, nikoli poskytovatelé. Uzavřené systémy jsou pak z působnosti nařízení vyloučeny zcela, subjekty v jejich rámci se nemusí nařízením eIDAS řídit. Podle bodu odův. 21 eIDAS *„Požadavky tohoto nařízení by se neměly například vztahovat na systémy zavedené v podnicích nebo v orgánech veřejné správy za účelem řízení vnitřních postupů využívajících služby vytvářející důvěru. Měly by jim podléhat pouze služby vytvářející důvěru, které jsou poskytovány veřejnosti a které mají vliv na třetí osoby."* Zcela vyloučeny z působnosti nařízení jsou tak vnitřní systémy veřejné správy, pokud v jejich rámci případně využívané služby vytvářející důvěru nejsou poskytovány veřejnosti. Obdobně to platí i pro uzavřené systémy podniků nebo skupin.

6.3.3 Vyloučení nařízení pro pravidla kontraktace a formy [transakce]

Dle článku 2 odst. 3 eIDAS nařízením *„není dotčeno vnitrostátní právo ani právo Unie týkající se [jednak] uzavírání a platnosti smluv",* jednak *„jiných právních nebo procesních povinností týkajících se formy"*.

Nařízením tedy nejsou dotčeny žádné existující nebo v budoucnu vzniklé požadavky práva členského státu (ev. práva unijního), které se kladou na uzavírání a platnost smluv, ani jiné povinnosti týkající se formy [něčeho], a to i v případě, že se jedná o právní povinnost procesního druhu. Oním nevyřčeným něčím je zjevně pojem *transakce* nebo *právní jednání* v širokém slova smyslu, jak je probráno výše (6.1.4). Jelikož však nařízení vylučuje, že by tyto požadavky na formu ovlivňovalo, je třeba obsah pojmu stanovit z používaného práva členského státu (ev. unijního).

Tím, že se ustanovení nachází v článku nadepsaném oblast působnosti, je potřeba jej z hlediska systematického výkladu nařízení vyložit jako právní normu, která má přednost před jinými právními normami v nařízení se dále vyskytujícími, jež by s ní případně byly v rozporu.

Do úvahy pochyb přicházejí nejprve čl. 25 odst. 2 eIDAS o stejném právním účinku QES jako vlastnoručního podpisu a čl. 25 odst. 3 eIDAS o přeshraničním uznávaní QES. V obou případech má před aplikací těchto právních norem přednost otázka, zda rozhodné právo (některého členského státu, unijní) vůbec připouští elektronickou formu jednání (transakce).

Tuto otázku je třeba řešit systematickým výkladem rozhodného práva, přičemž pro její zodpovězení někdy může být třeba brát zpětně zřetel i na existenci úpravy elektronického podpisu v nařízení eIDAS, ale rozhodující kritéria budou v rozhodném právu, a nikoli v nařízení. Jinak řečeno uvedené znamená, že právní řád členského státu může pro určitá právní jednání (transakce) stanovit jen listinnou (papírovou) formu, která je pochopitelně potvrditelná pouze vlastnoručním podpisem. V případě, že právo připustí elektronickou formu, může i pro ni klást určité požadavky navíc, jako například použití určitého formuláře, včetně upřesnění požadovaného technického formátu. Pouze připouští-li právo určitou elektronickou formu a stanoví-li pro ni požadavky, které mají charakter (vlastnoručního) podpisu, může pro ně stanovit některou úroveň požadavků na elektronický podpis podle eIDAS. V případě on-line služby, která je (přeshraničně) poskytována subjektem veřejného sektoru, je v požadavcích právo omezeno článkem 27 eIDAS, že subjekt veřejného sektoru nesmí požadovat rozsáhlejší soubor požadavků na podpis, než jsou v nařízení stanoveny pro QES.

Obdobně Roßnagel: „stejně málo jako jako čl. 5 odst. 1 DirES, tak i čl. 25 odst. 2 eIDAS nemění předpisy na požadavky formy členských států."[30] V otázce této kolize je třeba pouze upozornit a připustit, že části odůvodnění v bodu 21 od věty *„Toto nařízení by se nemělo vztahovat ..."* (o výlukách z oblasti působnosti nařízení) a v bodu 49 odůvodnění *„kvalifikovaný elektronický podpis [by měl mít] rovnocenný právní účinek jako podpis vlastnoruční"* jsou navzájem rozporné, a to tak, že nelze určit, který bod odůvodnění by měl mít přednost. V normativní části nařízení však výše uvedený výklad jednoznačně podat lze.

Druhou oblastí pochyb někdy je článek 46 o neupírání právních účinků a neodmítání jako důkazu pouze z důvodu elektronické podoby u elektronického dokumentu. Zde je řešení snadnější než výše, neboť se jedná o procesní a procesně důkazní právní normu, pro případ soudního, popř. i některého správního řízení. Z té nelze vůbec nijak implikovat, jaké požadavky rozhodné právo stanoví na formu právního jednání (transakce). Pokud rozhodné právo připustí elektronickou formu, ale stanoví pro ni další náležitosti, například na formuláře nebo technické formáty, daný elektronický dokument může být odmítnut, ovšem s poukazem na neodpovídání požadavkům formy. I zde může odpovídající bod odůvodnění 63 působit zmatečně: *„...cílem této zásady je zajistit, aby elektronická transakce nebyla odmítnuta jen z toho*

[30] ROSSNAGEL, A. *Das Recht ...,* cit. dílo, s. 53–54.

důvodu, že dokument má elektronickou podobu". Transakce ale může být odmítnuta, pokud pro daný druh transakce rozhodné právo vylučuje elektronickou formu apriori vůbec, pokud stanoví přídavné požadavky na elektronickou formu (dokumentu), které nejsou splněny, popř. jedná-li se o soukromé právní jednání mezi subjekty, mezi kterými platí zásada smluvní svobody, kdy může její provedení v elektronické podobě odmítnout kterákoli ze stran. Pro další souladný diskurs srov. 6.15.1.

6.3.4 Vyloučení nařízení pro trestní právo [v oblasti přípustnosti důkazů]

Již při své první analýze[31] nařízení postřehl Roßnagel, že nařízení není účinné v oblasti trestního práva, a to přinejmenším z hlediska důkazních účinků. Podle čl. 82 odst. 1 SFEU justiční spolupráce *„zahrnuje [pouze] sbližování právních předpisů členských států"*, přičemž modelem má být dosažení vzájemného uznávání rozsudků a soudních rozhodnutí. Sbližování není sjednocením a úměrně tomu v čl. 82 odst. 2 SFEU je pro některé účely omezen prostředek, totiž že určené orgány EU mohou *„stanovit formou směrnic minimální pravidla"*, která se týkají *„vzájemné přípustnosti důkazů mezi členskými státy"*, nebo dalších, taxativně vymezených možností.

Legislativní akt formy nařízení podle práva EU tedy není platným pramenem práva pro oblast trestního práva z hlediska přípustnosti vzájemných důkazů mezi členskými státy. Pravomoc vydávat nařízení v oblasti trestního práva a justiční spolupráce zde nebyla na EU přenesena.

Další vada případné platnosti pro tento účel spočívá i v procesu přijetí. Legislativní akt pro tuto oblast zřejmě musí od počátku v bodech odůvodnění obsahovat určení právního základu podle čl. 82 odst. 2 SFEU, aby členský stát měl přídavnou možnost modifikovat postup přijetí aktu v souladu s čl. 82 odst. 3 SFEU, tj. požadovat zabývání se návrhem Evropskou radou. Návrh zjevně musí obsahovat i další odůvodnění, jež dokládají oprávněnost obsahu nařízení, která v návrhu nařízení eIDAS ani v jeho výsledném znění obsažena nebyla a nejsou.

Z tohoto důvodu se autor domnívá, že nařízení se bez dalšího nemůže ani zpětně stát platným aktem pro oblast trestního práva v oblasti přípustnosti vzájemných důkazů, kdyby snad někdy v budoucnosti zakládací smlouvy i pro tuto oblast trestního práva připustily formu nařízení.

[31] ROSSNAGEL, A. Neue Regeln ..., cit. dílo, s. 3691.

6.4 Elektronický podpis (prostý)

Pro posouzení definice elektronického podpisu (prostého) z eIDAS je důležité analyzovat nejen jeho stručnou definici, ale zjistit i to, co se v ní již nenachází. To vyplyne ze srovnání s dosud platnými úpravami v DirES.

Dle směrnice DirES, zrušené od 1. 7. 2016 nařízením eIDAS, platilo dle čl. 2 bod 1, že elektronický podpis (prostý) jsou *„data v elektronické podobě, která jsou připojena nebo logicky spojena s jinými elektronickými daty, a která slouží jako metoda autentizace“*. Podpis jsou první data (v elektronické podobě), která slouží jako metoda autentizace druhých elektronických podepsaných dat. Autentizací je zde třeba rozumět ověření pravosti, tedy původnosti (data zůstala stejná) a původu (kdo, co je podepsal) podepsaných dat. Definice podle DirES obsahovala *autentizaci*, ale nevyžadovala identifikaci původu ani druh původce. Tím nemusela být jen fyzická osoba.

Definici podle DirES by kupř. vyhověl hypotetický digitální fotoaparát,[32] který by elektronicky podepisoval všechny vyfocené fotografie, než by je zapsal na paměťovou kartu. U výstupní fotografie by tak bylo například možné zjistit, že nebyla nijak upravena editorem obrázků[33] a že vznikla ve fotoaparátu určitého výrobce. Nemuselo by ale být nutně známo jedinečné sériové číslo fotoaparátu (identifikace) ani kdo fotoaparát ovládal a mačkal spoušť (fyzická osoba). Přesto by takový elektronický podpis byl užitečný například pro zvýšení přesvědčivosti důkazního použití jím pořízených digitálních fotografií. Podle čl. 5 odst. 2 DirES by takovému elektronickému podpisu obecně nesměly být upírány právní účinky ani důkazní přípustnost.[34]

Dle čl. 3 bodu 10 nového nařízení eIDAS se **elektronickým podpisem** rozumí: *„**data** v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a **která podepisující osoba používá k podepsání**“* (zvýraznil autor).

Podstatné je, že z definice eIDAS byl vyňat požadavek *autentizace*. Není již požadováno, aby z podpisu (z prvních dat) byla ověřitelná pravost druhých podepsaných dat.

---

[32] Existence takového fotoaparátu není autorovi známa. Byl by ale využitelný pro pořizování průkazně nezměněných fotografií. Obdobná funkce by byla využitelná např. u radarů pro měření rychlosti vozidel aj. technických sensorů, které snímají a zaznamenávají jakákoli data.

[33] Tedy pomocí softwaru, jako je Adobe Photoshop, Zoner ZPS apod.

[34] Pro důvody dále podrobně uvedené v čl. 5 odst. 2 DirES.

Pokud bychom měli demonstrovat, co by znamenala tato definice, za pomoci umělého znázornění v listinné praxi, vyhověl by postup, při kterém by fyzická osoba podepsala listinu tak, že by na papírovou listinu nalepila papírek Post-It a na něj vlastní rukou napsala křížek. Protože papírek s podpisem je nezjistitelně odstranitelný, nemůže sloužit jako metoda autentizace listiny. Nikdo nemůže ani vědět, že papírek nepodepsala osoba stejným způsobem v souvislosti s nějakou jinou listinou a že sem papírek nebyl přelepen dodatečně. A i kdyby věděl, že k přelepení nedošlo, z křížku nelze spolehlivě odvodit identitu osoby, která jej provedla. Nic z uvedeného však není na závadu, protože požadavek autentizace ani identifikace není v definici obsažen. Nevadí ani zpřísnění v eIDAS, že podepisující osobou je dle čl. 3 bodu 9 eIDAS výhradně fyzická osoba, která vytváří elektronický podpis, náš křížek byl vytvořen fyzickou osobou. Zatímco v listinné podobě bychom mohli vyslovit pochybnosti o svéprávnosti osoby, která by takový podpis vytvořila, popř. se na něj spoléhá, pro elektronický svět nám přímo evropský zákonodárce stanoví, že se jedná o „normální postup".

Než provedeme další přesnější výklad, odbočíme do práva v USA.

6.4.1 Pojetí elektronického podpisu ve Spojených státech

Ve Spojených státech došlo k právní úpravě na přelomu milénia. Nejprve uniformní zákon (předloha pro jednotnou úpravu ve státech federace) UETA[35] v roce 1999 a poté i federální zákon E-SIGN[36] v roce 2000 použily definici: *„Pojem **‚elektronický podpis'** znamená elektronický **zvuk**, **symbol** nebo **postup**, připojený nebo logicky spojený se smlouvou nebo jiným záznamem a **vytvořený nebo připojený osobou s úmyslem záznam podepsat.**"*[37] (zvýraznil autor).

Ani tato definice neobsahuje požadavek autentizace! Slovo *záznam* je v UETA i v E-SIGN definováno velmi obecně tak, že mu vyhovují i elektronická data, jedná se tedy o to, co se elektronicky podepisuje. *Smlouva* je uvedena jen jako příklad toho, co obsahově může být součástí záznamu. Zatímco *symbolem* může být například naskenovaný vlastnoruční podpis (tj. data), slovo *postup* pokrývá další případy, jejichž

[35] National conference of commissioners on uniform state laws: *Uniform Electronic Transactions Act (1999)*, Denver, 1999. Dostupné z: <http://uniformlaws.org/Act.aspx?title=Electronic%20Transactions%20Act>; navštíveno 8/2016.

[36] Electronic Signatures in Global and National Commerce Act (E-SIGN), 15 USC § 7001–7003, s. 106(5).

[37] Definice v E-SIGN je: *„The term ‚electronic signature' means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."* Definice UETA neobsahuje jednu čárku v interpunkci a nezmiňuje smlouvu jako příklad elektronického záznamu, jinak je zcela stejná.

výstupy opět mohou být různé datové výstupy (data), které lze následně považovat za podpis. Možnost *zvuku* byla zahrnuta spíše pro pokrytí případů použití elektronických záznamníků, hlasové pošty apod., které v době vyhlašování zákonů ani nemusely nutně používat digitální techniku, jakou jsou počítače, ale i jen analogovou techniku třeba tradičních magnetofonů. Dnes by i podpis zvukem mohl být hypoteticky vyjádřen formou digitálního záznamu a dat.

Zúžíme-li americkou definici na digitální techniku, lze ji parafrázovat, že elektronický podpis jsou „data **vytvořená nebo připojená osobou s úmyslem** jiná data **podepsat**."

Parafrázovaný evropský elektronický podpis (eIDAS) pak jsou „data, **která podepisující osoba používá k podepsání** jiných dat".

Nyní tedy již vidíme jasně, že nová evropská definice prostého elektronického podpisu není náhodná či neuvážená, ale že jejím trendem je přiblížit se americkému právnímu pojetí. V něm ovšem přitom platí podle § 7 písm. c) a d) UETA, že *„pokud právo vyžaduje písemný záznam, uspokojuje požadavek práva elektronický záznam"*[38] a *„pokud právo vyžaduje podpis, uspokojuje požadavek práva elektronický podpis"*.[39]

Je nutné zdůraznit, že zákony podle UETA i zákon E-SIGN mají omezenou působnost.[40] Mimo ni se jejich definice elektronického podpisu nemůže použít.

UETA i E-SIGN metodicky používají jen jednoúrovňový model (one-tier), který vyjadřuje pouze nejprostší elektronický podpis. Přesto jejich pojetí představuje v USA nejznámější obecnou úpravu pro nahrazování písemných listin a vlastnoručních podpisů jejich elektronickou podobou. Staly se určitým normálem nahrazení vlastnoručního podpisu, který pro nás překvapivě neobsahuje požadavek autentizace.

---

[38] „(c) If a law requires a record to be in writing, an electronic record satisfies the law."

[39] „(d) If a law requires a signature, an electronic signature satisfies the law."

[40] Například z působnosti E-SIGN jsou vyňaty podle § 7003 (a) závěti, odkazy nebo dědické trusty, záležitostí rodinného práva (adopce, rozvod...), z působnosti jednotného obchodního zákoníku UCC jsou vyloučeny: směnky apod. peněžní instrumenty, bankovní vklady a výběry, bankovní převody, akreditivy, skladní listy, nákladové listy aj. tituly ke zboží, investiční cenné papíry, zajišťovací transakce (zástavy movitých i nemovitých věcí); podle § 7003 (b) (1) soudní příkazy a oznámení, oficiální soudní dokumenty v souvislosti se soudním procesem; podle § 7003 (b) (2) oznámení výpovědi aj. ukončení dodávek infrastrukturních služeb (voda, teplo, energie), záležitosti týkající se primární rezidence jednotlivce, výpovědi aj. ukončení zdravotního pojištění nebo životního pojištění, stažení produktu, který ohrožuje zdraví nebo bezpečnost; a podle § 7003 (b) (3) doklady týkající se dopravy nebo zpracování nebezpečných materiálů, pesticidů aj. jedovatých nebo nebezečných materiálů.

Podíváme-li se nyní zpět (srov. 4.5) na *výčet druhů technik podpisu i) až viii)***,** jsou v případě působnosti UETA nebo E-SIGN všechny uvedené možnosti přijatelné, což potvrzují i američtí autoři.[41] Výjimkou snad je pouhá *iii) adresa elektronické pošty*, která je nutnou součástí každé její zprávy, a proto z její přítomnosti ještě nelze usuzovat na to, že ji odesilatel použil v úmyslu obsah zprávy podepsat. S nástupem různých chatovacích aplikací[42] v mobilních telefonech, pro které je charakteristická psaná komunikace holými větami, zkratkami a vynechávání jmen na konci zprávy, však bude pro jejich zprávy přicházet v úvahu i jen tato forma elektronického podpisu.

6.4.2 Výklad obratu „data používá k podepsání“ v eIDAS

Poučeni komparací z USA se nyní vraťme k definici v eIDAS. Musíme vyložit a zjistit, které implementace vyhoví obratu „**data**, která podepisující osoba **používá k podepsání** jiných dat“ z eIDAS.

Na první pohled může uvedený výtah z definice v eIDAS (podobně i z E-SIGN) působit téměř tautologicky, neboť další přepis výtahu zní: *podpis je něco, co se používá k podepsání*. Podpis je však výsledek činnosti, zatímco *použití k podepsání* se vztahuje k samé činnosti vytváření podpisu, k slovesu podepsat, popř. k účelu podepsání. Otázka tedy zní, co je právní podstatou činnosti vytváření podpisu?

Autor zde souhlasí s poznatkem Korbela a Melzera, že „podpis plní v našem sociokulturním prostředí funkci stvrzení konečnosti a vážnosti vlastní vůle ve vztahu k obsahu podepsané písemnosti“.[43] V této větě se netvrdí, že podpis následně musí být autentizačním prvkem písemnosti, ačkoli u papírové listiny tomu tak bude. Autor podpisu pouze musí jistým způsobem navenek projevit, že s obsahem listiny souhlasí, že je jeho vůlí ji podepsat a jistou činností listinu podepisuje.

Obdobně američtí autoři UETA: „**záměr provést právně významné jednání** [je] puncem podpisu“,[44] tj. jeho hlavním charakteristickým znakem. Proto z definice v USA vyjmuli i význam podpisu *autentizovat* a místo něj zavedli sloveso *podepsat*

---

[41] BUCKLEY, J. S. – TANK, M. H. K. – WHITAKER, R. D. – KROMER, J. P. *The Law of Electronic Signatures and Records*. 2016 edition: Thomson Reuters, 2016, s. 38, 89.

[42] Aplikací s funkcemi chatu ve formě konverzací je mnoho, např. WhatsApp, Skype, Viber, Facebook Messenger, ale i český BabelNet.

[43] KORBEL, F., MELZER, F., cit. dílo, s. 32. Korbel a Melzer doplňují i další požadavky, zde záměrně vynechané.

[44] *Uniform Electronic Transactions Act (1999) –,* cit. dílo, s. 11. Zvýraznil autor.

s tím, že zvláštní legislativa může vždy požadavek autentizace přidat.[45] Americký pojem záměru (intent) je velmi blízký pojmu vůle.

Vzniká otázka, zda v definičním obratu z eIDAS *„podepisující osoba používá k podepsání“* je přítomen požadavek na *vůli* podepisující osoby se podepsat. Autor je názoru, že požadavek přítomnosti vůle *lze z obratu odvodit*. Pokud by totiž podpis vznikl omylem nebo nedbalostí při používání informační techniky, neodpovídal by takový výsledek obratu „použít k podepsání.“ Znak vůle je pak v evropské definici přítomen podobně jako v definici americké.

Můžeme spekulovat, proč na rozdíl od UETA evropský zákonodárce v eIDAS o vůli výslovně nehovoří. Možností důvodů vynechání je rozhodně více. Jednou z možností je, aby se evropský předpis nedostával do kolize s vnitrostátní úpravou pro instituty, jako je právní jednání. Požadavky na přítomnost vůle mohou být upraveny rozdílně, stejně jako následky vad vůle. Autor zde proto nevylučuje případnou potřebu implementovat zde nařízení eIDAS vhodným doplněním.

Jinou možností absence je, že tím je sledována možnost vytváření elektronických podpisů elektronickými agenty, tj. počítačovými automaty,[46] které své elektronické podpisy vytváří bez přímého dohledu. Takové podpisy jsou spíše důsledkem nastavení a použití než bezprostřední vůle vytvořit podpis. Také americké právo elektronické podpisy vytvářené elektronickými agenty umožňuje, potřebuje však k tomu několik dalších ustanovení např. v § 5 a § 9 UETA.

Obrat „data používaná“ k podepsání musí být dle názoru autora vykládán *široce*. Úzkým výkladem by třeba bylo, kdyby se jako podpis připouštěla jen data přímo vkládaná uživatelem. Je tomu tak například při použití PIN nebo při zápisu svého jména na konci e-mailu nebo dokumentu. Je ale nutné připustit, že používanými daty pro podpis jsou i výsledky určitých operací, jejichž přímé hodnotové parametry uživatel nezadal. Jinak by nemohly elektronickým podpisem být ani kryptograficky silné digitální podpisy, což by byl absurdní závěr. V dnešním prostředí webových aplikací je nerozhodné i to, který počítač operaci podpisu a výpočet dat podpisu skutečně provedl.

[45] BUCKLEY, J. S. et al., cit. dílo, s. 8.

[46] Příkladem může být informační systém (software i hardware) obchodního domu, který objednává zboží v případě poklesu jeho počtu v obchodě pod určitou mez. Žádoucí množství zboží v obchodě i možní dodavatelé jsou předem určeni právně jednající osobou, jednotlivé objednávky jsou však vystaveny bez přímého dohledu osoby.

Není tedy nutné, aby elektronický podpis byl spočten celý na počítači vlastněném či drženém podepisující osobou.

Další otázkou je, zda výraz „používaná k podepsání“ má svůj referenční základ a vzor v praxi papírových listin, nebo se spíše vztahuje k praxi elektronické. Autor se domnívá, že počátek představy sice může z vlastnoručního podpisu vycházet, reflektovat možnosti a z toho pocházející zvyky elektronické praxe je však též nakonec nutné.

Za vhodnou definici slovesa *podepsat* v kontextu nařízení eIDAS pak autor považuje „stvrdit konečnost a vážnost vlastní vůle ve vztahu k obsahu podepisované písemnosti“.[47]

Je pochopitelně možné, že někdo namítne, že součástí slovesa podepsat v běžném chápání je výsledným podpisem i autentizovat podepsanou listinu. Proti tomuto výkladu však v případě elektronického podpisu (prostého) podle eIDAS hovoří vypuštění autentizace v definici při přechodu ze směrnice DirES k nařízení eIDAS a většina zde uvedeného diskursu.

S uvedenou analýzou můžeme dovodit, že *všechny uvedené druhy technik podpisů i) až vii)* mohou být elektronickým podpisem (prostým) podle eIDAS. Výjimkou může být *iii) jméno v adrese elektronické pošty* s důvody pro i proti již výše uvedenými.

Při zjišťování funkcí výsledného elektronického podpisu prostého autor nalézá pouze dvě: *funkci uzavírací* (konečnost vůle) a *funkci varovací* (vážnost vlastní vůle).

Téměř všechny uvedené druhy techniky mohou mít někdy potíž s naplněním varovací funkce, tedy se zajištěním vážnosti vůle právně jednající osoby. Implementace musí vymezit jasně konečné stadium před provedením právního jednání, dát jej dostatečně najevo a tím podepisující osobu varovat. Současně má ale implementátor protichůdný zájem, aby osobu od podpisu neodradil tím, že by vytvoření podpisu bylo uživatelsky příliš složité, nebo že by ji odradil právně.

Zatímco pro četné účely může být použití elektronického podpisu prostého velmi vhodné, autor považuje za vysoce sporné, aby se používal tam, kde právní řád povinně vyžaduje písemnou formu právního jednání. Pro další diskurs v tomto textu viz též části 5.1.3, 5.1.5 a 9.4.

[47] Definice je částečně inspirována u Korbela a Melzera, dle jejich citace výše.

6.5 Elektronické podpisy (autentizační)

Další druhy elektronického podpisu z eIDAS, popisované v této části, mají autentizační funkci. Tím se rozumí, že elektronický podpis (digitální objekt) autentizuje původ jím podepsaných dat. Úroveň zajištění této autentizace však může být různé.

6.5.1 Zaručený elektronický podpis (AdES)

První vyšší úrovní zajištění bezpečnosti je **zaručený elektronický podpis** (**AdES**[48]). Pojem znala již směrnice DirES. Definice[49] v čl. 2 odst. 2 DirES byla:[50]

> 2. **„zaručený elektronický podpis"** je elektronický podpis, který splňuje tyto požadavky:
>
> (a) je jedinečně spojen [uniquely linked] s podepisující osobou,
>
> (b) umožňuje zjistit totožnost [capable of identifying] podepisující osoby,
>
> (c) je vytvořen pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou [can maintain under his sole control],
>
> (d) je spojen s daty, ke kterým náleží, takovým způsobem, že jakákoliv následná změna dat je zjistitelná;

Při podrobné analýze by se zjistilo, že se jedná o poměrně univerzální definici, která se snaží přiblížit funkční ekvivalenci s vlastnoručním podpisem. Navíc se jednalo o definici technologicky nezávislou, kterou by bylo možné hypoteticky implementovat i jinými druhy techniky, než je digitální podpis, založený na PKI. V praxi ale převládl výklad techniků, kteří AdES začali prostě považovat za digitální podpis s nižší úrovní požadavků na zajištění funkcí PKI. Projevilo se to zejména ve tvorbě technických specifikací ETSI ve skupině ESI[51], která četné technické formáty podpisů začala navrhovat již pro úroveň AdES s tím, že vyšší úrovně je pak mohou používat rovněž. To je i důvod, proč se zkratka AdES ujala a proč ji zde nakonec používá i autor.

Definice v eIDAS víceméně odpovídá dřívější definici z DirES.

> Pro účely tohoto nařízení se rozumí:
>
> 11) „zaručeným elektronickým podpisem" elektronický podpis, který splňuje požadavky stanovené v článku 26; ...
>
> **Článek 26**
> **Požadavky na zaručené elektronické podpisy**
>
> Zaručený elektronický podpis musí splňovat tyto požadavky:
>
> a) je jednoznačně spojen [uniquely linked] s podepisující osobou;

[48] **Ad**vanced **E**lectronic **S**ignature.
[49] Definice pak inspirovala i definici stejně nazvaného pojmu v zák. č. 227/2000 Sb.
[50] Autor používá vlastní překlad přímo z anglického znění DirES.
[51] Electronic Signature Infrastructure. Normalizační skupina v rámci ETSI.

b) umožňuje identifikaci [capable of identifying] podepisující osoby;
c) je vytvořen pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry [confidence] použít pod svou výhradní kontrolou [under his sole control]; a
d) je k datům, která jsou tímto podpisem podepsána, připojen takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat.

Změnou je tedy pojetí třetího požadavku. Dříve se vyžadovalo pro elektronický podpis *„vytvoření pomocí **prostředků**, které podepisující osoba může udržet pod **svou výhradní kontrolou**"*.[52] Požadavek se mohl vykládat v užším i širším významu. V širším významu se jednalo o všechny prostředky, které se při vytváření elektronického podpisu používaly, tedy i systémové prostředí a aplikace vytvářející elektronický podpis (celý osobní počítač). V užším smyslu se prostředky mohla mínit jen zařízení, která obsahovala data pro vytváření podpisu (např. čipová karta nebo token obsahující soukromý klíč). Byť i jen užší výklad pak třeba v Německu vedl k tomu, že se vyžadovalo fyzické držení takového prostředku podepisující osobou.

Nařízení eIDAS se rozhodlo zavést i novou možnost či koncepci *„vytváření elektronického podpisu na dálku, jehož prostředí spravuje poskytovatel služeb vytvářejících důvěru"*.[53] Pro více srov. 6.2.5. Data pro vytváření podpisu nejsou již při této možnosti uložena v zařízení drženém podepisující osobou, ale v zařízení drženém a spravovaném kvalifikovaným poskytovatelem služeb. Podepisující osoba pak na dálku, po své autentizaci přes síť (internet), iniciuje vytvoření svého vlastního (zaručeného, kvalifikovaného) elektronického podpisu, který se fyzicky vytváří u poskytovatele, ale je pak zřejmě předán zpět do zařízení podepisující osoby, nebo jinak do dispozice podepisující osoby. Tento koncept by měl umožnit vytváření podpisu i na nových platformách, jako jsou *chytré mobilní telefony, tablety* apod., k nimž je nepraktické připojovat technické periferie. Zařízení u poskytovatele ale podepisující osoba již nemůže mít pod svou kontrolou, rozhodně ne fyzickou.

Třetí požadavek čl. 26 písm. c) eIDAS proto nově zní: *„je vytvořen **pomocí dat pro vytváření** elektronických podpisů, která **podepisující osoba může** s vysokou úrovní důvěry [přesvědčení] **použít pod svou výhradní kontrolou**"*.[54] Požadavek se tedy zúžil na výhradní kontrolu nad použitím dat pro vytváření elektronických podpisů. Na jednu stranu se jedná o elegantní řešení, na straně druhé se ztrácí dřívější širší výklad, který

[52] Čl. 2 odst. 2 písm. c) DirES. Zvýraznil autor.
[53] Bod odůvodnění 52.
[54] Zvýraznil autor. Slovo *přesvědčení* přidáno jako vhodnější vyjádření, než je slovo *důvěra*.

pokrýval věrnou službu všech prostředků použitých pro vytváření podpisu. Jelikož se *„data pro vytváření elektronických podpisů"* dostala přímo do definice AdES, jsou tím jiné druhy techniky než digitální podpis a PKI již zřejmě vyloučeny vůbec. Definice ztratila na své technologické neutralitě (srov. např. 6.16.12).

Diskurs o významu obratu *„s vysokou úrovní přesvědčení"*[55] je již uveden výše v 6.2.5. Dle autora je relaxaci nutno co nejvíce potlačit, jinak by celé nařízení eIDAS ztrácelo smysl, což dle výkladu užitečného účinku není možné. Jde proto o velmi vysokou úroveň přesvědčení a jedná se o přesvědčení osoby s odbornými znalostmi.

Při tradičním provedení technikou digitálního podpisu musí existovat určité prerekvizity pro vytvoření AdES. Musí existovat data pro vytváření elektronických podpisu (soukromý klíč) a certifikát vydaný poskytovatelem služeb, který obsahuje spojení dat pro ověřování platnosti (veřejný klíč) a určení totožnosti na základě jejího předchozího ověření poskytovatelem. Dále musí existovat technické prostředí, které podepisující osobě umožňuje mít s vysokou úrovní přesvědčení výhradní kontrolu nad daty pro vytváření elektronických podpisů. Z bodu odůvodnění 56 však víme, že toto technické prostředí nebude zahrnovat aplikaci pro vytváření podpisu ani systémové prostředí, ale jen část, která uchovová a chrání data pro vytváření podpisu a v eIDAS se nazývá *prostředek pro vytváření elektronických podpisů*. Operací vytvoření digitálního podpisu, iniciované podepisující osobou, pak vznikne AdES.

Požadavky z čl. 26 eIDAS jsou pak splněny následovně. Písm. **a)** je splněno operací ověření platnosti digitálního podpisu AdES, k čemuž se využije veřejný klíč (data pro ověřování platnosti) z certifikátu. Pro jeho splnění je nutná i silná kryptografie veřejného klíče (PKC) a splnění písm. c) při vytváření (srov. níže). Mason namítá,[56] že písm. a) není v principu vůbec splnitelné, neboť žádný druh elektronického podpisu, včetně AdES, nelze spojit s podepisující osobou, ale nejvýš s jejím soukromým klíčem.[57] Soukromý klíč si žádná fyzická osoba není schopna zapamatovat, musí tedy být uložen na technickém prostředku, který je v principu od podepisující osoby odloučitelný. AdES tedy podle Masona nejvýše osvědčuje, že elektronický podpis byl vytvořen pomocí určitého soukromého klíče (srov. též 6.15.7). Současně však z hlediska *užitečného účinku* pro výklad nařízení platí, že písm. a) musí být vyložitelné tak, že ono

[55] Anglické *confidence* je vhodnější překládat jako *přesvědčení* (zdůvodnitelné), a ne *důvěru* (slepou).
[56] MASON, S. *Electronic Signatures in Law*. 4th edition, London: Institute of Advanced Legal Studies – University of London, 2016, s. 152–155.
[57] Pojem PKI, v eIDAS mu odpovídají *data pro vytváření elektronického podpisu*.

uvedené spojení k podepisující fyzické osobě možné přesto je. Mason se s podobnou argumentací (teleologickou, racionality zákonodárce apod.) již setkal, je si vědom, že právě z tohoto důvodu se většina vykladatelů tváří, jakoby potíž vůbec neexistovala. Je s tímto stavem nespokojen, z jeho právního pohledu se jedná o politickou svévoli zákonodárce. Patrně se obává, že následně by soudy nemusely na jeho námitku vůbec hledět. Jak je uvedeno výše, v rámci právního předpisu EU, jako je eIDAS, je přesto nutno pracovat s výše uvedeným výkladem dle užitečného účinku, ovšem s tím, že vykladatel si námitku[58] Masona pečlivě poznamená a bude si možnosti této zásadní výhrady vědom. Jejím následkem bezpochyby je, že je třeba četná jiná ustanovení eIDAS vykládat v tom smyslu, aby v praxi k možnému „odpojení" soukromého klíče od podepisující osoby nemohlo dojít. Tomu musí čelit nikoli voluntaristicky optimisticky usnadňující výklad předpisu, zamlčující rizika, ale naopak výklad, který požadavky vykládá bez úlev tak, aby vznikům rizika bránily, nebo je aspoň významně snížily. Právě z odloučitelnosti soukromého klíče od fyzické osoby plyne rozdíl mezi platností a pravostí (zaručeného, kvalifikovaného) elektronického podpisu. Podpis ověřený vzhledem k soukromému klíči bude platný,[59] ale to ještě neimplikuje nutnou pravost.

Splnění identifikace pro písm. **b)** se provede přečtením údajů o totožnosti z certifikátu. Certifikátu se věří nebo se jeho ověření provede nezávisle.

Splnění písm. **d)** plyne z vlastností použitých kryptografických algoritmů PKC.

Potíží bývá ověřit splnění písm. **c)**, protože spoléhající osoba nemá běžně žádnou informaci o tom, jaký prostředek pro vytváření elektronických podpisů podepisující osoba použila. K tomu by bylo třeba, aby se v rámci výsledného podpisu AdES nacházel i nezpochybnitelný údaj o tom, že byl použit vyhovující prostředek pro vytváření elektronických podpisů. Takový údaj by se mohl nacházet i v certifikátu od poskytovatele, pokud si je poskytovatel jist, že data pro vytváření podpisu se v okamžiku vydání certifikátu již nacházejí ve vhodném prostředku pro vytváření elektronických podpisů, že jej nemohou opustit a že jej podepisující osoba bude muset používat i v budoucnosti, anebo žádný podpis AdES nevytvoří.

Komise dle čl. 27 odst. 4 eIDAS může vyhlásit technické normy pro AdES. Splnění těchto norem zakládá domněnku vyhovění, že jsou splněny požadavky na AdES podle čl. 26 (zde probírané) a rovněž dle čl. 27 odst. 1 a 2 eIDAS pro případy, když

[58] Autor s námitkou Masona jako v principu souhlasí. Prakticky ale vykládá, jak v textu uvedeno.

[59] Nařízení eIDAS i infrastruktura veřejného klíče pro platnost kladou další konkrétní požadavky. Zde je veden diskurs na obecnější úrovni infrastruktury veřejného klíče (PKI).

členský stát pro využívání on-line služeb veřejného sektoru požaduje podpis AdES nebo vyšší. Takové technické normy by měly vyřešit potíže se stanovením splnění písm. c).

V případě AdES vytvořeného kvalifikovaným poskytovatelem služeb se lze spolehnout na audit od subjektu potvrzujícího shodu a přezkoumání jeho zprávy orgánem dohledu. Kvalifikovaní poskytovatelé musí používat důvěryhodné systémy a produkty podle čl. 24 odst. 2 písm. f) eIDAS, které by měly splňovat požadavky na prostředek pro vytváření elektronických podpisů s rezervou.

Historicky se podpisy AdES podle úprav transpozic DirES prováděly i s daty pro vytváření elektronických podpisů, které byly uloženy jen na osobním počítači a na něm též byly vytvářeny. Je sporné, zda takový prostředek splňuje požadavky v čl. 2 odst. 2 písm. c) DirES nebo nově podle čl. 26 písm. c) eIDAS. Národní úpravy proto mohly zavést splnění této podmínky jako povinnost podepisující osoby ať již explicitně, nebo obecnějším ustanovením. Pro AdES pak dostačovalo vydávat již jen komerční certifikáty poskytovatelů služeb, neboť splnění písm. c) bylo pro spoléhající se osobu zajištěno zákonem členského státu.

Roßnagel udává, že do doby, než Komise vyhlásí technické normy, přičemž u fakultativních zmocnění není jisté, kdy a zda tak učiní, jsou členské státy oprávněny oblast upravit svými vlastními právními předpisy.

Mason je vůči požadavku c) ohledně *„výhradní kontroly"* opět vysoce skeptický,[60] zejména pokud se mají provádět na počítačích, které je obecně nutno považovat za nedůvěryhodné, neboť představují otevřený, složitý, flexibilní návrh a běžící software na nich též nebývá bez vad či zranitelností. Odkazuje na české autory Petra Švédu a Václava Matyáše ml., podle nichž by důvěryhodný podepisující systém vyžadoval restriktivní konfiguraci, která by poskytovala pouze několik jednoduchých funkcí. Jinak řečeno, bylo by potřeba mít jednoúčelové zařízení, sloužící jen k vytváření a ověřování elektronických podpisů.[61] Opět srov. též 6.15.7. Vzhledem k tomu, že taková zařízení nejsou běžně na trhu pro běžnou populaci, je třeba i zde eIDAS vyložit s pomocí užitečného účinku jako požadavek realizovatelný, byť s podobnými výhradami, jako jsou autorem uvedeny výše v rámci požadavku písm. a). Je možné, že právě kvůli již dříve panujícím námitkám[62] právě Masona byl do písm. c) zařazen obrat

[60] MASON, S. *Electronic Signatures in Law*. 2016, s. 155–159.

[61] Takové zařízení by skutečně bylo optimální bezpečnostně, ale možná není optimální ekonomicky. Zejména pak běžní uživatelé neprojevují dostatečnou poptávku po takto koncipovaných zařízeních.

[62] Námitky proti *„výhradní kontrole"* zmiňuje již v předchozím vydání své monografie MASON, S.

„… s vysokou úrovní důvěry [přesvědčení, confidence]…" Je tak již normativně podchyceno, že výhradní kontrola nemusí být v praxi zcela perfektně dosažitelná. K tomuto obratu srov. již výše uvedený diskurs v 6.2.5. Dle autora je obrat nutno vykládat jen jako velmi malé znejistění o skutečném stavu. Úroveň přesvědčení (důvěry) musí být velmi vysoká a musí se jednat o přesvědčení odborné osoby. Případné faktické nesplnění *výhradní kontroly* může opět vést k elektronickému podpisu, který bude pouze „platný", ale nikoli nutně „pravý".

Požadavky čl. 26 písm. a) až d) eIDAS v lze hodnotit i z hlediska teorie funkce vlastnoručního podpisu (srov. níže 6.5.1.1).

Někteří čeští komentátoři[63] srovnali rozdíl ryze českých znění mezi DirES a eIDAS a jsou názoru, že nové znění *„umožňuje identifikaci"* v písm. b) se má spojit s pojmem identifikace v čl. 3 odst. 1 eIDAS, který však plně zní *„elektronická identifikace"* a týká se kapitoly II eIDAS. Dochází pak k závěru, že v písm. b) dochází k rozšíření okruhu identifikovatelných osob, a to kromě fyzických osob i o osoby právnické a osoby fyzické zastupující osoby právnické.[64] Tento výklad autor považuje za nesprávný. Anglické znění, které bylo pracovním zněním v legislativním procesu, se nezměnilo *(capable of identifying)* a rozhodně jej nelze podřazovat pod pojem čl. 3 odst. 1 eIDAS. Podřaditelné není ani znění české. Především pak dle čl. 3 bod 9 eIDAS podepisující osobou je osoba fyzická jako jediná možná, je náležitostí elektronického podpisu prostého a potažmo i zaručeného elektronického podpisu.

Autor však nevylučuje, že by tento tvořivý omyl nemohl někoho inspirovat k netradičním propojením mezi kapitolou II a III eIDAS. Pokud by taková technická identifikace nebyla opřená o certifikát PKI, ale o provedení elektronické identifikace ve smyslu kapitoly II a stále by výsledek odpovídal definici AdES nebo představoval zajímavé faktické řešení jinak, není důvod se takové metodě bránit. Pokud dojde k identifikaci právnické osoby, bude se však jednat o AdESeal, a nikoli AdES.

6.5.1.1 Teoretické funkce AdES

V této části rozebíráme funkce AdES z hlediska splňování požadavků teorie na funkce vlastnoručního podpis (srov. 4.2), tj. otázku, do jaké míry je AdES pokrývá.

Electronic signatures in law. 3rd edition. New York: Cambridge University Press, 2012, s. 122–125.

[63] DONÁT, J. – MAISNER, M. – PIFFL, R. *Nařízení eIDAS : komentář.* Praha: C. H. Beck, 2017, s.123.

[64] DONÁT, J. – MAISNER, M. – PIFFL, R., cit. dílo, s. 123.

Podpis AdES již má podle čl. 26 písm. d) eIDAS autentizační funkci. Tato však zcela nezajišťuje *pravostní* funkci *(Echtheit)* z teorie funkcí vlastnoručního podpisu, což bude níže v textu patrné konkrétněji. Ani ve spojení s písm. c) nebyly totiž při vytvoření zajištěny podmínky jako při vlastnoručním podpisu. AdES se silnou kryptografií by měl mít lepší *ověřovací* funkci *(Verifikation)*, než má vlastnoruční podpis [čl. 26 písm. a) a c)], a rovněž lepší *uzavírací* funkci *(Abschluss)* ve smyslu ochrany před doplňováním [čl. 26 písm. d)]. AdES bude mít tak dobrou *identifikační* funkci *(Identifikation)*, jak kvalitní postupy užívá a jak důvěryhodný je poskytovatel certifikátu [čl. 26 písm. b)]. Funkce *zachovávací (Perpetuirung)* je v principu možná. Funkce *uzavírací (Abschluss)* ve smyslu konečnosti vůle a funkce *varovací (Warn)* by měla být zajištěna již elektronickým podpisem prostým, ale záznam AdES je prokazovat nebude. Spoléhající strana se zřejmě bude muset dovolávat zkušenostní domněnky. Funkce *důkazní (Beweis)* AdES je proto vůči ideálu vlastnoručního podpisu zeslabená zejména ve funkci pravostní (možnost podsunutí obsahu), uzavírací (konečnost vůle) a varovací (vážnost vůle). V případě úspěšného útoku na data pro vytváření podpisu může dojít k naprostému kolapsu ověřovací funkce *(Verifikation)*. V pojmech doktríny je zde mírně paradoxní, že výše zmiňovaný rozdíl „pravost – platnost" elektronického podpis tkví jen částečně v pravostní funkci, ale zejména ve funkci ověřovací. Srov. níže též 6.5.3.2.

6.5.2 AdES založený na kvalifikovaném certifikátu ($AdES_{QC}$)

Jako další stupeň úrovně zajištění se v eIDAS příležitostně vyskytuje *zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis* ($AdES_{QC}$).[65] V jeho rámci se požadavek čl. 26 písm. b) a částečně i písm. a) zajišťuje právě *kvalifikovaným certifikátem pro elektronický podpis*.

Nejedná se tedy ani tak o zásadní rozšíření požadavků na AdES, jako spíše o zajištění vyšší úrovně zjištění totožnosti kvalifikovaným poskytovatelem služeb vytvářejících důvěru [čl. 26 písm. b) eIDAS], stejně jako o vyšší úroveň zajištění správnosti přiřazení dat pro vytváření elektronických podpisů k podepisující osobě stejným poskytovatelem, což pomáhá ke splnění požadavku čl. 26 písm. a) eIDAS.

[65] Advanced Electronic Signature based on a Qualified Certificate.

6.5.3 Kvalifikovaný elektronický podpis (QES)

Před probráním kvalifikovaného elektronického podpisu (QES[66]) je třeba zmínit pojem *kvalifikovaného prostředku pro vytváření elektronických podpisů* (QSCD[67]). Jedná se o prostředek, jehož účelem je ukládat a chránit v sobě data pro vytváření elektronických podpisů a provádět s jejich pomocí operaci vytvoření digitálního podpisu, iniciované a autentizované podepisující osobou.

Pro podrobnosti ke QSCD srov. 6.10 a 6.2.5. Tradičně bývala na místě QSCD čipová karta nebo token, tj. kompaktní prostředek ve fyzickém držení podepisující osoby. Při vytváření elektronického podpisu na dálku bude hlavní část prostředku v držení kvalifikovaného poskytovatele a jen případná autentizační část v držení podepisující osoby.

QSCD představuje způsob zajišťování požadavků čl. 26 písm. a), c) a d) eIDAS.

Vrchol nařízení z hlediska podpisu pak představuje **kvalifikovaný elektronický podpis** (QES), kterým se dle čl. 3 bod 12 eIDAS rozumí *„[i]zaručený elektronický podpis, který je [ii] vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů a který je [iii] založen na kvalifikovaném certifikátu pro elektronické podpisy"*. V zásadě to je elektronický podpis vytvořený pomocí QSCD a založený na kvalifikovaném certifikátu pro elektronické podpisy. QSCD zajišťuje bezpečnost uložení, vytváření a vazbu na podepisující osobu, zatímco kvalifikovaný certifikát základní informace o totožnosti podepisující osoby a její spojení k datům pro ověřování platnosti. Tyto prostředky realizují i požadavky na zaručený elektronický podpis, takže jeho přítomnost v definici je pravděpodobně mírně navíc, spíše pro jistotu o výkladu požadavků na QSCD a kvalifikovaný certifikát.

6.5.3.1 Právní účinky QES

V čl. 25 odst. 1 eIDAS se stanoví obecný zákaz hrubé diskriminace QES z hlediska důkazních účinků i právních účinků. Srov výklad v 6.15.1.

Nařízení eIDAS stanoví v čl. 25 odst. 2, že: ***„Kvalifikovaný elektronický podpis má právní účinek rovnocenný vlastnoručnímu podpisu."*** Jedná se o účinek vyhovění formě pro jednání. Kdekoli právní předpis kteréhokoli členského státu nebo EU

[66] **Q**ualified **E**lectronic **S**ignature.
[67] **Q**ualified Electronic **S**ignature **C**reation **D**evice.

dovoluje elektronickou formu jednání a vyžaduje pro jednání podpis,[68] je možné splnit tento požadavek na formu v části podpisu kvalifikovaným elektronickým podpisem.

Čl. 25 odst. 2 eIDAS *představuje vrchol nařízení eIDAS*, přinejmenším v části věnované službám vytvářejícím důvěru, což je ta část nařízení, která se zabývá záležitostmi odvozenými od úpravy elektronických podpisů.

Splnění požadavku formy na podpis podle čl. 25 odst. 2 přesto neznamená nutně, že je přijímající osoba povinna příchozí elektronické jednání uznat nebo přijmout.

Předně jednání bude neplatné, není-li splněn případný požadavek práva na podepsaná data. Členský stát nebo EU má stále právo stanovit formu obsahu, a to včetně například i jen technického formátu podepsaných dat. Ačkoli platí a je uznán podpis, nemusí být tedy uznán celek jednání.

V soukromém právním styku zřejmě všude v EU běžně platí zásada smluvní svobody. Je proto zcela na vůli soukromé strany, zda bude s elektronickou formou obsahu a s QES souhlasit a přijímat je. Soukromé strany si mohou sjednat i vyšší úroveň zajištění bezpečnosti, než představuje QES, nebo nižší. I vnitrostátní soukromé právo ovšem může stanovit pro určité druhy jednání minimální požadavky na formu. Nařízení eIDAS však státům nestanoví, jaké požadavky to mají být. Nařízení eIDAS nevylučuje ani to, že pro určité druhy jednání vnitrostátní právo nepřipouští elektronickou formu vůbec, a to v právu soukromém i veřejném.

Připouští-li však veřejné právo elektronickou formu pro on-line službu poskytovanou subjektem veřejného sektoru, pak v případě jejího přeshraničního využívání *nesmí pro účel elektronického podpisu vyžadovat vyšší úroveň než QES a musí přeshraniční QES uznávat* (čl. 27 odst. 3 ve spojení s čl. 25 odst. 3 eIDAS).

Uvedené přesto zcela nevylučuje, že uznávání nelze torpédovat přídavným požadavkem na využívání on-line služby. Takový požadavek by mohl spočívat například v přesnějším způsobu určení totožnosti jednající osoby. V případě vnitrostátních subjektů může požadavek pak být splněn například pomocí zvláštních vnitrostátních atributů dle čl. 28 odst. 3 eIDAS, zatímco přeshraniční subjekty budou svou totožnost muset doložit nějak jinak.

eIDAS nebrání, aby stát stanovil další přídavné požadavky na vytváření aktů, jednání, dokumentů apod. v elektronické formě, které vytváří jeho správní úřady nebo

[68] Konstrukce takových právních předpisů mohou být různorodé, nemusí se vyjadřovat výslovně.

orgány veřejné moci v rámci veřejného práva. To je dokonce *více než vhodné* v případech, kdy se takové výstupy právně těší statutu **veřejné listiny** s presumpcí správnosti podle vnitrostátního práva, tj. k požadavkům na QES mohou přistoupit i požadavky na bezpečnost a vlastnosti systémového prostředí a na aplikace vytvářející podpis, popř. na další technické systémy, jako jsou i systémy spisové služby, středně- a dlouhodobé archivace. Čistě vnitřní systémy veřejné správy jsou z působnosti eIDAS vyloučeny vůbec.[69]

V soukromém právu lze zodpovědným podepisujícím doporučit, aby se přiměřeně podobně zařídili dobrovolně rovněž. Nařízení totiž neupravuje požadavky na systémové prostředí ani na aplikace vytvářející podpis.[70]

Nařízení eIDAS se dle zásady přenesených pravomocí netýká všech jednání, ale pouze těch, u nichž byly na EU přeneseny pravomoci a v nichž si nařízení vymezilo působnost. Ostatní jím zůstávají nedotčena. Jelikož se nařízení odvolává na pravomoci vnitřního trhu EU, může v praxi působit osobám potíže odlišit, která jednání ještě pod eIDAS spadají a která již nikoli. Měly by to případně vymezit implementační předpisy. V případě nejasností a při zvážení vhodnosti není od věci recipovat eIDAS nebo jeho části i pro ryze vnitrostátní druhy jednání nebo pro případy nejasného mixu možností.

Zvláštní důkazní účinek nařízení eIDAS pro QES nestanoví. Posuzuje se tedy pouze na základě obecné důkazní přípustnosti, tj. v ČR dle volného hodnocení důkazů. Současně by QES ale měl být běžně při volném hodnocení důkazů hodnocen jako vysoko přesvědčivý. Srov. 6.15.6.

Výše uvedená pravidla lze s jistou dávkou zjednodušení charakterizovat tak, že nařízení eIDAS stanoví QES jako nejvyšší úroveň elektronického podpisu, jež by se měla v EU běžně vyžadovat. Fyzická osoba vybavená prostředky pro vytváření QES by měla být schopná vytvořit svůj podpis a ten by měl být i přeshraničně uznáván. Výše je vysvětleno, že reálné situace mohou vyústit na základě platného práva často jinak, nebude se ale typicky jednat o selhání schopnosti se podepsat, ale o nesplňování jiných náležitostí, zejména podepisovaného obsahu nebo neochoty protistrany v soukromoprávním vztahu přijímat elektronickou formu.

[69] Uzavřený systém dle čl. 2 odst. 2 eIDAS.
[70] Bod odůvodnění 56 eIDAS.

Dlužno též upozornit, že bez ohledu na čl. 25 eIDAS mohou členské státy stanovit i nižší úrovně připouštěných elektronických podpisů nebo zcela jinak vytvářené elektronické podpisy.

V českém prostředí se však objevuje přepjatý výklad,[71] že elektronický dokument podepsaný kvalifikovaným elektronickým podpisem je univerzálně právně rovnocenný dokumentu v listinné formě podepsaným vlastnoručním podpisem. Účelem mohlo být motivovat úřady, aby veškeré své agendy přijímaly i v elektronické podobě.

Obdobně se uvádí v čerstvém komentáři k eIDAS: „elektronický dokument podepsaný kvalifikovaným elektronickým podpisem má právní postavení stejné jako listina podepsaná vlastnoručním podpisem, a to v rámci celé EU".[72] Tyto výklady zřejmě příliš extenzivně vychází ze zákazu hrubé diskriminace elektronické formy, jehož význam je ale jen velmi malý (srov. 6.15.1).

Uvedená tvrzení tedy nejsou správně ani vzhledem k důkazním účinkům, ani vzhledem k hledisku plnění požadavků na (písemnou) formu. Taková použití nařízení jsou z jeho působnosti vyloučena čl. 2 odst. 3 eIDAS, podle nějž: *„nařízením není dotčeno vnitrostátní právo ani právo Unie týkající se uzavírání a platnosti smluv či jiných právních nebo procesních povinností týkajících se formy"*. Obdobně bod odůvodnění 2 eIDAS. Ve vnitrostátním právu nebo v unijním právu lze tedy elektronický dokument pro určité účely užití zcela vyloučit nebo na něj stanovit požadavky. Nejsou-li splněny, žádné právní účinky vyvolávat nemusí.

6.5.3.2 Teoretické funkce QES

V této části rozebíráme funkce QES z hlediska splňování požadavků teorie na funkce vlastnoručního podpisu (srov. 4.2), tj. otázku, do jaké míry je QES pokrývá.

Vyšší úrovně podpisu zvyšují míru zajištění uvedených vlastností a funkcí, jako bylo u AdES (6.5.1.1), ale nikoli zásadně. Tak QES by měl mít silnou kryptografii implicitně, ochrana proti útoku na data pro vytváření podpisu by měla být značně vyšší,

---

[71] Například: „Pro elektronický dokument: • podepsaný kvalifikovaným elektronickým podpisem platí, že se na něj nahlíží stejně jako na dokument v listinné podobě podepsaný vlastnoručnim podpisem" citováno z: PIFFL, R. – FELIX, O. Nařízení eIDAS – Cíle, nástroje, důsledky, Metodický seminář – Dopady nařízení eIDAS po 1. 7. 2016, Ministerstvo vnitra, Praha – 14. 6. 2016, s.15/42. Dostupné z: <http://www.mvcr.cz/soubor/1-eidas-narizeni-eidas-cile-nastroje-dusledky.aspx>; navštíveno 22. 6. 2016.

[72] DONÁT, J. – MAISNER, M. – PIFFL, R. *Nařízení eIDAS: komentář.* Praha: C. H. Beck, 2017, s. 167.

funkce varovací aspoň částečně kryta druhým faktorem autentizace, identifikace postupy kvalifikovaného poskytovatele. Zopakujeme aktualizovaný přehled pro QES.

Podpis QES má podle čl. 26 písm. d) eIDAS autentizační funkci. Ani QES však zcela nezajišťuje pravostní funkci *(Echtheit)* z teorie funkcí vlastnoručního podpisu. Případný požadavek QSCD na druhý faktor autentizace (PIN) mírně zlepšuje pravostní funkci, ale stále ani QSCD nezajišťuje podmínky při vytvoření QES, z hlediska kontroly podepisovaného obsahu i vytváření obsahu lidskými smysly shodně tak, jako tomu je při vlastnoručním podpisu.

Požadavky na QSCD zajišťují silnou kryptografii a výbornou ověřovací funkci *(Verifikation)*, mnohem lepší, než má vlastnoruční podpis. QSCD též splňuje požadavky čl. 26 písm. a) a c). QES má rovněž výbornou uzavírací funkci *(Abschluss)* ve smyslu ochrany před doplňováním [požadavky na QSCD splňují i čl. 26 písm. d)]. QES má velmi dobrou identifikační funkci *(Identifikation)*, neboť kvalifikovaný poskytovatel se podrobil předchozímu auditu a přezkoumání výsledné zprávy, a lze tak splnit čl. 26 písm. b). Funkce zachovávací *(Perpetuirung)* je v principu možná. Funkce uzavírací *(Abschluss)* ve smyslu konečnosti vůle a funkce varovací *(Warn)* by měla být zajištěna již elektronickým podpisem prostým, záznam QES je plně neprokazuje, ale případný druhý faktor autentizace u QSCD zvyšuje pravděpodobnost, že podepisující osoba byla přinejmenším varována před tím, že k vytvoření QES má dojít. Spoléhající se osoba se ale zřejmě stále bude muset dovolávat zkušenostní domněnky. Funkce důkazní *(Beweis)* QES je proto vůči ideálu vlastnoručního podpisu stále mírně slabší ve funkci pravostní (možnost podsunutí obsahu), uzavírací (konečnost vůle) a varovací (vážnost vůle). Opět platí, že výše zmiňovaný rozdíl „pravost – platnost“ elektronického podpisu tkví v teorii jen částečně v pravostní funkci, ale zejména ve funkci ověřovací.

Bohužel i v případě QES může výjimečně dojít k úspěšnému útoku na data pro vytváření podpisu a následně k naprostému kolapsu ověřovací funkce *(Verifikation)*. Podrobněji jsou možnosti útoků na QES probrány v 6.15.7. Na druhou stranu misek vah je třeba vložit, že ověřovací, uzavírací (obsah), identifikační funkce jsou běžně mnohem kvalitnější, lze je provádět automatizovaně s velmi malými náklady. Též vlastnoruční podpis lze falšovat, a to s finančně výrazně skromnějšími prostředky než QES.

6.6 Elektronická pečeť

Elektronická pečeť je nový institut zavedený právem EU v nařízení eIDAS.

6.6.1 Elektronická pečeť prostá

Podle čl. 3 bod 25 eIDAS **elektronickou pečetí** jsou *„data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena* ***s cílem zaručit jejich původ a integritu****“*. Definice poměrně těsně sleduje definici **elektronického podpisu** (prostého) dle čl. 3 bodu 10 eIDAS, kterým se rozumí *„data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která* ***podepisující osoba používá k podepsání****“*. Rozdíl definic spočívá v tom, že elektronický podpis prostý výslovně zmiňuje subjekt jednající podepisující osoby a účel (cíl) je stanoven slovně rozdílně.

Než přistoupíme ke zkoumání pečetí, ještě připomeňme, že dle definice čl. 2 odst. 1 směrnice DirES byla předchozí definice *„‚elektronický podpis' znamená data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která* ***slouží jako metoda autentizace****“* (ve všech 3 definicích zvýraznil autor).

Ze srovnání těchto tří definic vyplývá, že elektronická pečeť je definičně velmi podobná definici dřívějšího elektronického podpisu z DirES. Z výkladů definice elektronického podpisu dle DirES je totiž ohledně autentizace zřejmě nejsprávnější ten, který praví, že data (elektronického podpisu) slouží k autentizaci druhých dat. Autentizací se běžně míní především pravost, tedy původnost a nepozměněnost. Nyní již je shodnost definic velmi markantní, a může nás tedy vést k předběžnému závěru, že nástupcem elektronického podpisu (prostého) je právě elektronická pečeť (prostá), zatímco definice elektronického podpisu (prostého) se změnila (srov. 6.4).

Důležité je nyní srovnat nejdříve změny definice elektronického podpisu prostého. Nově byla do definice zahrnuta podepisující osoba, dle v definičního bodu 9 je *„‚podepisující osobou' fyzická osoba, která vytváří elektronický podpis“*. Uvedené znamená, že vytvořitelem všech elektronických podpisů podle eIDAS je nově výhradně fyzická osoba. V definici dle DirES subjekt vytvářející elektronický podpis prostý specifikován nebyl, podepisující osobou mohla být jakákoli entita, tedy například i entita ryze technická,[73] entita bez právní osobnosti, fyzická osoba nebo i právnická osoba. Je nyní markantní, že v definici elektronické pečetě subjekt vytvářející elektronickou pečeť zmíněn také není, ačkoli tak zákonodárce zcela jistě mohl velmi snadno učinit. Jen podle definice tedy lze tvrdit, že elektronická pečeť (prostá) může být

[73] Např. fotoaparát, rychlostní radar, jakékoli technické hardwarové zařízení nebo modul softwaru.

vytvořena libovolnou entitou, tedy i jen entitou technickou, osobou právnickou nebo osobou fyzickou.

Dle čl. 3 bodu 24 pro účely nařízení eIDAS však je **pečetící osobou** *„právnická osoba, která vytváří elektronickou pečeť"*. Toto definiční ustanovení však podle uvození článku 3 *„Pro účely tohoto nařízení se rozumí: ..."* znamená pouze to, že kdekoli v eIDAS se vyskytuje pojem pečetící osoba, je třeba ho vykládat podle definice, tj. považovat pojem za osobu právnickou a potenciálně provádějící činnost vytváření elektronické pečeti. Definiční bod 24 rozhodně neznamená, že pouze a jen právnické osoby mohou vytvářet elektronické pečeti prosté, protože součástí definičního bodu 25 tento subjekt není. Pro entitu, která takovou elektronickou pečeť prostou vytváří, je pak pouze třeba použít jiné označení, např. „tvůrce pečeti," nebo jakýkoli jiný vhodný termín, který nebude v kolizi s termíny nařízení eIDAS.

Význam rozlišení je však spíše kosmetický. Elektronické pečeti prosté, ať již je vytvořil kdokoli nebo cokoli, nesmí být upírány právní účinky a má obecnou důkazní přípustnost dle čl. 35 odst. 1 eIDAS (srov. níže 6.15.1). Tyto právní vlastnosti nejsou příliš významné. Termín pak slouží v eIDAS jako stavební pojem pro další definované termíny. Nic ale nebrání tomu, aby pojem *elektronické pečeti* prosté (s libovolným tvůrcem pečeti) nerozvinulo a nevyužívalo vhodným způsobem vnitrostátní právo členského státu, pokud nebude v rozporu s úpravou v nařízení eIDAS. Rozpor by mohl vzniknout, pokud by národní právo využívalo pojmy *zaručená elektronická pečeť* nebo *kvalifikovaná elektronická pečeť* nebo *kvalifikovaný certifikát pro elektronickou pečeť* bez vazby na právnickou osobu.

Vnitrostátní právo ale může zavést určité ekvivalenty uvedených pojmů, pochopitelně s jiným označením, a pravděpodobně by mohlo též využít technických *kvalifikovaných prostředků pro vytváření elektronických pečetí*. Při takovém rozšíření použití elektronické pečeti prosté je třeba pouze dbát na to, aby rozšíření nemělo charakter rozporu vůči institutům zavedeným v nařízení eIDAS, aby nerušilo jejich smysl nebo účel. Pokud by ale účel rozšíření byl rozumný, pak unijní legislativa nemůže být dostatečným důvodem pro brzdění technického rozvoje.

Z hlediska právního u elektronické pečeti (prosté) není stanoven žádný explicitnější cíl použití. Definováno není ani využití vůle osoby v pozadí, která zapřičinila vytvoření elektronické pečeti. Nařízení eIDAS tedy neurčuje, zda se

elektronická pečet smí využívat k provedení soukromého právního jednání, např. k uzavření smlouvy nebo k potvrzení úředního správního aktu, jako součást vydání rozhodnutí apod. To je snadno pochopitelné, má-li být institut elektronické pečeti použitelný a upravený jednotně pro 28 rozdílných právních řádů členských států, z nichž každý může k výše uvedeným otázkám přistupovat mírně odlišně.

Současně však nařízení eIDAS žádné cíle ani důvody použití elektronické pečetě nezakazuje. Je tedy na vnitrostátním právu, aby stanovilo okolnosti použití elektronických pečetí (prostých). Není tedy vyloučeno ani to, aby národní zákonodárce stanovil, že i elektronická pečeť prostá má funkci podpisu, nebo ji má aspoň za některých dalších vymezujících okolností. Důvodem je výše zmíněná téměř ekvivalence k pojmu elektronického podpisu (prostého) podle DirES. I v případě, kdy zákonodárce členského státu na vymezení těchto okolností při implementaci nařízení rezignuje, mohou tyto podmínky být nalezeny či stanoveny též až zpětně judikaturou, je-li to v souladu s metodikou funkce a stanovení či nalézání práva v daném členském státu.

6.6.2 Zaručená elektronická pečeť

Výše uvedená obecnost subjektu či entity u elektronické pečeti prosté zaniká již v případě **zaručené elektronické pečeti**. V jejím případě dle čl. 36 písm. a) a b) eIDAS se požaduje jednoznačné spojení s pečetící osobou (tj. osobou právnickou) a umožnění její identifikace. V čl. 36 písm. c) eIDAS se vyžaduje při vytváření zaručené elektronické pečeti udržení dat pro vytváření elektronických pečetí (soukromého klíče) pod svou kontrolou, tedy pod kontrolou právnické osoby, a to s vysokou úrovní důvěry. Všechny tři písm. a), b) a c) čl. 36 eIDAS se soustředí na to, jak zajistit *původ* dle definice elektronické pečeti prosté, zatímco písm. d) stejného článku zajišťuje požadavek *integrity* z dané definice.

Zmiňování využití *„dat pro vytváření elektronických pečetí"* v čl. 36 písm. c) eIDAS, k nimž párově náleží *„data pro ověřování platnosti"* (čl. 3 bod 40 eIDAS), znamená, že zaručená elektronická pečeť bude technicky využívat tzv. asymetrickou kryptografii veřejného klíče, ve kterém datům pro ověřování platnosti odpovídá technický pojem *veřejný klíč* a datům pro vytváření elektronických pečetí odpovídá technický pojem *soukromý klíč*. Požadavky čl. 36 eIDAS by samy o sobě nemusely nutně vést k technickému využití služeb tzv. certifikační autority, v praxi však využívány zřejmě budou. Lze pak hovořit o infrastruktuře veřejného klíče, zkráceně

označované jako PKI.[74] Provozovatelé služeb certifkačních autorit pak často[75] budou spadat pod pojem *„poskytovatel služeb vytvářejících důvěru“* (čl. 3 bod 19 eIDAS), pro nějž z nařízení plynou určité povinnosti (srov. níže).

Z hlediska technického přístupu k věci je zaručená elektronická pečeť ekvivalentem zaručeného elektronického podpisu až na to, že pečeť vytváří osoba právnická a podpis osoba fyzická. To se odráží v mnoha ustanoveních eIDAS o zaručených (kvalifikovaných) elektronických pečetích, pro které se stanoví přiměřeně podobné *(mutatis mutandis[76])* používání ustanovení o zaručených (kvalifikovaných) elektronických podpisech. Dtto ustanovení o prostředcích QSealCD jsou přiměřeně podobná pro ustanovení o prostředcích QSCD. To umožňuje valnou část technologií použít s mírnou modifikací pro případy obou druhů institutů.

Z hlediska právního ovšem nalézáme určité rozdíly a nelze vždy uvažovat jen zcela analogicky. Srovnáme-li definiční požadavky v čl. 36 pro zaručenou elektronickou pečeť oproti podobným v čl. 26 eIDAS pro zaručený elektronický podpis, pak jeden z rozdílů je v písmenech c). V případě zaručeného elektronického podpisu se vyžaduje *„výhradní kontrola"*, zatímco v případě zaručené elektronické pečeti se vyžaduje pouze *„kontrola"*. Důvodů může být několik. První může spočívat v tom, že právnická osoba nemá fyzické tělo ani fyzický mozek s vůlí.[77] Chybí tedy hmotný substrát, vůči němuž by se výhradnost kontroly mohla jasně vztahovat. Definice by v tomto smyslu mohla působit dokonce jako kontradikce, tedy nesplnitelně. Z hlediska užitečného účinku by však výklad tuto potíž nejspíš překlenul.

Z praktického pohledu budou aspoň při úvodním nasazování zaručené elektronické pečeti nějaké fyzické osoby jednat, jedna nebo více. Nařízení sice nevylučuje, že budou jednat bez odhalení své totožnosti,[78] ale nějaké fyzické osoby přinejmenším fakticky určité činnosti budou muset provést. Nařízení definičními požadavky přičítá data opatřená *zaručenou elektronickou pečetí* přímo pečetící osobě,

---

[74] Public Key Infrastructure.

[75] Výjimkou jsou například uzavřené systémy podle čl. 2 odst. 2 eIDAS.

[76] Doslovně zřejmě *„změnitelné změněno"*, znamená *„po změně toho, co se změnit má/musí“* a spadá k českým právním pojmům *obdobně* či *přiměřeně*. Autor používání *mutatis mutandis* řadí prvotně spíše k významu *obdobně*, ovšem s tím, že v rámci *mutatis mutandis* je někdy umožněna i vyšší variabilita, kterou by české právo vyjadřovalo pojmem *přiměřeně*. Proto překládá *přiměřeně podobný*.

[77] Uvedená zvláštnost právnické osoby pochopitelně nezůstala právní naukou nepovšimnuta, existují desítky teorií podstaty právnické osoby, z nichž nejčastější jsou teorie fikce a teorie reality. Právo EU však právě proto musí respektovat, že pojetí právnických osob v právních řádech členských států může být značně odlišné, a nespoléhat se ani neodvolávat se na jedno teoretické pojetí.

[78] Záleží na tom, zda tuto možnost v souladu s čl. 24 odst. 1 eIDAS připouští vnitrostátní právo.

tedy osobě právnické, jejíž identifikace je možná, a to co do původu a co do integrity (nezměněnost). Nařízení tedy nevylučuje, že (aspoň fakticky) bude vytvářet elektronické pečetě více fyzických osob současně, ať již časově zároveň, nebo postupně. V tomto důvodu pak může spočívat druhý důvod vypuštění slova *výhradně*. Požadavky dle čl. 36 písm. c) pouze stanoví, že data pro vytváření elektronické pečetě může použít pod svou kontrolou, s vysokou úrovní důvěry, právnická osoba. Pro další rozdíly srov. diskurs o důkazních účincích kvalifikované elektronické pečeti v 6.15.8

Požadavky na zaručené elektronické pečetě například nevylučují ani to, že jsou data pro vytváření elektronických pečetí duplikována a poskytnuta do fyzického držení více fyzickým osobám. Obdobně je možné, že sice data pro vytváření elektronických pečetí duplikována fyzicky nejsou, ale více fyzických osob obdrží přístup k jejich současnému použití a k vytváření zaručené elektronické pečetě dané právnické osoby.

V nařízení bohužel chybí explicitní povinnosti pečetící osoby nebo jejích pracovníků pro způsob správy dat pro vytváření elektronických pečetí i pro samotné vytváření elektronických pečetí. Chybí i odpovědnost právnické osoby za tyto činnosti. Tyto povinnosti nebo odpovědnost může ale stanovit implementace členského státu jako doplnění nařízení. V některých členských státech může vyplývat (srov. níže) z obecných pravidel odpovídání za škodu.

Nařízení stanoví právně pro zaručené elektronické pečetě bez dalšího jen stejné právní účinky a stejnou důkazní přípustnost jako pro elektronické pečetě prosté, tj. podle čl. 35 odst. 1 eIDAS. Právní stejnost důkazní přípustnosti však neznamená, že důkaz bude v praxi stejně přesvědčivý. Je-li spoléhající osoba schopna prokázat, že jí předkládaná elektronická pečeť je zaručená elektronická pečeť, pak ze splňování jen zákonných požadavků na ni lze dovodit poměrně vysokou úroveň přesvědčivosti. Komise může dle čl. 37 odst. 4 vyhlásit referenční čísla norem. Odpovídání těmto normám zakládá domněnku vyhovění požadavkům na zaručené elektronické pečeti podle čl. 36 eIDAS, tj. že se jedná o zaručenou elektronickou pečeť.

Právo členského státu může případně implementací nařízení eIDAS doplnit jiné právní účinky nebo důkazní účinky, které chce ve svém právním řádu přičítat zaručeným elektronickým pečetím (bod odůvodnění 22 eIDAS).

6.6.3 Kvalifikovaná elektronická pečeť

Dle čl. 3 bod 27 eIDAS je **kvalifikovanou elektronickou pečetí** *„zaručená elektronická pečeť, která je vytvořena pomocí kvalifikovaného prostředku pro vytváření elektronických pečetí a která je založena na kvalifikovaném certifikátu pro elektronickou pečeť“*.

Všechny tři náležitosti jsou analogií tří náležitostí kvalifikovaného elektronického podpisu. Kvalifikovaný elektronický certifikát pro elektronickou pečeť (čl. 38 a příloha III) slouží pro zajištění požadavků čl. 36 písm. b) a liší se zejména v tom, že certifikovaným subjektem není fyzická osoba, ale právnická osoba, pro kterou v kvalifikovaném certifikátu musí být uvedeno *„alespoň jméno pečetící osoby a případné registrační číslo uvedené v úředních záznamech"* [příloha III písm. c)].

Pro prostředek QSealCD již ani nebyla sepsána zvláštní příloha, ale v čl. 39 eIDAS se přikazuje přiměřeně podobné *(mutatis mutandis)* použití čl. 29 až 31 eIDAS, které se týkají QSCD. Prostředek QSealCD zajišťuje splňování požadavků čl. 36 písm. a), c) a d) eIDAS, jako prostředek QSCD zajišťuje splňování požadavků čl. 26 písm. a), c) a d) eIDAS (srov. 6.10).

Pro ověřování platnosti kvalifikované elektronické pečeti se dle čl. 40 eIDAS používá přiměřeně podobně postup podle čl. 32 resp. dle čl. 33, pokud je delegováno na poskytovatele služeb.

Důkazní účinky kvalifikované elektronické pečeti (6.15.8) se nicméně významně liší a paradoxně jsou mnohem silnější než důkazní účinek kvalifikovaného elektronického podpisu (6.15.6).

6.6.4 Význam zaručené (kvalifikované) elektronické pečeti a automatizace

Asi každý právník při střetu s předpisy práva EU čelí té potíži, že má tendenci číst a vykládat tyto předpisy přes chápání pojmů, institutů a konceptů, které existují v jeho domácím právním řádu, na které je zvyklý. Sejmout tyto náhledové brýle je možné až po delším studiu daného předpisu, popř. důkladném osvojení si hledět na právo EU přes jeho vlastní metodiku, přístupy a paradigmata.

České odborné prostředí bylo zvyklé na používání elektronické značky pro účely automaticky vytvářených podpisů, například v rámci činnosti elektronických podatelen, potvrzujících přijaté zpráva. S nařízením eIDAS vzniká bolestná mezera, neboť institut

elektronické značky v nařízení eIDAS chybí. V německém právním řádu institut elektronické značky neexistoval, a proto jej němečtí právníci nepostrádají. V ČR tak vznikl dojem, že jelikož v případě úřadů aj. subjektů veřejné správy nebo veřejné moci se často jedná o subjekty, které částečně mají charakter právnických osob, bude možné nepřevzatou elektronickou značku nahradit zaručenou (kvalifikovanou) elektronickou pečetí. Tak kupříkladu: „Dosavadní právní úprava[79] znala institut elektronické značky, který bude nahrazen právě elektronickou pečetí".[80] Nebo: „...můžeme vyvodit, že elektronická pečeť je *de facto* elektronickou značkou právnické osoby."[81] De facto sice technické srovnání provádí i sám autor výše, aby odůvodnil technickou či organizační podobnost, nikoli však nutně stejné právní vlastnosti. Pro právní posuzování, stanovení právních účinků nemusí být argument vhodný. Dále: „Elektronická pečeť bude mít využití zejména v oblasti automatizace, příkladmo při vystavování elektronických daňových dokladů..."[82] Zde se je již možné ptát, proč by právnické osoby měly mít možnost vystavovat daňové doklady automaticky, ale podnikající fyzické osoby (v ČR) nikoli. Podobně i Kunt a Lechner: „Elektronickou značku ... nařízení nahrazuje elektronickou pečetí,"[83] přičemž ale připouští, že zde jsou největší rozdíly vůči dřívější úpravě.

Zcela obdobně uvažovali již dříve jiní autoři (Smejkal – Kodl – Uřičař): „V Nařízení se [české elektronické] značky objevily, neboť všeobecná užitečnost takového nástroje je známa, a to jako ‚elektronické pečeti'. Anglický termín ‚seal' mohl být ovšem přeložen také jako ‚razítko', neboť o to v Nařízení právě jde."[84] Konsekventně také uvažují o tom, že účelem (zaručené) elektronické pečeti je být přídavným autentizačním technickým prvkem, asi jako bývá tradiční gumové razítko. Tito autoři si však již kladou otázku, proč není zaručená elektronická pečeť připuštěna pro fyzické osoby, zejména fyzické osoby podnikající,[85] resp. to považují za vadu regulace v eIDAS.

Dle autora znak automatizace[86] vytváření však není v eIDAS znakem ani zaručeného elektronického podpisu, ale ani zaručené elektronické pečeti. Předně tento

[79] Míněn je zákon č. 227/2000 Sb., o elektronickém podpisu, ve znění před zrušením.
[80] DONÁT, J. – MAISNER, M. – PIFFL, R., cit. dílo, s. 37.
[81] DONÁT, J. – MAISNER, M. – PIFFL, R., cit. dílo, s. 149.
[82] DONÁT, J. – MAISNER, M. – PIFFL, R., cit. dílo, s. 149.
[83] KUNT, M. – LECHNER, T., cit. dílo, s. 61.
[84] SMEJKAL, V. – KODL, J. – UŘIČAŘ, M. Elektronický podpis podle nařízení eIDAS. *Revue pro právo a technologie* [online]. 2015, roč. 6, č. 11, s. 215–216.
[85] SMEJKAL, V. – KODL, J. – UŘIČAŘ, M., cit. dílo, s. 216–217.
[86] Jak byl uveden v § 3a odst. 2 zák. č. 227/2000 Sb. pro elektronickou značku.

znak nařízení eIDAS neuvádí v případě ani jednoho z těchto pojmů, ale ani pojmů podkladových, jako je elektronický podpis (prostý) nebo elektronická pečeť (prostá). To dle autora znamená, že znak automatizace ani nepředepisuje, ale ani nezakazuje.

Je-li třeba stvrzení *(„podpis")* vytvářet automatizovaně, lze využít zaručené elektronické podpisy a zaručené elektronické pečetě zcela rovnocenně. Stejný závěr poskytuje základní právo rovnosti před zákonem dle čl. 20 Listiny ZPEU, stejné právo v ústavách členských států, ale i obecná zásada nediskriminace v unijním právu.

Není možné nadat pouze právnické osoby zvláštním režimem provádění jednání, který by byl fyzickým osobám upřen a poskytoval právnickým osobám neospravedlnitelnou výhodu. Buď oba instituty (zaručený elektronický podpis, zaručená elektronická pečeť) lze použít i pro automatizovaná vytváření, anebo ani jeden. Z těchto možností se autor jednoznačně kloní k tomu, že automatizované vytváření lze provádět oběma instituty. Nezmínění podmínky automatizace znamená, že znak není zakázaný. Nařízení eIDAS pak navíc v řadě případů, ve kterých se fakticky jedná o automatizované vytváření,[87] explicitně stanoví použití zaručeného elektronického podpisu, anebo zaručené elektronické pečeti, a to jako rovnocenných možností.

Výše uvedené vede autora na odlišné právní hodnocení významu zaručené elektronické pečeti, než zastávají všichni výše uvedení čeští komentátoři a dost možná i další čeští právníci. Jestliže totiž znak automatizace právně není odlišujícím znakem zaručené elektronické pečeti, nemůže být ani jejím účelem. Pak je ale nutné se ptát, co je skutečným účelem zaručené elektronické pečeti v eIDAS. Dle autora jedinou zbylou odpovědí je, že právním účelem zaručené elektronické pečeti v eIDAS je být „něco jako podpis" osoby právnické, aniž by právně podpisem výslovně byla. Z tohoto úhlu pohledu již zanikají i námitky, proč není zaručená elektronická pečeť dovolená fyzickým osobám.Chyba: zdroj odkazu nenalezen

Zbývá zodpovědět, proč nařízení eIDAS zaručenou nebo kvalifikovanou elektronickou pečeť nedefinuje výslovně jako podpis právnické osoby. Důvodem zřejmě především je, že se jedná o unijní právní předpis, který musí být možné sloučit s právními řády všech 28 členských států. Z nich zřejmě pouze některé připouští, aby se právnická osoba podepisovala přímo, bez uvedení skutečně jednající fyzické osoby.

[87] Poskytovatelé služeb vytvářejících důvěru vytváří zaručený elektronický podpis nebo zaručenou elektronickou pečeť prakticky nutně automaticky pro účel čl. 33 odst. 1 písm. b), čl. 42 odst. 1 písm. c) a čl. 44 odst. 1 písm. d) eIDAS, a v praxi běžně automaticky pro účel čl. 28 odst. 1 ve spojení s přílohou I písm. g) a čl. 38 odst. 1 ve spojení s přílohou III písm. g) eIDAS.

Nařízení zde proto pouze nabízí právní pojem, který zajišťuje původ a integritu dat. Nařízení preventivně uhýbá národním právním řádům, aby v nich nevytvářelo kolizi.

Je věcí vnitrostátní implementace, jak bude unijní právní pojem recipovat. Nehodí-li se pro vnitrostátní právo, může jej implementace až ignorovat. V takovém členském státu zaručená elektronická pečeť pak zřejmě bude mít na první pohled zejména právní užití uvedená v nařízení eIDAS samém.Chyba: zdroj odkazu nenalezen Z mlčení implementace však ani pak neplyne, že zaručenou elektronickou pečeť nelze ve vnitrostátním právním styku vůbec využívat (srov. diskurs k významu pojmu níže). Jinou možností je, že implementace zaručenou elektronickou pečeť výslovně připustí pro některé účely potvrzování komunikace v elektronické podobě, které v právu daného členského státu zřejmě dosud neměly obdobu při komunikaci právnické osoby v listinné podobě. Vnitrostátní implementace může taková použití naopak i zakázat. Další možností je, že implementace pojem namapuje na některý tradičně užívaný autentizační prvek, jako je třeba právě tradiční vosková pečeť či modernější gumové inkoustové razítko, ovšem pouze pro právnické osoby. Konečně asi poslední možností je implementační připuštění, že bude představovat přímo podpis právnické osoby.

Namapování zaručené elektronické pečeti na voskovou pečeť ve vztahu k právnické osobě je dobře myslitelné v právu common law. V něm existuje institut tzv. korporátní pečetě[88] *(corporate seal)*, s nímž common law spojuje řadu právních účinků.[89] Používání korporátní pečeti v common law však mělo svůj vrchol před rokem 1900, součástí dnešního common law zůstává jen díky setrvačnosti, aniž by mělo původní význam.

Že je dobře myslitelné uvažovat o zaručené elektronické pečeti jako o svého druhu „podpisu" právnické osoby, plyne i z rozboru teorie komitmentů podpisu (srov. 4.7.2), jak je podáván evropskými technickými normami z ETSI. Podle nich důkaz původu *(proof of origin)* má význam, že podepisující uznává, že vytvořil, schválil a odeslal podepsaná data. Z toho zejména akt schválení *(approval)* v sobě obsahuje složku vůle. Záleží pak již čistě na obsahu samém, zda z něj vyplývá, že subjekt se považuje obsahem vázán ve smyslu právního jednání, nebo zda obsah poskytuje jiný smysl. Stejně by tomu bylo i v případě (vlastnoručního) podpisu. I v jeho případě může až podepsaný obsah určit, zda celek má charakter právního jednání, nebo jiný.

---

[88] LINDGREN, K. E. The Positive Corporate Seal Rule and Exceptions Thereto and the Rule in Turquand's Case. *Melbourne University Law Review*. Vol. 9, Sep 1973, s. 192–219.

[89] THOMPSON, S. D. *Commentaries on the Law of Private Corporations (1908–1915),* s. 997–1030.

Právě uvedené pojetí původu proráží tezi, že užití zaručené elektronické pečeti nemůže být či „není spojeno s vyjádřením vůle".[90] Nejsou-li na první pohled zcela zřejmé všechny možné funkce (vlastnoručního) podpisu, kterými jsme se zabývali v kapitole 4, není možné nijak úzce či omezeně chápat ani pojem původu a je nutné připustit, že někdy je původnost dokonce cennější a přímější vlastnost[91] než podpis, který bývá pouze prostředkujícím prvkem, z jehož pravosti se usuzuje na původnost či pravost jím podepsaného obsahu.

V podstatě stejně zachází s podpisem i kryptologie (srov. 4.6.1) v případě digitálních podpisů, tj. těch, které odpovídají metodice zaručených a kvalifikovaných elektronických podpisů a pečetí. Podpis pak spojuje zprávu se „způvodňující" *(originating)* entitou. Účelem digitálního podpisu v obecném smyslu tedy je určit původce zprávy, přičemž v kryptologii původcem může být obecná entita, nikoli nutně osoba fyzická, ev. osoba právnická. Zda celek je právním jednáním, bude opět plynout až z toho, kdo byl podepisující entitou, z obsahu zprávy samé, jakož i ze způsobu, kterým byla zpráva vytvořena a vytvořen její podpis.

Jinak řečeno, jestliže se při popisu funkcí podpisu právní teorie či kryptologie velmi často odkazují na určení původce či původu zprávy či písemnosti, platí uvedené relace i naopak. Z toho, že někdo je původcem zprávy či písemnosti, lze usuzovat, že na původce lze do značné míry hledět tak, jako kdyby zprávu podepsal. Právní rozdíl bude tehdy, pokud právo výslovně vyžaduje přítomnost podpisu, ale ten chybí.

Obdobně uvažoval i Polčák v kontextu starého i nového českého občanského zákoníku ohledně možných způsobů, kterými lze z elektronické písemosti vytvořit písemné právní jednání: „Postačí totiž, pokud je takový úkon buďto podepsán, nebo opatřen obdobnou autentizační informací doplněnou mechanicky... I v případě, pokud by zákon pro povinně poskytované informace [...vyžadoval formu...] písemného právního jednání, bylo by lze dostát zákonným požadavkům u elektronických písemností prostě tak, že by se na závěr textu umístila identifikační informace o jeho původci (tj. například firma a adresa příslušného podnikatele)."[92] Polčák zde tedy

[90] KUNT, M. – LECHNER, T., cit. dílo, s. 62.

[91] Tak kupř. § 562 odst. 1 obč. zák. umožňuje alternativní možnost splnění písemné formy právního jednání, která má za podmínky „zachycení jeho obsahu" a „určení jednající osoby". Druhou podmínku lze považovat i za určení *původu* či *původce* daného právního jednání. Jinou právní otázkou je, zda právní řád ČR připouští, aby jednající osobou byla osoba právnická, nebo zda ji musí být osoba fyzická. Pro podrobnosti k výkladu § 561 a § 562 obč. zák. srov.

[92] POLČÁK, R. Elektronické právní jednání – změny, problémy a nové možnosti v zákoně č. 89/2012 Sb. *Bulletin advokacie*. 2013, č. 10, s. 36.

připouští i jen autentizačně a důkazně mnohem slabší identifikační (autentizační) informaci, než je zaručená elektronická pečeť, pouhé „připojení dvou řádků prostého textu".[93]

Lze tedy říci, že právně má důkaz původu, zejména vedený ze stvrzujícího elementu jako je zaručená elektronická pečeť, v zásadě stejný charakter, jako má přítomnost podpisu, z nějž lze původ též prokázat, až na to, že je jazykově použito jiné označení. Bez dalšího tedy nebude možné v některém vnitrostátním právu tvrdit, že zaručená nebo kvalifikovaná elektronická pečeť splňuje právní požadavek na přítomnost podpisu. Není-li však tento požadavek právně stanoven, může zaručená nebo kvalifikovaná elektronická pečeť fakticky plnit i funkce podpisu v podstatě shodně, jako by to činil podpis. Z hlediska důkazního je pak v případě kvalifikované elektronické pečeti důkazní funkce dokonce silnější (srov. 6.15.8) než u kvalifikovaného elektronického podpisu (srov. 6.15.6), neboť přímo platí domněnka správnosti původu dat. Není tedy třeba ani dokazovat způsob vytvoření kvalifikované elektronické pečeti atp.

Ačkoli se tedy autor zdráhá vyslovit, stejně jako jiní autoři, že by zaručená elektronická pečeť byla právně podpisem, je na rozdíl od jiných názoru, že jejím účelem a smyslem je se institutu podpisu v maximální možné míře přiblížit, a to i pro potenciální případy použití jako stvrzení u právního jednání.

Bez dalšího ovšem nelze zaručenou elektronickou pečeť použít namísto podpisu pro písemné právní jednání, ev. právní jednání v písemné formě, neboť to typicky vyžaduje právě přítomnost podpisu. I v případě, když rozhodné právo tyto náležitosti nestanoví, je třeba zjistit, zda připouští, aby pro dané právní jednání byla vůle projevována přímo na úrovni právnické osoby. Pokud tomu tak není, tj. pokud z rozhodného práva plyne potřeba určení konkrétní fyzické osoby, která projevuje svou vůli a jedná za právnickou osobu, zaručená elektronická pečeť běžně nebude tím prvkem, který by uvedené náležitosti vyjadřoval. V těchto všech případech bude možné zaručenou elektronickou pečeť použít nejvýše jako doprovodný bezpečnostní prvek, který má určitý důkazní význam, z hlediska plnění náležitostí právního jednání je však na první pohled irelevantní.

Že se mají zaručené (kvalifikované) elektronické pečeti uvažovat i v kontextu právního jednání, plyne též z bodu odůvodnění 58 nařízení eIDAS, který vyjadřuje

[93] POLČÁK, R. Elektronické právní..., cit. dílo, s. 36.

předpoklad, že se kvalifikované elektronické pečeti mohou právně vyžadovat pro elektronické transakce (srov. 6.1.4). Nařízení zde obsahuje doporučení či výkladové vodítko, že požadavek má být nahraditelný kvalifikovaným elektronickým podpisem oprávněného zástupce právnické osoby.

Autor též upozorňuje na zvýšený normativní význam praxe či obyčejů. Jinak řečeno, to, k čemu se zaručené elektronické pečeti budou skutečně používat, může než příkazem shora dolů spíše plynout z autonomní seberealizace subjektů v právním styku, tedy z toho, k čemu je subjekty samy budou chtít především využívat (srov. též 4.7.4).

Znak automatizovatelnosti vytvoření u zaručené elektronické pečeti autor naopak považuje za právně irelevantní. Autor tím nijak nepopírá, že z hlediska praktických případů užití mohou být zaručené elektronické pečeti nakonec používány právě pro situace, v nichž dochází k automatizovanému potvrzení dat. Takové případy užití mohou zahrnovat i mnohé situace, kdy se stvrzuje obsah, který vůbec nemá povahu právního jednání, tedy například potvrzení výpisu z rejstříku, osvědčení určité informace, vydání datového záznamu z dlouhodobé úložiště apod. Autor však upozorňuje, že ve stejné situaci, za účelem automatizace, pak fyzická osoba může zcela shodně použít zaručený elektronický podpis. Používání obou pojmů by proto v právní rovině nemělo předpokládat dichotomii založenou na automatizaci.

Autor pochopitelně připouští, že pro činnosti právnických osob, které častěji mají povahu trvalejší průběžné činnosti, vyžadující vzájemnou zastupitelnost zúčastněných fyzických osob, bude současně charakteristická vyšší míra využití systémů informačních technologií pracujících v automatickém režimu. V důsledku toho se zaručené elektronické pečeti mohou v automatickém režimu používat častěji, než tomu bude v případě zaručených elektronických podpisů v automatickém režimu. Takový stav však nebude výsledkem právní definice nebo právních podmínek v eIDAS, ale působení ekonomických nebo organizačních vlivů.

Autor se dále domnívá, že pojem původu, jehož správnost mají zaručené nebo kvalifikované elektronické pečeti prokazovat, je rozšiřitelný a relativizovatelný i subjektově. Nedomnívá se proto, že AdESeal „není použitelná pro automatizované označování dokumentů v rámci digitálních úložišť ani systémů pro doporučené elektronické doporučování, jako je třeba informační systém datových schránek“,[94] tj. že by AdESeal mohl vytvořit jen ten, kdo dokument vytváří, tj. jeho nejpůvodnější

[94] KUNT, M. – LECHNER, T., cit. dílo, s. 62–63.

původce. Význam „původnosti“ se takovým použitím pochopitelně subjektově posouvá a uvedené posunutí musí být indikováno. To nemusí být ale vůbec na škodu, neboť se tím zřetelněji dává najevo, že v uložení dokumentu vystupoval prostředník. Použití AdESeal (nebo AdES) pro služby elektronického doporučeného doručování je pak výslovně uvedeno v čl. 44 odst. 1 písm. d) eIDAS, nic zásadního tedy nebrání v analogickém právním použití pro informační systém datových schránek. V obou případech pochopitelně musí právní i technická implementace dát najevo, že AdESeal (nebo AdES) potvrzuje především určitou doložku[95] o přijetí dat k odeslání nebo o jejich doručení, nikoli jen původní data samotná. Pokud by se potvrzovala pouze původní data, nebezpečí záměny významu „původnosti“ by bylo reálné a pro takový způsob chápání výše citovaná tezeChyba: zdroj odkazu nenalezen autorů Kunt a Lechner je plně případná.

6.6.5 Automatické vytváření kvalifikované elektronické pečeti?

Bezprostředně výše je dovozeno, že zaručené elektronické pečeti, popř. zaručené elektronické podpisy lze použít při požadavku na jejich automatické vytváření. Navazující otázkou je, zda pro automaticky vytvářená stvrzení (něco jako „podpisy“) je možné využívat i kvalifikované elektronické podpisy nebo kvalifikované elektronické pečeti. Dle názoru autora bude odpověď na tyto dvě otázky buď ano, anebo nikoli, ale opět shodně. Znovu je třeba konstatovat, že nařízení eIDAS znak automatizace výslovně nezmiňuje ani nezakazuje ani u kvalifikovaných verzí elektronického podpisu nebo elektronické pečeti.

Jelikož požadavky čl. 26, resp. čl. 36 eIDAS dle výkladu výše musí umožňovat automatické vytváření zaručených elektronických podpisů, resp. pečetí, je odpověď nutné hledat v požadavcích na QSCD, resp. QSealCD podle přílohy II eIDAS. Z těchto požadavků je jediný kritický dle přílohy II odst. 1 písm. c), že QSCD, resp. QSealCD musí zajistit, aby: *„oprávněná podepisující [pečetící] osoba měla možnost data pro vytváření elektronických podpisů [pečetí] použitá při vytváření elektronického podpisu [pečeti]* ***spolehlivě chránit*** *před jejich zneužitím třetí osobou"* (zvýraznil autor). Je otázkou, zda spolehlivá ochrana zahrnuje využití druhé formy autentizačního faktoru (např. PIN, otisk prstu apod.), anebo zda může být realizována i nějak jinak. Pokud by se výrobcům podařilo provést a zejména nechat certifikovat jiná řešení se spolehlivou ochranou před zneužitím třetí osobou v rámci automatického nasazení, je s takto

[95] Doložka by měla být jednoznačně navázaná na původní data, kterých se týká.

certifikovanými QSCD nebo QSealCD následně myslitelné i automatické vytváření QES nebo QESeal bez toho, aby to vyvolávalo právní pochybnosti z pohledu vyhovování nařízení eIDAS. Zda tomu tak bude, považuje autor za otevřenou otázku.

Prozatím o výkladu rozhoduje především obsah vyhlášených technických norem podle čl. 30 odst. 3 eIDAS, dle nichž se mají QSCD a potažmo i QSealCD certifikovat.

Podle dosud vyhlášené normy EN 419211-2 se vytvoření digitálního podpisu má provádět těmito „následujícími kroky:

1. vybrat SCD,[96] pokud jich je v SSCD přítomno více;
2. autentizovat podepisujícího a určit jeho úmysl podepsat;
3. přijmout data určená k podpisu nebo jejich jedinečnou reprezentaci (DTBS/R);[97]
4. použít patřičnou kryptografickou funkci vytvoření podpisu s použitím SCD na DTBS/R.“[98]

Postup tedy předpokládá provedení autentizace podepisujícího i ověření jeho úmyslu podepsat v rámci každého průběhu vytvoření digitálního podpisu pomocí SSCD. Jelikož technická norma je vyhlášena pro certifikaci QSCD, jedná se o vlastnosti QSCD a potažmo o možnost vytvoření QES ev. QESeal.

Současně je ale ve stejné technické normě uveden popis činnosti prostředku tak, že „TOE[99] může poskytovat přímé uživatelské rozhraní pro příjem ověřovacích autentizačních dat (VAD)[100] od uživatele; alternativně může TOE přijmout VAD od aplikace vytvářející podpis. Pokud aplikace vytvářející podpis zpracovává, vyžaduje nebo získává VAD od uživatele, předpokládá se ochrana důvěrnosti a integrity těchto dat.“[101] Provedení QSCD splňující EN 419211-2 tedy nevylučuje, že vůči němu externí aplikace vytvářející podpis nebude mít sama ověřovací data VAD uložena (kešována) a že je nepoužije samočinně, ať již v rámci dávkového podpisu, nebo zcela automatizovaného podpisu. Taková použití se sice zdají být proti záměru technické normy EN 419211-2, jelikož ale aplikace vytvářející podpis není předmětem regulace

96 SCD znamená *Signature Creation Data*. Jedná se o pojem zavedený technickými normami pro data pro vytváření elektronického podpisu v terminologii eIDAS, resp. soukromý klíč v terminologii PKI.
97 DTBS/R znamená *Data To Be Signed/or Representation*.
98 EN 419211-2 Protection profiles for secure creation device – Part 2: Device with key generation, s. 7.
99 TOE je Target of Evaluation, tj. předmět hodnocení. Zde SSCD resp. QSCD. Jedná se o pojem technických norem v rámci ISO 15408.
100 VAD jsou *Verification Authentication Data*, tedy ověřovací autentizační údaje, jako jsou PIN nebo výsledek biometrické operace. Jedná se o pojem technické normy.
101 EN 419211-2, cit. dílo, s. 6.

v nařízení eIDAS, nebude se její vývojář zřejmě dopouštět porušení žádné právní normy stanovené přímo v eIDAS. Praxe tak může přinést podpisy QES či pečetě QESeal, vytvořené prostředky QSCD nebo QSealCD certifikovanými dle uvedené normy, které budou mít všechny znaky QES nebo QESeal, ačkoli mohly být vytvořeny dávkově nebo automatizovaně. Jaké bude výsledné právní hodnocení takové situace, považuje autor zatím za nejasné, vyvolávající právní nejistotu. Případné zneužití třetí osobou za takové situace by autor měl tendenci přičítat k tíži podepisující osoby, neboť spoléhající se osoba běžně nemá možnost rozlišit, v jakém režimu daný QES nebo QESeal vznikl a předpokládá funkci QSCD nebo QSealCD v souladu s eIDAS a potažmo s technickou normou, podle níž byly certifikovány. Jelikož potřeby praxe jsou rozmanité a určitě směřují i tímto směrem (např. aspoň jako kešování PIN), autor předpokládá, že se i tyto případy v praxi vyskytnou a budou pak vznikat výše uvedené pochyby a úvahy.

6.6.6 Případy užití pro zaručenou a kvalifikovanou elektronickou pečeť

Z nařízení není patrné, jaký způsob užití nebo úprava kterého právního řádu byla předobrazem zařazení zaručených nebo kvalifkovaných elektronických pečetí do eIDAS. Z autorovi známých případů by do úvahy snad přicházelo považování pouhého uvedení názvu společnosti za podpis v některých kauzách common law,[102] ale rovněž případ korporátní pečeti,Chyba: zdroj odkazu nenalezen, Chyba: zdroj odkazu nenalezen opět z common law. Vyloučit ale nelze ani to, že se jedná o zcela originální počin unijního práva, přijatý s ohledem na elektronickou praxi.

Právně bezesporným případem užití *(use case)* zaručených elektronických pečetí je jejich využívání poskytovateli služeb vytvářejících důvěru, a to přímo podle znění samotného nařízení eIDAS.Chyba: zdroj odkazu nenalezen

Z analýzy provedené v kapitole 10.3 plyne, že zaručená elektronická pečeť je použitelná pro přídavné potvrzování informací poskytovaných v rámci provozu elektronického obchodu právnickou osobou, pro které unijní právo předpisuje formu takzvaného trvalého nosiče *(durable medium)*, jež pro český právní řád byla transponována na textovou podobu (§ 1819 obč. zák.). Takové potvrzování není právně nijak povinné, může být vynecháno. Fakticky však může poskytnout vyšší bezpečnost a právně vyšší právní jistotu v důkazní rovině. Jelikož i tento případ užití vychází z práva EU, vnitrostátní transpozice by měly být ve všech členských státech dostatečně

[102] MASON, S. *Electronic Signatures...*, cit. dílo, 2012, s. 45–50.

shodné a zakládat možnost automatizovaného uzavírání smlouvy v rámci obecného elektronického obchodu dle práva kteréhokoli státu EU bez toho, aby byla uváděna fyzická osoba zastupující právnickou osobu nebo požadován doklad projevu vůle takové fyzické osoby. Neplyne-li to již ze samotného znění vnitrostátního právního předpisu, mělo by to být možné vyložit eurokonformním výkladem při uvážení zásady přednosti práva EU. V praxi přesto lze doporučit právní kontrolu úpravy v uvažovaném právním řádu, vedenou i s ohledem na přesný předmět obchodování.

V přeshraničním styku by používání kvalifikované elektronické pečeti mohlo mít zvláštní smysl v kombinaci s používáním kvalifikovaného elektronického podpisu. Pečeť by zde jednoznačně identifikovala právnickou osobu, neboť kromě názvu musí být v kvalifikovaném certifikátu i případné registrační číslo uvedené v úředních záznamech. Pojmem název autor v kontextu unijního práva rozumí firmu včetně dodatku,[103] určujícího typicky právní formu právnické osoby. Podpis by pak identifikoval jednající fyzickou osobu. Nařízení nestanoví žádná pravidla o posloupnosti. Takový postup může být případně určen vnitrostátním právem nebo mohou být podpis a pečeť vytvořeny k potvrzovaným datům i souřadně, tj. bez pořadí. Z bodu odůvodnění 58 nařízení eIDAS plyne, že použití s QESeal by nemělo být vyžadováno právně, dobrovolné použití ale může poskytovat protistraně velmi dobrou důkazní jistotu o subjektu, který právně jedná, byť kvalifikovaná elektronická pečeť bez dalšího poskytuje pouze důkaz o původu, a nikoli o jednající osobě.

Používání pro potvrzování přímo jménem právnické osoby obecně může mít smysl tehdy, pokud je součástí nějakého informačního systému nebo provozu, který je vhodné mít v provozu buď nepřetržitě, nebo aspoň nezávisle na konkrétní fyzické osobě. Taková nahraditelnost či zastupitelnost je často požadována pro moderní obchodní procesy, ale i ve veřejné správě. Vztah fyzické osoby k osobě právnické může rychle zaniknout. Zaměstanec může obdržet nebo podat výpověď z pracovního vztahu, a dokonce i člen statutárního orgánu může být z funkce odvolán a nahrazen jinou osobou. Všechny fyzické osoby může potkat úraz nebo dojít k jejich i nenadálému úmrtí třeba v důsledku dopravní nehody. Ve všech takových případech může mít právnická osoba snahu udržet v chodu nějaký technický systém, který jejím jménem potvrzuje data. Takový systém nemusí provádět vytváření zaručené elektronické pečeti zcela

[103] Někdy je označován za přístavek.

automaticky, ovšem často bude. Zda je v těchto případech možné použití zaručené elektronické pečeti právně, je nutné ověřit v rozhodném právu.

Pro případy užití může mít význam i jiný důkazní účinek, který je u kvalifikované elektronické pečeti (6.15.8) vyšší než u kvalifikovaného elektronického podpisu (6.15.6).

Zaručené a kvalifikované elektronické pečetě pochopitelně mohou sloužit i pro potvrzování v rámci jiných činností, než je právní jednání. To plyne i z bodu odůvodnění 59 eIDAS, který pouze obecně stanoví, že mají poskytovat jistotu o původu a integritě elektronického dokumentu, že elektronický dokument určitá právnická osoba vydala. Mohou být používány i pro potvrzování softwarového kódu nebo serverů, tj. programů.

6.7 Elektronické časové razítko

Nařízení definuje pojem elektronického časového razítka.

6.7.1 Kvalifikované elektronické časové razítko (QTS)

Nařízení eIDAS zavádí i *kvalifikovaná elektronická časová razítka* (QTS[104]). Jejich účelem je potvrzovat existenci orazítkovaných dat k datu a času uvedeném v QTS. Vydává je kvalifikovaný poskytovatel.

Hlavním případem užití QTS v návaznosti na elektronický podpis je přerazítkovávat spojení podepsaných dat a podepisujícího QES,[105] aby se pokryla možnost zneplatnění nebo expirace kvalifikovaného certifikátu, na němž je QES založen.[106] To pak umožňuje ověřovat platnost QES i ve střednědobém horizontu (např. 3–5 let, podle doby platnosti QTS[107]).

Ačkoli znění eIDAS výslovně neuvádí, zda a kdy se má provádět ověřování platnosti QES, aby se mohly použít právní normy eIDAS používající pojem QES, autor je zde názoru, že existence QES není bez dalšího nijak zřejmá. Tj. kdykoli spoléhající osoba se chce spolehnout na právo v eIDAS, měla by si napřed provést technické ověření platnosti QES v souladu s čl. 32 nebo 33 eIDAS. Bez tohoto ověření není

[104] Qualified electronic Time Stamp.
[105] Ale třeba i s AdES, anebo spojení s pečetí AdESeal nebo QESeal. Alternativou zachovávající důvěrnost podepsaných dat i před poskytovatelem je přerazítkovávat jen samotný podpis QES, AdES atd.
[106] V tomto textu nuance s ověřováním času vytvoření podpisu do značné míry pomíjíme.
[107] Závažné podrobnosti dlouhodobého uchovávání zde také pomíjíme.

možné uvažovat o reálné existenci QES a aplikovat související právní normy z eIDAS. Časové razítko QTS je pomocným digitálním objektem, který prodlužuje dobu ověřitelnosti platnosti QES, ale i QESeal, AdES, AdESeal atd.

Dle čl. 42 odst. 2 eIDAS: *„U kvalifikovaného elektronického časového razítka platí domněnka **správnosti data a času**, které udává, a **integrity dat**, s nimiž jsou toto datum a tento čas spojeny."*[108] Dle čl. 42 odst. 3 eIDAS se kvalifikovaná elektronická časová razítka navíc uznávají i přeshraničně, ve všech členských státech EU.

Z hlediska *důvěrnosti dat* je služba zcela bezpečná, neboť poskytovateli služby se nezasílají celá data (např. elektronický dokument), ale jen jeho tzv. *hash* hodnota. Ta reprezentuje data zkráceně (má např. délku jen 256 bitů), ale dostatečně jednoznačně. Z hodnoty hash[109] nelze zpětně odvodit obsah dat, ze kterých byla kryptografickým hašovacím algoritmem spočtena. Hash si může laický čtenář představit jako jakýsi zkrácený otisk od dokumentu (dat). Z dokumentu může být otisk *(hash)* spočten opakovaně kdykoli znovu a bude mít stále stejnou hodnotu. Časové razítko, které potvrzuje otisk (*hash* hodnotu), tak tranzitivně potvrzuje i celý původní dokument.

Při správné technické implementaci by kvalifikovaný poskytovatel měl vést záznamy o souvislé řadě vydaných časových razítek QTS, která prakticky znemožňuje zpětně vsunutí nepravého časového razítka. Roßnagel zde kritizuje, že domněnka tu má charakter správnosti (tj. pravdivosti skutkového stavu), které se jinak těší pouze veřejné listiny. Jandt naopak považuje[110] domněnku za dostatečně bezpečnostně podepřenou. Autor je přesvědčen, že vydávání QTS by provozně mělo být nejjednodušší a potažmo i důkazně nejspolehlivější službou vytvářející důvěru vůbec. Je pouze třeba mít důvěryhodně ověřenu správnou praxi. Zda tomu tak je, může být ale otázka.

Autor by jednoznačně doporučoval použití QTS před nekvalifikovanými časovými razítky. QTS se těší důkazním domněnkám (pro důkazní účinky srov. 6.15.9) a mělo by představovat velmi věrohodný důkazní prostředek. Rozdíl ceny vůči nekvalifikované variantě by neměl být zásadní, a pokud existuje, pak je to spíše důvod k obavám o kvalitu doprovodného zabezpečení u nekvalifikovaného poskytovatele.

---

[108] Zvýraznil autor.
[109] Z hlediska bezpečnosti služby proto není kritické ani to, pokud by hodnota hash byla odposlechnuta.
[110] JANDT, S., cit. dílo, s. 1207.

6.7.2 Případy užití (kvalifikovaných) elektronických časových razítek

Hlavním případem užití časových razítek je bezesporu jejich využití v souvislosti se zaručenými elektronickými podpisy nebo pečetěmi a jejich vyššími úrovněmi, tj. pro AdES, AdESeal, QES a QESeal. Nařízení eIDAS povinné použití časových razítek pro případy podpisů nebo pečetí ale nepředepisuje. Dostačuje-li spoléhající se osobě jen jednorázové ověření platnosti podpisu po přijetí, nepředpokládá-li, že by z dané komunikace kdy mohl vzniknout právní spor, pak časová razítka skutečně používat nemusí. Přesto je použití časových razítek QTS vhodné pro potvrzení existence AdES, AdESeal, QES a QESeal k určitému času, neboť se tím prodloužuje doba jejich jednoznačné ověřitelnosti platnosti na střední dobu (3–5 let, podle doby platnosti QTS). Časová razítka lze ve spojitosti s elektronickými podpisy a pečetěmi používat několika v principu různými způsoby podle toho, kdo časové razítko nechá vytvořit, kolik jich je a jak těsně k okamžiku vytvoření podpisu nebo pečeti se vytváří. Nejběžnější je vytvoření časového razítka QTS po vytvoření elektronického podpisu (pečeti). Takové vytvoření může provést buď již přímo podepisující osoba, anebo spoléhající se osoba, jakmile jí podepsaná data s podpisem dojdou.

Existuje ale i možnost použít časové razítko dvakrát. První razítko potvrdí jen podepisovaná data, poté se vytvoří elektronický podpis (pečeť) přes vzniklé spojení a celek se opatří druhým časovým razítkem. Metoda zajišťuje, že elektronický podpis vznikl mezi časy obou časových razítek. Je-li vše automatizováno, může být čas vytvoření elektronického podpisu vymezen s přesností na sekundy. Tuto metodu musí použít podepisující osoba. Vytváří-li se však elektronický podpis v rámci webových služeb nějakého portálu, může mu tuto funkcionalitu zprostředkovat i spoléhající se osoba nebo provozovatel portálu. Druhá metoda je vhodná buď tehdy, když potřebujeme velmi přesně vědět čas vytvoření elektronického podpisu (pečeti), ale je v principu vhodná i pro všechny případy, když podepisující osoba používá kvalifikovaný certifikát s možností pozastavení platnosti.

Nařízení eIDAS předepisuje povinné použití QTS pro kvalifikovanou službu elektronického doporučeného doručování v čl. 44 odst. 1 písm. f).

Časová razítka mají i jiné druhy účelů. Běžně se uvádí jejich označování dokumentů, u kterých se chce prokázat, že existovaly k určitému času. To může mít někdy právní význam, například z hlediska práva přednosti při udělování patentů apod.

Časové razítko rovněž potvrzuje integritu dokumentu (orazítkovaných dat) od okamžiku vystavení razítka. Nebude tak sice osvědčen původ, ale bude zřejmé, že se data nějakou dobu nezměnila. Časové razítko se může používat například na průběžné (např. 1x denně, 1x za hodinu apod.) orazítkování některých výstupů z informačních systémů, jako jsou např. systémové žurnály apod. Časové razítko pak poskytne nezávislé ověření, že daný žurnál k danému okamžiku existoval a nemohl být dodatečně změněn. Neprokazuje však, že nedošlo ke změně před časem vytvoření razítka. Pro tyto potřeby ale může být uzpůsobena struktura žurnálu, aby svou sekvenčnost prokazovala sama.

Průvodce[111] od ENISA uvádí případy užití potvrzování času vytvoření podpisu, uložení, podání, vydání úředního aktu, uzavření smlouvy, ověřování časového plnění smluv, procesních aj. právních lhůt, dlouhodobé ověřování platnosti elektronických záznamů, uchovávání elektronických záznamů nebo notarizace přesné chronologie událostí.

Dumortier je k využitelnosti nutnosti používat časová razítka skeptický.[112] Domnívá se, že jejich činnost lze zajistit jinými prostředky, zejména systémovými žurnály *(logs)* různých portálů veřejné správy. Autor připouští, že ne každá on-line služba subjektu veřejného sektoru, zejména bude-li vystavěna spíše na principu elektronické identifikace (kap. II eIDAS), je potřebuje využívat. Obecně ale jeho skepsi nesdílí a domnívá se, že ověřování času od nezávislého kvalifikovaného poskytovatele zlepšuje důvěryhodnost mnoha systémů. K metodice PKI a digitálních objektů s AdES, AdESeal, QES a QESeal pak časová razítka nerozlučně patří a nařízení eIDAS by bez jejich úpravy silně kulhalo.

6.8 Služby vytvářející důvěru a jejich poskytovatelé

České vyjádření původního anglického pojmu *trust service* (snad důvěrová služba, služba pro důvěru apod.) jako **služba vytvářející důvěru** považuje autor za zdařilé. Dobře vyjadřuje, že podstata služby spočívá ve vytvoření či zprostředkování důvěry, nikoli pouze v tom, že by sama o sobě měla být důvěryhodná. V nařízení je pojem definován v čl. 2 bodu 16 eIDAS:

> 16) „službou vytvářející důvěru“ elektronická služba, která je zpravidla

[111] ENISA. *Security guidelines on the appropriate use of qualified electronic time stamps, Guidance for users.* Version 2.0, Final, December 2016, s. 19–20.
[112] Dumortier in LODDER, A. R., MURRAY, A. D. (eds)., cit. dílo, s. 285.

poskytována za úplatu a spočívá:

a) ve vytváření, ověřování shody a ověřování platnosti elektronických podpisů, elektronických pečetí nebo elektronických časových razítek, služeb elektronického doporučeného doručování a certifikátů souvisejících s těmito službami nebo

b) ve vytváření, ověřování shody a ověřování platnosti certifikátů pro autentizaci internetových stránek nebo

c) v uchovávání elektronických podpisů, pečetí nebo certifikátů souvisejících s těmito službami;

Jedná se tedy předně o službu, tedy plnění charakteru služby, které poskytuje osoba, již jinde nařízení nazývá *poskytovatel služeb vytvářejících důvěru* (čl. 2 bod 19 eIDAS; pojem se bude někdy v textu zkracovat jen na *poskytovatele služeb*, je-li z kontextu jasné, že se jedná o služby vytvářející důvěru). Jedná se o službu elektronického charakteru, zpravidla bývá poskytována za úplatu, výjimky z úplatnosti jsou však samotnou definicí připuštěné.

Písmena a) až c) pak popisují několik druhů služeb, v nichž může služba vytvářející důvěru spočívat. Písmena a) a c) spočívají téměř výhradně ve službách, které souvisejí nebo jsou odvozeny od využívání elektronických podpisů, zejména těch implementací elektronických podpisů, které využívající kryptografii veřejného klíče. Snad pouze službu elektronického doporučeného doručování lze považovat za jen mírně související, neboť má samostatný účel ověřovaného odesílání a doručování (čl. 3 bod 36 eIDAS). Nicméně i pro ni je v rámci eIDAS předepsáno využití zaručeného elektronického podpisu, popř. pečetě (čl. 44 odst. 1), takže s ním souvisí aspoň takto.

Služby podle písmene b) s elektronickým podpisem nesouvisí, nicméně se i v případě těchto certifikátů opět jedná o techniku kryptografie veřejného klíče. Slouží pro autentizaci webového místa (v dikci českého znění eIDAS *internetových stránek*) vůči vzdálenému uživateli a pro možnost šifrování komunikace s ním.[113]

Chceme-li nalézt spojující prvek v definici *služeb vytvářejících důvěru*, pak zjistíme, že jsou spojeny předně nepřímo přes je provozující typický subjekt. Souvislost tedy plyne přes obchodní zvyklostí a efektivitu subjektu, který vydává certifikáty veřejného klíče. Takový subjekt mívá tendenci nabízet celou škálu certifikátů, a nikoli pouze těch, které jsou určeny pro elektronické podpisy. K nim pak jsou přiřazeny další

[113] Typicky technickými protokoly SSL/TLS. Adrese webové stránky pak začíná na „https://...“.

služby, které se v technologii elektronických podpisů založených na asymetrické kryptografii osvědčily, jako např. elektronická časová razítka, problematika ověřování platnosti elektronických podpisů nebo dlouhodobé uchovávání.

Ze škály portfolia subjektů vydávajících certifikáty vypadla v eIDAS pouze jedna běžná kategorie, a to sice certifikáty sloužící pro autentizaci fyzické osoby (uživatele) při sezení vůči protějšku (webovému místu). Tyto certifikáty bývají běžně vydávány jako tzv. komerční certifikáty, přičemž bezpečnost jejich vydávání a výsledná důvěryhodnost může být i stejná, jako je u certifikátů pro elektronické podpisy nebo pečetě. Důvody tohoto opomenutí mohou být dva. Zákonodárce nemusí chtít podporovat autentizační certifikáty a klíče, které lze použít i pro šifrování sezení. Druhou a pravděpodobnější možností je, že předpokládá řešení těchto druhů služeb v rámci elektronické identifikace podle kapitoly II nařízení, aby se úprava netříštila.

6.8.1 Služby vytvářející důvěru – otevřený, či uzavřený výčet?

Z právního pohledu je důležité, že výše uvedená definice sice připouští poměrně bohaté možnosti kombinací, variant provedení, popř. asi i různá štěpení jednotlivých služeb do podslužeb, nicméně se ve výsledku jedná o taxativně uzavřený výčet druhů služeb. V normativní části nařízení eIDAS spadá pod pojem jen předem daný počet služeb vytvářejících důvěru. Čl. 2 bod 17 zdvojnásobuje počet variant tím, že připouští, že každá služba vytvářející důvěru může být též poskytována jako kvalifikovaná. *Kvalifikovaná služba vytvářející důvěru* musí navíc splňovat *„použitelné požadavky stanovené v ... nařízení"*. Jejím poskytovatelem pak může být pouze *kvalifikovaný poskytovatel služeb vytvářejících důvěru*, tj. takový, který podle čl. 2 bodu 20 eIDAS poskytuje některou kvalifikovanou službu vytvářející důvěru a *„kterému orgán dohledu udělil status kvalifikovaného poskytovatele"*, přičemž ten je podle nařízení eIDAS udělitelný jen při splnění řady požadavků na činnost, organizaci, technické vybavení, finanční zajištění, předběžné i následné kontroly a dohled orgánů dohledu nad poskytovatelem služeb.

Odlišné pojetí představuje bod odůvodnění 25 eIDAS v úvodní nenormativní části. Podle něj členské státy by *„měly mít možnost stanovit kromě služeb vytvářejících důvěru, jež jsou součástí uzavřeného seznamu služeb vytvářejících důvěru stanoveného v tomto nařízení, i jiné druhy služeb vytvářejících důvěru za účelem jejich uznávání na vnitrostátní úrovni jako kvalifikovaných služeb vytvářejících důvěru"*.

Bod potvrzuje, že výčet služeb v normativní části je konečný. Současně však členským státům při implementaci nařízení umožňuje, ba přímo doporučuje, aby ve svých právních řádech výčet otevřely, tj. zavedly či dovolily případně i jiné druhy služeb vytvářejících důvěru s tím, že se pro ně rovněž smí použít označení *kvalifikované* služby vytvářející důvěru, ovšem s účinkem uznání pouze v jeho vnitrostátní úrovni. Takto vnitrostátně legislativně založené a fakticky poskytované kvalifikované služby tedy netěží ze zásady vnitřního trhu vyjádřené v článku 4 eIDAS (např. volný pohyb, nevytváření omezení) ani z příležitostně vyjádřených povinností uznávat přeshraničně, některé v nařízení stanovené, kvalifikované služby vytvářející důvěru. Důvodem takového přístupu může být i bod odůvodnění 26, který apeluje, aby nařízení bylo provedeno způsobem, který umožňuje technické inovace.

Je ovšem třeba zvážit důvody, k čemu je vhodné vnitrostátním právem označit některé služby jako kvalifikované. Pro mnohé elektronicky poskytované služby bude z mnoha důvodů, včetně volného technického rozvoje, výhodnější, když nebudou podléhat žádné zvláštní legislativní ani úřední regulaci, ale budou činné v rámci smluvní svobody a soukromých právních vztahů. Vymezení některých služeb jako kvalifikovaných může mít zřejmě význam spíše tehdy, když se bude jednat o služby související s veřejným právem, popř. pokud zákonodárce nabude dojmu, že některou oblast služeb je třeba podrobit zvláštní právní regulaci s ohledem na chráněné hodnoty nebo rizika, která by u nich hrozila.

Odpověď na otázku lze tedy shrnout, že v rámci nařízení eIDAS existuje pouze taxativní výčet *(kvalifikovaných) služeb vytvářejících důvěru*, v rámci právních řádů členských států je povoleno prolomit *numerus clausus*, byť ovšem jen s vnitrostátními právními účinky.

6.8.2 Ověřování totožnosti a obsahu kvalifikovaného certifikátu

Čl. 24 odst. 1 eIDAS zmiňuje, že poskytovatel ověří *„v souladu s vnitrostátním právem totožnost a případně zvláštní znaky fyzické nebo právnické osoby"*. Možnost úpravy kontroly totožnosti nebo ověřování zvláštních znaků (tj. výše zmíněných atributů) fyzické osoby, resp. právnické osoby je tedy v dispozici *implementace* nařízení členským státem. Národní implementaci zde pro případ ověřování atributů zcela shodně

uvažuje Roßnagel.[114] Podle alinea 2 smí kvalifikovaný poskytovatel vždy ověřit výše uvedené informace přímo.

Alternativně se poskytovatel může *„v souladu s vnitrostátním právem spolehnout na třetí osobu"* a s její pomocí ověřit informace podle písmen a) až d). Předmětem *implementace* právem členského státu jsou zde zjevně i písmena a) až d) čl. 24 odst. 1 eIDAS. Dle autora se zde nejedná pouze o využití institutu zastoupení z práva členského státu, ale o možnost úplné úpravy metody, pokud poskytovatel neověřuje informace přímo. Členský stát tak dle autora má možnost i některou z možností a) až d) ve svém právu zakázat, např. písm. b), popř. ji omezit pouze na případ vysoké úrovně záruky.

Zajímavá situace s určitou právní nejistotou vzniká, pokud členský stát žádnou implementaci pro ověřování totožnosti a atributů nepřijme. V takovém případě zřejmě poskytovatel bude informace ověřovat na základě smluvních podmínek, které sám vydá, neboť běžně právo členských států zřejmě nebude upravovat nemožnost soukromoprávního stanovení způsobu ověřování totožnosti nebo jiných atributů osoby.

Další situace nastává, pokud členský stát neprovede implementaci čl. 24 odst. 1 písm. a) až d) eIDAS. I zde pak zřejmě poskytovatel může chybějící podmínky písm. a) až c) nahradit smluvně se třetí osobou, ledaže by takovou soukromou úpravu právo členského státu zakazovalo. Pouze v případě písm. d) bude muset vždy být získáno potvrzení subjektu posuzování shody, než bude případně daná metoda zahrnuta do smluvních podmínek používaných kvalifikovaným poskytovatelem.

6.8.3 Ověřování totožnosti u kvalifikovaného certifikátu právnické osoby

Znění čl. 24 odst. 1 eIDAS v principu umožňuje ověřit totožnost právnické osoby abstraktně, tj. bez určení konkrétní jednající fyzické osoby.

Nařízení pak pouze v bodu odůvodnění 60 uvádí, že *„Poskytovatelé služeb vytvářejících důvěru vydávající kvalifikované certifikáty pro elektronické pečetě by měli zavést nezbytná opatření, aby byli schopni určit totožnost fyzické osoby zastupující právnickou osobu, které je kvalifikovaný certifikát pro elektronickou pečeť poskytován, je-li tato identifikace nezbytná na vnitrostátní úrovni v soudním nebo správním řízení."*

[114] ROSSNAGEL, A. Der Anwendungsvorrang der eIDAS-Verordnung — Welche Regelungen des deutschen Rechts sind weiterhin für elektronische Signaturen anwendbar? *Multimedia und Recht*. 2015, s. 359–364, s. 362.

Nařízení zde tedy avizuje, že členský stát může implementovat povinnost evidovat a ověřit totožnost fyzické osoby, které byl vydán kvalifikovaný certifikát pro elektronické pečetě, popř. i související kvalifikovaný prostředek pro vytváření elektronických pečetí.

Autor je zde názoru, že pokud poskytovatel služeb nechce čelit žalobám, popř. i trestnímu postihu z důvodu, že vydal kvalifikovaný certifikát pro elektronickou pečeť právnické osoby nějaké neznámé fyzické osobě, popř. fyzické osobě bez oprávnění od právnické osoby nechat si takový certifikát vystavit a převzít, čímž této fyzické osobě umožnil vydávat se za danou právnickou osobu, popř. jí umožnil páchat trestný čin podvodu, měl by si totožnost a oprávnění dané fyzické osoby ověřit vždy, a to přinejmenším při vydání prvního takového certifikátu.

Otázkou pouze je, zda ověření fyzické osoby je nutné v případě vydávání tzv. následných certifikátů, tedy pokud by žádost o následný certifikát byla podepsána pouze (kvalifikovanou) elektronickou pečetí, z níž pochopitelně není patrné, která fyzická osoba žádost takovou pečetí opatřila. Obdobnou otázkou a snad výjimkou z potřeby ověřit totožnost fyzické osoby, které se vydává kvalifikovaný certifikát pro elektronickou pečeť, by mohlo být, pokud by v členském státě existoval prostředek identifikace na dálku, který by byl vztažen přímo k právnické osobě a umožňoval za ni jednat. Vždy by bylo vhodné, aby tyto situace byly upraveny právem členského státu. Není-li tomu tak, pak by je měl upravit aspoň kvalifikovaný poskytovatel služeb vytvářejících důvěru v podmínkách podle čl. 24 odst. 2 písm. d) eIDAS, jinak bude strana pečetící právnické osoby i spoléhající osoby v právní nejistotě o tom, za jakých okolností byl certifikát vydán a předán.

6.9 Důvěryhodné seznamy (poskytovatelů služeb)

Nařízení eIDAS obsahuje úpravu vydávání tzv. důvěryhodných seznamů poskytovatelů služeb vytvářejících důvěru. Těžištěm úpravy je článek 22 eIDAS. Jedná se o kriticky důležitý prvek systému služeb vytvářejících důvěru v konceptu podle nařízení eIDAS, zejména pro možnost jejich snadného přeshraničního uznávání a využívání, tj. zejména schopnosti rychle zjistit, že některý poskytovatel je kvalifikovaným poskytovatelem a některá jeho služba je kvalifikovanou službou vytvářející důvěru v rámci metodiky nařízení eIDAS. Právě z přítomnosti na tomto seznamu může spoléhající strana vyvozovat, že konkrétní kvalifikovaný poskytovatel

a jeho kvalifikované služby podléhají systému dohledu podle nařízení eIDAS v rámci členského státu, v němž je usazen, tj. jak subjekt sám, tak jeho služby by měly představovat nařízením eIDAS stanovenou úroveň kvality a důvěryhodnosti.

Existenci seznamu přitom lze hodnotit ze dvou hledisek. První hledisko je informativní, přehledové. Souhrn seznamů ze všech členských států teoreticky může sloužit jako kompletní adresář všech kvalifikovaných poskytovatelů na území EU, tj. i pro určité marketingové účely. Druhý význam je technicko-právní a přeshraniční a má význam pro spoléhající se stranu. Spoléhající se strana má pohotový prostředek ověření, že se jedná o kvalifikovaného poskytovatele a kvalifikovanou službu vytvářející důvěru.

6.9.1 Historie vývoje důvěryhodných seznamů a jejich význam

Důvěryhodné seznamy služeb byly navrženy a později zavedeny již v průběhu zpracování studie CROBIES[115] v roce 2009 jako pomocná metoda, která měla sloužit spoléhajícím stranám při přeshraniční komunikaci k tomu, aby si rychle ověřily důvěryhodnost poskytovatele certifikačních služeb z jiného členského státu. V té době již v rámci celé EU existovalo více než sto poskytovatelů certifikačních služeb vydávajících kvalifikované certifikáty, kteří byli rozptýleni v různých členských státech a svou činnost provozovali podle pravidel práva členského státu, v němž byli usazeni.

Došel-li adresátovi komunikace přeshraničně dokument nebo jiná data podepsaná zaručeným elektronickým podpisem, kvalifikovaným elektronickým podpisem, popř. jiným druhem elektronického podpisu, které požadovalo vnitrostátní právo na základě výjimek pro veřejný sektor, umožněných v DirES, byl postaven v zásadě před tři problémy. Prvním bylo ověření platnosti podpisu a certifikátů v certifikační cestě. Ověřování vždy skončilo u nějakého kořenového certifikátu, který subjekt podepisoval sám sobě. Někdy byl subjektem poskytovatel, jindy národní dohlížející úřad. Druhým úkolem a potíží spoléhající osoby bylo, že musela nějakou pomocnou metodou (mimo certifikáty) ověřit, že tento poslední kořenový certifikát je autentický, tj. že náleží v něm tvrzenému subjektu a ten nějak jinak nezávisle potvrzuje, že ho skutečně vydal. Za třetí musela i ověřit funkci subjektu, že je k vydání certifikátů právně zmocněn, tj. i jeho právní postavení a význam certifikátu. Pokud byla certifikační cesta od národního úřadu, musela spoléhající osoba ověřit, že přítomnost certifikátu má význam potvrzení, že se jedná o poskytovatele certifikačních služeb

[115] SEALED, TIME.LEX. SIEMENS: *CROBIES: Study on Cross-Border Interoperability of eSignatures – Head Document*, 2010.

vydávajícího kvalifikované certifikáty. Byl-li kořenový certifikát od samotného poskytovatele, musela ověřit status poskytovatele a jeho služby (mimo certifikáty). Vše ve stavu, kdy dokumenty takových subjektů (certifikační politika apod.) bývají sepsány v cizím jazyce, nejvýše ještě někdy i v angličtině, mívají výrazně technický charakter, jehož právní význam je případ od případu nejasný i právníkům. Takové úlohy mohly zabrat i několik dnů práce, včetně potřeby najmutí specialistů v oboru.

Studie CROBIES navrhla opatření, které zde mělo vést k rychlé nápravě, aniž by bylo nutno přijímat příliš rozsáhlou novou legislativu. Každý členský stát měl vydat a udržovat právě jeden důvěryhodný seznam, v němž by byli uvedeni všichni *poskytovatelé certifikačních služeb* (terminologie DirES) usazení na jeho území, včetně případného stavu dohledu nebo akreditace. Kromě překlenutí jazykových a právních rozdílů a hranice mezi členskými státy se současně jednalo i o inovativní technické řešení, neboť umožňovalo mít k dispozici souhrn poskytovatelů a jejich služeb, ačkoli podstata jejich technického řešení poskytované služby mohla být značně rozdílná.

Během první dekády století existovaly i jiné snahy o vzájemné propojení mezi poskytovateli a jejich službami. Častou první snahou bylo vytvořit hierarchické pyramidy poskytovatelů, resp. jejich certifikačních služeb, v nichž by ti výše položení potvrzovali ty níže položené, čímž by se ověřovala platnost certifikátů níže v hierarchii i reálnost existence subjektů poskytovatelů a jejich status poskytovatele. V některých státech byl rolí kořenového poskytovatele služeb pověřen některý státní úřad. Například ve Slovenské republice jím byl NBÚ SR. Výsledkem byly příliš vysoké pyramidy, v nichž vznikaly příliš dlouhé řetězce certifikátů, tzv. certifikačních cest. To je nepraktické již z hlediska technického ověřování posledního užitečného elektronického podpisu, kdy je zapotřebí ověřit platnost i všech certifikátů stojících v hierarchii výše. Různí poskytovatelé v řetězci totiž mohou používat navzájem mírně či více odlišné certifikační politiky. Výsledek zřetězení těchto politik bývá obtížné vyložit či se na něj spolehnout již ryze technicky. Stejné nebo ještě horší potíže kombinace po certifikační cestě vznikají, pokusíme-li se vyložit právní význam cesty, včetně všech krajních možností týkajících se zneplatňování certifikátů apod.

Další uvažovanou metodou, která měla vést již k plošším strukturám, jež by obcházely kořeny příliš vysokých a právně nejistých pyramid, byly tzv. přímé mosty *(bridge)* mezi poskytovateli. I tyto snahy však narážely jak na malou technickou homogenitu a potažmo návaznost služeb od různých poskytovatelů, tak i na jejich příliš

odlišné právní podmínky, které by následně byly prostředkovány přes bilaterální soukromoprávní smlouvy mezi subjekty poskytovatelů. Pro spoléhající strany pak takové kombinace byly opět právně málo přehledné, s nízkou právní jistotou. Poskytovatelé k uzavírání smluv a vytváření mostů nebyli ani nijak zvlášť nuceni, nemuseli mít o ně vůbec zájem a ani tato koncepce se nakonec nijak zvlášť v praxi neujala.

Souhrnně lze říci, že poskytovatelé nemají zvláštní zájem být součástí složitých organizačních pyramid nebo jiných struktur. Z jejich pohledu se tím komplikuje jak jejich obchodní autonomie, stěžejní zásada soukromého práva, tak se případně použití jejich služby komplikuje technicky u zákazníka. Obojí ovlivňuje i právní podmínky. Jejich zájmem naopak je, aby všechny technické prostředky poskytované služby měli pod svou vlastní kontrolou, nebyli tak závislí na třetích osobách technicky a nebyli jimi proto omezováni. To jim umožňuje formulovat své nabídky v maximální možné míře svobodně podle vlastního uvážení, jakož i stanovit smluvní aj. právní podmínky.

V zásadě jediným organizačně funkčním uspořádáním, spontánně častěji rozšířeným, je případné oddělení služeb technického jádra certifikační autority, které poskytuje technologické řešení vydávání kvalifikovaných certifikátů a jeho vysokou fyzickou, technickou i organizační bezpečnost, v kombinaci se sítí poboček tzv. registračních autorit, které jsou rozmístěny v území a provádějí zejména fyzické ověřování totožnosti žadatelů o kvalifikovaný certifikát. Tímto způsobem v ČR funguje zejména První certifikační autorita, a. s., která využívá sítě registračních míst v jiných subjektech, zejména bankách, jež jsou současně jejími významnými akcionáři. V rámci služby PostSignum od poskytovatele certifikačních služeb Česká pošta, s. p., existuje v zásadě stejný model rozdělení činností, registračními místy jsou však četné pobočky samotné České pošty. Pouze třetí akreditovaný poskytovatel, společnost eIdentity, a. s., se specializoval v zásadě zejména na velké společnosti či úřady s tím, že byl schopen v jejich rámci nabízet vytvoření outsourcovaného registračního místa. V Německu lze nalézt i další modely, např. spolupráci poskytovatele (certifikační autority) s notáři nebo s oborovými organizacemi (např. v oblasti e-Health), které pomáhají šířit kvalifikované služby. Šiřiteli služeb v roli registračních míst mohou být i tvůrci určitých softwarových aplikací či systémů s významně početnou klientelou, kterou chtějí komplexně obsloužit.

Neuvrhnutí všech poskytovatelů pod jediný pyramidový model, byť jen v rámci členského státu EU, rozhodně mnohem lépe umožňuje jejich následnou marketingovou a tržní diverzifikaci, lepší uspokojování potřeb různých segmentů trhu.

Seznamy důvěryhodných služeb vycházely vstříc jak této potřebě, tak i realitě toho, že v různých členských státech byla situace rozdílná. V některých členských státech centrální úřední certifikační autority existovaly, v jiných nikoli a bylo pochybné, zda je vhodné je zřizovat, nebo státy nechtěly vynakládat prostředky k tomu nezbytné.

Seznamy umožňují uvést všechny poskytovatele a jejich služby v zásadě lineárním způsobem vedle sebe, bez zvýrazňování jedněch nebo druhých, bez komplikací s právní rozdílností významu jejich přítomnosti v různých částech pyramidy nebo za propojujícími mosty. Právní význam přítomnosti v seznamu je dán zejména předpisem unijního práva, který je pro celou EU shodný. Právní význam sice mohl být modifikován transpozičním právním předpisem práva členského státu, kvůli jejich harmonizaci vůči směrnici DirES by však rozdíly neměly být velké (a po přijetí nařízení eIDAS jsou ještě mnohem menší).

Seznamy důvěryhodných služeb tak umožnily do přehledů sdružit služby podstatně heterogenější technicky i právně. Nevyžadují ani, aby mezi poskytovateli musely vznikat navzájem obtížně dohodnutelné smluvní vztahy. Členské státy nemusí činnost poskytovatelů reglementovat technicky příliš podrobně, což poskytovatelům umožňuje svobodnější a tím i širší možnosti profilace.

Spoléhající se strana pak v zásadě musí znát pouze právní význam přítomnosti v seznamu a právní podmínky služby daného jednoho poskytovatele, což její situaci nejen technicky, ale i právně významně zjednodušuje.

Vydávání seznamů bylo upraveno v Rozhodnutí Komise 2009/767/ES ze dne 16. října 2009, vydáno bylo 20. října v Úředním věstníku EU od strany L 274/36, s účinností od 28. prosince 2009. Důvěryhodný seznam služeb *(TSL ~ Trust Services List)* měl mít formát podle šablony v příloze rozhodnutí, která ale ve věstníku přítomna nebyla. Po zjištění této chyby byla ve věstníku vydána dne 14. 11. 2009 oprava na straně L 299/18 až L 299/54, která obsahuje opět úplné znění rozhodnutí, tentokrát včetně přílohy. Rozsáhlá příloha jednak sama definuje obsah důvěryhodného seznamu poměrně podrobně, jednak se odvolává na technickou specifikaci[116] právně vágní

[116] ETSI TS 102 231 – Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information.

formulací, že navrhovaná šablona v příloze je „slučitelná s prováděním založeným na specifikacích z ETSI TS 102 231“.

Během roku 2010 byly zjištěny nedostatky[117] spočívající jednak v tom, že členským státům nebyla uložena povinnost zveřejňovat informaci v důvěryhodném seznamu nejen v lidsky čitelné *(human-readable)*, ale rovněž ve strojově zpracovatelné *(machine-processable)* podobě pro automatizované ověřování, a jednak v pouze doporučujícím ustanovení ohledně důvěryhodnosti (elektronický podpis nebo přístup přes zabezpečený kanál) vydaného důvěryhodného seznamu. Komise proto vydala 28. července 2010 nové Rozhodnutí Komise 2010/425/EU, které novelizovalo výše uvedené rozhodnutí 2009/767/ES tak, že s účinností od 1. 12. 2010 členské státy měly nově „povinnosti:

- publikovat jak lidsky čitelnou, tak strojově zpracovatelnou podobu TL,
- elektronicky podepsat strojově zpracovatelnou podobu,
- publikovat lidsky čitelnou podobu bezpečným způsobem (tj. zabezpečeným kanálem nebo elektronicky podepsanou),
- předat Evropské komisi veřejné klíče potřebné k ověření podpisů TL, která následně zajistí jejich důvěryhodnou distribuci přes centrální seznam (tzv. LOTL – List of Trusted Lists).“[118]

Nařízení pak prodělalo ještě několik novelizací, které reflektovaly, že se jednalo o nový přístup k pokrytí mnoha subjektů poskytovatelů a jejich služeb, který byl v rámci EU zřejmě navržen a vyvinut vůbec poprvé na světě.

Z právního hlediska je pozoruhodné, že právním základem rozhodnutí nikdy nebyla směrnice DirES, o rámci pro elektronické podpisy. Příčinou bylo, že směrnice z roku 1999 existenci nástroje druhu důvěryhodných seznamů neznala, nepředpověděla, a proto ani neobsahovala ustanovení zmocňující Komisi k jejich právní úpravě.

Komise si náhradně vypomohla tím, že rozhodnutí 2009/767/ES právně založila na směrnici 2006/123/ES o službách na vnitřním trhu, což předpokládá zřízení tzv. jednotného kontaktního místa v každém členském státu. Aby jednotné kontaktní místo jednoho členského státu mohlo co nejhladčeji provozovat své on-line služby a v jejich

[117] Novela rozhodnutí Komise 2009/767/ES. Dostupné z: <http://www.mvcr.cz/clanek/novela-rozhodnuti-komise-2009-767-es.aspx>; navštíveno 11/2013.

[118] Citace z webové stránky zmíněné v poznámce pod čarou č. Chyba: zdroj odkazu nenalezen.

rámci přijímat elektronicky podepsané písemnosti od osob z jiných členských států, je v rozhodnutí navržen výše uvedený mechanismus seznamů důvěryhodných služeb.

Z hlediska čistě právních kompetencí neexistovalo žádné právní zmocnění, které by seznamy důvěryhodných služeb umožňovalo používat v rámci jiných kontextů, než jsou služby jednotného kontaktního místa. Jejich faktická existence nicméně přesto znamenala, že používány zřejmě byly, nebo se aspoň vyjevila jejich praktičnost.

6.9.2 Nařízení eIDAS – důvěryhodné seznamy

Úprava důvěryhodných seznamů se nachází zejména v článku 22 eIDAS. Jedná se zde o důvěryhodné seznamy poskytovatelů služeb vytvářejících důvěru a jejich kvalifikovaných služeb vytvářejících důvěru. Budeme je zde krátce nazývat jen jako **důvěryhodné seznamy**, což je i název článku 22 eIDAS. Jen pro úplnost předešleme, že nařízení eIDAS zná i další a odlišný druh seznamů, a to sice *seznam certifikovaných kvalifikovaných prostředků pro vytváření elektronických podpisů*, resp. *pečetí* podle čl. 31 resp. čl. 39 odst. 3. eIDAS.

Podle jeho čl. 22 odst. 1 eIDAS *„Každý členský stát zřizuje, udržuje a zveřejňuje důvěryhodné seznamy obsahující informace týkající se kvalifikovaných poskytovatelů služeb vytvářejících důvěru v jeho působnosti spolu s informacemi o jimi poskytovaných kvalifikovaných službách vytvářejících důvěru."*

Obrat *„v jeho působnosti"* se nezdá jasný. V angličtině celý úvod zní *„Each Member State shall establish ... trusted lists, including information related to the qualified trust service providers for which it is responsible, together with ... "* Jedná se tedy o zveřejnění poskytovatelů, za něž členský stát odpovídá. Obdobně v němčině je *„für die er verantowortlich ist"*. Český překladatel zřejmě chtěl vztah státu k poskytovateli vyjádřit vztahem *„působnosti"* a vynechat možnou odpovědnost. Ve skutečnosti jsou v působnosti členského státu pouze dohledové činnosti stanovené v nařízení, nikoli samotný poskytovatel nebo všechny jeho činnosti.

Provedený výklad vysvětluje, proč se obratem *„v jeho působnosti"* nemůže rozumět ani *„působnost"* samotného poskytovatele certifikačních služeb v oblasti jím poskytovaných služeb vytvářejících důvěru.

V důvěryhodném seznamu budou tedy uvedeny ty subjekty, které na základě rozhodnutí orgánu dohledu [čl. 17 odst. 4 písm. g) eIDAS] splňují požadavky na

kvalifikovaného poskytovatele služeb vytvářejících důvěru, jakož i informace o všech kvalifikovaných službách vytvářejících důvěru, které poskytují.

Článek 22 odst. 2 upravuje formu a zabezpečení výše uvedených důvěryhodných seznamů. Ty musí být zřízeny ve formě *„vhodné pro automatické zpracování"*, musí být udržovány a zabezpečeným způsobem zveřejněny. Kromě toho musí být opatřeny elektronickým podpisem nebo elektronickou pečetí (bez stanovení druhu). Právně závaznou formou důvěryhodných seznamů tedy je forma vhodná pro automatické zpracování, jiné formy nařízení eIDAS v čl. 22 nezmiňuje.

eIDAS zde ani jinde nestanoví žádné požadavky požadavky na použité elektronické podpisy, popř. elektronické pečetě, zřejmě z toho důvodu, že tvorba důvěryhodných seznamů předchází vlastní činnosti kteréhokoli poskytovatele služeb vytvářejících důvěru. Ti nesmí zahájit svou činnost dříve, než dojde k vydání důvěryhodného seznamu, na němž jsou sami teprve uvedeni.

Článek 22 odst. 2 eIDAS přesto zřejmě předpokládá použití elektronických podpisů s asymetrickou kryptografií a certifikátem veřejného klíče. Aby byla zajištěna důvěryhodnost těchto elektronických podpisů (pečetí), musí podle čl. 22 odst. 3 eIDAS členský stát totiž oznámit Komisi informaci o certifikátu (tj. zřejmě samotný certifikát nebo jeho otisk) nebo o změně certifikátu. Dále členský stát informuje Komisi i o *„subjektu odpovědném za zřízení, udržování a zveřejnění vnitrostátních důvěryhodných seznamů"* a o místě zveřejnění důvěryhodných seznamů.

Všechny tyto informace z odst. 3 Komise podle čl. 22 odst. 4 *zpřístupní veřejnosti ve formě* opatřené elektronickým podpisem nebo pečetí a *vhodné pro automatické zpracování*.

Podle čl. 22 odst. 5 eIDAS Komise je zmocněna a současně musí do 18. 9. 2015 vydat prováděcí akt, ve kterém *„upřesní informace uvedené v odstavci 1 a stanoví technické specifikace a formáty pro důvěryhodné seznamy, které se použijí pro účely odstavců 1 až 4"*.

Uvedená ustanovení můžeme shrnout, že nařízení eIDAS upravuje důvěryhodné seznamy pouze ve *formě vhodné pro automatické zpracování*, rovněž Komisí zpětně zveřejňovaná informace má být *ve formě vhodné pro automatické zpracování*. Jiné formy nařízení nezmiňuje.

6.9.3 Účinky uvedení v důvěryhodném seznamu

Uvedení ve zveřejněném důvěryhodném seznamu je podmínkou pro to, aby kvalifikovaný poskytovatel služeb vytvářejících důvěru mohl začít danou kvalifikovanou službu vytvářející důvěru poskytovat (čl. 21 odst. 3 eIDAS). Je též podmínkou, aby kvalifikovaný poskytovatel služeb svou kvalifikovanou službu vytvářející důvěru mohl označovat značkou důvěry EU (čl. 23 odst. 1 eIDAS).

Nařízení eIDAS však výslovně nestanoví, že uvedení ve zveřejněném důvěryhodném seznam má dokladovací nebo důkazní účinek. Takový právní účinek ani právní domněnka v nařízení eIDAS stanoveny nejsou. Tento potřebný důkazní účinek však může vyplývat z práva členského státu, podle nějž jedná jeho subjekt odpovědný za vedení důvěryhodných seznamů. Roli pak může hrát i to, zda se jedná o subjekt soukromý, anebo subjekt veřejný či státní, v jakém režimu práva jedná apod.

V ČR např.[119] podle § 134 o. s. ř. listiny vydané *„státními orgány v mezích jejich pravomoci ... potvrzují, že jde o ... prohlášení orgánu, který listinu vydal, a není-li dokázán opak, i pravdivost toho, co je v nich osvědčeno nebo potvrzeno"*. V ČR je působnost takového státního orgánu založena čl. 13 odst. 3 zák. č. 297/2016 Sb. a je udělena Ministerstvu vnitra. Důvěryhodný seznam jím vydaný proto bude tzv. veřejnou listinou a bude se u něj presumovat správnost jejího obsahu. Právní vlastnosti důvěryhodných seznamů vydaných v jiných členských státech by bylo třeba stanovit obdobným způsobem, stát po státu.

Při zvážení klíčového významu, které důvěryhodný seznam v eIDAS má, zejména s ohledem na ověřování platnosti kvalifikovaného elektronického podpisu dle čl. 32 eIDAS, došel však autor k přesvědčení, že na základě výkladu užitečného účinku je nutné nařízení eIDAS vyložit tak, že *uvedení ve zveřejněném důvěryhodném seznamu dokladovací a důkazní účinek má*, bez ohledu na vnitrostátní právní úpravu. Bez předpokladu správnosti údajů v důvěryhodném seznamu, zejména toho, že se jedná o kvalifikovaného poskytovatele a kvalifikovanou službu vytvářející důvěru, nelze totiž naplnit účel nařízení eIDAS, aby jím upraveny služby vytvářející důvěru bylo možné využívat přeshraničně.

[119] Mírně odlišně upravuje veřejnou listinu § 567–569 obč. zák.

6.9.4 Rozhodnutí (EU) 2015/1505 – specifikace důvěryhodných seznamů

Výše předeslaným aktem dle čl. 22 odst. 5 eIDAS se stalo *„Prováděcí rozhodnutí Komise (EU) 2015/1505 ze dne 8. září 2015, kterým se stanoví technické specifikace a formáty důvěryhodných seznamů..."* Za určitý právní nedostatek a zdroje právní nejistoty v rozhodnutí (EU) 2015/1505 lze považovat, že v něm chybí určení místa, webové adresy nebo způsobu, jak spolehlivě nalézt klíčový evropský seznam seznamů členských států, který vydává Komise podle čl. 22 odst. 4 eIDAS, resp. podle čl. 4 odst. 3 rozhodnutí (EU) 2015/1505.

Podle druhého uvedeného ustanovení: *„zpřístupní Komise veřejnosti"* seznam seznamů *„bezpečnou cestou na ověřeném webovém serveru"*, a to *„ve formě vhodné pro automatické zpracování opatřené podpisem nebo pečetí"*. Jak má veřejnost seznam seznamů nalézt, popř. ověřit jeho platnost a pravost, však již rozhodnutí nestanoví.

Nejedná se přitom úplně o maličkost. Tento seznam bývá označován jako LOTL *(List of Trusted Lists)*, popř. jako EU LOTL. Jen na základě informací shromážděných do LOTL, zahrnujících i certifikáty různých národních úřadů a webové adresy národních důvěryhodných seznamů, lze totiž vůbec jednoznačně nalézt jak národní důvěryhodné seznamy, tak provést ověření platnosti jejich podpisu vydávajícím národním úřadem, tj. ověřit pravost obsahu národního důvěryhodného seznamu a potažmo zjistit či ověřit názvy kvalifikovaných poskytovatelů a druhy jimi poskytovaných kvalifikovaných služeb vytvářejícícch důvěru.

Bez přístupu k LOTL a bez jistoty o tom, že je k dispozici pravý LOTL, se celý systém dostává do potíží. Nařízení eIDAS přitom výslovně nestanoví jiné náhradní způsoby zjišťování stavu kvalifikovanosti poskytovatele a jeho služeb. Jen na základě použití mimoprávních nástrojů webových vyhledávačů se autorovi podařilo zjistit, že vždy nejaktuálnější seznam LOTL se pravděpodobně nachází na webové adrese (1): <https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml>.

Až z tohoto seznamu, který je ve formě pro automatické zpracování, autor zpětně odvodil, že informativní stránka o důvěryhodných seznamech se zřejmě nachází na adrese (2): <https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers>.[120]

[120] Stránka má i navigací: European Commission > Strategy > Digital Single Market > EU Trusted Lists.

Z této webové stránky (2) vede hyperlinkový odkaz na LOTL výše pod textem „EU Trusted List of Trust Service Providers“, adresa (1) zřejmě je správná. Analogii informativní stránky (2) v češtině se autorovi nalézt nepodařilo vůbec. Teprve později autor náhodně zjistil, že existuje informační sdělení (2016/C 233/01),[121] které webovou adresu (1) zveřejňuje v Úředním věstníku EU, a poskytuje tak potřebnou právní jistotu o její správnosti a trvalosti. Sdělení lze v systému EUR-Lex dohledat,[122] k čemuž je ovšem třeba vědět, že vůbec má být hledáno. Sdělení dále zveřejňuje i otisky (hašovací hodnoty) čtyř certifikátů a v příloze dokonce i samotné certifikáty ve formátu PEM, kterými je zajištěn (podepsán) samotný LOTL. Současně však informační sdělení uvádí, že další verze LOTL budou obsahovat hodnoty certifikátů v sobě samém. O důvodech, proč vydání informačního sdělení nebylo avizováno v rozhodnutí (EU) 2015/1505, lze jen spekulovat. Jeho sepisovatel pravděpodobně vycházel ze zaběhnuté praxe důvěryhodných seznamů nebo měl za to, že hlavním právním základem k jejich vydávání je rozhodnutí Komise 2009/767/ES, které je založeno na směrnici 2006/123/ES o službách na vnitřním trhu.

6.9.5 Prohlížeč důvěryhodných seznamů

Komise nechala vytvořit on-line systém tzv. prohlížeče důvěryhodných seznamů *(TL – Browser)*, který umožňuje prohlížet důvěryhodné seznamy vydávané členskými státy. Je k dispozici na adrese: <https://webgate.ec.europa.eu/tl-browser/>.

6.9.6 Uvádění služeb, které nejsou kvalifikovanými podle eIDAS

Výsledkem úpravy je, že podle prohlížeče důvěryhodných seznamů zařazuje na důvěryhodný seznam nekvalifikované služby, popř. kvalifikované pouze podle práva daného členského státu, následující první skupina států: Itálie, Francie, Spojené království, Maďarsko, Bulharsko, Polsko, Rakousko, Chorvatsko, Dánsko, Portugalsko, Estonsko, Lotyšsko, Lichtenštejnsko, Lucembursko a Slovinsko (pořadí zhruba odpovídá početnosti takových záznamů).

Oproti tomu na seznamu naopak nemají zařazenu žádnou takovou komerční službu v druhé skupině států: Německo, Španělsko, Nizozemsko, Belgie, ČR, Slovensko, Finsko, Norsko, Island, Irsko, Litva, Malta, Švédsko. Z toho Německo

[121] Informace týkající se údajů na důvěryhodných seznamech členských států oznámené podle rozhodnutí Komise 2009/767/ES, ve znění rozhodnutí 2010/425/EU a prováděcího rozhodnutí 2013/662/EU, a podle prováděcího rozhodnutí (EU) 2015/1505 (2016/C 233/01)

[122] Z dokumentu CELEX: 32015D1505, tj. prováděcí rozhodnutí Komise (EU) 2015/1505, v záložce | Document information| přes položku a hyperlink ‘– Select all documents based on this document’.

a Slovensko mají uvedenu jednu „Non-regulatory“ službu u svého dohledového orgánu, Řecko ji má u orgánu pro veřejnou správu. Takové záznamy jsou ještě přijatelné z hlediska soutěžního, neboť tyto služby nenarušují tržní prostředí jiných poskytovatelů.

Autor považuje přitom za jisté, že z uvedených států přinejmenším v Německu, Španělsku, Nizozemsku, Belgii, ČR a na Slovensku existují mnozí (kvalifikovaní) poskytovatelé služeb vytvářejících důvěru poskytující i služby, které však nejsou kvalifikované ve smyslu nařízení eIDAS.

Pro úplnost dodejme, že žádného poskytovatele neuvádí Kypr. V případě Rumunska v den nahlížení prohlížeč seznamů nezobrazoval žádné údaje, ačkoli v seznamu LOTL jeho záznam existuje.

Proč tato situace vznikla? Mohou existovat přinejmenším tři důvody. Prvním důvodem může být, že členský stát vydávající důvěryhodný seznam respektuje zásadu *lex superior derogat inferiori*, tj. postupuje podle výkladu nařízení a neuplatňuje kolidující výklad rozhodnutí, které má nižší právní sílu, v dobré víře a z hlediska zásady zákonnosti. Druhým motivem členského státu může být obava, že výklad rozhodnutí v rozporu s nařízením může být právně někdy napaden a mohlo by případně dojít k postihu daného členského státu. Třetím důvodem může být, že se členský stát snaží minimalizovat rozsah a počet služeb, za které případně odpovídá v důsledku jejich zařazení na důvěryhodný seznam. Ve všech těchto třech případech je poskytovatel služeb vůči svému vlastnímu státu bezmocný, zařazení na důvěryhodný seznam si jen obtížně může vynutit, výsledky případných sporů se státem by byly nejisté.

Ať již je důvod jakýkoli, je patrné, že poskytovatelé služeb z druhé skupiny států jsou částečně diskriminováni oproti poskytovatelům služeb z první skupiny tím, že jim v důvěryhodných seznamech nejsou uvedeny všechny služby. Uvedené nechť je dokladem, že snad i dobře míněné úpravy v prováděcích aktech, které se zdají překračovat oprávnění prováděcího aktu, nemají pouze a jen dobré následky, zde ze soutěžního hlediska.

6.10 Kvalifikované prostředky pro vytváření elektronického podpisu

Jednou ze tří definičních podmínek kvalifikovaného elektronického podpisu podle čl. 3 bod 12 eIDAS je, že je vytvořen *kvalifikovaným prostředkem pro vytváření*

elektronických podpisů. Pro tento prostředek zde používáme zkratku QSCD.[123] Prostředek je definičně určen (čl. 3 bod 23 eIDAS) jako takový, který splňuje požadavky stanovené v *příloze II* eIDAS.

Požadavky v příloze II jsou členěny do odstavců 1 až 4, které musí být splněny kumulativně, byť nový odstavec 4 se zřejmě týká jen případů vytváření kvalifikovaných elektronických podpisů na dálku. Odst. 1 odpovídá téměř doslovně[124] příloze III odst. 1 DirES. Uvádí taxativní výčet minimálních požadavků, které se týkají všech možností provedení QSCD (srov. 6.2.5). Konkrétní provedení QSCD tedy může poskytovat i vlastnosti či funkce navíc, takové vlastnosti však nejsou povinné a pochopitelně nesmí být v rozporu s požadavky povinnými.

Dle odst. 1 přílohy II eIDAS datům pro vytváření elektronických podpisů musí být přiměřeně zajištěna důvěrnost (tajnost), smí se prakticky vyskytnout pouze jednou, nesmí být možné[125] je odvodit a s nimi vytvořený elektronický podpis je spolehlivě chráněn proti padělání při použití[126] v současnosti dostupných technických prostředků. Uvedené požadavky musí jednak zajišťovat určitá dobře zvolená kryptografická schémata, jednak sama technická implementace technickým prostředkem či spolupráce více technickými prostředky. Z hlediska článku 26 eIDAS se jedná zejména o pokrytí požadavků jednoznačného spojení s podepisující osobou. Požadavek na spolehlivou ochranu před zneužitím třetí osobou pak z článku 26 eIDAS pokrývá zejména udržení výhradní kontroly nad daty pro vytváření elektronického podpisu. Požadavky odst. 1 přílohy II lze však vyložit i tak, že všechny přispívají a společně zajišťují oba požadavky z písm. a) i c) článku 26 eIDAS. Zmíněný požadavek na ochranu elektronického podpisu před padělaním zajišťuje i požadavek písm. d) z článku 26 eIDAS na integritu podepsaných dat.[127]

Podle přílohy II odst. 2 QSCD *„nesmějí měnit podepisovaná data ani bránit tomu, aby byla tato data předložena podepisující osobě před vlastním podepsáním"*. Uvedené dva požadavky sice směřují k tomu, aby podepisující osoba elektronicky

[123] Z anglického ***Q**ualified Electronic **S**ignature **C**reation **D**evice*. Zkratka QSCD se někdy v technických dokumentech používá i pro současné zastřešení *pojmu kvalifikovaný prostředek pro vytváření elektronických pečetí (Qualified Electronic Seal Creation Device)*, v tomto textu tak ale není používána.

[124] Anglické znění je prakticky totožné. Český překlad směrnice DirES je považován za problematický.

[125] V úrovni přiměřeného zajištění. Stejné obraty však zde byly i součástí DirES.

[126] Které by mohl použít útočník na elektronický podpis podepisující osoby.

[127] Jediný zbylý požadavek z článku 26 písm. b) pak pokrývají kvalifikované certifikáty pro elektronický podpis, a nikoli samotné QSCD.

podepsala právě to, co jí bylo předloženo,[128] obě podmínky je ale třeba chápat úzce. Ve smyslu bodu odůvodnění 56 eIDAS prostředek QSCD nezahrnuje ani systémové prostředí, ani aplikaci pro vytváření podpisu. Bez jejich správné funkce QSCD není schopen zajistit, že data případně předložená podepisující osobě jsou skutečně ta, která potom QSCD elektronicky podepíše, tj. není schopen zabránit útoku podvržení (podsunutí) jiných dat. Ohledně obratu *„nesmějí ... bránit [předložení]"* je autor názoru, že tato podmínka dokonce připouští, že podepisující osoba může ze své vlastní vůle potlačit předložení dat určených k podpisu. QSCD pouze nesmí být konstruován tak, aby tomuto předložení bránil. Vedle jazykového výkladu důvodem autora je i to, že odst. 2 přílohy II eIDAS opět téměř doslovně odpovídá dříve platné úpravě v příloze III odst. 2 DirES. Přinejmenším v Německu pak byla dosud běžná praxe tzv. dávkových elektronických podpisů, kdy podepisující osoba si sice mohla nechat zobrazit seznam jednotlivých dat určených k podpisu, ale bylo na ní, zda si je nechá postupně či namátkově předkládat nebo je elektronicky podepíše bez těchto předložení.

I v případě požadavku na nebránění předložení platí, že bez kontroly systémového prostředí a aplikace vytvářející podpis nemusí být vůbec možné tento požadavek plně realizovat vůči podepisující osobě. Podepisující osoba může tedy případně pomocí QSCD nechtěně podepsat nějaká data, aniž by jí byly vůbec předloženy a aniž by je chtěla mít nepředloženy. Prostředek QSCD by zde nicméně měl být konstruován tak, aby s ohledem na požadavek spolehlivé ochrany před zneužitím podle přílohy II odst. 1 písm. d) eIDAS dal podepisující se osobě na vědomí, že k vytvoření elektronického podpisu má právě dojít, a sám vyžadoval provedení nějaké bezprostředně předcházející autentizační činnosti. Pokud podepisující osoba nemá předložena žádná data určená k podpisu, popř. právě nic elektronicky podepisovat nehodlá, pak by bezpečnostně skeptická osoba neměla požadovanou autentizaci vůči QSCD provést. V případě dávkových podpisů však nelze vyloučit, že vadné či bezpečnostně narušené systémové prostředí nebo aplikace pro vytváření elektronického podpisu nechají QSCD podepsat i jiná data, než která podepisující osoba podepsat chtěla.

Uvedená ochranná autentizační činnost vůči QSCD je i důvodem, proč by data pro vytváření elektronického podpisu neměla být využívána k žádným jiným

[128] Předložení bude typicky vizuální ve formě dokumentu, formuláře aj. písemností, ale může se jednat i o předložení obrázků nebo předložení zvukového záznamu nebo obrazově zvukového záznamu, předložení hmatové aj. smyslově vnímatelné.

kryptografickým účelům, jako je například autentizace osoby nebo šifrování dat, byť by čistě technicky takové činnosti někdy bylo možné sloučit. V rámci těchto jiných operací nejsou osobě předkládána žádná data, což zvyšuje riziko nechtěného vytvoření elektronického podpisu podvržených dat. K překonání uvedeného rizika je potřeba vytvoření a používání jiných kryptografických klíčových dvojic, ale i odlišení autentizační činnosti nebo jiné činnosti. Při vytváření elektronického podpisu by proto QSCD mělo vyžadovat například jiné PIN nebo pomocí uživatelského rozhraní výrazně odlišit, že se má jednat o operaci vytvoření elektronického podpisu.

Příloha II odst. 3 eIDAS obsahuje podmínku, že data pro vytváření elektronických podpisů *„může jménem podepisující osoby vytvářet nebo spravovat pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru"*. Podmínka má smysl jednak pro případy elektronických podpisů vytvářených na dálku (srov. též níže), ale řeší i dosud používanou praxi podle DirES, kdy data pro vytváření elektronických podpisů vytvářel poskytovatel certifikačních služeb,[129] aby je bezprostředně po vytvoření[130] přenesl do té části QSCD, která byla poté vydána do držení podepisující osobě. Smyslem odst. 3 zde tak je dovolit takovou činnost. Současně však bohužel není podmínka normativně omezena jen na zmíněné případy, omezení tedy představuje odst. 1 přílohy II eIDAS.

Příloha II odst. 4 eIDAS upravuje situaci, kdy data pro vytváření elektronických podpisů podepisující osoby spravují kvalifikovaní poskytovatelé služeb vytvářejících důvěru. K této situaci zřejmě dochází či by mělo docházet zatím pouze tehdy, pokud poskytovatel služeb poskytuje službu vytváření kvalifikovaných elektronických podpisů na dálku. Odst. 4 dovoluje vytváření kopií dat pro vytváření elektronických podpisů pro účely jejich zálohování, přičemž počet kopií nesmí přesáhnout minimum pro zajištění kontinuity služby a bezpečnost zkopírovaných souborů dat musí být na stejné úrovni jako u původních souborů dat.

Vytváření záloh dat pro vytváření elektronických podpisů je bezpečnostně sporná praxe. V případně tradičního provedení QSCD (provedení 1 v 6.2.5) se zálohy nevytvářely žádné. Jejich vytváření nebylo v příloze III DirES dovoleno, z požadavku prakticky pouze jediného výskytu se pak implikovalo spíše to, že zálohy jsou zakázané.

[129] Terminologii DirES, v pojmech eIDAS se jedná o kvalifikovaného poskytovatele služeb vytvářejících důvěru, který vydává kvalifikované certifikáty pro elektronický podpis.

[130] Účelem této metodiky vytvoření je použití kvalitních kryptografických generátorů náhodných čísel, které zlepšují možnosti ochrany QSCD z hlediska *neodvoditelnosti* dat pro vytváření elektronického podpisu.

V případě ojedinělého technického selhání SSCD dostačovalo dané podepisující osobě vydat nové SSCD s novými daty pro vytváření elektronického podpisu. Takový postup nezpůsoboval neplatnost dříve vytvořených elektronických podpisů, byl ekonomický a bezpečnostně ideální. V případě, že však technicky selže zařízení QSCD v držení poskytovatele služeb vytvářejících důvěru pro vytváření elektronických podpisů na dálku, v němž mohou být uložena data pro vytváření elektronických podpisů tisíců až stovek tisíců podepisujících osob, nové vydávání nových dat pro vytváření elektronických podpisů a souvisejících kvalifikovaných certifikátů by znamenalo citelnou zátěž na straně uživatelů i poskytovatele, jakož i újmu na renomé poskytovatele. Nařízení proto umožňuje vytvářet zálohy, což z hlediska bezpečnosti určitě představuje kompromis. Kompromisem je však už i svěření dat pro vytváření elektronických podpisů do správy poskytovatele. Konkrétní bezpečnost řešení je možné hodnotit či posuzovat pouze vůči konkrétnímu provedení.

Odst. 4 explicitně uvádí, že jeho ustanovení se nedotýkají požadavku podle odst. 1 písm. d), tj. že i nadále musí být podepisující osoba schopna data pro vytváření elektronických podpisů spolehlivě chránit před jejich zneužitím třetí osobou. Je ovšem třeba zdůraznit, že odst. 4 se nedotýká platnosti ani žádného z jiných požadavků odst. 1 s výjimkou těch, vůči nimž v jistém smyslu tvoří *lex specialis*. Z požadavků odst. 1 pouze požadavek praktického výskytu pouze jednou je odstavcem 4 zmírněn v tom smyslu, že se jím nerozumí případy pořízení záloh v souladu s odst. 4.

6.10.1 Otázka vyhovění požadavkům na QSCD

Jak je uvedeno výše, požadavky přílohy II eIDAS na QSCD zajišťují splnění požadavků na zaručený elektronický podpis podle písm. a), c) a d) čl. 26 eIDAS.

Současně znamená jejich splnění i vyhovění požadavku na použití QSCD, který je sám jednou ze tří podmínek pro možnost vytvoření kvalifikovaného elektronického podpisu (QES). Osoby mající zájem o využití právního rámce eIDAS pro elektronické podpisy, zejména v úrovni kvalifikovaného elektronického podpisu, budou proto mít i zájem pořídit si QSCD.

Je proto praktickou otázka, jak lze o nějakém zařízení, prostředku či souboru prostředků sestávajících z více částí určit, že jsou QSCD ve smyslu nařízení eIDAS. Dle autora vzniká ne zcela zanedbatelný rozpor metodiky zodpovězení takové otázky podle článku 29 a článku 30 eIDAS. Tyto metodiky jsou probírány níže.

6.10.2 Výklad článku 29 eIDAS podle New Approach?

Před právním výkladem článku 29 eIDAS je zde třeba provést určitou aspoň minimalistickou vsuvku o přístupu k technické normalizaci v EU.[131] Zastánci technické normalizace mohou uvádět její obecné výhody. Například evropská normalizační organizace CEN[132] tvrdí, že technické normy: „zvyšují bezpečnost výrobků, povzbuzují ekonomiku úspor z velikosti, dovolují výrobcům splňovat evropskou legislativu, podporují intereoperabilitu produktů a služeb, povzbuzují vyšší konkurenci, usnadňují obchod odstraňováním obchodních překážek, podporují ekologickou bezpečnost a udržitelnost, chrání životní prostředí, odrážejí výzkum a vývoj, podporují společné porozumění“. Zda lze tato tvrzení prokázat, je podstatně spornější. Autoři Blind a Jungmittag ve své důkladné analýze[133] z r. 2008 o vlivu vydávání patentů a technických norem na ekonomický růst uvádí, že zatímco studie o účinku patentů na ekonomiku existují, teoretická literatura k otázce vlivu normalizace na hospodářský růst prakticky neexistuje.

Z hlediska práva Evropských společenství představovaly případné národní závazné technické normy netarifní překážku obchodu. Kromě toho zejména v rychle se rozvíjejících odvětvích, jakým je i oblast elektrotechniky nebo nověji informačních technologií, může normalizace hrubě zaostávat za vývojem. Svázat výrobu a obchod požadavky technických norem, pomalých postupů jejich vytváření a rovněž pomalých a navíc nákladných postupů jejich nezávislého ověřování může efektivně znamenat zničení daného sektoru průmyslu ve srovnání se zahraničím, pokud to je liberálnější.

V moderní výrobě a obchodu se právo stanovení závaznosti technických norem spíše vyhýbá. Dle německé judikatury například: „DIN-Normy nejsou žádné právní normy, nýbrž soukromá technická pravidla doporučujícího charakteru. Mohou vyjadřovat uznávaná pravidla techniky nebo za nimi zaostávat.“[134] Obdobně informuje i sama německá normalizační organizace DIN: „Normy nemají samy o sobě žádnou sílu zákona. Použití norem je dobrovolené. Ačkoli mají pouze charakter doporučení, spočívá jejich síla prosazení se na jejich značném používání a na v nich shromážděné

[131] Výklad technické normalizace je zde s ohledem na rozsah práce značně zjednodušen a směrován k potřebám právního výkladu článků 29 a 30 eIDAS. Mnohé otázky, jako organizační podstata normalizačních organizací, požadavky na jejich činnost, práva duševního vlastnictví v jejich výsledných produktech, vliv komerčních konsorcií v oblasti IT atd., jsou zde proto zcela opomenuty.

[132] CEN. *Compass, European Standardisation in a nutshell.* September 2004, s. 2.

[133] BLIND, K. – JUNGMITTAG, A. The impact of patents and standards on macroeconomic growth: a panel approach covering four countries and 12 sectors. *Journal of Productivity Analysis.* Volume 29, Issue 1, February 2008, s. 51–60.

[134] BGH, Urteil vom 14. Mai 1998, Az. VII ZR 184/97, Volltext = BGHZ 139, 16.

kvalifikované odborné znalosti. Teprve použitím v právních aktech mohou dosáhnout právní závaznost, například v soukromých smlouvách, nebo zákonech a nařízeních, které se na ně odvolávají. Použitím norem se lze vyhnout právním sporům, neboť obsahují jednoznačná ustanovení.“[135] Technické normy se tedy mohou prostřednictvím příkazů práva stát právně závazné. Současně však taková ustanovení a technické normy mohou určitou oblast nežádoucím způsobem petrifikovat a umrtvit její vývoj.

Evropské právo zde nalezlo zcela zvláštní přístup propojení technické normalizace s právem, který je označován jako ***New Approach*** (nový přístup). Podle Van Eeckeho „filosofie použití technických norem podle *New Approach* je:

1. Právní harmonizace je omezena na podstatné požadavky ...
2. Technické normy a specifikace jsou prostředkem určení dosažení podstatných právních požadavků.
3. Tvorbou technických norem v rámci *New Approach* jsou pověřeny kompetentní organizace z oblasti technické normalizace.
4. Použití technických norem i v rámci New Approach zůstává dobrovolné ... Členské státy jsou však zavázány, aby uznávaly technické normy přijaté v rámci New Approach ‚domněnkou vyhovění' [‚presumption of conformity']. Prakticky tato domněnka znamená, že pokud výrobce dodržuje řečenou technickou normu, nemusí dokazovat, jak jeho produkt je ve shodě s právními pravidly. Přidržení se řečené technické normě automaticky implikuje dodržení právních požadavků.“[136]

Z hlediska problémů, které technická normalizace přináší, poskytuje *New Approach* několik zcela podstatných výhod. Požadavky lze formulovat právně bez toho, aby v době tvorby právního předpisu musela předem existovat technická norma. Právní předpis nemusí zacházet do příliš velkých podrobností. Příslušnou normalizační instituci[137] lze poté pověřit, aby vypracovala technickou normu pro dané právní

[135] DIN – Fragen und Antworten: Sind Normen mit Gesetzen gleichzusetzen? Dostupné z: <http://www.din.de/cmd?cmsrubid=47513&menurubricid=47513&level=tpl-rubrik&menuid=47391&languageid=de&cmsareaid=47391 - Normen%20und%20Gesetze>.

[136] VAN EECKE, P. (team supervisor). *Final Report of the Study on the specific policy needs for ICT standardisation*. European Union, 10. 5. 2007.,s. 25. Dostupné z: <http://ec.europa.eu/idabc/en/document/7040/254.html>; navštíveno 10/2017.

[137] V rámci evropského práva se pověřuje k vypracování příslušné technické normy, na základě tzv. mandátu, typicky některá evropská normalizační instituce, tj. CEN, CENELEC nebo ETSI.

požadavky. Je-li výsledná technická norma dodržována, vzniká na základě toho právní presumpce vyhovění právním požadavkům právního předpisu.[138]

Je třeba zdůraznit, že *domněnka vyhovění* je odlišná od *právní domněnky*, jak je pojem běžně užíván českou právní naukou. Právní domněnka je součástí práva a stanoví určité zjištění o záležitosti skutkového stavu jako právem předpokládané. Takové právní ustanovení se zpravidla opírá o obecné životní zkušenosti tím, že se z jedné skutkové okolnosti přes právní normu usuzuje na jinou skutkovou okolnost.[139] Právní domněnky bývají v českém právu zpravidla vyvratitelné důkazem opaku. Právní domněnky jsou užitečné z hlediska dokazování ve fázi řízení před soudem. Též ve fázi realizace práva právní domněnka umožňuje, aby se mohla použít některá právní norma, jejíž hypotézou je skutkový stav předpokládaný právní domněnkou.

Domněnka vyhovění však prvotně stanoví splnění dispozice právní normy. Uvedené může být zastřeno tím, že příloha II v eIDAS (popř. III v DirES) není psána na první pohled jako rozeznatelná právní norma. Přílohu II lze ale reformulovat tak, že pokud jsou splněna všechna jednotlivá kritéria z přílohy (konjunkce podmínek v hypotéze), pak právním následkem (dispozicí právní normy) je, že prostředek je QSCD. Domněnkou vyhovění z vyhovění technické normě presumujeme právní dispozici, tedy že prostředek je QSCD. Kritéria přílohy II lze nyní běžně ignorovat, neboť se lze opřít o domněnku vyhovění.

Právní následek, že prostředek je QSCD, se poté pochopitelně může sám stát součástí hypotéz jiných právních norem, např. požadavků na kvalifikovaný elektronický podpis. Rozdíl však spočívá v tom, že právní domněnka neovlivňuje platnost jiných právních norem. Domněnka vyhovění oproti tomu běžně fakticky téměř deroguje některou právní normu (v nařízení eIDAS například přílohu II), resp. činí její vyhodnocování běžně zbytečným. Jelikož však zákonodárce zde stanoví, že se jedná o pouhou domněnku, může se některá strana pokusit ji vyvrátit. K tomu pochopitelně musí mít znění právní normy stále k dispozici (např. přílohu II eIDAS), k právní derogaci přeci jen nedošlo. Dostačuje pak vyvrátit kteroukoli potřebnou podmínku právní normy v hypotéze. Tuto analýzu lze uzavřít, že na domněnku vyhovení lze hledět buď jako na přímé stanovení dispozice právní normy, nebo jako na velmi komplexní právní domněnku, která zahrnuje splnění mnoha dílčích podmínek nebo hypotéz

[138] Pro výklad *New Approach* (nový přístup) srov. též SVOBODA, P., cit. dílo, s. 253–254.
[139] GERLOCH, A., cit. dílo, 2004, s. 205–206.

právních norem současně, jejichž výběr je proveden tak, aby došlo ke splnění dispozice určité právní normy.

V rámci metodiky *New Approach* se však technická norma nestává závaznou v tom smyslu, že by byla právně nutnou podmínkou splnění právních požadavků. Metodika nevylučuje, aby například výrobce neprohlásil shodu přímo vůči právním požadavkům. Může tak rychle reagovat na vývoj trhu, technologické změny, pomalost tvorby technické normy apod. V případě soudního sporu nicméně bude na výrobci či tom, kdo tvrdí splnění právních požadavků, aby je u soudu dokázal, například znalecky.

Naopak ani vyhovění vyhlášené technické normě nezaručuje v případě sporu u soudu úplnou jistotu úspěchu, neboť dodržení technické normy poskytuje pouhou domněnku vyhovění. K vyvrácení je však i zde třeba důkaz opaku. Protistrana by musela dokázat, že požadavky technické normy nestačí obecně nebo v daném případě konkrétně ke splnění právních požadavků.[140] Snadnější běžně bude tvrzení, že produkt nesplňuje danou technickou normu a že domněnku vyhovění nelze uplatnit, což je však zcela odlišná strategie postupu při řízení, než je vyvrácení domněnky vyhovění. Důkazní břemeno o dodržení technické normy může často spočívat na výrobci.

Z procedurálního hlediska bývá právní regulace *New Approach* dvoufázová. V první fázi je vytvořena obecná právní úprava, která stanoví právní požadavky i možnost presumpce jejich vyhovění při splňování technické normy. Technická norma ještě nebývá určena, pouze je stanoven způsob, kterým určena bude. Poté následuje vytvoření technické normy anebo výběr z plejády případně do úvahy již přicházejících technických norem či specifikací, anebo jejich dotvoření. V druhé fázi navazující právní předpis vyhlásí určitou technickou normu nebo specifikaci jako tu, která zakládá domněnku vyhovění požadavkům z právního předpisu první fáze. Dodržování vyhlášené technické normy může být předepsáno samoregulací, tj. samotným výrobcem, anebo může být právem přikázána certifikace produktu výrobce vhodně zvolenou zkušebnou.

Historickým předobrazem pro *New Approach* byla směrnice o nízkém napětí[141] 73/23/EES. Za první vědomé formulování principu je považována[142] Rezoluce Rady z května 1985 o novém přístupu k technické harmonizaci a normám. Byla dále

[140] V případě použití technických norem renomovaných normalizačních organizací by taková možnost měla být prakticky téměř vyloučena.
[141] Tzv. *Low Voltage Directive*. V mezidobí několikrát nahrazena novou úpravou.
[142] VAN EECKE, P. (team supervisor), cit. dílo, s. 25.

implementována v takzvané transparenční[143] směrnici 98/34/ES. Metoda *New Approach* poté byla použita v řadě případů. V oblasti aspoň související s elektronikou se například kromě výše uvedené směrnice o nízkém napětí jednalo ještě o směrnici o elektromagnetické kompatibilitě 83/336/EHS nebo o směrnici 1999/5/ES o rádiových zařízeních a telekomunikačních koncových zařízeních a vzájemném uznávání jejich shody.[144] Jak však udává Van Eecke, metoda *New Approach* se používala i mimo typické oblasti použití. Jako jeden z těchto příkladů udává[145] právě směrnici DirES, tj. 1999/93/ES. Explicitně zmiňuje prostředky pro bezpečné vytváření podpisu[146] (tj. SSCD) podle čl. 3 odst. 5 DirES. Z toho lze vyvodit, že dle jeho názoru tedy SSCD lze vyrobit a dodat jak přímo podle právních požadavků DirES (tj. zejména přílohy III), tak podle technické specifikace vyhlášené podle čl. 3 odst. 5 DirES. V druhém případě se ze shody s technickou specifikací bude předpokládat vyhovění právním požadavkům.

Zvláštností DirES podle Van Eeckeho je, že odkazovanou technickou specifikací není skutečná evropská norma (tj. s označením EN), ale pouze dokument ranější normalizační fáze (s označením CWA). Důvodem toho pravděpodobně byl spěch přijetí daného dokumentu. Technickou specifikaci určilo až po 3 letech od vydání směrnice DirES rozhodnutí Komise 2003/511/EC. Konkrétně pro SSCD došlo k rozlišení až v příloze B, která určila, že obecně uznávanou normou[147] pro produkty elektronického podpisu, v jejichž případě členské státy budou předpokládat, že jsou v souladu s požadavky uloženými v příloze III směrnice 1999/93/ES, je *„**CWA 14169 (March 2002)**: prostředky pro bezpečné vytváření podpisu"* (zvýraznil autor).

Čl. 29 odst. 1 eIDAS odpovídá čl. 2 bod 6 DirES. Předpisy zde pro QSCD, resp. SSCD stanoví povinnost splňovat požadavky relevantní přílohy právního předpisu

Čl. 29. odst. 2 eIDAS pak odpovídá čl. 3 odst. 5 DirES.[148] Dle druhé věty odstavce vyhovění určeným technickým normám *(meets those standards)* zakládá předpokládání shody *(shall presume ... compliance)* s právními požadavky stanovenými v příloze II eIDAS.[149]

---

[143] Rovněž nazývaná směrnice o *New Approach*. Účelem této směrnice je rovněž zabránit duplicitní technické normalizace na národní úrovni. I tato směrnice byla mezitím nahrazena novou úpravou.

[144] Obě směrnice jsou již nahrazeny novou úpravou.

[145] VAN EECKE, P. (team supervisor), cit. dílo, s. 45 a s. 35.

[146] VAN EECKE, P. (team supervisor), cit. dílo, s. 45.

[147] V teorie panoval nikdy nevyjasněný diskurs o tom, co se má rozumět „obecně uznávanou" normou. Citované rozhodnutí za tuto normu určilo uvedený specifikační dokument.

[148] Zejména anglické znění je téměř totožné.

[149] Znění právního předpisu je zde nevhodné (prohození termínů), ovšem je shodně nevhodné v DirES jako v eIDAS. Obrat *„comply with requirements" (být ve shodě s požadavky)* se běžněji používá jako

Oba předpisy rovněž předpokládají, že členské státy stanoví určité subjekty jako zkušebny, které budou provádět posouzení shody QSCD, resp. SSCD (srov. níže).

Autor souhlasí s názorem Van Eeckeho, že i v případě DirES se jednalo o použití metodiky *New Approach*, byť s určitými specifiky. Určitou zvláštností z hlediska metodiky v případě DirES je dovolení v čl. 3 odst. 4 DirES, že zkušebny *„stanoví shodu prostředků pro bezpečné vytváření podpisů* ***s požadavky uvedenými v příloze III****. Komise postupem podle článku 9 vymezí kritéria, podle nichž členské státy stanoví, zda může být subjekt [tj. zkušebna] pověřen"* (zvýraznil a doplnil autor). Tento obrat v zásadě umožňuje, aby nejen výrobce, ale i zkušebna hodnotila prostředek přímo vůči právním požadavkům. Stejné znění právního předpisu může být obsaženo i přímo v národní transpozici směrnice. Ačkoli Komise může stanovit určité požadavky na subjekt (zkušebnu), použitý proces hodnocení je ponechán neupraven, úroveň zajištění ověření shody s právními požadavky není v DirES stanovena.

Paradoxní je, že uvedené rozhodnutí 2003/511/EC platilo až do roku 2016 a že citovaný technický dokument je uveden v takzvané datované verzi, zde z března 2002. Běžný právní výklad u odkazů na datované verze technických specifikací bývá, že odkaz je zcela statický, mělo by se používat právě a jen znění oné datované verze. Metoda poskytuje optimální právní jistotu, nevýhodou může být zastarávání. K tomu skutečně došlo. Ačkoli u dokumentu CWA 14169 vznikly další verze v letech 2004 a 2005, právní reference stále odkazovala na technicky již zastaralý dokument.

Jestliže zkušebny určené členskými státy přesto v letech 2005–2016 certifikovaly určité prostředky jako SSCD, pak tak činily v souladu s národními předpisy vzešlými z transpozice směrnice DirES, a rozhodně nikoli na základě již zastaralé technické normy z roku 2002.

Používání SSCD tak v praxi bylo výsledkem volnosti metodiky *New Approach* splňovat přímo právní požadavky v kombinaci s další volností, kterou se vyznačují transpozice unijních směrnic obecně. Nejprve pozdní a později zase zastaralé vyhlášení jediné technické specifikace Komisí proto nemělo zcela fatální dopady.

určení právní podmínky v hypotéze právní normy na vyhovění technickým požadavkům v technické normě, která následně má nějaká právní následek (dispozici právní normy). Zde je obrat použit pro vyjádření dispozice v právní normě.

Ke čtení a výkladu čl. 29. odst. 2 eIDAS nebo čl. 3 odst. 5 DirES je pak vhodné poznamenat, že bez povědomí[150] o metodice *New Approach*[151] může být obtížné pochopit smysl těchto ustanovení. Dle Dumortiera čl. 3 odst. 4 DirES nestanoví povinnost předkládat SSCD k certifikaci (tj. shodu lze určit přímo vůči právu i bez zkušebny) a odstavec pak lze číst a vykládat různými způsoby, podle toho, co si čtenář právě přeje zdůraznit. Dle něj ale hlavním účelem je zajistit, že pokud je SSCD předkládán k hodnocení, pak patřičnému subjektu. To dle něj členským státům umožňuje uznávat SSCD splňující právní požadavky. Podmínkou navíc je dle něj nutnost předpokládat vyhovění v případě splňování vyhlášené technické normy.[152] Dumortierův výklad zde není úplně jasný. Otvírá dveře národním způsobům hodnocení SSCD, které pochopitelně mohly být a nakonec i byly procesně odlišné. Podle čl. 3 odst. 4 druhá alinea DirES však členské státy měly uznávat SSCD, které byly hodnocené určenými subjekty (zkušebnami) v jiném členském státu, ačkoli byly případně hodnoceny jinak či s jinou úrovní zajištění splnění kritérií, což je závěr značně paradoxní.

Značnou nejistotu způsobuje znění čl. 29 odst. 2 eIDAS u Roßnagela. Německé znění eIDAS totiž používá obrat *„wird davon ausgegangen" (bude z toho vycházet [odvozeno])* tam, kde je v češtině *„předpokládá se shoda"* a anglicky *„shall be presumed"*. Německé znění je skutečně obtížné pochopit jako zápis domněnky, navíc domněnky vyhovění, která se vymyká běžné metodice vyjadřování legislativy u právníka středoevropské právní kultury.

Autor je souhrnně názoru, že jestliže směrnice DirES byla vystavěna podle metodiky *New Approach*, s čímž souhlasí, pak i v případě nařízení eIDAS, jehož dotčená ustanovení těsně sledují ustanovení DirES, je nutné hovořit o použití metodiky *New Approach*. Na první pohled se tedy zdá, že ani QSCD podle eIDAS nemusí být zcela nutné nechat certifikovat podle některé technické normy, což v případě DirES

[150] Takové povědomí by pravděpodobně bylo u citovaných právníků Dumortiera a Roßnagela zmíněno. V jejich argumentaci však metodika *New Approach* zmiňována není.

[151] Metodika je pak zvláštní až raritní tím, že se zřejmě vyskytuje pouze v kontextu unijního práva a pouze v kontextu technických norem. Valná většina právníků se přitom soustřeďuje mnohem spíše na právo než na technickou normalizaci, a i pak spíše na právo svého domovského členského státu.

[152] DUMORTIER, J. – KELM, S. – NILSSON, H. – SKOUMA, G. – VAN EECKE, P. *The legal and market aspects of electronic singnatures – final report, Legal and market aspects of the application of Directive 1999/93/EC and practical applications of electronic signatures in the Member States, the EEA, the Candidate and the Accession countries*. Interdisciplinary centre for Law & Information Technology (ICRI) – Katholieke Universiteit Leuven, Leuven: October 2003, s. 46.

připouštěl i Dumortier. V případě DirES i eIDAS se však uplatňují určité zvláštnosti, které bude třeba dále podrobně sledovat, v případě eIDAS i zcela nově.

Zde je namístě též upozornit, že do října 2017 Komise explicitně neurčila referenční čísla norem na právním základě čl. 29 odst. 2 eIDAS. V důsledku toho chybí i technické normy, které by byly základem pro možnost uplatnit domněnku vyhovění podle metodiky *New Approach*. Komise není povinna čísla těchto referenčních norem určit, pouze tak učinit může.

Komise pouze vydala prováděcí rozhodnutí (EU) 2016/650, ve kterém se však odvolává na právní základ čl. 30 odst. 3 písm. a) nebo čl. 39 odst. 2 eIDAS a i terminologicky se přidržuje pojmosloví z článku 30 eIDAS.[153] Tato situace je zvláštní, neboť rozhodnutím (EU) 2016/650 též stanovené technické normy EN 419 211[154], představují profily ochrany, které všechny byly vyvinuty ze specifikace CWA 14169, jejíž datovaná verze byla Komisí vyhlášena[155] podle DirES právě pro účel domněnky vyhovění. Specifikace tak byla formálně platná až do roku 2016. Pro více srov. níže.

6.10.3 Certifikace QSCD podle eIDAS (čl. 30 a 31 eIDAS)

Článek 30 eIDAS se zabývá možnostmi certifikace QSCD. Certifikaci mají provádět veřejné nebo soukromé subjekty (dále „zkušebny") určené některým členským státem, jejichž názvy a adresy stát rovněž ohlásí Komisi (čl. 30 odst. 1 a 2 eIDAS). Komise může dle čl. 30 odst. 4 aktem v přenesené působnosti stanovit zvláštní kritéria na tyto subjekty (srov 6.1.6.2), ale zatím jej nevydala.

Cílem certifikace je stanovit shodu prostředku s požadavky v příloze II eIDAS. Certifikace ale může být založena výhradně na dvou postupech posouzení bezpečnosti určených v čl. 30 odst. 3 eIDAS, a nikoli pouze přímo podle přílohy II eIDAS.

První možný postup posouzení bezpečnosti se provádí podle technických norem pro posuzování bezpečnosti produktů informačních technologií [čl. 30 odst. 3 písm. a) eIDAS], které Komise vyhlásí prováděcím aktem podle čl. 30 odst. 3 druhá alinea eIDAS.

[153] Prováděcí rozhodnutí Komise (EU) 2016/650 je probíráno bezprostředně níže v další části textu.

[154] Konkrétně EN 419211-1:2014, EN 419211-2:2013, EN 419211-3:2013, EN 419211-4:2013 a nezávazně (orientačně) též normy zahrnující komunikaci s aplikací vytvářející elektronický podpis: EN 419211-5:2013 a EN 419211-6:2014.

[155] Rozhodnutí Komise 2003/511/ES z 14. července 2003 o zveřejnění referenčních čísel obecně uznávaných technických norem pro produkty elektronického podpisu v souladu se směrnicí 1999/93/ES.

Druhý možný postup posouzení bezpečnosti [čl. 30 odst. 3 písm. b) eIDAS] se provádí jiným postupem a slouží pro možnost certifikace prostředků, které jsou inovativní. Je možné ho použít *„pouze v případě, že normy uvedené v písmenu a) neexistují nebo že postup posouzení bezpečnosti podle písmene a) dosud probíhá"*. Význam dikce druhého případu není zcela zřejmý, protože některá technická norma podle písm. a) buď existuje a je Komisí vyhlášena, anebo není. Výkladu nepomáhá ani náhled do bodů odůvodnění či do jiné jazykové verze. Pravděpodobně je nutné jej vykládat tak, že tím zákonodárce mínil vytváření technické normy, které ale ještě není dohotoveno, přičemž připouští i interaktivní tvorbu takové technické normy současně s postupem posouzení podle písm. b). Podmínkami použití druhého postupu rovněž je, že *„používá srovnatelné úrovně bezpečnosti"* [tj. jako technické normy podle písm. a)] a že zkušebna *„daný postup oznámí Komisi"*, a to zřejmě předem. O tomto druhém postupu jako o alternativním postupu hovoří i bod odůvodnění 55 eIDAS. Z jeho znění vyplývá, že oznámení postupu má sloužit k usnadnění vzájemného hodnocení *(peer-review)*. Nařízení eIDAS ale nestanoví, že by alternativní postup měl být Komisí postoupen někomu dalšímu, například jiným členským státům nebo jiným určeným zkušebnám. Hodnocení *(peer-review)* tedy bude zřejmě provádět výlučně Komise sama.

Komise vydala prováděcí rozhodnutí (EU) 2016/650, kterým se stanoví technické normy pro účely čl. 30 odst. 3 písm. a) eIDAS certifikace shody QSCD,[156] až 25. dubna 2016, tedy pouhé dva měsíce před nabytím účinnosti nařízení části eIDAS, týkající se služeb vytvářejících důvěru. Vypracováním technických norem jsou podle bodu odůvodnění 2 rozhodnutí pověřeny organizace odpovědné za normalizaci, konkrétně podle bodu odůvodnění 4 se jedná o organizaci CEN, jednající na základě mandátu M/460, který vydala Komise, ovšem již 22. 12. 2009, za doby platnosti směrnice DirES. Mandát M/460 byl proto ještě založen na terminologii DirES, výstupy technické normalizace z něj je však tendence vyhlašovat až pro nařízení eIDAS.

Podle čl. 1 rozhodnutí (EU) 2016/650 toto vyhlašuje ve své příloze technické normy, zde výše zmiňované, ovšem pouze pro případ, *„pokud jsou data pro vytváření elektronických podpisů ... uchovávána v prostředí spravovaném zcela, nikoli však nutně výhradně uživatelem"*.

Citovaný obrat se zdá být protichůdný. Obrat není součástí nařízení eIDAS, ale ani technických norem, které vyhlašuje příloha rozhodnutí. Z analýzy vyhlášených

[156] Rovněž podle čl. 39 odst. 2 eIDAS pro certifikaci shody prostředku QSealCD.

technických norem EN 419 211Chyba: zdroj odkazu nenalezen však plyne, že obratem se zřejmě míní zahrnutí i toho případu, kdy ke generaci párové dvojice[157] sice dochází v doplňkovém zařízení u kvalifikovaného poskytovatele služeb, ale poté se bezprostředně přenese do prostředku QSCD, který následně již zcela spravuje uživatel.

Kromě šestice profilů ochrany rozhodnutí v příloze vyhlašuje i dva metodické rámce technických norem z oblasti bezpečnosti informačních technologií, a to ISO/IEC 15408 a ISO/IEC 18045:2008. Oba slouží pro posuzování bezpečnosti IT zcela obecně, nejsou omezeny na posuzováním prostředků druhu QSCD.

Obratem v čl. 1 rozhodnutí (EU) 2016/650 proto nejsou míněny inovativní druhy prostředků QSCD pracující na dálku. Jak uvádí bod odůvodnění 6 rozhodnutí, pro tyto prostředky se technické normy teprve vypracovávají. Komise rozhodnutí doplní, až budou k dispozici. Touto připravovanou technickou normou se zřejmě časem stane EN 419241[158], která stanoví požadavky pro tzv. *„server signing“*.

Vzniká otázka, jaký je právní význam provedení certifikace určenou zkušebnou. Nařízení eIDAS právní význam certifikace výslovně nestanoví. Podle bodu odůvodnění 55 eIDAS je certifikace důležitým nástrojem ověřování bezpečnosti. Nařízení nestanoví dokonce ani povinnost certifikaci provést. Zřejmě lze pouze dovodit, že pokud se certifikace provádí, tak ji jednak musí provádět členským státem určená zkušebna a jednak certifikace musí proběhnout jedním ze dvou výše popsaných způsobů. Pokud by zkušebna vyslovila shodu v souladu s některou normou, která by byla určena podle čl. 29 odst. 2 eIDAS, uplatnila by se i domněnka vyhovění. Jinak se ovšem domněnka vyhovění uplatnit nemůže. Pro další význam certifikace srov. 6.10.6.

Podle čl. 31 odst. 1 eIDAS má členský stát bez zbytečného odkladu a nejpozději do měsíce od certifikace některého prostředku jako QSCD oznámit tuto skutečnost Komisi. Obdobně v případě ukončení certifikace, tj. běžného vypršení platnosti, nebo i předčasného ukončení. Komise pak podle čl. 31 odst. 2 eIDAS zřizuje, zveřejňuje a udržuje seznam všech aktuálně certifikovaných QSCD. Jelikož však ani pro členský stát, ani pro Komisi nejsou určeny žádné požadavky při provádění této činnosti, je nutné za právně rozhodnou považovat samotnou certifikaci určenou zkušebnou. Z nařízení

[157] Data pro vytváření elektronických podpisů (soukromý klíč) a data pro ověřování platnosti (veřejný klíč).

[158] V říjnu 2017 jsou k dispozici pouze předběžně normalizační produkty: prEN 419241-1:2017 Part 1: General System Security Requirements; prEN 419241-2:2017 Part 2: Protection profile for QSCD for Server Signing.

eIDAS nevyplývá, že by oznámení členským státem Komisi nebo zveřejnění Komisí mělo nějaký zvláštní přídavný právní účinek ke statusu QSCD.

Mezery existující v čl. 30 a čl. 31 eIDAS by zřejmě mohly být předmětem vnitrostátní implementace, jako kombinace doplnění a provedení.

Prakticky Komise nyní vydává[159] orientační seznam, který shrnuje po jednotlivých členských státech jednak určenou zkušebnu(y), jednak QSCD nahlášená daným členským státem. Komise seznam prohlašuje za ryze orientační a výslovně za jeho obsah odmítá jakoukoli odpovědnost, včetně odpovědnosti za škodu.[160] Z hlediska čl. 30 odst. 2 eIDAS je zveřejnění zkušeben Komisí krokem navíc, neboť povinnost je tyto pouze oznámit členským státům. Zveřejnění přikazuje nařízení eIDAS výslovně pouze v případě nahlášených QSCD. Zveřejnění i zkušeben je však důvodné, neboť bez veřejné znalosti o tom, které zkušebny jsou členskými státy určené, je obtížné v jiných členských státech hodnotit, zda certifikát skutečně pochází od státem určené zkušebny.

Právní status prohlášení o shodě (certifikaci QSCD) bude třeba hodnotit podle práva členského státu, kterým se daná zkušebna během provádění certikace řídí. Běžně to bude zřejmě právo toho státu, který danou zkušebnu určil.

Je zjevné, že pro běžného žadatele o kvalifikovaný certifikát není příliš schůdné pořizovat si QSCD a ověřovat si přímo i stav jeho certifikace, jak byl proveden podle čl. 30 eIDAS. Ověřování na základě seznamu, který zveřejňuje Komise, je orientační. Praktický způsob ověření, že určitý prostředek splňuje požadavky na QSCD, nařízení eIDAS běžné fyzické osobě tedy neposkytuje. Pro žadatele o kvalifikovaný certifikát je nejjednodušší se spolehnout, že potřebné QSCD mu dodá kvalifikovaný poskytovatel služeb vytvářejících důvěru, který vydává kvalifikované certifikáty pro elektronický podpis. O jeho totožnosti se snadno přesvědčí v důvěryhodném seznamu.

Není jasné, proč Komise neurčila technické normy podle čl. 29 odst. 2 eIDAS, ačkoli by se k tomu technické normy EN 419 211Chyba: zdroj odkazu nenalezen z prováděcího rozhodnutí (EU) 2016/650 hodily. Může se jednat o chybu, může se jednat o snahu určit všechny technické normy najednou, aby některý druh QSCD nebyl právně zvýhodňován, může se též jednat o důsledek toho, že Komise dosud nepřijala akt v přenesené působnosti podle čl. 30 odst. 4 eIDAS. Poslední případ by znamenal, že si

[159] Dostupné z: <https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds>.

[160] *„The European Commission maintains this list only as an informative tool... the Commission accepts no responsibility or liability whatsoever with regard to the content or completeness of the list.“*

Komise nemusí být jista, že členské státy určily zkušebny zodpovědně a že jimi provedené prohlášení o shodě lze vedle režimu certifikace dle čl. 30 eIDAS použít i pro účel čl. 29 odst. 2 eIDAS.

6.10.4 Uznávání historických SSCD za QSCD

Podle čl. 51 (Přechodná opatření) odst. 1 eIDAS *„Prostředky pro bezpečné vytváření podpisu, jejichž shoda byla stanovena podle čl. 3 odst. 4 směrnice 1999/93/ES, se považují za kvalifikované prostředky pro vytváření elektronických podpisů podle tohoto nařízení."* Odvolávka na čl. 3 odst. 4 DirES, a nikoli na čl. 3 odst. 5 DirES,[161] znamená, že za QSCD se považují SSCD na základě kritéria, že subjekt určený členským státem (zkušebna) stanovil shodu prostředku s požadavky na SSCD v příloze III DirES a postupoval přitom v souladu s národní transpozicí DirES.

Hodnocení prováděná podle národních transpozic mohla mít vzájemně různou kvalitu úrovně zajištění kontroly shody s požadavky přílohy III. Ačkoli si státy měly status SSCD vzájemně uznávat, v praxi tomu tak vždy zřejmě nebylo.

6.10.5 Uznávání certifikace QSCD z přeshraniční zkušebny

Nařízení eIDAS se vyhýbá zodpovězení otázky, zda se má přeshraničně uznávat certifikace QSCD zkušebnou určenou jiným členským státem. Toto opomenutí je přinejmenším zvláštní, neboť příkaz uznávání byl součástí dřívější DirES v čl. 3 odst 4: *„Rozhodnutí subjektů [určených zkušeben] vedených v prvním pododstavci o shodě s požadavky uvedenými v příloze III bude uznáno všemi členskými státy."*

V čl. 4 eIDAS jsou stanovena pravidla pro uplatnění zásad vnitřního trhu. Podle čl. 4 odst. 2 eIDAS *„Produkty a služby vytvářející důvěru, které vyhovují tomuto nařízení, se mohou volně pohybovat na vnitřním trhu."* Potíž je, že pojmem produkt se podle čl. 3 bod 21 eIDAS rozumí *„technické zařízení nebo programové vybavení či jejich příslušné součásti, které jsou určeny k používání pro poskytování služeb vytvářejících důvěru"*. Tomu odpovídá i použití pojmu produkt v čl. 24 odst. 2 písm. e) eIDAS, tj. jedná se o hardwarové zařízení nebo softwarové vybavení používané samotným poskytovatelem služeb, nikoli podepisující osobou. Podle anglického znění *„... are **intended to be used** for the provision of trust services"* (zvýraznil autor) by pro překlad přicházel do úvahy i obrat „... myšlen pro užití v rámci poskytování služeb pro

[161] V okamžiku účinnosti relevantní části eIDAS od července 2016 by stejně nemělo smysl brát ohled na jedinou vyhlášenou a zastaralou technickou specifikaci s datací z roku 2002.

vytváření důvěry", který by hypoteticky QSCD zahrnoval. Zatímco jazykové znění vede spíš na první význam, tj. prostředek poskytovatele, z hlediska účelu vnitřního trhu jazykový výklad tolik smysl nedává a bylo by logičtější zajistit volný pohyb i pro QSCD. Příležitostně nařízení eIDAS používá pojem *produkt* zřejmě i v jiném smyslu. Například podle čl. 15 by měly být služby vytvářející důvěru *„a konečné uživatelské produkty používané při poskytování těchto služeb dostupné osobám se zdravotním postižením"*.

Nařízení eIDAS ovšem obsahuje ustanovení o přeshraničním uznávání QES. Podle čl. 25 odst. 3 eIDAS: *„Kvalifikovaný elektronický podpis založený na kvalifikovaném certifikátu vydaném v jednom členském státě se uznává jako kvalifikovaný elektronický podpis ve všech ostatních členských státech."*

Jelikož ustanovení nezmiňuje QSCD ani způsob jeho certifikace, tyto okolnosti je třeba považovat z hlediska uznání za podružné. Použití QSCD přitom je samozřejmou náležitostí existence kvalifikovaného elektronického podpisu (QES) v hypotéze i dispozici této právní normy. Z argumentu *a maiori ad minus*, popř. stejně i výkladem užitečného účinku, lze dovodit, že uznává-li se kvalifikovaný elektronický podpis, tím spíše se musí uznat QSCD, se kterým byl daný QES vytvořen.

Přesto uvedený argument nemusí znamenat všeobecné uznávání certifikace QSCD, ale pouze to, že přijímající subjekt (obecně je k přijímání a potažmo uznávání zavázán pouze subjekt veřejného sektoru, srov. 6.14.2) uznává QES a QSCD protější strany, a to i přeshraničně. Pro své vlastní použití stále zbývá prostor pro tvrzení, že certifikaci QSCD od zkušebny určené jiným členským státem neuznává. Jinak řečeno, ačkoli subjekt veřejného sektoru je přes QES povinen uznat použití QSCD subjektem z jiného členského státu, pro vytváření svých vlastních kvalifikovaných elektronických podpisů se může chtít spolehnout pouze na QSCD certifikované zkušebnou z vlastního členského státu a uznat pouze takové certifikace QSCD. Takový výklad je racionální z hlediska zájmů členského státu, který pro své vlastní subjekty veřejného sektoru chce použít velmi vysoký stupeň ochrany, tj. takové technologie, které byly ověřeny určenou zkušebnou v jeho vlastní sféře veřejné moci. Současně takový vyspělý členský stát nechce bránit, nebo dokonce nemá zájem bránit, aby jiné členské státy uznávaly certifikace QSCD z jiných členských států, protože tím může podporovat i své vlastní výrobce a vlastní zkušebny.

Neurčení právního významu certifikace dokonce zcela nevylučuje možnost, aby členský stát a jeho subjekty veřejného sektoru postupovaly diskriminačně uvnitř svého členského státu, tj. aby uznávaly certifikaci QSCD pouze z některé určené zkušebny.

Tato právní situace by se pravděpodobně změnila ve prospěch přeshraničního uznávání certifikace QSCD, pokud by Komise určila technické normy podle čl. 29 odst. 2 eIDAS a určená zkušebna tuto shodu certifikovala. Nicméně i pak by se mohlo vyskytnout tvrzení o neuznání přeshraniční certifikace a potažmo i o neuplatnění domněnky vyhovění podle čl. 29 odst. 2 eIDAS.

Ve prospěch toho, že se certifikace QSCD mají uznávat přeshraničně, působí přechodné opatření o uznávání SSCD za QSCD (srov. 6.10.4), které nařízení stanoví bez ohledu na to, ve kterém členském státu k ověření shody SSCD došlo.

Faktický stav je takový, že k říjnu 2017 určilo zkušebny podle nařízení eIDAS z 28 členských států pouze 6 států (Rakousko, Německo, Španělsko, Francie, Itálie a Slovensko), z čehož pouze Německo určilo více než 1 zkušebnu, konkrétně 5 zkušeben.Chyba: zdroj odkazu nenalezen Z uvedeného plyne, že mají-li subjekty z 22 ostatních členských států vytvářet kvalifikované elektronické podpisy, musí kvalifikovaní poskytovatelé, subjekty veřejného sektoru i podepisující osoby uznávat i pro své vlastní užití certifikace QSCD z jiných členských států.

Celkově lze shrnout, že jsou myslitelné a právně odůvodnitelné obě možné odpovědi, přinejmenším co se týká opatření QSCD pro své subjekty veřejného sektoru. Současně je patrné, že koncept aspoň jedné vlastní určené zkušebny každým členským státem je technologicky v současné EU nerealizovatelný. Státy, na jejichž území nejsou aktivní výrobci pokročilých technologií bezpečnosti informačních technologií, nemají ekonomický zájem a dost často ani možnosti, aby zkušebny vytvořily a poté určily.

Možnost uplatnění domněnky vyhovění podle čl. 29 odst. 2 eIDAS by působila ve prospěch obecného přeshraničního uznávání certifikace QSCD. Je možné, že o otázce rozhodne praktický přístup subjektů veřejného sektoru, a nikoli právní výklad.

6.10.6 Kdo odpovídá za to, že prostředek je QSCD?

Dle výše uvedeného výkladu zatím Komise neurčila technické normy dle čl. 29 odst. 2 eIDAS, na jejichž základě by platila domněnka vyhovění, že prostředek je QSCD. Jediné způsoby, jak nezávisle stanovit, že prostředek je QSCD, jsou certifikace

podle čl. 30 eIDAS anebo certifikace SSCD podle čl. 51 eIDAS (oboje viz výše). Povinnost certifikací však jednoznačně uložena není, takže zcela vyloučit nelze ani přímé prohlášení výrobce, že prostředek je QSCD, na základě přímého vyhovění právním požadavkům podle čl. 29 odst. 1 eIDAS.

Podepisující osoba téměř bezvýjimečně není schopna sama ověřit, zda prostředek je QSCD. Může se tedy spolehnout buď na prohlášení výrobce, anebo na certifikát zkušebny. Ani jedna z možností však dnes neposkytuje domněnku vyhovění, jiné možnosti však zřejmě dnes neexistují. Pro možnost vytvoření kvalifikovaného elektronického podpisu však bude potřebovat připojit též kvalifikovaný certifikát (pro elektronický podpis), který obsahuje příznak o používání QSCD. Aby jí takový certifikát byl vystaven, musí zřejmě kvalifikovaný poskytovatel služeb důvěřovat tomu, že podepisující osoba používá a bude používat QSCD.

Zde se naskýtá otázka, zda kvalifikovaný poskytovatel služeb bude vydávat své kvalifikované certifikáty výlučně na sebou samým dodávaná QSCD, u nichž typicky má od dodavatele nebo výrobce předem doložen certifikát zkušebny,[162] anebo zda ji může vydat i na prostředek fyzicky přinesený žadatelem o kvalifikovaný certifikát (budoucí podepisující osobou), o němž žadatel buď jen tvrdí, anebo dokládá certifikátem zkušebny, že se jedná o QSCD. Autor je zde názoru, že pouhé tvrzení žadatele nestačí, neboť obsah údajů kvalifikovaného certifikátu je zásadně poskytovatelem ověřován.

Pro poskytovatele pak bude typicky obchodně mnohem výhodnější vydávat kvalifikované certifikáty pouze na QSCD poskytovaná sebou samým, přinejmenším kvůli ekonomickým úsporám z rozsahu. Může mít lépe automatizované technické aj. procesy, mít faktickou jistotu, že prostředek nebyl zaměněn na cestě od výrobce k uživateli i mít získán certifikát zkušebny důvěryhodným způsobem. Přesto mohou existovat aplikace a případy užití, kdy by žadatel o certifikát potřeboval použít prostředek jiný, protože má odlišné technické vlastnosti, nutné pro jeho případ užití. Nařízení eIDAS neukládá poskytovateli, aby požadavky takových žadatelů uspokojoval, ale ani vyhovění nevylučuje.

Další úrovní v řetězci je orgán dohledu, který rozhoduje o statusu kvalifikovanosti služby vydávání kvalifikovaných certifikátů pro elektronické podpisy. Má orgán dohledu ověřovat, pro jaké přesně prostředky kvalifikovaný poskytovatel služeb vydává své kvalifikované certifikáty? Má vyžadovat takové doložení předem,

[162] Zcela vyloučeno ale není ani jen prohlášení renomovaného výrobce podle čl. 29 odst. 1 eIDAS.

například podle čl. 21 odst. 1 eIDAS? Má mu dostačovat následné oznamování? Anebo mu má stačit obecné ověření, že poskytovatel kvalifikovaných služeb má hodnověrný postup, kterým vždy ověří, že použitý prostředek je QSCD? Nařízení eIDAS na tyto otázky neposkytuje jednoznačnou odpověď.

Orgán dohledu může postupovat defenzivně, tj. požadovat oznamování předem a vydávání prostředku poskytovatelem umožnit až po svém povolení určitého prostředku v rámci dané služby kvalifikovaného poskytovatele, např. s ohledem na čl. 22 odst. 1 eIDAS, že za poskytovatele a jejich služby, které jsou uvedeny v důvěryhodném seznamu, členský stát odpovídá. Takový požadavek lze podpořit i tím, že vedle činností kvalifikovaného poskytovatele je to právě QSCD a jeho vlastnosti, které jsou rozhodující pro splnění požadavků na kvalifikovaný elektronický podpis. Proti tomu lze však namítnout, že takový postup velmi zpomalí nasazování QSCD na trh; je velmi byrokratický. Jestliže členský stát o nasazování určitého QSCD aktivně rozhoduje, lze mu i spíše připsat odpovědnost za to, že byl povolen správný QSCD. Tomuto přístupu neodpovídá ani určitá ortogonalita požadavků na QSCD s požadavky na činnost kvalifikovaného poskytovatele služeb. Tyto jsou v rámci nařízení eIDAS vyjadřovány na sobě nezávisle. Pokud by se měl používat defenzivní přístup, mělo být nařízení napsáno strukturně odlišně a vydávání QSCD jednoznačně podřazeno do služby vydávání kvalifikovaných certifikátů pro elektronický podpis.

Subjektem, pro který je status QSCD finálně důležitý, je spoléhající se osoba. Tato osoba se spoléhá na to, že se jedná o kvalifikovaný elektronický podpis, jehož platnost navíc může ověřit postupem podle čl. 32 eIDAS. V rámci ověření platnosti se spoléhá jednak na obsah kvalifikovaného certifikátu vydaného kvalifikovaným poskytovatelem služeb, jednak na zápis kvalifikovaného poskytovatele a jeho kvalifikované služby v důvěryhodném seznamu, za nějž odpovídá členský stát.

Jestliže by přesto podepisující osoba následně prokázala, že při podpisu nebyl použit QSCD, měla by spoléhající osoba mít právem jednoznačně určeno, vůči komu se může domáhat aspoň náhrady škody. Takové určení nařízení eIDAS postrádá. Explicitně je zmíněna odpovědnost poskytovatele služeb podle čl. 13 odst. 1 eIDAS za *„nesplnění povinností podle tohoto nařízení"*. Mezi tyto povinnosti náleží obecně podle čl. 19 odst. 1 eIDAS přijmout vhodná technická a organizační *„opatření k řízení rizik ohrožujících bezpečnost jimi poskytovaných služeb vytvářejících důvěru"*. Mezi ně teleologicky náleží i zajištění ověření správnosti údajů ve vydávaných certifikátech,

v určité míře zajištění této správnosti. Podle čl. 24 odst. 1 eIDAS kvalifikovaní poskytovatelé *„**ověří** ... pomocí vhodných prostředků a v souladu s vnitrostátním právem totožnost a případně **zvláštní znaky fyzické** nebo právnické **osoby**, jíž je kvalifikovaný certifikát vydáván"* (zvýraznil autor).

Dle výkladu užitečného účinku se zdá zřejmé, že by nemělo smysl, aby kvalifikovaný poskytovatel ověřoval jedny údaje, které jsou povinnou součástí kvalifikovaného certifikátu pro elektronický podpis (příloha I eIDAS), zatímco jiné by jím ověřovány nebyly vůbec. Je otevřenou otázkou, zda příznak obsažení dat pro vytváření elektronického podpisu v QSCD [příloha I písm. j) eIDAS] spadá pod *„zvláštní znak fyzické osoby"*. Kladná odpověď by umožnila použít vnitrostátní právo pro implementaci eIDAS ohledně ověřování tohoto příznaku. Proti tomu lze argumentovat částečně tím, že nařízení eIDAS obsahuje v článcích 29 až 31 vlastní úpravu o QSCD. Jejich podrobný výklad zde provedený vede k závěru, že způsob ověření příznaku poskytovatelem v eIDAS ani v těchto článcích stanoven není. To by opět umožnilo doplnit nařízení eIDAS vnitrostátní implementací, ať již v rámci čl. 24 odst. 1 eIDAS, nebo obecně vůči celému nařízení.

Vzhledem k výše uvedenému autor je obecně názoru, že kvalifikovaný poskytovatel příznak QSCD ověřovat musí, tj. v žádném případě pro uvedení příznaku nestačí pouze tvrzení žadatele o certifikát, že používá QSCD. Autor se domnívá, že vnitrostátní úprava může obsahovat implementaci způsobu ověřování příznaku QSCD kvalifikovaným poskytovatelem a popř. i orgánem dohledu, neboť nařízení eIDAS lze v této oblasti doplnit.

Chybí-li taková vnitrostátní implementace, pak by podle autora kvalifikovaný poskytovatel měl být oprávněn příznak uvést tehdy, má-li k dispozici certifikát zkušebny, který na základě čl. 29 odst. 2 eIDAS zakládá domněnku vyhovění, a neměl by pak potřebovat předběžný souhlas orgánu dohledu.

Jestliže nejsou určeny technické normy, které zakládají domněnku vyhovění, pak by dle názoru autora poskytovatel měl mít k dispozici certifikát určené zkušebny vystavený dle čl. 30 eIDAS a současně si být přiměřeně jist, že způsob nasazení prostředku je takový, že bude i během používání stav QSCD udržen. Důvodem je zde autorovi to, že smyslem kvalifikovaných služeb, jak jsou vyjádřeny v eIDAS, je mít v rámci všech jejich použitých prvků systém čtyř očí, které pochází od navzájem

nezávislých subjektů. Důvodem je i akcent čl. 30 eIDAS na certifikaci, přičemž certifikační metody zahrnují i variantu pro případ inovativních řešení. Z toho autor soudí, že by použití článku 30 odst. 3 písm. b) eIDAS mělo mít pro inovativní řešení přednost před použitím článku 29 odst. 1 eIDAS v rámci *New Approach*.

Ze stejného důvodu se autor domnívá, že uvést příznak QSCD do kvalifikovaného certifikátu, který by byl opřen pouze o potvrzení výrobce, že se jedná o QSCD, by kvalifikovaný poskytovatel měl mít možnost pouze tehdy, jestliže tuto skutečnost dá jednoznačně najevo spoléhající se osobě. Takovou možnost by představovalo například vyjádření omezení využívání podle čl. 13 odst. 2 eIDAS. Bez poskytnutí takové informace by se jinak odpovědnost kvalifikovaného poskytovatele podle čl. 13 eIDAS vytratila. Docházelo by k absurdnímu rozdílu úrovně zajištění příznaku QSCD mezi poskytovateli navzájem a ztrácela by se motivace k provádění certifikací podle čl. 30 eIDAS vůbec. Dle názoru autora musí být tato informace ale strojově zjistitelná buď z kvalifikovaného certifikátu, nebo z důvěryhodných seznamů, nebo z jejich kombinace.[163] Důvodem je, že čl. 32 eIDAS o ověřování platnosti pracuje zřejmě výhradně s automatizovatelně získatelným informacemi.

Uvedené však nevylučuje, aby se některé strany, které sice využívají služby některého poskytovatele, mezi sebou navzájem dohodly, že podepisující osoba bude používat určitý konkrétní prostředek, k němuž existuje pouze potvrzení výrobce, že splňuje právní požadavky na QSCD, budou obě smluvní strany ve svých vztazích navzájem uznávat za QSCD. Od poskytovatele služeb mohou pak používat pouze kvalifikované certifikáty bez příznaku QSCD. V případě laické strany, která by takové ujednání přijala, však hodnota takového uznání nemusí být vysoká, nelze vyloučit zpětné zpochybnění uznání.

Chybí-li vnitrostátní implementace nařízení v oblasti ověřování QSCD, pak orgán dohledu zřejmě může používat kteroukoli výše zmíněnou metodu dohledu s ohledem na uvedení příznaku QSCD v kvalifikovaném certifikátu kvalifikovaným poskytovatelem služeb. Mezi povinnosti orgánu dohledu spadá podle čl. 17 odst. 3 písm. a) eIDAS *„**vykonávat dohled** nad kvalifikovanými poskytovateli služeb ..., aby prostřednictvím činností **předběžného** a **následného** dohledu **splňovali požadavky** stanovené v tomto nařízení"* (zvýraznil autor). Orgán dohledu tedy neručí bezprostředně

[163] Autor se domnívá, že technické normy obsah této informace k současnosti neumožňují spolehlivě vyjádřit a že tato možnost tedy zatím nepřipadá do úvahy.

za to, že kvalifikovaní poskytovatelé v každém jednotlivém případě splní požadavky na ně kladené, ale může odpovídat za to, že je řádně vykonáván předběžný i následný dohled. Požadavek platí jak takto obecně, tak i podle dílčích upřesnění v eIDAS.

6.11 Ověřování platnosti elektronického podpisu (pečetě)

V oblasti ověřování platnosti elektronického podpisu panuje v nařízení eIDAS značně nepřehledná pojmová situace. Bez znalosti technologických možností faktické implementace, tj. techologiemi PKI, je čistě pro právníka v podstatě nemožné nařízení eIDAS vyložit.

6.11.1 Výklad terminologie

Jak je patrné z definice elektronického podpisu prostého (čl. 3 bod 10 eIdAS), jsou elektronický podpis první „data v elektronické podobě“, která jsou připojena nebo logicky spojena s druhými „daty v elektronické podobě“. První data se i v eIDAS nazývají *elektronický podpis*, druhá můžeme pracovně zvát *podepsaná data*. V rámci podmínek na zaručený elektronický podpis konkrétně požadavek podle čl. 26 písm. d) eIDAS na zajištění integrity podepsaných dat v sobě skrývá i požadavek, který jsme v rámci obecného rozboru funkcí vlastnoručního podpisu označovali jako autentizační funkci (srov. 4.2). Elektronický podpis autentizuje podepsaná data. Další požadavky v čl. 26 písm. a) až c) eIDAS umožňují k elektronickému podpisu nalézt fyzickou osobu, která jej vytvořila. Požadavky na kvalifikovaný elektronický podpis jsou pouze konkrétnějším a více kontrolovaným provedením těchto požadavků na zaručený elektronický podpis.

6.11.1.1 Exkurz do terminologie a postupů PKI

Asi jedinou technologií, která je schopná splňovat požadavky na zaručený elektronický podpis, je kryptografie veřejného klíče, typicky v rámci infrastruktury veřejného klíče (PKI). Technologie PKI hovoří vlastním jazykem, používá pojmy *soukromý klíč* a *veřejný klíč* podepisující osoby. Oba klíče bývají například velmi vysoká přirozená čísla (např. s vyššími jednotkami stovek desetinných míst) a navzájem se doplňují. Ze znalosti veřejného klíče je matematicky neschůdné odvodit soukromý klíč, a to i při použití nejmodernější výpočetní techniky. Tyto dva klíče tedy spolu tvoří pár (dvojici) a současně jsou oba přiřazeny právě k jedné podepisující osobě.

Soukromý klíč je udržován v tajnosti a je ve výhradní dispozici podepisující osoby. Elektronický podpis se v rámci činnosti vytvoření elektronického podpisu získá kryptologickou operací, jejímiž vstupy jsou soukromý klíč a podepisovaná data. Poté jsou podepsaná data a elektronický podpis odeslány či jinak zpřístupněny jiné osobě. Současně bude taková osoba mít k dispozici i nějakým způsobem získaný veřejný klíč podepisující osoby. Tuto jinou osobu zde nazýváme spoléhající se osobou.

Jestliže se jakákoli spoléhající se osoba má přesvědčit, že elektronický podpis (nějaká data) jsou skutečně zaručeným elektronickým podpisem, pak v rámci technologie PKI se v zásadě provádějí 2 postupné kroky.

V prvním kroku se provede doplňková kryptologická operace, jejímiž vstupy jsou veřejný klíč, podepsaná data a elektronický podpis. Výsledek této operace je binární. Buď se potvrdí, že elektronický podpis je podpisem podepsaných dat, anebo není.

Druhým krokem bývá zjišťování, zda použitý veřejný klíč skutečně náleží k nějaké konkrétní fyzické osobě. To se v PKI děje za pomocí certifikátu, který již předem vystavil poskytovatel služeb, v terminologii PKI označovaný za certifikační autoritu. Veřejný klíč je uložen uvnitř certifikátu a současně jsou v tomtéž certifikátu uloženy určité osobní údaje o podepisující osobě. V rámci druhého kroku se proto zejména zkoumá obsah tohoto certifikátu, zjišťuje se jeho vydavatel (poskytovatel služeb), zda je certifikát platný z hlediska doby své platnosti (bývá vystaven na nějakou dobu od–do), a též se ověřuje, zda certifikát nebyl zneplatněn. Zneplatnění se může stát například na žádost podepisující osoby. Protože samotný certifikát bývá elektronicky podepsán od vydavatele certifikátu, musí se zjistit, zda i tento elektronický podpis je podpisem vydavatele. Tj. i pro tento podpis se musí provést kroky jedna a dvě. Skutečně může být třeba ověřit někdy i více certifikátů, ty se pak označují jako tzv. certifikační cesta. Zde se zdá, že by se kroky 1 a 2 mohly opakovat do nekonečna. Naštěstí tomu tak v metodologii PKI není. V určité iteraci těchto dvou kroků se proces zastaví, protože se narazí na certifikát, jemuž podepisující osoba důvěřuje ohledně toho, jaký vydavatel jej vydal i v něm zapsaný veřejný klíč považuje za pravý. Pokud se k takovému certifikátu nedojde, i pak se postup zastaví, ale s tím, že druhý krok je třeba považovat za neprovedený, všechny údaje o podepisující osobě je pak typicky třeba považovat za pouze tvrzené, ale žádným spolehlivým vydavatelem certifikátu nepotvrzené. Postup provedení celého druhého kroku může být značně složitý, neboť může docházet

k různým potížím platnosti certifikátů po certifikační cestě, popř. mohou obsahovat některé nevhodné technické parametry apod.

Zatím se zde autor důsledně vyhýbal použití obratu „ověření platnosti“, ať již elektronického podpisu, certifikátu, nebo čehokoli jiného. Pojmovou potíží techniky PKI zde je, že finálním účelem je vždy „ověření platnosti“ elektronického podpisu, tedy provedení obou výše uvedených kroků. Přesto řada autorů, ať již v rámci odborných textů PKI, nebo textů právních, bude promiscue hovořit o „ověření platnosti“ elektronického podpisu pouze v rámci prvního kroku. V rámci druhého kroku se hovoří o různých „ověřeních platnosti“ jednotlivých certifikátů, aniž by bylo vždy nutně zřejmé, zda je aspoň celý krok dokončen. Současně jen v rámci techniky PKI mají výsledky postupů „ověření platnosti“ vždy jen pouze technický význam. Právní význam výsledku závisí až na právu samém.

Nejdůkladněji kroky 1 a 2 odlišoval německý zákonodárce, např. v § 2 bod 11 SigG. V kontextu prvního kroku používal pojem ověřit *(prüfen)* a v kontextu druhého kroku pojem prověřit *(nachzuprüfen)* příslušný kvalifikovaný certifikát podepisující osoby. Tím bylo z právního textu vždy jasno, o který krok a jakou činnost se zhruba jedná. Současně byly v němčině tyto termíny jasně odděleny od právních pojmů, jako je platnost *(Gültigkeit)* nebo účinnost *(Wirksamkeit)*.

V angličtině se s různými významy a kontexty používají zejména slovesa *to verify* a *to validate* nebo jejich odvozeniny

V češtině prakticky vždy hovoříme o platnosti (podpisu, certifikátu ...) nebo o ověřování platnosti a situace bývá asi nejméně přehledná vůbec.

6.11.1.2 Terminologie eIDAS

Návrh nařízení eIDAS vznikal v angličtině. Autoři použili na různých místech pojmy a obraty: *verification*, *validation*, *validation data*, *confirming that is ... valid*, *confirm the validity*. Do češtiny si překladatelé různě vypomohli zejména se slovy ověřování a platnost. Význam pojmů v nařízení eIDAS však není jednoduše odvoditelný ani v angličtině. Níže proto autor provádí systematický výklad pojmů spojených s ověřováním platnosti elektronického podpisu podle nařízení eIDAS. Ačkoli sám vycházel z právního textu, jen se zpětným ohledem na technologie PKI, výklad se snaží vést co nejjednodušeji.

Předně je třeba nalézt právní pojmy pro soukromý a veřejný klíč. Tak soukromým klíčem jsou „data pro vytváření elektronických podpisů“ (čl. 3 bod 13) nebo „data pro vytváření elektronických pečetí“ (čl. 3 bod 28). Pro veřejný klíč však nařízení používá **„data pro ověřování platnosti“** *(validation data)* (čl. 3 bod 40), kterými jsou *„data, která se používají k ověření platnosti elektronického podpisu nebo elektronické pečeti“*. Jelikož článek 32 eIDAS je nadepsán jako *Požadavky na ověřování platnosti kvalifikovaných elektronických podpisů*, přičemž se zabývá výše uvedenými kroky jedna i dvě z PKI, mohlo by se zdát, že daty pro ověřování platnosti mohou být míněna všechna data, která jsou k ověření kvalifikovaného elektronického podpisu potřebná, tedy například i certifikáty a mnohé jiné informace výše uvedené jako potřebné pro krok 2. Není tomu tak. Uvedené plyne například z čl. 3 bod 14 eIDAS, podle nějž certifikát pro elektronický podpis spojuje data pro ověřování platnosti (pro elektronický podpis) s určitou fyzickou osobou. Ještě explicitnější je písm. d) v příloze I eIDAS, podle nějž součástí kvalifikovaného certifikátu pro elektronický podpis musí být: *„data pro ověřování platnosti elektronických podpisů, která odpovídají datům pro vytváření elektronických podpisů“*. Obě ustanovení nelze vyložit jinak, než že daty pro ověřování platnosti je míněn pouze veřejný klíč.[164]

Další značná nejasnost vzniká z taxativní definice v čl. 3 bod 16 eIDAS, podle nějž služba vytvářející důvěru spočívá:

> *„a) ve vytváření, **ověřování shody [verification]** a **ověřování platnosti [validation]** elektronických podpisů, elektronických pečetí nebo elektronických časových razítek, služeb elektronického doporučeného doručování a certifikátů souvisejících s těmito službami nebo*
>
> *b) ve vytváření, **ověřování shody [verification]** a **ověřování platnosti [validation]** certifikátů pro autentizaci internetových stránek nebo ...“* (zvýraznil a doplnil autor).

Otázka zní, v čem spočívá ***ověřování shody*** a v čem ***ověřování platnosti***, v čem se liší, jaký je jejich vzájemný vztah. Jak je vyvozeno níže, bohužel či naštěstí neplatí, že by jeden termín souvisel s prvním krokem a druhý s druhým krokem v PKI. Z citace plyne, že je možné ověřovat shodu i ověřovat platnost jak elektronického podpisu (písm. a), tak ale certifikátu [podle písm. b, ale zřejmě též i podle písm. a)].

Článek 32 eIDAS (Požadavky na ověřování platnosti QES) v první větě uvádí: *„Postup ověření platnosti*[165] *[for validation] kvalifikovaného elektronického podpisu*

[164] Obdobně pro elektronické pečetě v čl. 3 bod 29 eIDAS a příloha III písm. d) eIDAS.

[165] *Ověření platnosti* je zde uvedeno jen jako mluvnicky čistší varianta od *ověřování platnosti*, je třeba je vykládat jako shodný obrat, v angličtině je pro oba případy použito *validation*.

potvrdí platnost [shall confirm the validity] kvalifikovaného elektronického podpisu, pokud: ..." (anglické znění přidal autor).

Podle čl. 3 bod 41 eIDAS se **ověřováním platnosti** (validation) definičně míní *„postup ověřující shodu [verifying] a potvrzující [confirming] platnost elektronického podpisu nebo elektronické pečeti"* (anglické znění přidal autor).

Po dosazení definice získáme v češtině i angličtině nesmyslný text, dle nějž se v čl. 32 bude jednat o postup postupu. Rovněž se zdá, že by mohlo dojít k vyjádřením tautologií. Zde se nařízení eIDAS poněkud zákonodárci vymklo ze sémantiky jazyka a musíme připustit určitou jazykovou toleranci při výkladu. Předně z obou citovaných ustanovení, nadpisu čl. 32, znění čl. 32 i znění čl. 33 eIDAS plyne, že ověřování platnosti je zde považováno za souhrnné ověření platnosti elektronického podpisu, tedy souhrn kroků jedna a dva z PKI. Podle definice v čl. 3 bodu 41 navíc zahrnuje potvrzení platnosti.

Ustanovení v čl. 3 bod 41 eIDAS je pak jediné, kde jsou pojmy ověřování shody a ověřování platnosti dávány do vzájemné relace. Jestliže nad ověřováním platnosti již není ověřovat co, pak ověřování shody se může týkat jen dílčích kritérií pro ověřování platnosti. Taková dílčí kritéria jsou uvedena v například čl. 32 odst. 1 písm. a) až h) eIDAS. Autor se tedy domnívá, že pod pojmem **ověřování shody** *(verification)* je třeba mínit kontroly dílčích kritérií **ověřování platnosti** *(validation)*. V případě kvalifikovaného elektronického podpisu jsou pak jednotlivá dílčí kritéria zmíněna v čl. 32 odst. 1 písm. a) až h) eIDAS.[166] V případech jiných elektronických podpisů je případně možné pouze je odvodit z normativních požadavků (podmínek).

6.11.1.3 Ověřovací modely digitálního podpisu

Podle německé nauky existují tři základní modely ověřování digitálních podpisů. Jsou popsány například v glosáři[167] k pojmu *elektronický podpis* německého úřadu BSI.

Za základní je považován **řetězový model** *(Kettenmodell)*. Vyžaduje, aby v řetězci podpisu podepisující osoby a potom jejího certifikátu a všech dalších certifikátů v certifikační cestě bylo splněno, že k času vytvoření podpisů jsou (nebo byly) platné jejich příslušné certifikáty. Na případné pozdější zneplatnění certifikátu se

[166] Je přiměřeně použitelný i pro kvalifikované elektronické pečeti podle čl. 40 eIDAS.

[167] Dostupné z: <https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/ElektronischeSignatur/Glossar/esigglossar.html>; navštíveno 10/2017.

nebere zřetel. Model předpokládá, že čas vytvoření každého podpisu v certifikačním řetězci lze přesně určit a že se lze spoléhat i na dřívější podpisy v certifikačním řetězci, jejichž certifikáty již expirovaly nebo byly zneplatněny, pokud samotné podpisy byly vytvořeny za doby platnosti. Navzdory složitosti se jedná o model, který byl například uplatňován v německém SigG pro kvalifikované elektronické podpisy.

Druhý typový je **ulitový model** *(Schalenmodell)*. Ten vyžaduje, aby k okamžiku ověřování podpisu podepisující osoby bylo splněno, že její certifikát i všechny další certifikáty v certifikační cestě jsou platné. Tento ověřovací model je defenzivní z hlediska jistoty spoléhající se osoby a je technicky nejjednodušší na ověření. Má-li však být výsledek ověření zachován pro budoucnost, například pro důkazní použití, musí být stejně opatřen časovým razítkem a následně být platnost všech certifikátů zkoumána zpětně k danému času. Ověřovací prostředky pak stejně musí být schopny pracovat s uvážením jiného času, než je ten právě aktuální. Název modelu je zřejmě odvozený od toho, že přijímající osoba je jakoby ve své ulitě a příliš ji nezajímá, co se kdy dělo předtím, než k ní podpis dorazil.

Třetí je **hybridní model** *(Hybridmodell)*. Hybridní model je v zásadě shodný jako ulitový model, až na to, že platnost všech certifikátů (podepisující osoby i autorit v certifikační cestě) je požadována k času vytvoření podpisu podepisující osoby. Tento model je nejjednodušší z hlediska jistoty osoby, která podpis vytváří. Její prostředky vytvářející podpis by měly být schopny dané podmínky ověřit a tím i samotnou podepisující osobu ubezpečit o tom, že její podpis je a bude platný. Chce-li předejít možnému zpochybnění, může podpis opatřit časovým razítkem, aby bylo zřejmé, ke kdy nejpozději se má platnost podpisu ověřovat.

6.11.2 Ověřování platnosti podle čl. 32 odst. 1 eIDAS

Vzhledem k tomu, že dosud Komise nevydala prováděcí akt podle čl. 32 odst. 3 eIDAS, je nejen možné, ale i nutné provádět ověřování platnosti přímo vůči právním kritériím v čl. 32 odst. 1 písm. a) až h) eIDAS. Autor níže vykládá, v čem kontrola kritérií spočívá, resp. v čem může spočívat z hlediska co nejjednoduššího a automatizovaného provedení. Autor přitom netvrdí, že uvedené možnosti jsou jediné možné, ale jsou to ty, které jsou poměrně snadno nalezitelné za současné právní a technické praxe. Nelze vyloučit ani to, že výrobci či vývojáři systémů použitých k ověření platnosti budou používat nebo naleznou i jiné metody ověřování kritérií a že

jejich systémy pak budou indikovat i podrobnější výsledky splnění jednotlivých kritérií. Spíše se zde jedná o demonstraci toho, že ověření platnosti na základě čl. 32 odst. 1 eIDAS je možné a jakým způsobem se provádí. Zákonodárce přitom nevolí pořadí podle dvou kroků v PKI, ale začíná od certifikátu, na němž je podpis založen,[168] tedy spíše krokem číslo dva z technické praxe PKI.

a) certifikát, na němž je podpis založen, byl v okamžiku podpisu kvalifikovaným certifikátem pro elektronický podpis, jenž je v souladu s přílohou I;

Zjištění, že se jedná o kvalifikovaný certifikát pro elektronický podpis, je možné dvěma základními způsoby. První metoda spočívá na kontrole technických parametrů, které jsou uvedeny v certifikátu.[169] Takové parametry fakticky ale může do certifikátu vložit i jiný vydavatel, než který je podle eIDAS oprávněný kvalifikované certifikáty pro elektronické podpisy vydávat. Z hlediska eIDAS je proto právně jistější druhá možnost, která spočívá nejprve v ověření následného kritéria b). Jím se ověří přítomnost kvalifikované služby vydávání kvalifikovaných certifikátů v důvěryhodném seznamu některého členského státu. Pak se buď již lze na výše uvedené technické parametry zřejmě spolehnout s tím, že by orgán dohledu nepřipustil uvádění chybných technických parametrů, anebo lze kvalifikátory dokládající požadované vlastnosti dohledat přímo v důvěryhodném seznamu.

Na závěr lze zkontrolovat obsah certifikátu na soulad s přílohou I, tj. přítomnost a obsah jednotlivých položek. K těmto kontrolám lze přistoupit s různou mírou přesnosti. Lze je provádět fragmentovaně podle certifikačních politiky jednotlivých poskytovatelů, lze je provádět podle přímého právního výkladu přílohy I eIDAS anebo lze využít metodické nápovědy v technické normě.[170] K okamžiku podpisu srov. níže.

Kontrolu tohoto kritéria lze automatizovat.

b) kvalifikovaný certifikát byl vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a v okamžiku podpisu byl platný;

---

[168] Obrat *„elektronický podpis založený na certifikátu"* se již v češtině právních předpisů bohužel vžil. Ve skutečnosti je elektronický podpis z PKI spíše založen a využívá soukromý klíč (data pro vytváření elektronického podpisu) a podepisovaná data. Certifikát se k výsledku typicky pouze přikládá, pro vlastní fázi vytvoření elektronického podpisu vůbec není potřeba. V angličtině se používá vazba *„the certificate that supports the signature"*, tj. certifikát podporující podpis, která je mnohem výstižnější.

[169] Současná přítomnost *id-etsi-qcs-QcCompliance* z bodu 4.2.1 a *id-etsi-qct-esign* z bodu 4.2.3 ETSI EN 319 412-5 V2.1.1. Norma dosud nebyla vyhlášená žádným prováděcím aktem v rámci eIDAS.

[170] Příloha A – Table A.1: Mapping with Annex I of the Regulation (EU) No 910/2014. ETSI EN 319 412-5 V2.1.1. Norma dosud nebyla vyhlášená žádným prováděcím aktem v rámci eIDAS.

Spolehlivé zjištění, že vydavatel certifikátu je kvalifikovaným poskytovatelem služeb vytvářejícím důvěru, včetně toho, že se jedná o jím vydaný kvalifikovaný certifikát pro elektronický podpis, je možné provést z důvěryhodného seznamu (čl. 22 eIDAS), který vydal některý členský stát EU. V rámci ověření tohoto kritéria je nutné provést i ověření platnosti zaručeného elektronického podpisu nebo zaručené elektronické pečeti kvalifikovaného poskytovatele služeb vytvářejících důvěru, který daný kvalifikovaný certifikát pro elektronický podpis podepsané osoby vydal. K tomu potřebný certifikát kvalifkovaného poskytovatele je rovněž k dispozici v důvěryhodném seznamu. K okamžiku podpisu srov. níže. Lze automatizovat.

c) data pro ověřování platnosti podpisu odpovídají datům poskytnutým spoléhající se straně;

Jedná se o nepříliš šťastně formulované provedení prvního kroku ověření elektronického podpisu z metodologie PKI, které poskytuje kladný výsledek. Pojem *„data poskytnutá spoléhající se straně"* je třeba chápat tak, že zahrnuje podepsaná data, elektronický podpis aj. doprovodná data.[171] Kryptologicky správná formulace by byla, že na základě podepsaných dat, elektronického podpisu, dalších doprovodných a dat pro ověřování platnosti se ověří, že se skutečně jedná o elektronický podpis podepsaných dat. Obecně k provedení prvního kroku ověření elektronického podpisu je nutné podporovat určitá kryptografická schémata. Nařízení eIDAS zcela opomnělo, kdo tato dovolená kryptografická schémata bude stanovovat nebo vyhlašovat. V rámci ETSI ESI existuje pouze nezávazná technická norma.[172] Ověření lze automatizovat.

d) spoléhající se straně je řádně poskytnut jedinečný soubor dat identifikujících podepisující osobu v certifikátu;

Vyjadřuje zřejmě požadavek, aby obsah certifikátu byl tak jednoznačný, že splňuje požadavky čl. 26 písm. a) a b) eIDAS, aby bylo jednoznačné spojení na podepisující osobu a aby se umožnila identifikace podepisující osoby. Jelikož podepisující osoba může být v certifikátu podle přílohy I písm. c) určena pouze jménem podepisující osoby nebo jejím pseudonymem, vyplývá jednoznačná identifikace až z obsahu podle přílohy I písm. f) eIDAS *„identifikační číslo certifikátu, které musí být*

[171] Všechna uvedená data jsou běžně součástí formátů zaručených elektronických podpisů XAdES, PAdES, CAdES stanovených Komisí podle čl. 27 odst. 5 eIDAS.

[172] ETSI TS 119 312 V1.2.1 – obsahuje řadu identifikačních určení a parametrů pro kryptografická schémata a pomocné kryptografické algoritmy. Norma na jedné straně může přispívat k lepší interoperabilitě, na straně druhé obsahuje příliš velké množství různých schémat, což bude interoperabilitu spíše stěžovat. Právní status normy je nejasný. Norma nemohla a nemůže být vyhlášena v rámci eIDAS, neboť k jejímu vyhlášení chybí v eIDAS zmocnění.

jedinečné pro daného kvalifikovaného poskytovatele služeb vytvářejících důvěru". Pole má charakter technického parametru.[173] Jeho zjištění lze automatizovat.

Jedinou další možností by bylo, že zákonodárce zde mínil možnost vyžadování identifikace osob podle bodů odůvodnění 33 nebo 54 eIDAS. Oba se však týkají pouze vnitrostátní úrovně, zatímco kritéria podle článku 32 odst. 1 eIDAS mají charakter jednotné úpravy unijním právem. Autor se proto zatím nedomnívá, že by tyto možnosti identifikace na národní úrovni byly tímto kritériem míněny.

e) pokud byl v okamžiku podpisu použit pseudonym, je jeho použití jednoznačně sděleno spoléhající se straně;

Použití pseudonymu v kvalifikovaném certifikátu pro elektronický podpis namísto pravého jména fyzické osoby je v příloze I písm. c) eIDAS povoleno s tím, že ale musí být jasně vyznačeno. Přítomnost může být rozlišitelná i strojově podle technické normy.[174] Lze automatizovat.

f) elektronický podpis byl vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů;

Tato informace bude běžně uvedena v kvalifikovaném certifikátu pro elektronický podpis podle přílohy I písm. j) eIDAS. Lze zjistit z technického parametru certifikátu,[175] anebo z kvalifikátorů v důvěryhodném seznamu. Lze automatizovat.

g) nebyla ohrožena integrita podepsaných dat;

Integrita podepsaných dat vyplývá v běžných případech použití kryptografických schémat PKI již z ověření kritéria c) výše. Lze automatizovat.

h) v okamžiku podpisu byly splněny požadavky stanovené v článku 26;

Jedná se o požadavky na zaručený elektronický podpis. Při striktním výkladu kritéria je třeba uvést, že spoléhající osoba není schopna objektivně zjistit, zda podmínky článku 26 eIDAS byly splněny. Splnění článku 26 však lze implikovat z toho, že certifikát je kvalifikovaný certifikát pro elektronický podpis a že byl použit kvalifikovaný prostředek pro vytváření elektronických podpisů, vše ověřeno vůči času okamžiku podpisu. Splnění kritérií a) až f) implikuje proto i splnění kritéria h). Lze automatizovat.

Podmínky spojené s časem okamžiku podpisu

[173] Jedná se o tzv. *serial number* certifikátu podle IETF RFC 5280. Tato specifikace není závazná.

[174] Alternativní přítomnost pole *pseudonym* podle bodu 4.2.4 ETSI EN 319 412-2 V2.1.1 Norma dosud nebyla vyhlášená žádným prováděcím aktem eIDAS.

[175] Např. z *id-etsi-qcs-QcSSCD* v bodě 4.2.2 ETSI EN 319 412-5 V2.1.1. Norma dosud nebyla vyhlášená žádným prováděcím aktem eIDAS.

Okamžik podpisu se vyskytuje v různých kritériích výše. Čas vytvoření podpisu by v rámci formátů podpisů PAdES, CAdES a XAdES[176] měl být uveden v poli zvaném *SigningTime*, a díky tomu by měl být automaticky zjistitelný, ať již je pak samotný obsah a formát podepsaných dat jakýkoli. Nachází se v rámci tzv. podepsaných atributů, které se v rámci výše uvedených formátů podpisují společně s podepisovanými daty, což znamená, že po vytvoření zaručeného elektronického podpisu již danou hodnotu nelze zpětně měnit. To však nutně neznamená, že uvedený datum a čas vytvoření podpisu v *SigningTime* jsou pravé, nebyly posunuty na časové ose dozadu, ale ani dopředu.[177] V zásadě se jedná o podepisující osobou tvrzené datum a čas vytvoření podpisu. V praxi bude čas podpisu nejčastěji nastavovat aplikace, s jejíž pomocí podepisující osoba vytváří elektronický podpis, přičemž ta k tomu může využívat buď informaci o času ze systémového prostředí (který může být i nezáměrně různě nepřesně posunut), ale může aktuální čas zjišťovat i pomocí síťových protokolů ze sítě internet s přesností na sekundy.

Pro splnění výše uvedených podmínek je pak následně v zásadě potřeba ověřit, zda tvrzený čas vytvoření elektronického podpisu je důvěryhodný. Pokud tvrzený čas vytvoření elektronického podpisu je například v pondělí, ve středu poté došlo ke zneplatnění[178] certifikátu, na němž je elektronický založen a spoléhající osoba ověřuje čerstvě došlá data s elektronickým podpisem poté v pátek, pak si nemůže být jista, zda daný elektronický podpis byl opravdu vytvořen v tvrzené pondělí podepisující osobou, anebo jej vytvořil případný útočník ve čtvrtek s tím, že pouze podvrhl pondělí jako tvrzené datum vytvoření podpisu.

Pro úplnost dodejme, že ve středu nemusí dojít nutně jen k uvedenému zneplatnění certifikátu na popud podepisující osoby z důvodu bezpečnostního incidentu, ale mohla třeba uplynout doba platnosti certifikátu, na němž je podpis založen. Jelikož po vypršení platnosti certifikátu poskytovatel služeb, který certifikát vydal, již běžně nepřijímá ani neprovádí zneplatnění takového certifikátu, mohl bezpečnostní incident nastat až ve čtvrtek, aniž by byl poskytovatelem zaznamenán a byl spoléhající osobě jakkoli sdělitelný podle čl. 24 odst. 4 eIDAS. Skeptická spoléhající osoba proto bude na expirovaný certifikát hledět jako na takový, u nějž těsně po expiraci došlo

[176] Ve verzích vyhlášených rozhodnutím Komise podle čl. 27 odst. 5 eIDAS.

[177] Posunutí dopředu je však poměrně riskantní. Dojde-li elektronický podpis s tvrzeným podpisem dříve, než mohl nastat, spoléhající osoba situaci poměrně rychle odhalí a může vyvodit i právní důsledky proti podepisující osobě.

[178] Zejména je-li důvodem zneplatnění bezpečnostní incident, pro náš příklad třeba krádež QSCD.

k bezpečnostnímu incidentu, popř. umožňující podepsané osobě kdykoli později tvrdit, že k němu došlo a že proto popírá nejen pravost, ale i ověření platnosti elektronického podpisu ve smyslu článku 32 eIDAS.

Pro prevenci těchto případů je vhodné, aby buď sama podepisující osoba, anebo spoléhající se osoba co nejdříve po přijetí podepsaných dat a elektronického podpisu opatřila celý výsledek (kvalifikovaným) elektronickým časovým razítkem. Časové razítko prokazuje, že jím orazítkovaná data existovala před datem a časem v razítku uvedeném. Kdyby ve výše uvedeném příkladě podepisující osoba odeslala data i s elektronickým podpisem již v pondělí odpoledne a ihned po přijetí bylo vše opatřeno elektronickým časovým razítkem, pak i v pátek si spoléhající osoba může být jista, že čas vytvoření podpisu skutečně nastal někdy v době před datem a časem z časového razítka (tj. i tvrzené pondělí je realistické), tedy v době, kdy certifikát, na němž je elektronický podpis založen, byl platný.

Spodní hranicí časového intervalu býval dříve běžně rozuměn okamžik začátku platnosti certifikátu, který dříve i dnes je podle přílohy I písm. e) v rámci *„označení začátku a konce doby platnosti certifikátu"* přítomen uvnitř kvalifikovaného certifikátu pro elektronický podpis. Nařízení eIDAS nicméně zmiňuje v čl. 28 odst. 4 eIDAS *„počáteční aktivaci"* kvalifikovaného certifikátu pro elektronický podpis. Uvedené zřejmě znamená, že okamžik počáteční aktivace se nemusí krýt s označením začátku platnosti certifikátu a spoléhající osoba by si měla případný čas aktivace zjistit od poskytovatele podle čl. 24 odst. 4 eIDAS. Rozlišování času aktivace a začátku platnosti je však zbytečné u těch poskytovatelů, u nichž se dle jejich certifikačních politik oba časy shodují.

Výše uvedené pouze nastiňuje, jaké zhruba potíže nastávají, když se elektronický podpis ověřuje v jiném čase než v okamžiku vytvoření. Matematickými kontrolami různých časových intervalů lze s jistotou rozhodnout, zda tvrzený čas spadá do období, kdy certifikát, na němž byl podpis založen, stejně jako jiné relevantní certifikáty v certifikační cestě byly všechny aktivní i platné. Jinak řečeno, tvrzený čas nemusí být postupem podle čl. 32 odst. 1 objektivně ověřitelný, zda skutečně byl *okamžikem* vytvoření elektronického podpisu, jak s pojmem pracuje konzistentně nařízení eIDAS, ale je ověřitelné, že nebyl vytvořen mimo období, kdy by některý z uvedených certifikátů nebyl platný. Postup je automatizovatelný.

6.11.3 Pokrok ve stanovení postupu dle čl. 32 odst. 1 eIDAS

Čtenáře nařízení, kterému by úprava podle čl. 32 odst. 1 eIDAS přišla nadbytečná, je vhodné upozornit, že vůči dřívější směrnici DirES existovala například kritika Reeda. Ve své publikaci[179] zjišťuje, že kvalifikovaný elektronický podpis podle DirES znamená splnění požadavků z přílohy 1, přílohy 2 i přílohy 3 směrnice DirES: „Sourhnně, směrnice obsahuje kontrolní seznam o 30 položkách, které, pokud jsou splněny, znamenají naplnění čl. 5 odst. 1.“[180] Dále upozorňoval: „... otázka, zda zaručený elektronický podpis splnil požadavky směrnice o elektronických podpisech, a má tak být považován za právně rovnocenný vlastnoručnímu podpisu, je zodpovězena odkazem na kontrolní seznam o 30 položkách. Pokud podpis splňuje objektivní testy v seznamu, vytváří stejné právní účinky jako vlastnoruční podpis, i když podstatné datové prvky, jako identita podpisujícího, jsou nepřesné. Účel legislativy bezpochybně je, aby spoléhající strana mohla objektivně zodpovědět otázku, zda-li podpis je právně platný. Pokud před akceptací podpisu spoléhající strana musí zkoumat přesnost dat v certifikátu, efektivitu technických procesů použitých pro zachování bezpečnosti, pak právo nedosáhlo ničeho.“ [181]

Legislativní technika nařízení eIDAS je do značné míry podobná. Také stanoví seznamy podmínek (požadavků) pro různé pojmy. Reed přitom upozorňoval: „Problém se směrnicí o elektronickém podpisu je, že její zdánlivě objektivní testy nejsou objektivní.“[182] Stejným nedostatkem se ovšem zdají trpět i některá ustanovení eIDAS. Ve skutečnosti je značně obtížné stanovit, zda například podmínky čl. 26 eIDAS pro zaručený elektronický podpis jsou splněny. Reed pak soudil: „Pro rozhodnutí, zda určitá technologie e-podpisu může být akceptována jako produkující ekvivalent vlastnoručního podpisu, spoléhající strana nejprve musí konzultovat právního specialistu, aby určil, které složky ze 30 položek kontrolního seznamu jsou důležité a co znamenají v kontextu určité transakce. Poté musí být povoláni techničtí experti, aby poskytli mínění, zda dané požadavky seznamu byly splněny. Konečně právní experti musí zkontrolovat stanovisko technických expertů, aby vydali další stanovisko, zda by soud byl přesvědčen argumenty technických expertů. **Pokud toto je jistota, pak se**

[179] REED, C. *How To Make Bad Law: Lessons from the computing and communications sector.* Queen Mary University of London, School of Law, Legal Studies Research Paper No. 40/2010, London: 2010.
[180] REED, C., cit. dílo, s. 7.
[181] REED, C., cit. dílo, s. 11.
[182] REED, C., cit. dílo, s. 11.

jedná o velmi nejistý druh jistoty a není překvapující, že právo nedosáhlo téměř ničeho, aby podnítilo zájem používat elektronické podpisy“.[183] (zvýraznil autor).

Z hlediska právní jistoty spoléhající osoby je proto přítomnost postupu podle čl. 32 odst. 1 eIDAS značným pokrokem. Celý čl. 32 eIDAS v zásadě odpovídá na tuto jednu kritiku, že spolehnutí se na QES musí být jednoduché. Ultimátně je účelem čl. 32 eIDAS to, aby celý proces byl plně automatizovatelný.

Určité pochybnosti pochopitelně mohou zůstat a nelze vyloučit, že budou vzneseny i v rámci některých právních sporů. Například o tom, jak přesně provádět jednotlivé kroky. Zda i správný postup podle písmen a) až h) skutečně ověřuje všechny podmínky definovaných pojmů, zejména cílového kvalifikovaného elektronického podpisu. Zdá se být nesporné, že obsahem kvalifikovaného certifikátu pro elektronický podpis podle přílohy I písm. c) je jméno podepisující osoby (nebo pseudonym).

Certifikát však může obsahovat podle čl. 28 odst. 3 eIDAS i další zvláštní atributy. Ačkoli nebudou vytvářet potíže technické interoperability a nezmění právní požadavek na status uznávání kvalifikovaných elektronických podpisů, z pohledu právníka mohou představovat podstatnou informaci, kterou spoléhající osoba získává společně s kvalifikovaným elektronickým podpisem. Autor je zde názoru, že bez uvedení názvu organizace (pole O), funkce v organizaci (např. v poli OU) nebo adresy elektronické pošty (e-mail), které jsou všechny ověřené poskytovatelem, ztrácí použití mnoha kvalifikovaných elektronických podpisů do značné míry smysl, neboť spoléhající osoba pak musí velmi pracně sama zjišťovat, zda osoba daného jména nějak souvisí s organizací, za niž vystupuje.

Technické normy takovým atributům připisují nějaký význam, o nichž se technika domnívá, že by mohly být v praxi užitečné. Způsob jejich ověřování u poskytovatele služeb, jak je například vyjádřen v dokumentu jeho certifikační politiky, může mírně posunout jejich význam. První právní otázkou pak bude, jaký právní význam hodnotě v určitém poli (atributu certifikátu) přisoudit. Lze se nicméně domnívat, že právo bude přisuzovat ty významy, které za daných okolností působí přirozeně. I obsah certifikátu kupř. je součástí právního jednání podepisující osoby a až na zvláštní potřebu ohledu vůči technickým normám nebo certifikačním politikám není zvláštní důvod, aby se jeho obsah nepovažoval za tvrzené informace, s určitou mírou ověření poskytovatele, ze strany podepisující osoby.

[183] REED, C., cit. dílo, s. 11.

Druhý okruh právních otázek může vyvstat, pokud vznikne kolize obsahu certifikátu se skutečností. Určité pole v certifikátu nemusí v době vytvoření elektronického podpisu již odpovídat faktickému stavu. Zvláštním případem může být, pokud vzniká kolize údaje z certifikátu s některým veřejným rejstříkem. V certifikátu kupř. bude zapsána pozice „jednatel" a v poli O = „Obchodní společnost s. r. o." Běžné jazykové pochopení takových informací je, že podepisující osoba je jednatelem uvedené obchodní společnosti. Tyto údaje mohly být i ověřeny v době vystavení certifikátu a být pravdivé. Později dotyčná podepisující osoba jednatelem být přestala, ale nedošlo ke zneplatnění certifikátu. Jestliže s jeho pomocí provede právní jednání, bezesporu vzniknou právní otázky druhu, zda se jedná o platné právní jednání uvedené obchodní společnosti, a pokud nikoli, které všechny subjekty lze případně žalovat o náhradu škody. Jinak řečeno, do jaké míry může spoléhající se osoba spoléhat, a to i právně, na údaje uvedené v certifikátu.

Autor zde záměrně nebude provádět rozbor takového případu. Nařízení eIDAS neobsahuje dostatek právní úpravy. Právní úprava v jednotlivých členských státech se může lišit, a to významně. V ČR je velmi snadno dostupný obchodní rejstřík, ze kterého lze přes internet ověřit, kdo je aktuálním jednatelem společnosti. V řadě členských států však takový rejstřík není nebo je pouze nesnadno přístupný.

6.11.4 Ověření platnosti vs. pravost elektronického podpisu

Jak upozorňuje Mason, co skutečně chybí v čl. 32 odst. 1 eIDAS, je „ujištění, že podpis byl připojen [k podepsaným datům] osobou, o jejíž podpis se údajně jedná".[184] Postup podle čl. 32 odst. 1 eIDAS je schopen nanejvýš ověřit (technickou) *platnost* QES, tj. ujistit spoléhající osobu o tom, že byl vytvořen pomocí dat pro vytváření podpisu, která jsou přes svůj komplement, tj. přes data pro ověřování platnosti v rámci kvalifikovaného certifikátu pro elektronický podpis, přiřazena podepisující osobě. Zda byl podpis *pravý* v tom smyslu, že jej podepisující osoba chtěla k podepsaným datům vytvořit, zcela jisté není. Proti této skeptické linii je vhodné vést v patrnosti, že celý systém PKI je v rámci nařízení eIDAS budován právně-organizačně za tím účelem, aby se možnost takového odloučení dat pro vytváření platnosti od podepisující osoby minimalizovala. Srov. AdES (6.5.1), QES (6.5.3), ale též možnosti útoků na QES (6.15.7).

[184] MASON, S. *Electronic Signatures in Law*, cit.dílo, 2016, s. 162.

6.12 Odpovědnost poskytovatele služeb vytvářejících důvěru

Odpovědnost poskytovatele služeb vytvářejících důvěru je upravena v čl. 13 eIDAS. Poskytovatel služeb je povinen dodržovat všechny povinnosti, které mu nařízení eIDAS určuje buď jako subjektu poskytovateli služby, popř. v rámci druhu služby poskytující důvěru, kterou poskytuje. Nařízení přitom stanoví více povinností pro kvalifikované poskytovatele služeb a více povinností pro kvalifikovanou verzi služeb vytvářejících důvěru.

Podle čl. 13 odst. 1 eIDAS *„poskytovatelé služeb vytvářejících důvěru odpovídají za škodu, kterou úmyslně nebo z nedbalosti způsobí fyzické nebo právnické osobě nesplněním povinností podle tohoto nařízení"*.

V případě běžného (nekvalifikovaného) poskytovatele služeb je na poškozeném, aby dokázal, že se poskytovatel dopustil nedbalosti. Jelikož toto poškozeného nerealisticky zatěžuje, je v případě kvalifikovaného poskytovatele služeb důkazní břemeno přeneseno na poskytovatele. Dle čl. 13 odst. 1 druhá alinea eIDAS se nedbalost nebo úmysl presumuje. Poskytovatel ale má možnost se vyvinit, když prokáže, že *„škoda ... nastala bez jeho úmyslu nebo nedbalosti"*. To je bezpochyby dobrým motivem k tomu, aby vedl co nejpečlivější dokumentaci o svých činnostech.

Dle čl. 13 odst. 2 eIDAS mají poskytovatelé možnost omezit výši své odpovědnosti za škodu, pokud „své zákazníky předem řádně informují o omezeních týkajících se využívání jimi poskytovaných služeb a tato omezení jsou rozpoznatelná pro třetí osoby". V čl. 13 odst. 3 eIDAS se pak stanoví, že uvedená pravidla o vymáhání škody se použijí v souladu s vnitrostátním právem upravujícím odpovědnost za škodu.

V rámci obecných požadavků na kvalifikované poskytovatele v čl. 24 odst. 2 písm. b) eIDAS se stanoví podmínky na jím využité *„zaměstnance případně subdodavatele"*. Podle pravidel článku 13 eIDAS však odpovědnost za škodu třetí straně nese vždy poskytovatel služeb vytvářejících důvěru, a nikoli jejich zaměstnanec nebo subdodavatel.

Podle článku 24 odst. 2 písm. c) eIDAS musí mít kvalifikovaný poskytovatel buď dostatek finančních prostředků, nebo vhodné pojištění odpovědnosti.

6.13 Odpovědnost členského státu

Členský stát bezpochyby může v důsledku rozhodnutí o udělení statutu kvalifikovaného poskytovatele [čl. 17 odst. 4 písm. g) eIDAS] a jeho zapsání na důvěryhodný seznam [čl. 17 odst. 4 písm. h) ve spojení s čl. 22 odst. 1 a 2 nař. eIDAS] za daného poskytovatele odpovídat,[185] ale jen pokud by zanedbal některé ze svých povinností, které nařízení eIDAS členskému státu nebo jím ustaveným orgánům dohledu ukládá. Nařízení eIDAS nezakládá žádný zvláštní způsob odpovědnosti členského státu za poskytovatele služeb vytvářejících důvěru, kteří jsou *„usazenými na území členského státu"* [čl. 17 odst. 3 písm. a) a b) eIDAS].

Otázka, do jaké míry členský stát za kvalifikovaného poskytovatele odpovídá, není nařízením podrobně upravena. Lze se domnívat, že členský stát odpovídá tehdy, pokud by jemu předepsané činnosti jeho orgán dohledu zanedbal, kupř. by řádně neověřil zprávu o posouzení shody. Jestliže však členský stát, resp. jeho orgán dohledu všechny předepsané povinnosti splnil a kvalifikovaný poskytovatel přesto nedokáže nahradit veškerou vzniklou škodu ani z pojištění, pak dovodit odpovědnost státu ve formě ručení za poskytovatele z čl. 22 odst. 1 eIDAS nelze. Obdobně například neručí členský stát za trvalou solventnost obchodních společností, k nimž jeho orgány vedou údaje například v obchodním rejstříku. Domáhání se náhrady škody vůči členskému státu bude záviset i na jeho vnitrostátní právní úpravě řešení takových případů.

6.14 Přijímání elektronických podpisů

Jednou z právních otázek provádění elektronických transakcí je, zda příjemce či adresát dat podepsaných elektronickým podpisem musí souhlasit s tím, že původce mu zasílá obsah svého jednání ve formě dat a svůj podpis ve formě elektronického podpisu. Nejčastěji se bude jednat o písemnost v elektronické podobě, čemuž zpravidla bude odpovídat i pojem elektronického dokumentu. Přesné definice těchto pojmů se nicméně mohou lišit podle členského státu. S touto situací souvisí otázky nejen právní, ale technické, například pro jaké technické specifikace se příjemce musí vybavit technickými prostředky, aby taková data opatřená elektronickým podpisem byl schopen technicky zpracovávat.

[185] V českém znění eIDAS je *odpovídání* nahrazeno vazbou *„být v působnosti"*, zatímco německé i anglické znění hovoří o odpovídání.

Obě složky, tedy data a jejich podpis, mohou v případě soukromoprávního vztahu tvořit elektronické právní jednání, někdy může být tato podoba rozhodným právem uznána za rovnu nebo splňující požadavky na právní jednání v písemné podobě.

V případě veřejného práva se opět budou rozlišovat obě složky, tj. data a podpis, přičemž právní úprava rozhodného práva zde bude zpravidla rigidnější, tj. může požadovat případně i nějaké další náležitosti, popř. náležitosti na formát a obsah dat, která pravidelně budou dokumentem či písemností v elektronické podobě.

6.14.1 Přijetí elektronických podpisů příjemci v soukromém právu

Jedná-li se o styk mezi subjekty soukromého práva a *v rámci vztahů soukromého práva*, pak autor je jednoznačně názoru, že příjemce sdělení zaslané mu v elektronické formě bez dalšího akceptovat nemusí, ať jsou data opatřena jakýmkoli druhem elektronického podpisu, včetně kvalifikovaného elektronického podpisu (QES). Uvedené vyplývá z obecné zásady smluvní svobody, která běžně stanoví, že smluvní strana má svobodu rozhodnout se o tom, s kým chce smlouvu uzavřít, jaký obsah má smlouva mít, zda má být smlouva vůbec uzavřena, a zahrnuje i souhlas s druhem formy použité pro uzavření smlouvy. Nařízení eIDAS výše uvedenou smluvní svobodu příjemce neomezuje, neboť podle čl. 2 odst. 3 eIDAS: *„tímto nařízením není dotčeno vnitrostátní právo ani právo Unie týkající se uzavírání a platnosti smluv či jiných právních nebo procesních povinností týkajících se formy"*. Obdobně i bod odůvodnění 21. Přiznává-li vnitrostátní právo členského státu smluvní svobodu k právnímu jednání, nemůže ji pak nařízení eIDAS měnit nebo narušovat, a to ani svým ustanovením o ekvivalenci QES s vlastnoručním podpisem v čl. 25 odst. 2 eIDAS a ani čl. 25 odst. 3 eIDAS o přeshraničním uznávání QES. Obdobná volnost volby formy zpravidla platí i pro obecné právní jednání, tedy i pro právní jednání jednostranné. Autor se domnívá, že tato zásada smluvní svobody bude obsažena prakticky ve všech právních řádech členských států EU. Prakticky je jím ověřena v právních řádech ČR a Německa níže v tomto textu.

Podrobnosti nebo dílčí odchylky je potřeba dohledat v rozhodném právním řádu, který se na jednání uplatňuje, zpravidla v rámci obecné úpravy soukromého práva, někdy však i v její zvláštní části. Reaguje-li však příjemce na přijatá elektronická data s elektronickým podpisem souhlasně, lze mít zpravidla za to, že tím vyslovil i souhlas ohledně zvolené formy. Příjemce může být k přijímání určitého druhu zpráv s daty,

potvrzenými určitými druhy elektronického podpisu, zavázán i smluvně. V případě důvodných pochybností to však zřejmě nevylučuje, aby příjemce žádal potvrzení dané elektronické zprávy i nějak jinak. Některé právní řády umožňují, aby dříve udělený souhlas s elektronickou formou právního jednání byl kdykoli vzat zpět. Zde je výhodou např. dohoda na kvalifikovaném elektronickém podpisu, neboť zřejmě bude běžně budit nejméně důvodů k pochybnostem než méně bezpečnostně zajištěné formy elektronického podpisu.

Původce i příjemce mohou být též omezeni tím, že pro určité druhy právního jednání, ev. druhy smluv rozhodné právo elektronickou formu nepřipouští nebo pro ni vyžaduje, ať pro obsah dat, nebo pro druh elektronického podpisu, zvláštní náležitosti. Tyto požadavky pak nelze zpravidla podkročit ani na základě vzájemné úmluvy, jednání bude neplatné pro nedostatek formy. Tento nedostatek je možné někdy zhojit. Vytvářet však záměrně neplatné právní jednání neposkytuje právní jistotu a nelze to doporučit.

Zásada smluvní svobody nebude ale nutně znamenat, že příjemce má úplnou svobodu ignorovat jakékoli sdělení, které obdrží v elektronické formě, jen na základě svého volního rozhodnutí. Rozhodné právo nebo judikatura soudů může tuto svobodu pro některé situace výjimečně nebo i pravidelněji prolomit. Nebude se však jednat o stavy při samotném zakládání nebo změně právních vztahů, ale spíše o režim různých upomínek, upozornění, varování, například v souvislosti s předcházením nebo mírněním škod apod. Poslední nevylučuje, ale naopak je spíše v souladu s tím, že některému sdělení v elektronické podobě (dokumentu) a jeho elektronickému podpisu může být přiznán právní účinek podle čl. 46 a čl. 25 odst. 1 eIDAS, popř. že pak může být použit jako důkaz v řízení, který třeba i jen osvědčuje některou skutkovou okolnost.

6.14.2 Přijetí elektronických podpisů příjemci ve veřejném právu

V roli přijímacích subjektů budou i subjekty veřejného práva. Pro podrobnosti dopadu nařízení eIDAS na tuto oblast viz 6.1.4 o pojmu elektronické transakce. Pro ustanovení týkající se této oblasti a role příjímajícího subjektu nařízení používá pojem *„subjekt veřejného sektoru“* (čl. 3 bod 7 eIDAS, podrobněji srov. 6.1.6.3), který zřejmě má být reprezentantem označení přijímacího subjektu z oblasti veřejného práva. Některá ustanovení eIDAS jsou však koncipována bez použití tohoto pojmu. Není pak zřejmé, zda to je pouze kvůli jejich použitelnosti vůči soukromým subjektům a pro soukromé právo, anebo obecné znění (např. čl. 25 odst. 3 eIDAS) má případně zahrnout i nějakou

další formu veřejnoprávního styku. Autor druhou možnost zcela nevylučuje, ale nebude takové případy na straně veřejných subjektů zde zvlášť vyhledávat.

Článek 27 odst. 1 až 3 eIDAS zmiňuje tři druhy elektronického podpisu, se vzrůstající mírou zajištění bezpečnosti:

1. Zaručený elektronický podpis.
2. Zaručený elektronický podpis založený na kvalifikovaném certifikátu.
3. Kvalifikovaný elektronický podpis.

Jestliže pak subjekt veřejného sektoru poskytuje nebo jeho jménem je poskytována nějaká on-line služba, může vnitrostátní právo přikázat pro její použití některý z výše uvedených 3 druhů elektronického podpisu. Článek 27 odst. 1 a 2 eIDAS pak stanoví, že jsou-li používány první nebo druhý druh, musí členský stát uznávat podpisy stejného druhu nebo vyšší míry zajištění bezpečnosti. Uznáním se zde podle autora míní, že dané druhy elektronického podpisu budou uznávany bez ohledu na to, ze kterého členského státu daný elektronický podpis pochází. Původem se zde neníní to, na jakém místě se podepisující osoba právě nachází, ale podle práva kterého členského státu jí byl potřebný prostředek a související potvrzení, typicky certifikát pro elektronický podpis, vydán nebo zpřístupněn. Účelem je zajistit uznávání přeshraniční, formulace je však taková, že zajišťuje i uznávání vnitrostátní. Uznání lze odmítnout, pokud by zaručený elektronický podpis, nebo jiný s vyšší mírou zajištění bezpečnosti, nebyl v některém z formátů, které vyhlásila Komise podle čl. 27 odst. 5 eIDAS. Takový požadavek je rozumný, neboť úplná volnost formátu by příliš často způsobovala technickou nečitelnost.

V článku 27 se nenachází analogický odstavec pro případ podpisu třetího druhu (QES), zřejmě z toho důvodu, že se namísto toho má použít obecněji formulovaný čl. 25 odst. 3 eIDAS, který stanoví povinnost uznávání QES přeshraničně obecně, nejen subjektem veřejného sektoru. Chybí bohužel ustanovení o dodržení formátu podpisu, které je třeba dovodit analogicky, popř. v kombinaci s výkladem užitečného účinku uznávání, popř. opřené o bod odůvodnění 6 a 23 eIDAS. Autor se proto domnívá, že kvalifikovaný elektronický podpis, který by nebyl ve formátu podle čl. 27 odst. 5 eIDAS, může subjekt veřejného sektoru odmítnout. Toto tvrzení autora by mohlo doznat změny, pokud Komisí případně zveřejněný postup podle čl. 32 odst. 3 eIDAS by stanovil nějakou jinou metodiku, což však autor zatím nepředpokládá.

V článku 27 odst. 3 eIDAS se stanoví, že členské státy *„nesmějí v případě přeshraničního využívání on-line služby poskytované subjektem veřejného sektoru vyžadovat elektronický podpis s vyšší zárukou bezpečnosti než kvalifikovaný elektronický podpis"*.

Tuto podmínku je prakticky obtížné vyložit jinak, než že kvalifikovaný elektronický podpis (QES) představuje nejvyšší laťku požadavků na elektronický podpis, kterou může členský stát vyžadovat vůči uživatelům on-line služby, jež je poskytována subjektem veřejného sektoru přeshraničně. Členský stát může svým vnitrostátním právem nedovolit poskytovat určitou službu elektronickou formou, resp. dle textu nařízení jako „on-line službu". Pokud ji však dovoluje, pak v rámci požadavků na využití takové služby smí být pro účely podpisu vyžadován nejvýše druh kvalifikovaného elektronického podpisu (QES) a musí být uznávány i přeshraničně. Členský stát může stanovit jako náležité i druhy nižší úrovně zajištění bezpečnosti, než je QES, pak ale musí, a to i přeshraničně, uznávat podpisy stejné úrovně zajištění bezpečnosti nebo vyšší (srov. výklad výše).

Autor zde nesouhlasí například s tvrzením Dumortiera, že: *„uznání kvalifikovaného elektronického podpisu založeného na kvalifikovaném certifikátu vydaném v jiném členském státu neznemožňuje členskému státu, aby přikázal použití zvláštního prostředku pro vytváření, například národní identifikační kartu, pro určitou transakci nebo postupy"*.[186] Dle názoru autora je toto možné pouze v případě, že danou službu nelze používat přeshraničně nebo pokud použití takového prostředku přináší nějakou vlastnost vedle funkce (kvalifikovaného) elektronického podpisu (obě možnosti diskutovány níže). Jinak by tvrzení bylo v rozporu s normativním textem čl. 25 odst. 3 ve spojení s čl. 27 odst. 3 eIDAS, a zejména pak s užitečným účinkem nařízení jako celku, jak je třeba vyjádřen v bodě odůvodnění 6 eIDAS.

Podmínku *„přeshraničního využívání"* v čl. 27 odst. 3 eIDAS je v zásadě potřeba chápat tak, že zde nařízení znovu indikuje oblast své působnosti, tj. že se vztahuje pouze na oblasti spadající do práva EU na základě přenosu pravomocí, tj. zejména na oblasti indikované v nařízení zmíněným právním základem (srov. 6.1.4). V praxi však může být pro subjekt veřejného sektoru v řadě agend nemožné předem určit, zda vůči němu směřující podání bude mít charakter ryze vnitrostátní, anebo bude obsahovat evropský prvek. Jediným praktickým přístupem pak je preventivně přijímat

[186] Dumortier in LODDER, A. R. – MURRAY, A. D. (eds)., cit. dílo, s. 282. Poznámka pod čarou 35.

všechna podání tak, jako by mohla obsahovat evropský prvek. V důsledku toho bude mít nařízení eIDAS dopad i na on-line služby, které budou využívány téměř čistě vnitrostátně. Tento vliv nařízení je však třeba považovat spíše za pozitivní, neboť může vést k obecnější jednotnosti forem správní praxe v elektronické podobě napříč členskými státy, bez ohledu na agendu.

Kvalifikovaný elektronický podpis nemusí být subjektem veřejného sektoru uznán, jestliže postup podle čl. 32 eIDAS nevede k ověření platnosti. Obdobně ani druhy elektronických podpisů s nižší mírou zajištění bezpečnosti nemusí být uznány, pokud jejich platnost nelze ověřit.

Vzhledem k tomu, že nařízení eIDAS ani jeho prováděcí akty nestanoví druhy akceptovatelných kryptografických sad, je možné, že subjektu veřejného sektoru dojde QES, zejména přeshraničního původu, který bude používat kryptografickou sadu, jež bude jeho prostředkům pro ověřování neznámá, nebudou ji podporovat. Obecně dle bodu odůvodnění 23 eIDAS by nařízení nemělo znamenat, že *„veřejný subjekt musí získat technické zařízení a programové vybavení nezbytné pro technickou čitelnost všech existujících služeb vytvářejících důvěru"*. Důvod nepodporování použité kryptografické sady je tedy legitimní pro odmítnutí uznání (srov. 6.16.14). Vstřícné subjekty veřejného sektoru však mohou aspoň v těchto případech využít služeb některého poskytovatele kvalifikovaných služeb ověřování platnosti kvalifikovaných elektronických podpisů podle čl. 33 eIDAS, pokud nabízí pokrytí širšího spektra možných parametrů kvalifikovaných elektronických podpisů. Výsledek ověření je od poskytovatele *„opatřen zaručeným elektronickým podpisem nebo zaručenou elektronickou pečetí"*. Subjekt veřejného sektoru by si pochopitelně měl vybrat takového poskytovatele, jímž poskytnutý *„výsledek postupu ověření platnosti"* bude schopen automaticky zpracovat, a to včetně ověření platnosti zaručené elektronické pečetě nebo zaručené elektronické pečetě poskytovatele. Subjekt veřejného sektoru bude tedy aspoň s takovým svým poskytovatelem ověřování používat shodnou kryptografickou sadu. Zda využívat služby takového poskytovatele ověření, je v praxi zřejmě zejména otázkou toho, kolik protějšků komunikace může být v dané agendě on-line služby přeshraničních, popř. vlastností prostředků pro ověřování, které subjekt veřejného sektoru užívá nebo hodlá užívat.

Článek 27 odst. 3 eIDAS, a to ani v kombinaci s článkem 46 eIDAS o právních účincích elektronických dokumentů, neznamená, že členský stát, resp. subjekt veřejného

sektoru musí uznat podepsaný obsah. I pokud je podpis ve formátu dle čl. 27 odst. 5 eIDAS a jeho platnost ověřena dle čl. 32 eIDSA, ale vlastní podepsaný obsah nebude ve formátu, který je předepsán vnitrostátním právem, nebo v souladu s ním subjektem veřejného sektoru, povinnost uznání obsahu není nařízením dána.

Obecně lze říci, že náležitostí obsahu, kvůli kterým nebude podepsaný obsah (přeshraničně) uznatelný, může být mnoho. Může tak vznikat paradoxní situace, že sice podpis uznán je, nikoli však obsah. Obsah například nemusí splňovat požadavky na úřední řeč. Takovému požadavku lze vyjít vstříc nejsnáze tak, že systém pro přípravu podání obsahuje formulářové prvky, které provedou samočinný překlad do cílového úředního jazyka subjektu veřejného sektoru. Uznávání obsahu pak může být paradoxně nejjednodušší, pokud obsahem podání je projev vůle podepsané osoby. Složitější naopak mohou být situace dokladování, pokud je předkládána nějaká veřejná listina, byť elektronicky podepsaná, pokud mezi státy neexistuje dohoda o přímém vzájemném uznávání veřejných listin.

Ani Úmluva o zrušení požadavku ověřování cizích veřejných listin, přijatá v Haagu dne 5. 10. 1961, platná pro ČR od 16. 3. 1999, neznamená možnost přímého předkládání cizích veřejných listin, ale jen určité zjednodušení postupu, v němž odpadá zejména ověřování listiny zastupitelským úřadem státu, v němž má být listina použita.

Kromě režimu vzájemného uznávání mezi členskými státy může existovat v rámci práva EU i zavedení transnacionálních správních aktů,[187] které překonávají tradiční teritorialitu účinku produktu veřejné správy. Příkladem takové listiny či dokladu je řidičský průkaz, kteýé členské státy vydávají podle směrnice 91/439/EHS o řidičských průkazech. Ta v příloze I stanoví vzor národního řidičského průkazu a na základě článku 1 odst. 2 této směrnici se *„řidičské průkazy vydané členskými státy vzájemně uznávají"*. Uznávání se ovšem týká pouze samotného fyzického provedení průkazu, nikoli například jeho naskenované podoby. Jelikož nařízení eIDAS neobsahuje žádná ustanovení o provádění konverzí, z výše uvedené směrnice ani jejích národních transpozic uznávaní kopií nebo konverzí řidičských průkazů bez dalšího neplyne.

Připuštění a uznání dokladování soukromou listinou, například potvrzením zaměstnavatele vůči zaměstnanci, bude záviset na tom, zda je vnitrostátní předpis v případě dané on-line služby, popř. obecněji, připouští, popř. za jakých podmínek. Obdobně tomu bude i v případě svépomocně prováděných konverzí veřejných listin

[187] POMAHAČ, R. – HANDRLICA, J. *Evropské správní právo*. Praha: C. H. Beck, 2012, s. 10.

a dokladů do elektronické podoby, které by jinak uznatelné byly, například výše uvedených řidičských průkazů.

Jiným potenciálním požadavkem na elektronické podání vůči on-line službě subjektu veřejného sektoru může být i určitý způsob dostatečně přesvědčivého prokázání totožnosti. Podle bodu odůvodnění 54 eIDAS je připuštěna vnitrostátní implementace nařízení eIDAS o vkládání jedinečných identifikátorů do kvalifikovaných certifikátů, čemuž odpovídá i normativní čl. 28 odst. 3 eIDAS. Takový požadavek pak může být tedy splněn kvalifikovaným elektronickým podpisem a s ním souvisejícím kvalifikovaným certifikátem, vytvořeným dle vnitrostátního práva a obsahujícím takový jedinečný identifikátor, zatímco kvalifikovaný certifikát vydaný v přeshraničí tuto kontrolu a požadavek nezajistí. Vnitrostátní právní předpis by v takovém případě pouze měl stanovit jiné prostředky nebo způsoby, jak může podávající osoba svoji totožnost prokázat. Tímto způsobem se nezvýší požadavky na přeshraniční elektronický podpis a nedojde k porušení článku 27 odst. 3 eIDAS.

Formulace čl. 27 odst. 3 eIDAS ponechává možnost výjimky pro případy, kdy on-line služba nemůže být využívána přeshraničně. V takových případech je možné na elektronický podpis podepisující osoby mít stanoveny i vyšší požadavky, než představuje QES. Takovou možností je, pokud on-line agenda sice je přístupná veřejně, ale nemůže mít přeshraniční prvek. Příkladem takových agend mohou být ty, které se týkají výlučně občanů některého státu a nemohou se týkat občanů jiného členského státu. Jen v takovém případě je dle autora přípustné výše citované tvrzení Dumortiera, že vnitrostátní právo může stanovit například použití občanské identifikační karty (průkazu) jako QSCD, tj. využívat některé jeho zvláštní technické vlastnosti. Taková zvláštní vlastnost by se měla projevit v kvalifikovaném certifikátu pro elektronický podpis a může přímo nebo nepřímo být potvrzením o občanství daného státu.

Dalšími možnostmi jsou případy, kdy agendy nejsou veřejné a nepoužívají se přeshraničně. Do těchto případů spadají vnitřní postupy veřejné správy, popř. státních orgánů, které se neprojevují navenek správních úřadů nebo státních orgánů.

Požadavek čl. 27 odst. 3 eIDAS neznamená ani to, že na samotné elektronické podpisy vytvářené subjektem veřejného sektoru nemůže vnitrostátní právo klást vyšší požadavky. Nařízení eIDAS je v případě předchozích dvou vět třeba vyložit souladně s bodem odůvodnění 24, podle nějž členské státy mohou *„zachovat nebo zavést*

vnitrostátní předpisy týkající se služeb vytvářejících důvěru, pokud dané služby nejsou tímto nařízením plně harmonizovány". Pro subjekty veřejného sektoru je tak kupříkladu možné zpřísnit požadavky na aplikace vytvářející podpis nebo na systémové prostředí, které sami používají. Služby podle eIDAS by však měly mít na vnitřním trhu zajištěn volný pohyb, tj. uvedené požadavky musí být formulovány tak, aby byly právně souladné a technicky kompatibilní či interoperabilní se službami vytvářejícími důvěru, jak jsou koncipovány nařízením eIDAS. Tohoto cíle lze podle názoru autora dosáhnout.

Vyšší požadavky, než stanoví QES, ale nelze klást na podepisující osoby, které tvoří protějšek on-line služby subjektu veřejného sektoru. Tato skutečnost se nezdá být kritická, neboť například ve správní praxi ČR se osvědčil systém datových schránek, který využívá asymetrický model míry zajištění bezpečnosti. Na straně soukromoprávních subjektů dostačuje nejjednodušší možná autentizace zadáním přihlašovacího jména a hesla, zatímco dokumenty veřejnoprávních původců musely být podepsány uznávaným elektronickým podpisem.

Až dosud jsme se v této části zabývali uznáváním podpisu a podepsaného obsahu subjektem veřejného sektoru. Existuje pochopitelně i opačná otázka po uznávání dat a elektronického podpisu, vytvořených subjektem veřejného sektoru, protějškem subjektu veřejného sektoru, typicky občanem, právnickou osobou apod., popř. obecnou třetí stranou. Tyto protějšky a třetí strany níže v této části zjednodušeně označujeme jako soukromé osoby.

Ohledně kvalifikovaného elektronického podpisu se zde zřejmě i v tomto případě uplatní čl. 25 odst. 3 eIDAS o jeho přeshraničním uznávání. Určitou komplikací může být, že samotné nařízení eIDAS nepřikazuje subjektům veřejného sektoru vytvářet své vlastní elektronické podpisy ve formátech vyhlášených Komisí dle čl. 27 odst. 5 eIDAS. Lze spíše jen apelovat na národní zákonodárce, aby jejich použití předepisovali, popř. na zdravý rozum samotných subjektů veřejného sektoru, ale i jejich dodavatelů, aby zaručené a kvalifikované elektronické podpisy vytvářeli v těchto formátech. Je v zájmu všech uživatelů, aby se tyto formáty používaly a nedocházelo k fragmentarizaci technologií a uživatelské základny. Ve prospěch používání formátů podpisu podle čl. 27 odst. 5 eIDAS lze argumentovat i teleologicky. Je totiž možné, že příjemce elektronické písemnosti ji bude někdy v budoucnu chtít použít vůči subjektu veřejného sektoru vlastního nebo jiného členského státu.[188] Ten je však podle eIDAS povinen přijímat

[188] Výše zmíněnou otázku přeshraničního uznávání obsahu zde odhlédněme. Nelze vyloučit, že časem

pouze elektronické podpisy ve formátech podle čl. 27 odst. 5 eIDAS. Stát, jehož subjekty veřejného sektoru nebudou vydávat své vlastní elektronické písemnosti s podpisem tohoto formátu, by tak znevýhodňoval své soukromé subjekty ve vztahu vůči soukromým subjektům jiných států, které tak postupovat budou.

Opět nezávislou otázkou je, zda soukromý subjekt musí uznat podepsaný obsah. Zřejmě tomu tak bude v případě vnitrostátních dokumentů, pokud společně s elektronickým podpisem jsou veřejnou listinou, které se pak těší presumpci správnosti. Naplnění požadavků bude záležet na vnitrostátním právu. V případě přeshraničního dokumentu bude zřejmě záležet jen na soukromém subjektu, zda je ochoten daný podepsaný dokument uznat, ačkoli byl vytvořen podle práva jiného členského státu, často je v jiné řeči apod. Zejména v praxi elektronických obchodů, kdy se obchodníci zatím spokojují ryze s tvrzenými údaji, však i takovéto dokumenty mohou představovat značný pokrok důvěryhodnosti. Elektronické dokumenty je nebo bude stále častěji možné konvertovat automatickými překladači do vlastní řeči nebo aspoň do angličtiny, takže příjemce může aspoň rámcově vytušit, co daný dokument vyjadřuje nebo potvrzuje. Opatření kvalifikovaným elektronickým podpisem (popř. i kvalifikovanou elektronickou pečetí) by pak příjemci mělo poskytnout slušnou jistotu o tom, jakým subjektem veřejného sektoru byl dokument vydán. V případě kvalifikovaného elektronického podpisu to ovšem předpokládá, že kvalifikovaný certifikát pro elektronický podpis bude vybaven dalšími poli, zejména polem O *(Organization)*, které uvádí daný subjekt veřejného sektoru. Pro možnost jeho určení a ověření totožnosti je vhodné i obsažení webové adresy organizace, popř. e-mailové adresy podepisující osoby, která obsahuje doménové jméno používané danou organizací. Právní význam těchto polí sice není nařízením eIDAS upraven, ke zvýšení důvěryhodnosti o jistotě původu však mohou pomoci. Zajištění jejich právního významu by jistě přispěla vnitrostátní implementace nařízení, byť by se právně omezovala jen na právní řád členského státu.

Ještě jinou otázkou je, zda soukromý subjekt vůbec je povinen přijímat a potažmo uznávat písemnosti od subjektů veřejného sektoru v elektronické podobě. Nařízení eIDAS žádnou takovou povinnost nestanoví. Takovou povinnost snad může uložit některé vnitrostátní právo pro některé případy,[189] popř. i unijní právo pro některé

vzniknou služby překladu a následně právní úpravy uznávání, které budou flexibilnější, než je současná právní praxe.

[189] V ČR je mnoho druhů právnických osob povinno být vybaveny datovou schránkou a přes ni přijímat písemnosti doručované veřejnou správou aj. státními subjekty.

případy, obecně uložitelná však podle autora není, neboť bezpochyby existuje a bude existovat množství soukromých subjektů, zejména fyzických osob, které elektronickými prostředky nevládnou vůbec nebo jimi nevládnou dostatečně jistě, aby byly schopny ověřovat jejich pravost. Zábranu obecného ukládání povinnosti přijímat písemnosti v elektronické podobě je pak třeba hledat v rámci ochrany lidských práv, platných ať již z hlediska práva členských států, nebo z hlediska práva unijního.

Dokonce i tehdy, pokud soukromý subjekt běžně elektronické písemnosti přijímá, mělo by být spíše vždy na něm a na jeho uvážení, zda se mu jeví dostatečně průkazné pro ten účel, který potřebuje. Výjimkou z toho jsou výše zmíněné veřejné listiny v elektronické podobě vystavené podle práva členského státu, jemuž běžně podléhá, nicméně i v jejich případě lze mít někdy pochybnosti o tom, zda jsou pravé, popř. zda mají všechny náležitosti, které daný druh veřejné listiny má mít, a zda netrpí nějakou vadou. Kupříkladu nepravá, nebo chybně potvrzená, veřejná listina presumpci správnosti pochopitelně nezakládá. Posuzování těchto situací může být ale složitější, druhy vad listin mohou být různé a způsob řešení se může stát od státu právně lišit.

6.15 Důkazní účinky

Nařízení eIDAS obsahuje v některých případech i stanovení důkazních účinků. Ta se vesměs nalézají v článcích, které jsou nadepsané jako *„Právní účinky..."*, byť ne všechna ustanovení v těchto článcích jsou skutečně vždy důkazními pravidly.

Obecně by struktura právního předpisu, jako je nařízení eIDAS, měla být taková, že se nejprve stanoví požadavky na určitý digitální objekt nebo na technický prostředek. V další části by měl být stanoven procesní způsob, jakým způsobem se ověří, že určitý digitální objekt nebo technický prostředek odpovídá těmto požadavkům. Až následně pak právní předpis případně může stanovit důkazní účinky, tj. právní pravidla pro dokazování, která se uplatní při existenci ověřeného digitálního objektu nebo technického prostředku.

Nařízení eIDAS tuto logiku sleduje, nicméně některá jeho ustanovení působí z hlediska právě uvedené metodiky rozostřeně. Například pravidla pro uznávání QSCD nejsou stanovena zcela zřejmě, ověřování platnosti QES není výslovně přikázáno apod. Některá ustanovení též mohou působit tak, že se mohou používat nejen jako požadavek, ale i deduktivně. Například článek 36 odst. d) eIDAS na zaručení integrity dat

opatřených zaručenou elektronickou pečetí může někdo vykládat i tak, že je-li pak někde přítomna zaručená elektronická pečeť, plyne z toho samozřejmě i integrita dat.

Důkazní domněnka integrity dat podle čl. 35 odst. 2 eIDAS v případě kvalifikované elektronické pečeti se pak může jevit skoro až nadbytečně. Není tomu tak. Důkazní domněnka se použije přímo na základě doložení existence kvalifikované elektronické pečetě na základě čl. 35 odst. 2 eIDAS.

Dokazování tvrzení pomocí odkazu na požadovanou vlastnost podle čl. 36 odst. d) eIDAS by sice též přicházelo do úvahy, ale zatěžovalo by dokazující stranu ohledně toho, zda v existujícím digitálním objektu je taková vlastnost nutně přítomna, a mohlo by to být předmětem četných zpochybnění. Například domněnka z čl. 35 odst. 2 eIDAS integritu váže přímo i k původu, což jen z dílčího ustanovení čl. 36 odst. d) eIDAS neplyne.

Jak upozorňuje Jandt: „Soudní dvůr v případě domněnek vychází, stejně jako národní důkazní pravidla, z toho, že odpůrce důkazu může vyvrátit domněnkou dokázaný skutkový stav důkazem opaku.“[190] Jandt souhlasí, že pro elektronický právní styk je vytvoření silných důkazních prostředků žádoucí, aby se mohla vytvořit důvěra v elektronické obchodování apod. Podotýká však, že: „Obecně je ale otázkou, zda za důkazní domněnkou stojící technické bezpečnostní nástroje jsou dostatečné k tomu, aby takové právní účinky na sebe vázaly.“[191] Při hodnocení nařízení jako právního předpisu Jandt tedy zpochybňuje, zda v něm právní ustanovení na požadavky a ustanovení na ověření požadavků jsou dostatečná, aby ospravedlňovala ustanovení důkazní. Hledá kongruenci a nenachází ji. Jandt pak vykládá jednotlivé případy z eIDAS v kontextu německého důkazního práva z civilního procesu a dochází již k výše citovaným pochybám (srov. 6.2.1) a k závěru, že se jedná o „evropskou harmonizaci od ruky“.[192]

Snad nejvíce kritické hodnocení měl Roßnagel ještě k návrhu nařízení od Komise: „Zavádí důkazní domněnky, aniž by pro domněnky stanovilo základy.“[193] Ačkoli některé nejvíce nepodložené úpravy (například důkazní domněnky o elektronickém dokumentu) byly z návrhu vypuštěny, návrh Komise prošel legislativním procesem v zásadě bez podstatných koncepčních změn. Není proto divu,

[190] JANDT, S., cit. dílo, s. 1206. Odkazuje též na rozsudek C-10/55 z 12. 12. 1956.
[191] JANDT, S., cit. dílo, s. 1206.
[192] Tj. nepromyšlenou, nedbalou, odbytou *(„Europäische Harmonisierung mit Augenmaß?“)*. JANDT, S., cit. dílo, s. 1210.
[193] ROSSNAGEL, A. Rechtsetzung zu Sicherheitsdiensten : Europäisierung ja, Monopolisierung nein! *Multimedia und Recht*. 2012, s. 781–782, s. 782.

že se postoj Roßnagela k výslednému nařízení příliš nezměnil. Ve svém článku[194] hodnotícím důkazní vliv eIDAS na německé právo z roku 2016 o nich hovoří jako „domněnkách" a navrhuje, že není nezbytně nutné, aby tento pojem unijního práva byl vykládán tak, jak je běžně vykládán pojem *právní domněnka* v právu německém. Dovozuje, že unijní akt se pochopitelně nemůže jednotně přizpůsobit důkazním systémům všech 28 členských států a jejich terminologii. Podle něj je třeba „se ptát na základě systematiky a stanovení cílů unijního práva, co určité nařízení použitím určitého označení chtělo sledovat".[195] Z disproporce mezi základy a domněnkami v eIDAS potom vyvozuje, že například „v případě aplikace čl. 35 odst. 2 [eIDAS] musí být v německém důkazním právu pojmu ‚domněnka' [z eIDAS] rozuměno jinak než věcně odpovídající ‚zákonné domněnce' podle § 292 ZPO".[196] Na závěr shrnuje: „Příspěvek ukazuje, že rozpory mezi nařízením eIDAS a ZPO se mohou snížit nebo odstranit, pokud by se ‚domněnky' z nařízení eIDAS vykládaly jako důkazy prvního dojmu [*Anscheinsbeweise*[197]], které lze vyvrátit odporujícími skutečnostmi, které zakládají vážnou pochybnost o oprávněnosti dojmu."[198] Jinak řečeno, taková domněnka představuje důkaz, k jeho vyvrácení však dostačuje otřást jím do úrovně vážných pochyb a není třeba podávat důkaz opaku. Dle něj takový výklad neodporuje ani systematice, ani cílům nařízení eIDAS. Apeluje pak na německého zákonodárce, aby v připravovaném implementačně-přizpůsobovacím zákonu z důvodu právní jistoty jasně vyjádřil, že se domněnky z eIDAS mají vykládat jako důkazy prvního dojmu *(prima facie*, *Anscheinsbeweis)*. Ve prospěch této teze by mohlo hovořit i to, že během legislativního procesu zákonodárce vypustil z návrhu Komise před slovem domněnka přídavné jméno „právní" *(„legal")*. Obraty „platí právní domněnka" *(„shall enjoy a legal presumption of")* jsou zkráceny na „platí domněnka" *(„shall enjoy the presumption of")*.

V této kapitole vykládáme nařízení eIDAS jako právní předpis práva EU. Autor souhlasí s Roßnagelem, že by bylo věcně a z hlediska spravedlnosti vhodnější, aby domněnky z eIDAS mohly být vyvráceny i nižší úrovní protidůkazu, než je důkaz opaku. V praxi bude záležet na soudech členských států, popř. i na Soudním dvoru, jakým způsobem k výkladu domněnek v nařízení eIDAS přistoupí. Při napadání

[194] ROSSNAGEL, A. Beweiswirkungen elektronischer Vertrauensdienste Neue Regelungen durch die eIDAS-Verordnung der Europäischen Union. *Multimedia und Recht*. 2016, s. 647–652.
[195] ROSSNAGEL, A. Beweiswirkungen elektronischer Vertrauensdienste, cit. dílo, Část IV.3.
[196] ROSSNAGEL, A. Beweiswirkungen..., cit. dílo, Část IV.3. Doplnil autor.
[197] *Anscheinsbeweis* je pojem německého práva a bývá do češtiny překládán i jako *důkaz prima facie*.
[198] ROSSNAGEL, A. Beweiswirkungen..., cit. dílo, Část VI. Doplnil autor.

běžného výkladu, tj. ve smyslu právní domněnky, se lze odvolávat i na podkladové hodnoty a principy, které by měly být vlastní každému právnímu řádu, tj. zejména na zásady právního státu, právní jistoty apod.

Vzhledem k tomu, že problematika důkazních účinků je mimořádně významná, jsou v této části probrány stručně i důkazní účinky jiných digitálních objektů, než je pouze kvalifikovaný elektronický podpis. Jistá disproporce totiž vychází najevo již i jen ze srovnání jejich různých důkazních účinků navzájem.

6.15.1 Obecná důkazní přípustnost a zákaz upírání právních účinků

Z nařízení eIDAS lze vyčíst, že podle čl. 25 odst. 1, čl. 35 odst. 1, čl. 41 odst. 1, čl. 43 odst. 1 a čl. 46 elektronickému podpisu, elektronické pečeti, elektronickému časovému razítku, datům odeslaným a přijatým prostřednictvím služby elektronického doporučeného doručování, elektronickému dokumentu *„nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu"* nebo z toho důvodu, že nesplňuje požadavky na svou kvalifikovanou verzi.[199]

Uvedená pravidla mají jen malý význam. V zemích a řízeních s volným hodnocením důkazů je přikázaná důkazní přípustnost již součástí důkazního práva. Důkaz lze odmítnout z jiných důvodů, nemůže-li například nijak sloužit pro dokázání tvrzené skutečnosti. I pokud je daný digitální objekt připuštěn jako důkaz, uvedená pravidla neznamenají, že bude z hlediska posuzování skutkového stavu brán jako něco dokazující. Úroveň jeho věrohodnosti, míry přesvědčivosti apod. není stanovena.

Odmítnutí právních účinků pak přichází do úvahy vždy tehdy, jestliže rozhodné právo buď nepřipouští elektronickou formu transakce vůbec, anebo pro elektronickou formu přikazuje pro vyslovení právních účinků použití určité formy těchto digitálních objektů, která není dodržena. Digitální objekt pak může být neplatný nebo je zatížen jinou vadou, pro kterou vzniknou jiné právní účinky než kupříkladu očekávané tím, kdo se digitálního objektu dovolává ve svůj prospěch. Příkaz práva na formu se může týkat jak míry zajištění bezpečnosti, tak ale například i jen formátů dat. Shodně např. Dumortier považuje[200] ustanovení tohoto druhu jen za obecnou „nediskriminaci" elektronické formy a s malým významem.

[199] Z výčtu uvedených digitálních objektů nařízení eIDAS neupravuje kvalifikovanou verzi v případě elektronického dokumentu.

[200] Dumortier in J. LODDER, A. R. – MURRAY, A. D. (eds)., cit. dílo, s. 282.

6.15.2 Objektivita existence digitálních objektů

Jednou z potíží výkladu nařízení eIDAS je, jak zacházet se zněním některých ustanovení, která se zdají jasná na první pohled, na druhý však vyvolávají pochyby. Jandt kupříkladu namítá: „Právní domněnky budou, jak se zdá, přijímány v jednotlivých případech bez přezkoušení aktuální platnosti kvalifikovaných bezpečnostních prvků.“ Jandt zde naráží třeba na formulaci ustanovení čl. 35 odst. 2 eIDAS, tj. zápis (i): *„U kvalifikované elektronické pečeti platí domněnka integrity dat a správnosti původu těch dat, s nimiž je kvalifikovaná elektronická pečeť spojena."* Nařízení eIDAS je zde, ale i jinde, formulováno tak, jako by existence kvalifikované elektronické pečeti i jejího spojení s daty byly samozřejmé. Na obdobný problém dříve upozorňoval již i Reed ve vztahu k DirES: „Problém se směrnicí o elektronickém podpisu je, že její zdánlivě objektivní testy nejsou objektivní.“[201] Zde citované ustanovení (ale i jiné v DirES i v eIDAS) je napsáno tak, jako by existoval nadpřirozený subjekt, nadaný bystrozrakostí prohlédnout předložená data a s jistotou v nich určit přítomnost kvalifikované elektronické pečeti a jejího spojení k datům. Že je situace komplikovanější, plyne již ze systematického přihlédnutí k čl. 32 odst. 1 písm. b) eIDAS, kde se vyžaduje pro možnost ověření platnosti kvalifikovaného elektronického podpisu (podobně pro kvalifikovanou elektronickou pečeť) platnost kvalifikovaného certifikátu v okamžiku podpisu (vytváření pečeti). Má se tedy číst výše uvedené ustanovení tak, jako by norma byla zapsána (ii): *„U kvalifikované elektronické pečeti,* ***která byla vytvořena v okamžiku, kdy kvalifikovaný certifikát, na němž je založena, byl platný****, platí domněnka integrity dat a správnosti původu těch dat, s nimiž je kvalifikovaná elektronická pečeť spojena"*(zvýrazněný text přidal autor)? Nároky na náš nadpřirozený subjekt se zvyšují, neboť musí být omniprezentní v místech i časech, aby byl schopen kontrolovat platnost certifikátů u pečetících osob a vést tuto informaci ve své patrnosti pro případ budoucích dotazů. Požadavků na ověření platnosti je však v čl. 32 odst. 1 eIDAS dlouhá řada. Má se tedy výše uvedené ustanovení číst tak, jako by norma byla zapsána (iii): *„U kvalifikované elektronické pečeti,* ***s ověřenou platností****, platí domněnka integrity dat a správnosti původu těch dat, s nimiž je kvalifikovaná elektronická pečeť spojena"* (zvýrazněný text přidal autor)? Autor je zde názoru, že právě toto čtení výkladu je ze všech tří nejvhodnější.

[201] REED, C., cit. dílo, s. 11.

Výše fingovaná nadpřirozená bytost k dispozici pochopitelně není. Jedinou možností, jak interpretovat zápis (i) v nařízení s přihlédnutím k potřebě jeho objektivizace, je, že nařízení někde jinde v rámci systematického výkladu objektivně určuje pro každého, jak se má z předložených dat rozpoznat, že obsahují určitý digitální objekt, o němž nařízení eIDAS pojmově pojednává. Směrnice DirES skutečně sama o sobě neposkytovala v tomto ohledu dostatek systematicky doplňujících ustanovení, a proto by, jen v případě aplikace samotné DirES, skutečně byl nutný postup Reeda citovaný výše (6.11.3).

V případě nařízení eIDAS je situace značně lepší. Předně si rozlišme, že pro možnost objektivizace existence digitálního objektu musí existovat dva základní předpoklady, které mají odlišný charakter. První nezbytností je, že digitální objekt existuje ve **formátu dat**, který je ověřujícím očekáván, ideálně na základě právního předpisu.[202] Druhou nutností je znát stanovený postup, který umožňuje **ověřit platnost** digitálního objektu.

Ohledně formátu dat obsahu vyhlásila Komise formáty podle čl. 27 odst. 5 eIDAS (srov. 6.14.2). I když jsou povinné pouze pro příjem subjekty veřejného sektoru, není rozumný důvod, aby nebyly používány i v jiných případech. Formát vydávacích certifikátů a dalších údajů o kvalifikovaných poskytovatelích certifikačních služeb a jejich kvalifikovaných služeb Komise vydala čl. 22 odst. 5 eIDAS. Komise rovněž může vyhlásit formáty kvalifikovaných elektronických časových razítek podle čl. 42 odst. 2. eIDAS. Je-li digitální objekt ve formátu, který příjemce neumí přečíst, mohou právně vznikat různé situace. Srov např. 6.14.

Co se týče ověřování platnosti digitálních objektů, finálním účelem ve většině[203] případů je schopnost ověřit platnost zaručeného elektronického podpisu nebo zaručené elektronické pečeti. V technické a právní praxi již před eIDAS existovalo několik ověřovacích modelů. Jmenovitě řetězový model, ulitový model a hybridní model (srov. 6.11.1.3). V závislosti na tom, který z nich se používá, je zapotřebí zkoumat časy a platnosti různých dalších digitálních objektů (certifikátu podepisující nebo pečetící osoby, certifikátů poskytovatelů služeb, poskytovatelů elektronických časových razítek, tvůrců záznamů důvěryhodného seznamu...). I pro tyto další digitální objekty pochopitelně platí potřeba zjištění objektivní existence, tedy rozeznatelnosti formátu dat

[202] Mezi uzavřeným počtem účastníků lze dohodnout i zvláštní formáty digitálních objektů, nařízení eIDAS je však určeno pro elektronický styk v široce otevřených komunitách.

[203] Elektronická časová razítka lze vzácně použít i mimo kontext elektronických podpisů.

a platnosti ověření objektu, způsob ověření platnosti je již však částečně zvenku shora dán právě použitým ověřovacím modelem.

Rozepsat tyto postupy přesně je mimo rozsah tohoto textu a vymyká se i z možností úpravy v právním předpise, jako je i nařízení eIDAS. Správným zdrojem pro jejich zápis je technická specifikace, popř. technická norma. V právním předpise jako eIDAS by však měly být stanoveny aspoň hlavní zásady, které se pro ověření mají použít. Nařízení eIDAS obsahuje explicitně požadavky pro ověřování platnosti pouze pro případ kvalifikovaných elektronických podpisů v čl. 32, který se přiměřeně podobně má použít i pro kvalifikované elektronické pečetě (čl. 40). Na základě čl. 32 odst. 1 písm. b) eIDAS se např. Roßnagel domnívá, že eIDAS uplatňuje řetězový model. Dle autora není však vyloučeno ani to, že se má uplatňovat hybridní model.

Jak autor uvádí v 6.11.1.1, používají se v rámci postupu ověření platnosti v praxi PKI dva rozdílné kroky ověření. Prvním z nich je kryptografický výsledek operace ověření, druhým je zkoumání certifikátu a příp. jiných digitálních objektů, souvisejících s daným elektronickým podpisem, což může být předmětem oněch značně složitých výše naznačených ověřovacích modelů a postupů.[204]

Z hlediska objektivizace existence digitálního objektu je autor zcela přesvědčen, že je podmínkou nutnou, aby kryptografický výsledek operace ověření byl kladný. V postupu podle čl. 32 se jedná o podmínku dle čl. 32 odst. 1 písm. c. (srov. 6.11.2) eIDAS. Pokud výsledek této operace splněn není, pak vůbec nelze hovořit o objektivní existenci daného digitálního objektu. Namísto ověřovací kryptografické informace jsou přítomna nějaká jiná data, která rozhodně nelze považovat za právním ustanovením nařízení zmíněný právní pojem.

Komise může vyhlásit technické normy podle čl. 27 odst. 4 eIDAS. Odpovídání těmto technickým normám má zakládat domněnku vyhovění pro potřeby příjmu zaručených elektronických podpisů subjekty veřejného sektoru podle čl. 27 odst. 1 a 2 eIDAS, ale i domněnku vyhovění požadavků čl. 26 na zaručený elektronický podpis. Druhá domněnka vyhovění by zřejmě představovala i objektivizaci existence digitálního objektu. Komise však tyto technické normy zatím nevyhlásila, takže definitivní posouzení této možnosti je nutné odložit až na dobu, kdy se tak případně stane.

[204] Německý zákonodárce je v SigG dříve rozlišoval i pojmově. Pro první krok se užívalo sloveso ověřit *(prüfen)* a pro druhý krok prověřit *(nachzuprüfen)*.

Komise může též vyhlásit technické normy podle čl. 32 odst. 3 eIDAS, které by obsahovaly žádoucí přesný popis algoritmů pro ověření kvalifikovaného elektronického podpisu. Dodržení takové technické normy zakládá domněnku vyhovění ověření podle čl. 32 odst. 1 eIDAS. Do té doby autor v tomto textu vykládá ověření platnosti elektronického podpisu podle čl. 32 odst. 1 (srov. 6.11.2) jako technicky proveditelné. Vede-li výsledek k potvrzení platnosti kvalifikovaného elektronického podpisu (QES), je tím objektivně ověřena technická existence daného digitálního objektu, zde QES.[205] Právní ustanovení, která daný digitální objekt zmiňují, lze pak již vykládat tak, jako by jejich přítomnost byla objektivně daná.[206]

Ani to však neznamená, že jsme se přiblížili objektivitě nadpřirozeného subjektu úplně. Technicky platný digitální objekt neznamená zcela nutně, že se jedná o pravý digitální objekt. Pravý v tom smyslu, že jej původce digitálního objektu vytvořit chtěl, a to se chtěným obsahem. Námitky tohoto druhu vůči objektivitě mohou být různorodé, bude se jednat o různé druhy popření původnosti, tedy falešnosti. Některé z nich popisujeme níže.

Postupy ověření jiných digitálních objektů nařízení eIDAS neuvádí. Zákonodárce se buď spoléhá na to, že postup ověření je technicky samozřejmý, popř. že technické algoritmy pro jejich ověřování budou například stanoveny v rámci technických norem, k jejichž vyhlášení Komise zmocněna je.

Opačnou potíží může být, že postup ověření (např. podle čl. 32 odst. 1 eIDAS) vyhoví ve značném množství kritérií, některé však selžou, resp. budou nerozhodné. Rovněž technické specifikace s ověřovacími algoritmy jsou někdy koncipovány tak, že na otázku platnosti poskytují tři odpovědi: ano, ne a možná (nelze rozhodnout). Důvodem nerozhodnosti bývá zejména situace, když se ověření provádí až po čase a některý certifikát expiroval, aniž by podpis byl časově zafixován elektronickým časovým razítkem. Zda přijímající subjekt nebo soudce v řízení bude poté považovat daný digitální objekt za objektivně existující, je otázkou jeho posouzení.

Souhrnně na hlavní otázku této části, totiž zde se *má provádět ověřování platnosti digitálních objektů*, aniž to je v ustanoveních nařízení eIDAS výslovně zmíněno, autor zodpovídá, že *zásadně ano*. Důvodem mu je, že jinak nelze právní ustanovení z eIDAS vůbec používat, neboť není nijak jisté, že dané digitální objekty

[205] Přiměřeně podobně i kvalifikované elektronické pečeti.

[206] Byť nelze zcela vyloučit, že některá strana sporu splnění některého kritéria vyloženého (např. autorem) jen čistě na základě ustanovení čl. 32 odst. 1 eIDAS zpochybní.

existují objektivně. Objektivita zjištění existence je sice omezená na technickou platnost, více je však bez dalšího již z hlediska příjemce nedosažitelné. Z ověření platnosti kryptografické operace autor nepřipouští výjimky vůbec. Možné výjimky nebo omezení z dalšího ověřitelnosti platnosti jsou zmíněny výše, z hlediska právní jistoty ale nejsou žádoucí. Pro spoléhající se osobu je nejjistější úplné kladné ověření platnosti.

Důvody, proč podmínku ověření platnosti zákonodárce v eIDAS neuvádí, jsou zřejmě několikeré. První důvod je, že znění ustanovení by se stalo zcela nepřehledným. Druhým důvodem je, že při zápisu všech podmínek objektivizace existence by mohlo dojít k omylu, popř. by se nároky na ně mohly v čase měnit. Novelizovat legislativní akt úrovně evropského nařízení je ale velmi pomalý proces. Vhodnější metodou proto je takové podmínky přesunout až do prováděcích aktů nebo do technických norem. Třetím důvodem konečně je, že zápis právních předpisů v objektivním modu a pohled na právo přes objektivní modalitu jsou běžné.[207] Zvláštností v nařízení eIDAS však je, že užívá mnohé pojmy, zejména pro digitální objekty, u kterých používané druhy techniky založené na PKI, které je skutkově představují, umožňují provádět zneplatnění. Mnoho digitálních objektů tak ve skutkové rovině sice může existovat, ale pro zjištění jejich platnosti či eventuální neplatnosti je přesto zapotřebí provést určité dodatečné kontroly, které musí brát do úvahy i jiné okolnosti a informace, než které poskytuje jen samotný digitální objekt. To v jiných právních předpisech běžné není.

Další specifikou nařízení eIDAS je, že mnoho ustanovení představuje pouhé definice či explikace, které jsou formálně závazné, samy ale právními normami nejsou, avšak „normativně působí ve vazbě na právní normy".[208] Konečně, v mnoha jiných právních předpisech pak pojmy vyjadřující složitou skutkovou situaci, lidskými smysly přímo nepřístupnou, se sice mohou vyskytovat, avšak k jejich zkoumání se přistupuje pouze v případě sporu, například znaleckým posudkem. Z povahy nařízení eIDAS, které má sloužit pro elektronické transakce, pro intenzivní právní styk, naopak plyne, že je třeba mít k dispozici rychlou a levnou technickou možnost určení platnosti, potřeba jasné a schůdné metody objektivizace existence je mnohem naléhavější.

Pro právo pak situace, kdy právní norma, definice či explikace není zcela totožná s textem právního předpisu, není nijak mimořádná. Naopak se připouští, že jako

[207] GERLOCH, A. *Teorie práva*. 3., rozšířené vydání, Aleš Čeněk: Plzeň, 2004. s. 31.
[208] GERLOCH, A., cit. dílo, 2004, s. 33.

součást právního vědomí může často „být a je konkrétnější a bohatší“,[209] zejména v důsledku relevantního právního výkladu.

6.15.3 Elektronický podpis prostý

Podle čl. 25 odst. 1 eIDAS nesmí být elektronickému podpisu (tj. i prostému nebo zaručenému) upírány právní účinky a nesmí být upírán jako důkaz v soudním nebo správním řízení pouze z toho důvodu, že *„má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické podpisy"*.

Tento požadavek nepředstavuje vysokou laťku a v právních řádech členských států by již dříve měl existovat s ohledem na povinnou transpozici čl. 5 odst. 2 DirES, byť zde byla užita náročnější definice elektronického podpisu (prostého) s požadavkem autentizace. Byl také samozřejmý v členských státech, které v uvedených řízeních připouštěly zásadu volného hodnocení důkazů. Nyní požadavek platí jako přímo aplikovatelná právní norma evropského nařízení a má přednost před případně odlišnou právní úpravou členského státu. Uvedené je důležité i z hlediska nově širokého uplatnění elektronického podpisu prostého pro různé druhy techniky (srov. 4.5).

V rámci volného hodnocení důkazů nicméně nemusí elektronický podpis, jehož platnost, pravost či vztah k jím podepsaným datům jsou nepřesvědčivé, být správním úřadem nebo soudem posouzen jako osvědčující sporné skutečnosti.

Obdobně může členský stát zde nařízení *implementovat* podle bodu odůvodnění 49, že *„právní účinky elektronických podpisů v členských státech by ... měly být vymezeny vnitrostátním právem, s výjimkou požadavků stanovených v tomto nařízení."* Členský stát tedy může důkazní účinky elektronických podpisů (prostých) upravit v rámci důkazních pravidel svého právního řádu, zejména pokud má zaveden nějaký systém hodnocení pro dokazování v rámci svých procesních předpisů. V těchto pravidlech je omezen pouze tím, že nesmí důkaz znemožňovat jen na základě elektronické podoby nebo toho, že se nejedná o kvalifikovaný elektronický podpis.

Zde uvedené důkazní pravidlo se nedotýká toho, že pro určité druhy právního jednání může právní řád členského státu stanovit určité požadavky na jeho formu, včetně úrovní zajištění elektronického podpisu. Splnění těchto požadavků se hodnotí nezávisle na důkazní přesvědčivosti a přípustnosti, zde diskutované. Právní následky

[209] BOGUSZAK, J. – ČAPEK, J. – GERLOCH, A. *Teorie práva*. 2., přeprac. vydání. Praha: ASPI Publishing, 2004, s. 82.

nesplnění formy mohou být různé (např. neplatnost, jednostranná neplatnost, různé druhy omezení účinku, možnosti zhojení...) a je třeba je dohledat v právním řádu členského státu, který je rozhodný pro danou elektronickou transakci.

6.15.4 Zaručený elektronický podpis

Pro zaručený elektronický podpis platí podle nařízení eIDAS zcela stejný důkazní účinek jako pro elektronický podpis prostý výše, podle stejného ustanovení čl. 25 odst. 1 eIDAS. Toto právní zjištění se zdá paradoxní, neboť nařízení stanoví pro zaručený elektronický podpis mnohem více požadavků. Tento právní stav, jemuž by následně měl odpovídat i stav faktický, by zřejmě reflektoval až správní úřad nebo soud v rámci skutkových otázek, tj. v rámci posouzení toho, že zaručený elektronický podpis běžně poskytuje mnohem vyšší míru přesvědčivosti. Stejná důkazní pravidla v nařízení eIDAS přesto mohou vést k flexibilním výsledkům hodnocení skutkového stavu.

Lepší důkazní situaci zaručeného elektronického podpisu může stanovit členský stát v rámci své vnitrostátní implementace. Měl by přitom zřejmě pouze respektovat určitou hierarchii v účincích mezi jednotlivými druhy elektronických podpisů.

Reálnou potíží, na kterou může narazit spoléhající se osoba, je, že pro ni nemusí být vůbec jednoduché prokázat, že elektronický podpis, kterého se dovolává a který předkládá, je zaručeným elektronickým podpisem. Kupříkladu ani z kvalifikovaného certifikátu pro elektronický podpis neplyne, že v něm certifikovaná podepisující osoba vytvořila elektronický podpis v souladu se čtyřmi požadavky písm. a) až d) článku 26 eIDAS, tj. že např. podle písm. c) data pro vytváření podpisu podepisující osoba mohla *„s vysokou úrovní důvěry použít pod svou výhradní kontrolou"*. V tomto kontextu je stále platná kritika[210] Reeda. Ani z odpovídání vyhlášeným technickým normám pro formáty zaručeného elektronického podpisu dle čl. 27 odst. 5 eIDAS dle autora bez dalšího neplyne, že se jedná o zaručený elektronický podpis.

Prováděcí akt podle čl. 27 odst. 4 eIDAS by měl tuto nejistotu spoléhající se osoby podstatně zmírnit a zlepšit její důkazní postavení, Komise jej však dosud nevydala a technické normy tak nevyhlásila. Odpovídání těmto normám by zakládalo i domněnku vyhovění požadavkům na zaručený elektronický podpis podle čl. 26 eIDAS. Dosud není zřejmé, zda se bude jednat jen o technické normy týkající se zajištění míry bezpečnosti anebo i postupu ověřování platnosti.

[210] REED, CH., cit. dílo,

Za dosud existující situace může průkaz o použití zaručených elektronických podpisů ještě vyplývat buď ze vzájemného smluvního ujednání obou stran, anebo z certifikační politiky poskytovatele, který vydal kvalifikovaný certifikát pro elektronický podpis a potvrzuje vůči všem třetím stranám, že žadatelé o certifikát jsou zavázáni používat zaručený elektronický podpis. Důkazní přesvědčivost těchto ujednání nebo prohlášení poskytovatele bude záviset na pečlivosti jejich sepsání i zajištění jejich provedení v praxi a na konečném posouzení soudcem.

Znovu upozorněme, že samo nařízení eIDAS z hlediska důkazních účinků pro zaručený elektronický podpis žádné odlišné pravidlo, než platí pro elektronický podpis prostý, nestanoví a důkazní přesvědčivost je především záležitostí schopnosti dokázat faktickou bezpečnost postupů, s nimiž byl daný druh elektronického podpisu vytvořen. Jiné důkazní pravidlo pro zaručený elektronický podpis může být jen součástí práva členského státu, pokud jej vytvoří v rámci své implementace nařízení podle bodu odůvodnění článku 49 eIDAS.

Dále též upozorněme, že skutečná realizace zaručeného elektronického podpisu může být jak na průměrné bezpečnostní výši, tak ale i může být bezpečnostně značně vysoká. Může být fakticky i vyšší, než je jiná realizace, která formálně splňuje třeba i kritéria kvalifikovaného elektronického podpisu. Pro určité srovnání též připomeňme, že v ČR byl v období let 2002–2016 jako vrchol druhů elektronických podpisů používán tzv. *uznávaný elektronický podpis*, požadavky na nějž v zásadě odpovídaly právě zaručenému elektronickém podpisu z eIDAS.

6.15.5 Zaručený elektronický podpis kvalifikovaných poskytovatelů

V současnosti je bez dalšího uspokojivá situace s prokazováním použití zaručených elektronických podpisů, resp. zaručených elektronických pečetí, které pocházejí od kvalifikovaných poskytovatelů služeb vytvářejících důvěru, již jsou zapsáni v důvěryhodných seznamech, a které vytvořili v rámci svých kvalifikovaných služeb vytvářejících důvěru, rovněž zapsaných v důvěryhodných seznamech.

Takoví kvalifikovaní poskytovatelé se totiž museli již předběžně podrobit auditu, jehož účelem je podle čl. 20 odst. 1 eIDAS *„potvrzení toho, že kvalifikovaní poskytovatelé služeb vytvářejících důvěru i jimi poskytované kvalifikované služby vytvářející důvěru splňují požadavky stanovené v tomto nařízení"*. Mezi podmínky nařízení spadá i požadavek na vytváření zaručených elektronických podpisů (pečetí),

jimiž se potvrzují četné kvalifikované služby vytvářející důvěru. Výsledná zpráva o posouzení shody by tedy měla hodnotit i tuto skutečnost. Orgán dohledu ověří zprávu (čl. 21 odst. 2 eIDAS) popř. i jinak, že poskytovatel *splňuje požadavky nařízení*. Na základě úspěšného ověření rozhodne o udělení statusu kvalifikovaného poskytovatele a statusu kvalifikované služby vytvářející důvěru (čl. 21 odst. 2 alinea 2 eIDAS) a následně požádá subjekt odpovědný za důvěryhodný seznam, aby na něj poskytovatele a jím poskytovanou službu uvedl. Pro právní význam uvedení v důvěryhodném seznamu podrobněji viz 6.9.3. Prokáže-li se přesto, že elektronické podpisy nebo elektronické pečetě kvalifkovaného poskytovatele nejsou zaručené, lze pak po kvalifikovaném poskytovateli vymáhat náhradu škody dle čl. 13 eIDAS.

6.15.6 Kvalifikovaný elektronický podpis (QES)

Kvalifikovaný elektronický podpis má dle eIDAS jen stejné důkazní účinky, jako má elektronický podpis prostý nebo zaručený, uvedené výše (srov též 6.15.1). Snadnější než u jiných druhů elektronických podpisů bude dokázat jeho platnost, neboť nařízení postup výslovně upravuje v čl. 32 (srov 6.11.2).

Nařízení eIDAS však neobsahuje právní domněnku projevu vůle podepsané osoby v podepsaném obsahu (podepsaných datech), a to ani v případě kvalifikovaného elektronického podpisu. Nařízení obsahuje pouze čl. 25 odst. 2 eIDAS: *„Kvalifikovaný elektronický podpis má právní účinek rovnocenný vlastnoručnímu podpisu."* Toto pravidlo dle názoru autora nemá důkazní účinek, ale mělo by sloužit pouze k posouzení vyhovění požadavkům na přítomnost podpisu. Srov. 6.5.3. Důvodem pro tuto úvahu je, že v jiných případech, například v čl. 35 odst. 2 eIDAS pro elektronickou pečeť, nařízení výslovně důkazní účinek stanoví. Dalším důvodem je vypuštění právě této autentizační domněnky vůči elektronickému dokumentu během legislativního procesu přijímání nařízení (srov. 6.15.11). Konečně lze namítat, že v nařízení eIDAS nejsou stanoveny dostatečné požadavky na to, aby takovou domněnku bylo možné považovat za podloženou (srov též 6.16.1, 6.16.2 a 6.16.3). Shodně důkazní účinek dle čl. 25 odst. 2 eIDAS odmítá např. Roßnagel: „Zvláštní důkazní pravidla však nařízení eIDAS pro kvalifikovaný elektronický podpis neobsahuje."[211] K tomuto výkladu se přiklonil i německý zákonodárce, když v rámci implementace nařízení eIDAS stanovil u soukromých listin důkazní význam QES ve svém vnitrostátním právo, konkrétně v § 371a odst. 1 ZPO (srov. 7.4).

[211] ROSSNAGEL, A. Beweiswirkungen..., cit. dílo, s. 648.

V případě běžné papírové listiny a vlastnoručního podpisu vnímá podepisující osoba svými smysly listinu a její obsah bezprostředně, stejně jako svou vůlí ovládá pero, jímž podepisuje a svými smysly opět přímo ověřuje, že se vytvářený podpis nachází na té listině, kterou chce podepsat. V případě elektronického podpisu jsou však všechny součásti pouze prostředkovány elektronickými prostředky.

Domněnku projevu vůle v podepsaném obsahu by mohlo stanovit vnitrostátní právo nebo judikatura jeho soudů. Je-li právní domněnka projevu vůle v některém státu čistě právním obyčejem (srov. 4.1) pro vlastnoruční podpis, jak tomu bylo například v ČR před přijetím občanského zákoníku č. 89/2012 Sb., mohou být osoby z dané jurisdikce v pokušení uplatnit ji i v případě kvalifikovaného elektronického podpisu. Obdobně takové pokušení vzniká i v případě, je-li domněnka projevu vůle součástí důkazního práva. Jak je již výše uvedeno, autor se domnívá, že v případě kvalifikovaného elektronického podpisu, jen na základě eIDAS, by se tato právní domněnka bez dalšího ve vnitrostátním právu uplatňovat neměla.

Právní domněnku projevu vůle v obsahu podepsaném kvalifikovaným elektronickým podpisem by vnitrostátní právo stanovit mohlo. Podle názoru autora však pouze tehdy, pokud nařízení eIDAS současně doplní dalšími implementačními požadavky, které důsledně pokryjí i vlastnosti na aplikaci vytvářející elektronický podpis, popř. požadavky na systémové prostředí, aby bylo zajištěno, že aplikace předkládají podepisující osobě shodný obsah, který je následně v QSCD podepsán, anebo je-li vytváření QES dávkové nebo automatické, že jsou splněny všechny podmínky pro to, aby podepisující osoba byla schopna jistě ovládat, jaké obsahy (data) jí budou elektronicky podepisovány. Vyloučeno není ani stanovení zvláštních požadavků na QSCD, které třeba vyloučí vytváření podpisů QES na dálku apod.

Současně však uveďme, že bez dalšího je opravdový projev vůle v obsahu podepsaném QES velmi pravděpodobný a v běžném styku jej spoléhající se osoba zřejmě bude předpokládat. Je též důkazně z hlediska posuzování skutkového stavu významně více přesvědčivý, než je jen elektronický podpis prostý.[212]

Důvodem proti zavedení právní domněnky je spíše to, že dojde-li ke sporu, může být již četnost správnosti této domněnky problematická. Dalším důvodem proti

[212] Dumortier je k nařízení eIDAS obecně kritický v tom smyslu, že poukazuje na to, že se v obchodním styku vyvinula pro elektronické transakce jiná praxe, a obává se, aby se uživatelé nepodřizovali podmínkám nařízení eIDAS zbytečně. In DUMORTIER, J. *Regulation (EU)...,* cit. dílo, s. 288–289.

této domněnce je i to, že není realistické předpokládat, že podepisující osoba má prakticky vůbec možnost provést důkaz opaku a tím domněnku vyvrátit.

Vnitrostátní právo může též již historicky obsahovat presumpci správnosti obsahu (podepsaných dat) v případech veřejných listin. Je pak v nejvlastnějším zájmu takového členského státu, aby ve své implementaci eIDAS upravil podmínky pro vytváření kvalifikovaných elektronických podpisů nebo kvalifikovaných elektronických pečetí tak, aby u jeho subjektů veřejného sektoru nebo orgánů veřejné moci nehrozilo, že dojde k falšování obsahu. Takové podmínky se mohou týkat jak výše zmíněných aplikací pro vytváření elektronických podpisů, systémového prostředí. Nejméně stejně významné pak budou i právní pravidla na navazující informační systémy, jakými typicky budou systémy spisové služby, na ně navazující střednědobá (do 10 let) a případně i dlouhodobá archivace elektronických spisů nebo dokumentů.

6.15.7 Možnosti technických útoků na kvalifikovaný elektronický podpis

V této části je stručný výčet možných útoků na kvalifikovaný elektronický podpis. Zařazení této části zde má ten účel, aby si i právní čtenáři uvědomili, jakými zhruba možnostmi může dojít k napadení. Ve všech případech úspěšného útoku bude výsledek ověření platnosti potvrzovat platnost podpisu, podpis ale nebude pravý.

I. Kompromitace soukromého klíče z QSCD

I.i Soukromý klíč kryptoanalyticky odvozen z veřejného klíče
I.ii Soukromý klíč kryptoanalyticky prolomen z QSCD
I.iii Ztráta kontroly nad soukromým klíčem (vzdálené QES)

II. Kompromitace prostředí QSCD

II.i Podsunutí obsahu v aplikaci vytvářející podpis
II.ii Podsunutí obsahu v systémovém prostředí
II.iii Ztráta kontroly nad druhým autentizačním faktorem

III. Vydání kvalifikovaného certifikátu jiné osobě

III.i Vnější útok (podvod vůči poskytovateli)
III.ii Vnitřní útok (podvod pracovníka poskytovatele)

Rozdíly mezi útoky I, II a III spočívají v tom, kde k útoku dochází. Velmi ničivé jsou útoky druhu I, zejména pokud si jich podepisující osoba není vědoma. Umožňují vytvářet libovolné množství kvalifikovaných elektronických podpisů namísto podepisující osoby. Prostředky odpovídající požadavkům na QSCD podle přílohy II eIDAS nebo podle technických norem pro certifikaci QSCD, vyhlášených Komisí, by se útokům I.i a I.ii měly bránit poměrně spolehlivě. K útoku I.ii by měla být potřebná

ztráta fyzické kontroly nad QSCD. Méně intruzivní útoky na prostředek QSCD ale nemusí být destruktivní, takže k nim může dostačovat i jen dočasná ztráta fyzické kontroly. Kvůli útokům I.ii je nicméně vhodnější, pokud je chráněna fyzická kontrola nad QSCD, což běžně zajišťuje podepisující osoba svým dohledem na čipovou kartou nebo tokenem. V případě vzdálených podpisů ji musí zabezpečovat poskytovatel.

Útok I.iii přichází do úvahy jen při vzdáleném podepisování, pokud se pro vzdálený podpis používá autentizace pouze znalostí. Zda tomu tak bude, není zatím jasné, neboť technické normy nebyly dosud vydány. Jandt se této možnosti obává.[213]

Souhrnně lze říci, že nařízení eIDAS útokům druhu I. brání, ovšem až na to, že podepisující osobě nestanoví povinnosti péče o QSCD, zejména jeho neustále fyzické kontroly. Zatím není zřejmé, jak bude bráněno útokům I.iii.

Přes používané kontrolní a certifikační postupy v oblasti zajišťování bezpečnosti produktů IT, zejména těch určených pro jádro bezpečnostních funkcí, došlo v lednu 2017 k úspěšnému nalezení zranitelnosti druhu I.i, nyní označované jako ROCA (Return of the Coppersmith Attack), českými akademiky z laboratoře CRoCS[214] na Masarykově univerzitě. Napadnutelná součást byla výpočtový knihovní modul, který je součástí čipů německého výrobce *Infineon Technologies AG* nejméně od roku 2012 a byl pravděpodobně distribuován do několika desítek milionů prodaných zařízení, z nichž některé měly i certifikace na úroveň záruk bezpečnosti CC EAL 5+ nebo NIST FIPS 140-2. Prostředky QSCD nebo dřívější SSCD se certifikují sice podle jiného bezpečnostního profilu ochrany, ale na nižší úroveň záruky bezpečnosti CC EAL 4+. Daný knihovní modul nevytvářel vždy klíčové páry s tou úrovní náhodnosti, která je potřebná. To vědcům umožnilo mnohořádově snížit počet zkoumaných klíčů, čímž se překonala teoretická „výpočtová neschůdnosť". Útok byl ihned v únoru nahlášen výrobci, aby měl čas vytvoření technické nápravy, nebo aspoň varování svých zákazníků, aby produkty stáhli z použití.

Informace o útoku přesto prosakovaly do médií postupně během roku 2017, jak jednotlivé vlády byly nuceny připustit, že i jimi distribuované čipové karty, například v rámci národních identifikačních průkazů, mohou obsahovat zranitelnost, a začaly provádět opravné postupy. Zasaženo bylo potenciálně kupř. cca 750 tisíc průkazů

[213] JANDT, S., cit. dílo, s. 1207.
[214] Centre for Research on Cryptography and Security, Fakulta informatiky, Masarykova univerzita. Dostupné z: <https://www.fi.muni.cz/research/crocs/index.xhtml.cs>; navštíveno 9/2017.

v Estonsku,[215] asi 300 tisíc osob na Slovensku.[216] Zasaženy jsou i bezpečnostní produkty jiných výrobců, kteří dané čipy přebírali do svých výrobků, včetně prvořadých značek na trhu IT. Ke zveřejnění metody došlo až 30. října 2017.[217] Podle popisu není zranitelný úplně každý klíčový pár, ale pravděpodobně jen každý desáty až dvacátý. Výzkumníci reálně identifikovali asi 750 tisíc používaných zranitelných klíčových párů, prakticky jich však bude asi třikrát více. Výskyt zranitelnosti je odhalitelný z některých znaků veřejného klíče v řádu milisekund na běžném notebooku. V závislosti na délce klíče algoritmu RSA je pak zapotřebí vynaložení určitého výpočetního času na prolomení. Na klíč RSA délky 1024 bitů jsou v nejhorším případě zapotřebí asi 3 CPU-měsíce, na klíč RSA délky 2048 bitů zhruba 140 CPU-roků. Útok však lze zcela masivně paralelizovat, potřebné prostředky si najmout v cloudu a následně se potřebný čas přemění jen na částku, kterou je třeba vynaložit. V případě útoku na klíč RSA 2048 bitů si například dostačuje pronajmout 1400 ks 4jádrových CPU, aby nejhorší čas na prolomení byl 9 dnů. Nejvyšší náklady na prolomení klíče o délce 1024 bitů jsou $76 a na klíč délky 2048 bitů částka $ 40 000, přičemž průměrně se bude jednat jen o polovinu uvedeného obnosu. Výzkumníci uvádí, že po optimalizaci bude útok pravděpodobně reálný i pro klíče RSA o délce 4096 bitů, pocházející z oné zranitelné knihovny. Zatím je však jen v řádu 10^9 roků, což zhruba odpovídá době celé historie vesmíru dle teorie velkého třesku. Výrobce pravděpodobně reagoval updatem výpočetní knihovny a možností jejího přehrání na čipu za novou verzi. Současně je nutné zneplatnit starý klíčový pár a vygenerovat nový. Je lepší, pokud takovou úpravu provádí specializované pracoviště. Situaci lze zhruba přirovnat k tomu, když po odhalení skryté závady výrobci vozidel stahují některé prodané řady do autoservisů pro servisní zásah.

Záludnost útoku I.i spočívá v tom, že v době pěti let (2012 až 2016) by zřejmě žádný odborník bezpečnosti IT nebo soudní znalec nepřipustil, že po provedení bezpečnostních certifikací by existovala realistická možnost útoku tohoto druhu na zařízení jednoho z předních výrobců prvků bezpečnosti IT, pokud by ji v případné soudní při podepisující osoba namítala. Pochopitelně nelze vyloučit, že zranitelnost

[215] Dostupné z: <https://www.ft.com/content/874359dc-925b-11e7-a9e6-11d2f0ebb7f0>; navštíveno 9/2017.

[216] Dostupné z: <http://www.ceskatelevize.cz/ct24/svet/2290126-slovaci-konci-s-rizikovymi-e-podpisy-chybu-odhalili-cesti-vedci>; navštíveno 9/2017.

[217] NEMEC, M. – SYS, M. – SVENDA, P. – KLINEC, D. – MATYAS, V. *The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli*, předpublikační verze, 2017. Dostupné z: <https://crocs.fi.muni.cz/_media/public/papers/nemec_roca_ccs17_preprint.pdf>; navštíveno 11/2017.

některé vládní agentury zjistily nezávisle, ale nehlásily ji. Stejná situace může existovat i dnes ohledně jiných bezpečnostních prvků IT.

Při útocích druhu II. útočník běžně nezíská soukromý klíč k dispozici pro vytvoření libovolného počtu podpisů, ale podvrhne falešný obsah během jednoho vytváření podpisu. Oblast těchto útoků bývá nazývána i jako prezentační problém,[218] popř. je známa jako zásada WIPIWIS.[219] Chránit zde není třeba QSCD, ale celou výpočetní platformu, v jejímž rámci se QSCD používá, tj. zejména systémové prostředí (v širším slova smyslu) a aplikaci vytvářející podpis. Pokud útočník získá možnost změnit jejich funkci, například počítačovým virem, může se mu podařit podvrhnout jiný obsah k podpisu, než který osoba má předložen. Možnost podvržení je i hlavním důvodem, proč by se podpisový klíčový pár neměl používat pro jiné účely, jako je autentizace osoby v sezení nebo šifrování obsahu.

Nebezpečí zneužití útoků druhu II. je vyšší, pokud se používají dávkové podpisy nebo zejména automatické podpisy. V takovém případě bývá autentizační informace zadána pouze jednorázově. V případě II.iii může dojít k zachycení autentizační informace (PIN, otisku prstu apod.) tak, že vytváření množství falešných podpisů je opět zcela neomezeno, aspoň dokud je QSCD připojeno. Předpokladem útoku II.iii je předchozí úspěšný útok na systémové prostředí. Útokům II.iii se čelí používáním tzv. PINPadů, tj. speciálních klávesnic, na nichž se zadává PIN před bezprostředním vytvořením elektronického podpisu na čipové kartě, vsunuté v PINPadu.

Útok druhu III. lze provést vůči jakékoli fyzické osobě, včetně takové, která prostředky IT vůbec nepoužívá. Dostačuje zfalšovat ověřovací informace, které se používají při ověřování totožnosti žadatele o certifikát. Pro předcházení útokům tohoto druhu je nutná podmínka naprosté důvěryhodnosti pracovníků poskytovatele služeb vytvářejících důvěru nebo jeho pracoviště, které ověřování provádí. Kriticky důležitý je i dohled nad poskytovatelem orgány dohledu. Obě podmínky jsou v nařízení eIDAS uvedeny, ale může být otázkou, jak dalece jsou dodržovány, zejména v rámci celé EU.

Autor upozorňuje, že provedený výčet nemusí být nutně vyčerpávající. Může docházet i ke kombinacím útoků, popř. k vytváření útoků podobných.

---

[218] JANDT, S., cit. dílo, s. 1210.

[219] What Is Presented Is What Is Signed – Co je předloženo, to je podepsáno. Někdy se namísto WIPIWIS používá zkratka WYSIWYS s významem What You See Is What You Sign, která však příliš zdůrazňuje vizuální smysl vnímání. Obecně je možné elektronicky podepsat i zvukový záznam.

Účelem této technické vsuvky je varování všem právníkům, že výše uvedené technické útoky jsou realistické! Na jedné straně jsou velmi nepravděpodobné, na druhé straně při zaostřené činnosti útočníka s vyšším útočným potenciálem jsou možné.

Spoléhající se osoba většinou nemá vůbec žádnou možnost ovlivnit udržování bezpečnosti proti útokům I. až III. Ovšem ani podepisující osoba, zejména z okruhu laických uživatelů, nemusí mít vůbec schopnosti pro odolání útokům I. až III. Údržba jejího technického prostředí se ještě subjektově zkomplikuje, pokud je určeno a zajišťováno jejím zaměstnavatelem (srov. 6.16.8).

Výše uvedený útok druhu I.i může kromě výrobce být zachycen již jen zkušebnou. Žádný další subjekt, včetně poskytovatele služeb nebo orgánu dohledu, již ověřování nemá v rámci své činnosti a spoléhá se na certifikát zkušebny.

Při pohledu na výše naznačenou skutkovou situaci z *právního hlediska* je poté obtížné stanovit jak vhodná a na vše myslící pravidla rozdělení odpovědnosti, tak případně soudně rozhodovat spory stran. Z hlediska právní jistoty by bylo optimální, kdyby odpovědnost za selhání bezpečnosti byla některé straně jednoznačně přiřazena, například formou právní domněnky nebo formou povinnosti k náhradě škody, která takto vznikne. Takové právní přiřazení však může tuto stranu dostat do situace, ve které nebude schopna realisticky obstát, bezpečnost udržet nebo prokázat porušení bezpečnosti konkrétním útočníkem. Při jakémkoli plošném nasazování kvalifikovaných elektronických podpisů pak bude zaděláno na situace, ve kterých někdo začne striktní právní rámec zneužívat. Právně se pak taková úprava začne dostávat do rozporu s obecnými hodnotami spravedlnosti, konkrétněji například se zásadami právního státu. Ten nemůže vytvořit stav, kdy sice právo bude jasné, ale skutkový stav potenciálně neovladatelný. To vytvoří stejnou svévoli a existenční nejistotu, jako kdyby právo jasné nebylo. Zasažena tedy bude i zásada právní jistoty a potažmo i ochrany vlastnictví.

Zákonodárce, a to i evropský zákonodárce, proto reaguje raději opatrným přístupem, kdy jednoznačná pravidla nestanoví a případnou zátěž rozhodování nechává na soudech. Za nejednoznačných pravidel nese ovšem určité riziko i spoléhající se osoba, která proto učiní dobře, pokud u rizikových transakcí podnikne i nějaká další preventivní opatření než jen spoléhání se na ověřenou platnost QES.

Současně však rizika mohou být i důvodem, proč zejména podepisující se osoba nemusí mít vůbec zájem na používání kvalifikovaných elektronických podpisů (QES),

nepracuje-li v oblasti vyšších rizik, ale jen malých nebo středních. Neomezená použitelnost prostředku pro QES naopak přináší nová rizika pro podepisující se osobu.

Autor se proto domnívá, že jednou z podmínek pro plošnější přijatelnost kvalifikovaného elektronického podpisu populací je možnost nastavit *právní* omezení užití, které by bylo rozeznatelné z kvalifikovaného certifikátu pro elektronický podpis spoléhající se stranou. Taková užití pak buď nebudou riskantní (6.16.9), nebo omezí riziko na nějakou přijatelnou finanční mez (6.16.10). Zjevně přitom platí, že pro jedny účely a některé osoby budou hranice přijatelného rizika vystavěny odlišně než pro účely či osoby jiné. Analogií tohoto přístupu kupř. je používání platebních karet, které mají stanoveny určité finanční limity na časovou periodu týdne nebo měsíce a jsou široce rozšířené. Riziko bylo akceptováno běžnou veřejností. Omezená rizika pak pochopitelně lze i pojistit. Jakmile bude patrná a případně pojištěná maximální škoda, která z použití kvalifikovaného elektronického podpisu může vzniknout, nic nebrání tomu, aby se právní pravidla odpovědnosti za bezpečnost součástí nastavila striktně.

Právně je jednodušší stanovit právní pravidla ve vertikálních vztazích, tj. pro případ komunikace jedince se státem a naopak. Rizika z neudržení bezpečností pak vesměs lze připsat státu. Je to právě stát, který použití nařizuje či promotuje a současně provádí dohled orgány dohledu a popř. i nad zkušebnami. Navíc jeho procesy správních řízení bývají složitější, takže falešné podání lze odhalit v navazujících krocích řízení. I k takovému scénáři je však třeba mít možnost nastavit v kvalifikovaném certifikátu *právní omezení použitelnosti* jen na vertikální vztahy, tj. v terminologii eIDAS například právě jen na jednání vůči subjektům veřejného sektoru.

Právě proto autor navrhuje možnosti mít v kvalifikovaném certifikátu uvedeny a celkově systematicky zavedeny možnosti omezení účelu (6.16.9) nebo finančního omezení (6.16.10).

6.15.8 Kvalifikovaná elektronická pečeť

Zvláštní důkazní účinek kvalifikované elektronické pečeti je stanoven v čl. 35 odst. 2 eIDAS: *„U kvalifikované elektronické pečeti platí domněnka integrity dat a správnosti původu těch dat, s nimiž je kvalifikovaná elektronická pečeť spojena."*

Ačkoli to laikovi nebude na první pohled patrné, má toto ustanovení silnější důkazní účinek, než může mít jakýkoliv výklad důkazního účinku kvalifikovaného elektronického podpisu, který bude soustředěn pouze na samotné nařízení eIDAS. Obě

domněnky v ustanovení se týkají dat, a nikoli samotné kvalifikované elektronické pečeti. Výklad pak je, že z existence této pečeti, která je spojena s nějakými daty, platí skutkové tvrzení, že svým **původem** data pochází od právnické osoby, jejíž kvalifikovaná elektronická pečeť je přítomna, a současně že data mají zachovánu **integritu**, tj. jsou stejná, jako byla v době vytvoření kvalifikované elektronické pečeti danou právnickou osobou.

Zápis ustanovení o kvalifikované elektronické pečeti je v eIDAS stejně objektivizovaný jako v případě ustanovení o kvalifikovaném elektronickém podpisu. Při dokazování bude třeba existenci takové pečetě subjektivně posoudit, což se nejsnáze provede ověřením platnosti kvalifikované elektronické pečetě postupem, který podle čl. 40 eIDAS je přiměřeně podobný ověření platnosti QES, jež se provádí dle čl. 32 eIDAS. Je možné též ověření platnosti provedené kvalifikovaným poskytovatelem, tj. přiměřeně podobně jako dle čl. 33 eIDAS.

Je-li této pečeti a dat se dovolávající strana schopna prokázat platnost ověření kvalifikované elektronické pečeti, nastupují obě výše zmíněné právní domněnky. Dovolávající se strana nemusí nijak dokazovat, že pečetící osoba, její pracovník nebo jakýkoli jiný zástupce měl daná data nějak předložena, že on nebo právnická osoba chtěli tato data opatřit kvalifikovanou elektronickou pečetí, nemusí se dokazovat, že QSealCD byl použit v souladu se správnými organizačními postupy právnické osoby, že s QSealCD a daty pro vytváření elektronické pečeti nakládala oprávněná osoba jednat za právnickou osobu. Tato všechna tvrzení jsou dle názoru autora pro důkaz irelevantní a jsou překlenuta domněnkou původu a integrity. Irelevantní se zdá i schopnost právnické osoby dokázat, že něco z výše uvedeného nebylo splněno. Výjimkou by snad bylo, kdyby některé vnitrostátní právo provedlo takovou implementaci podmínek vytváření elektronické pečetě, kterou by výše uvedené podmínky stanovily jako náležitost patřičnosti vytvoření kvalifikované elektronické pečeti. Jelikož takové podmínky by nejspíš byly v rozporu s přímo účinným zněním nařízení eIDAS, je málo pravděpodobné, že se některý členský stát touto cestou vydá.

Možnost vyvrácení právních domněnek je možná pouze důkazem opaku. Jelikož u metod PKI jsou obě vlastnosti spolu prakticky nerozlučně kryptograficky spjaty, dostačuje vyvrátit kteroukoli z nich, aby padly obě domněnky. To ale současně znamená to, že možnost vyvrácení domněnky je pouze jediná,[220] totiž dokázat nepůvodnost, tj.

[220] Dokázat neintegritu dat při zachování důkazu původnosti dat by bylo v případě používaných

nepravost (falešnost) kvalifikované elektronické pečetě. K tomu například rozhodně nestačí pouze prokázat to, že s QSealCD nebo se systémovým prostředím bylo zacházeno ze strany pečetící právnické osoby nedbale. Nedbalost zacházení neimplikuje, že daná kvalifikovaná elektronická pečeť není pravá. Možnost provést protidůkaz je proto velmi obtížně proveditelná. Prakticky znamená být schopen dokázat existenci útoku na QSealCD, na jeho aplikační nebo systémové prostředí. Opět nestačí dokázat jen možnost existence útoku (dále k tomuto též níže).

Jedinou další možností vyvrácení právních domněnek je, že kvalifikovaná elektronická pečeť vůbec nenáleží právnické osobě, která je uvedena v kvalifikovaném certifikátu pro elektronickou pečeť. Takový důkaz by musel směřovat k dokázání toho, že někde v postupu žádosti o tento certifikát nebo jeho vydávání certifikátu došlo k chybě nebo k podvodu, že se někdo za danou právnickou osobu při této žádosti zvnějšku vydával (vnější podvod) nebo někdo její žádost simuloval v prostředí kvalifikovaného poskytovatele služeb (vnitřní podvod). Důkazy pro takovou událost by se musely nacházet zejména v rámci dokumentace kvalifikovaného poskytovatele služeb.

Další právní otázkou je, zda data nebo dokument opatřený kvalifikovanou elektronickou pečetí lze považovat za právní jednání. K němu může vnitrostátní právo vyžadovat, aby aktivně jednala osoba oprávněná za právnickou osobu jednat. Jednající osoba však z kvalifikované elektronické pečeti není patrná a může být známa jen z vnitřních předpisů právnické osoby. Podle Jandta pak v německém právu při předkládání důkazu ve prospěch právnické osoby nemá protistrana prakticky žádnou možnost dokázat, že pečeť nevytvořila oprávněná osoba. Pokud je důkaz v neprospěch právnické osoby, musela by ta dokázat, že pečeť mohl někdo zneužít.[221] Autor zde upozorňuje, že může záviset na důkazních pravidlech vnitrostátního práva a na tom, jakou míru důkazu stanoví.

Jandt na závěr uvádí: „Ve vztahu k zavedení kvalifikované pečeti zůstává nezohledněno, že kvalifikovaná pečeť nezakládá předpoklad pro právní domněnku určení oprávněné osoby.“[222] Autor je však názoru, že není předem zcela zřejmé, jak budou soudy právní jednání jen s pomocí elektronické pečeti posuzovat.

kryptografických algoritům značně překvapivé. Jednalo by se v zásadě o matematické vyvrácení elementární správnosti daného algoritmu.

[221] JANDT, S., cit. dílo, s. 1207.

[222] JANDT, S., cit. dílo, s. 1211.

V elektronickém právním styku existuje právní i faktický příklad elektronických obchodů, ve kterých informační systém v případě právnické osoby jako provozovatele obchodu prakticky nikdy neuvádí, která fyzická osoba kupní či jinou smlouvu za stranu elektronického obchodu provádí. Není to totiž ani právně povinné (srov. 10.3 a 10.3.3).

Nelze rovněž vyloučit, že soudy budou posuzovat odlišně případy dokazování ztráty kontroly nad daty pro vytváření elektronické pečeti než nad daty pro vytváření elektronického podpisu. Určitou roli může hrát charakter právnické osoby, která běžně nemá vlastní smysly, rozum ani vůli, a určité rozprostření prostředků, s jejichž pomocí jedná, mezi více osob u ní může být proto přirozené a posuzované jako nikoli ztráta kontroly, ale pouze dodatečné účelové tvrzení. Rozdíl je zohledněn nebo vyplývá i z toho, že podmínka v čl. 36 písm. c) u zaručené elektronické pečeti nevyžaduje *výhradnost* kontroly, tak jako u zaručeného elektronického podpisu v čl. 26 písm. c) eIDAS, ale pouze kontrolu.

Roßnagel považuje i domněnku v čl. 35 odst. 2 eIDAS za příliš silnou na to, aby byla považována za právní domněnku ve smyslu německého práva. Mimo jiné mu je důvodem, že kvalifikovaná elektronická pečeť nemůže být přiřazena fyzické osobě. V rámci předchozího důkazního práva v Německu však právní domněnka odpovídající čl. 35 odst. 2 eIDAS nikdy nebyla přiřazena ani datům podepsaným kvalifikovaným elektronickým podpisem.[223] Přitom riziko zneužití u kvalifikované elektronické pečeti považuje za vyšší, z důvodu participace více fyzických osob navenek neurčených. Roßnagela proto navrhuje „domněnku" v eIDAS nepovažovat za právní domněnku, ale jen za důkaz *prima facie*, který je vyvrátitelný snadněji. V takovém případě by tedy dostačovalo dokázat jen vážné pochyby o tom, že pečeť je pravá, tj. mohlo by dostačovat jen dokázání toho, že útok byl pravděpodobný. Podrobněji k názorům Roßnagela o domněnkách v eIDAS viz úvod o dokazování (6.15).

Jak již je zmíněno výše, vůči kvalifkované elektronické pečeti může být vznesen stejný druh námitky jako vůči QES, totiž že i pokud se jedná o technicky **platnou** kvalifikovanou elektronickou pečeť, s úspěšně ověřenou platností ve smyslu čl. 40 a čl. 32 eIDAS, nemusí se jednat o pečeť **pravou**, tj. takovou, kterou by skutečně vytvořila údajná pečetící právnická osoba v úmyslu vytvořit pečeť, jenž by jí byl přičitatelný v tom smyslu, jak právnické osobě vůli či úmysl přičítat lze. Do úvahy připadají podobné druhy útoků jako v případě QES (srov. 6.15.7). Kromě toho se zde

[223] ROSSNAGEL, A. Beweiswirkungen..., cit. dílo, s. 649.

ale jistě projeví jako důležité koncepce pojetí právnické osoby v různých členských státech. Zda spíše uplatňují teorii fikce, teorii reálnou či jakoukoli jinou, popř. i eklektickou směs či modifikace. Pojetí se dále může lišit i podle toho, zda se jedná o právnickou osobu soukromého práva nebo práva veřejného.

Při odhlédnutí od těchto rozdílů však vždy bude moci spoléhající osoba protinamítnout, že účel elektronické pečeti spočívá v možnosti vztahovat určitý obsah, který zřejmě buď je právním jednáním (v širokém slova smyslu), nebo potvrzením o určité skutkové okolnosti, přímo k právnické osobě samotné. Spoléhající osoba může namítnout i to, že právnická osoba by běžně měla disponovat vyšší úrovní znalostí a dovedností a potažmo vyšší schopností ochrany bezpečnosti svých technických prostředků. Z povahy právnické osoby, která nemá vlastní smysly a tvorba její vůle je pak složitým právně-faktickým konstruktem, pak plyne, že nařízení eIDAS dost dobře ani nemůže upravit, jak se ta či ona právnická osoba má postarat o to, aby jí zapečetěný obsah ve formě elektronických dat odpovídal její pravé vůli či úmyslu. Praktické potřeby různých právnických osob budou velmi rozmanité. Navíc je třeba zohlednit, že by nařízení mělo i vyhovět různým pojetím právnické osoby a jejího jednání ve 28 právních řádech členských států naráz.

Charakter mezery, který vyplývá z bodu odůvodnění 56, že nařízení by svými požadavky „nemělo zahrnovat celé systémové prostředí", zde proto nepůsobí již tolik jako opomenutí zákonodárce, ale jako reflexe reality, že na úrovni EU nelze jednotně stanovit, vůči čím smyslům a vůli by se měly funkce systémového prostředí a aplikací vytvářejících elektronickou pečeť vztahovat, ani jakým způsobem. Současně to ale znamená i to, že námitka nepravosti kvalifikované nebo zaručené elektronické **pečeti** z důvodu možnosti podsunutí obsahu nemusí proto být vyhodnocena vůbec stejně jako v případě stejné námitky v případě elektronického podpisu fyzické osoby.

Zdá se proto, že zde je prostor pro *implementaci* nařízení právním řádem členského státu, aby tuto mezeru zaplnil v souladu s tím, jaké pojetí právnických osob a jejich jednání uplatňuje. Bylo by pochopitelně žádoucí, aby nařízení členský stát na tuto možnost implementace upozornilo, a to aspoň v bodech odůvodnění.

Autor souhlasí s německými autory, že důkazní presumpce u kvalifikované elektronické pečetě, jak je vyjádřena v nařízení eIDAS, má silnější důkazní účinek než kvalifikovaný elektronický podpis, pro nějž v eIDAS tento účinek vyjádřen není.

Souhrnně lze uzavřít, že se autorovi jeví použití kvalifikované elektronické pečeti, bez podrobné implementace vnitrostátním právem, jako málo právně jisté a současně jako poskytující potenciálně vysokou důkazní sílu. Bez vhodné vnitrostátní úpravy nebo vzájemné smluvní úpravy by proto doporučoval používat kvalifikovanou elektronickou pečeť zatím jen zdrženlivě, a to oběma stranám jednání.

Autor nepovažuje za správný názor, že (kvalifikovaná, zaručená) elektronická pečeť představuje automatizovaný způsob „podepisování" (srov. 6.6.4).

6.15.9 Kvalifikované elektronické časové razítko

Podle čl. 42 odst. 2 eIDAS platí: *„U kvalifikovaného elektronického časového razítka platí domněnka **správnosti data a času**, které udává, a **integrity dat**, s nimiž jsou toto datum a tento čas spojeny"* (zvýraznil autor). Dle čl. 42 odst. 3 se kvalifikovaná elektronická časová razítka navíc uznávají i přeshraničně, ve všech členských státech EU. Prokazují, že k okamžiku vytvoření razítka data existovala.

Při správné technické implementaci by poskytovatel měl vést záznamy o souvislé řadě vydaných časových razítek, která prakticky znemožňuje zpětně vsunutí nepravého časového razítka. Vydání jakéhokoli kvalifikovaného elektronického časového razítka by mělo být zpětně kontrolovatelné. Razítka by měla být generována ryze automaticky, bez zásahů pracovníků poskytovatele. Jandt proto považuje[224] domněnku za dostatečně bezpečnostně podepřenou. Roßnagel vůči domněnce však namítá,[225] že se nejedná pouze o pravost elektronických dat (určení poskytovatele), nýbrž i o obsahovou správnost. Tou zřejmě míní správnost data a času ve vztahu k datům. Domněnky o správnosti skutkového stavu *(Vermutung von Tatsachen)* však podle Roßnagela byly v německém právu dosud vyhrazeny pouze veřejným listinám. Proto rozpor doporučuje řešit tím, že se domněnka má považovat pouze za důkaz *prima facie (Anscheinsbeweis)*.

Autor je přesvědčen, že vydávání kvalifikovaných elektronických časových razítek by provozně mělo být nejjednodušší a potažmo i důkazně nejspolehlivější službou vytvářející důvěru vůbec. Je pouze třeba mít ověřeno, že nasazení a použité důvěryhodné systémy a produkty odpovídají správné praxi. Zda toto ověření subjektem ověřování shody je korektní, může být v praxi ale sporné, zejména při použití služeb z některého přeshraničí. Při případném auditu podle čl. 20 odst. 2 eIDAS orgánem

[224] JANDT, S., cit. dílo, s. 1207.
[225] ROSSNAGEL, A. Beweiswirkungen..., cit. dílo, s. 650.

dohledu může tento ale i zpětně posoudit, zda záznamy o vydaných kvalifikovaných časových razítkách jsou věrohodné. Orgány dohledu z různých členských států by si mezi sebou měly navzájem poskytovat pomoc podle čl. 18 eIDAS.

6.15.10 Služba elektronického doporučeného doručování

Podle čl. 3 bod 36 eIDAS se jedná o službu, *„která umožňuje přenášet data mezi [odesilatelem a příjemcem] elektronickými prostředky a poskytuje důkazy týkající se nakládání s přenášenými daty, včetně dokladu o odeslání a přijetí dat, a která chrání přenášená data před rizikem ztráty, odcizení, poškození nebo neoprávněných změn“* (mírně změnil autor). Službu může poskytovat jeden poskytovatel služeb vytvářejících důvěru, ale i více takových poskytovatelů, vzájemně propojených. Pro kvalifikovanou verzi služby jsou stanoveny obecné požadavky v čl. 44 eIDAS. Poskytovatelé zejména musí zajistit identifikaci odesilatele i příjemce, datum a čas odeslání i přijetí a vytvářet o nich samostatné záznamy, potvrzované kvalifikovaným poskytovatelem.

Podle čl. 43 odst. 2 eIDAS: *„U dat odeslaných a přijatých prostřednictvím kvalifikované služby elektronického doporučeného doručování platí domněnka* ***integrity dat****,* ***odeslání*** *těchto* ***dat identifikovaným odesílatelem****, jejich* ***přijetí identifikovaným příjemcem*** *a* ***správnosti data a času odeslání*** *a* ***přijetí****, jež jsou u kvalifikované služby elektronického doporučeného doručování uvedeny."* (zvýraznil autor).

Předpokladem domněnky tedy je, že se jedná o data odeslaná a přijatá (doručená) prostřednictvím kvalifikované verze služby. Nařízení bohužel neurčuje, čím se tato skutečnost dokládá, zřejmě se bude jednat o samostatné záznamy o odeslání a o přijetí dat, které vystavuje kvalifikovaný poskytovatel, včetně data a času odeslání nebo přijetí, a která potvrzuje zaručeným elektronickým podpisem nebo zaručenou elektronickou pečetí. Záznamy by zřejmě měly být předány odesilateli i příjemci, což však nařízení výslovně nestanoví.

Dumortier míní, že služby doručování imitující tradiční poštovní služby elektronicky jsou velmi složité a drahé a je otázkou, zda se komerčně ujmou. Dle něj mohou být „snadno nahrazeny silnou autentizací kombinovanou s bezpečným nahráváním obsahu na websajt."[226] Jandt považuje[227] nařízením vznesené požadavky za v principu dostatečné k pokrytí citované důkazní domněnky. Roßnagel rozlišuje, že nezměněnost doručených dat je domněnkou o pravosti (původu) dat, zatímco ostatní

[226] Dumortier in LODDER, A. R. – MURRAY, A. D. (eds)., cit. dílo, s. 286.
[227] JANDT, S., cit. dílo, s. 1207.

domněnky odeslání odesilatelem, přijetí příjemcem, správnosti data a času se týkají skutkového stavu *(Tatsachen)*, který s pravostí dat nemá nic společného. Jelikož správnost je v německém právu vyhrazena jen veřejným listinám, opět navrhuje[228] všechny tyto domněnky považovat pouze za důkaz *prima facie (Anscheinsbeweis)*.

Autor souhlasí, že v komerčním styku strany zprostředkovatele s touto úrovní zajištění služeb doručování sami dobrovolně nepoužívají ani nevyhledávají. Pro doručování od subjektů veřejného sektoru nebo jiných orgánů veřejné moci vůči jedincům, anebo podání v opačném směru, však služby takového druhu využitelné být mohou, neboť umožňují určovat datum a čas doručení, resp. podání, které mohou mít podstatný procesní význam ve správních řízeních nebo v soudních řízeních. Současně se jedná o právní styk, v němž, na rozdíl od běžného obchodního styku, může jedna nebo více stran mít zájem vyhýbat své součinnosti při přijímání dat. Vzhledem k těmto okolnostem je patrné, že každý takový systém vyžaduje podstatnou implementaci nařízení vnitrostátním právem. Hodnotit důkazní přesvědčivost záznamů z těchto systémů lze až po případném zvážení technických norem, pokud budou vyhlášeny Komisí podle čl. 44 odst. 2 eIDAS a v kontextu vnitrostátní implementace.

Služby (kvalifikovaného) elektronického doporučeného doručování mají smysl též v tom ohledu, že mohou představovat dodatečnou a technicky nezávislou bezpečnostní úroveň k ověřování původu elektronických dokumentů kvalifikovaným elektronickým podpisem (pečetí).

6.15.11 Elektronický dokument

Dle čl. 3 bod 35 eIDAS se elektronickým dokumentem rozumí *„jakýkoli obsah [content] uchovávaný v elektronické podobě, zejména jako text nebo zvuková, vizuální nebo audiovizuální nahrávka [recording]“*. V definici je podstatné slovo obsah a demonstrativní vymezení, že obsahem je text nebo nahrávky zvukové, vizuální nebo audiovizuální. Pro obsah je tedy charakteristické, že se jedná o lidskými smysly vnímatelnou informaci. Tím by se dokument mohl lišit od ještě obecnějšího pojmu dat, používaného v eIDAS, jimiž je dnes třeba zřejmě rozumět jakoukoli informaci vyjádřenou v digitální podobě, která má konečný rozsah, tj. jedná se o konečnou posloupnost bitů. Daty podle eIDAS tedy je i libovolný datový soubor nebo datový objekt, nikoli však proud dat *(stream)*. Uvedenou konečnost dat lze dovodit z toho, že

[228] ROSSNAGEL, A. Beweiswirkungen..., cit. dílo, s. 650.

nařízení eIDAS definičně uvádí u pojmů, jako je zaručený elektronický podpis, vztah právě k datům. Daty však může být v rámci eIDAS i program, tj. programový soubor, neboť zaručená elektronická pečeť je právní a zejména technickou analogií zaručeného elektronického podpisu a podle bodu odůvodnění 65 lze právě elektronickou pečeť využít i pro autentizaci softwarového kódu.

Obsah je však i širší pojem než písemnost, která nazahrnuje uvedené možnosti nahrávek. Obsah též je uchováván, tj. je zachycen aspoň nějaký čas stabilně, a to zřejmě z hlediska lidského chápání plynutí času i pojmu uložení. Vzhledem k inherentní duplikovatelnosti elektronického dokumentu je však zřejmě nerozhodné fyzické místo uložení, jímž lze nejnověji chápat i jen ryze virtuální úložiště „v cloudu". Dokumentem není ani vysílání či přenos lidsky vnímatelné informace v reálném čase,[229] nedojde-li k jejímu uložení.

Zajímavým kontrastem je, že velmi důležitým prvkem v nařízení eIDAS jsou důvěryhodné seznamy a že nařízení je prosazuje ve *„formě vhodné pro automatické zpracování"* (čl. 22 odst. 2 eIDAS). Jsou důvěryhodné seznamy ještě dokumentem? Nařízení se k této otázce nevyjadřuje. Autor si dokáže představit, že *forma vhodná pro automatické zpracování* ještě nevylučuje vnímatelnost i lidskými smysly, takže se jednat o dokument může, byť nebude v uživatelsky a graficky přívětivé podobě. Oproti tomu by obrat *strojově čitelná podoba*, zdánlivě stejného významu, byl spíše jen daty, byť v některých případech může existovat metoda jejich vnímatelné vizualizace.

V nařízení eIDAS zbylo o elektronickém dokumentu jen stručné ustanovení čl. 46 (Právní účinky elektronických dokumentů): *„Elektronickému dokumentu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu."* Článek stanoví jen obecnou důkazní přípustnost a obecný zákaz upírání právních účinků (srov. 6.15.1). Jakákoli jiná důkazní pravidla nejsou obsažena.

Stručnost úpravy působí až zmatečným dojmem. Původní návrh nařízení Komise obsahoval[230] tři ustanovení, jež lze hodnotit v rámci zbývající úpravy v návrhu nařízení jako obzvlášť nepodložená. Elektronický dokument měl být důkazně považován za ekvivalent papírového dokumentu. Elektronickému dokumentu opatřenému kvalifikovaným elektronickým podpisem nebo kvalifikovanou elektronickou pečetí

[229] Pod reálným časem zde míníme i případ jakéhokoli dopravního zpoždění, neprovádí-li přenosová technologie uložení obsahu.

[230] V článku 34 návrhu nařízení Komise.

měla svědčit právní domněnka autenticity (původnosti, pravosti) a integrity, pokud neobsahuje dynamické prvky. Třetí odstavec se měl týkat přeshraničního uznávání elektronických dokumentů jakékoli kompetentní osoby. Všechna tato ustanovení byla během legislativního procesu vypuštěna. Shodně například Jandt.[231] Za důležité požadavky na elektronický dokument Jandt považuje například přímou a trvalou čitelnost, trvalou integritu a autenticitu. Jelikož předpoklady k zajištění takových vlastností elektronických dokumentů v návrhu nařízení nebyly vůbec přítomny, je nakonec vhodnější, když byla tato pravidla o elektronickém dokumentu vypuštěna.[232]

Právě vynechání těchto ustanovení potvrzuje i to, že článek 25 odst. 2 eIDAS[233] nelze považovat za důkazní pravidlo (srov. 6.15.6). Sepisovatel návrhu považoval za nutné takové důkazní pravidlo mít výslovně zapsáno, zákonodárce měl tuto důkazní domněnku autenticity dokumentu opatřeného kvalifikovaným elektronickým podpisem nabídnutu, ale odmítl ji. Pojem elektronického dokumentu však v nařízení ponechal, neboť mu zcela nesmyslný nepřišel. Vypuštění stejné domněnky o autenticitě elektronického dokumentu i ve vztahu ke kvalifikované elektronické pečeti zeslabuje zřejmě i význam domněnky v čl. 35 odst. 2 eIDAS (srov. 6.15.8).

V českém prostředí se ve vztahu k pojmu elektronický dokument a čl. 46 eIDAS objevuje přepjatý výklad, že elektronický dokument má být považován za právně univerzálně rovnocenný papírové listině, elektronický dokument s QES pak listině vlastnoručně podepsané. Výklad byl prezentován například na semináři[234] Ministerstva vnitra a zůstává na jeho stránkách. Účelem mělo zřejmě být motivovat zejména úřady, aby veškeré své agendy přijímaly i v elektronické podobě. Obdobně se uvádí v čerstvém komentáři k eIDAS: „elektronický dokument podepsaný kvalifikovaným elektronickým podpisem má právní postavení stejné jako listina podepsaná vlastnoručním podpisem,

---

[231] JANDT, S., cit. dílo, s. 1205.
[232] JANDT, S., cit. dílo, s. 1206.
[233] Téměř totožné znění bylo obsaženo v čl. 20 odst. 2 návrhu nařízení.
[234] Například tvrzení:
„Elektronický dokument podepsaný
• kvalifikovaným podpisem po 1. 7. 2016 je roven listině s vlastnoručním podpisem a musí být akceptován ve všech řízeních včetně spravních, soudních a podobně.“
„Pro elektronický dokument:
• podepsaný kvalifikovaným elektronickým podpisem platí, že se na něj nahlíží stejně jako na dokument v listinné podobě podepsaný vlastnoručnim podpisem“.
citováno z: PIFFL, R. – FELIX, O. Nařizeni eIDAS – Cíle, nástroje, důsledky, Metodický seminář – Dopady nařízení eIDAS po 1. 7. 2016, Ministerstvo vnitra, Praha – 14. 6. 2016, s. 14–15/42. Dostupné z: <http://www.mvcr.cz/soubor/1-eidas-narizeni-eidas-cile-nastroje-dusledky.aspx>; navštíveno 22. 6. 2016.

a to v rámci celé EU."[235] Tato tvrzení nejsou správně ani vzhledem k hledisku plnění požadavků na písemnou formu (srov. 6.14), ani vzhledem k důkazním účinkům. K prvému ještě znovu zdůrazněme, že tyto možnosti použití nařízení jsou z jeho působnosti vyloučeny čl. 2 odst. 3, podle nějž: *„nařízením není dotčeno vnitrostátní právo ani právo Unie týkající se uzavírání a platnosti smluv či jiných právních nebo procesních povinností týkajících se formy"*. Obdobně bod odůvodnění 2 eIDAS. K důkaznímu významu elektronického dokumentu pak výklad v této části, popř. poukaz na absenci domněnky o projevu vůle i v rámci ustanovení o kvalifikovaném elektronickém podpisu (srov. 6.15.6).

Dumortier považuje ustanovení obdobná čl. 46 za tzv. pouhá nediskriminační ustanovení, která mají jen „velmi omezený" dopad. Výslovně pak zdůrazňuje, že „právní účinek kvalifikovaného elektronického podpisu bude rozdílný v každém členském státu".[236] Tím spíše bude rozdílný právní účinek jeho kombinace s elektronickým dokumentem. Srov. též 6.15.6.

6.15.12 Souhrn o důkazních účincích

Německá nauka hledí na důkazní účinky zavedené nařízením eIDAS značně kriticky. Jednotlivé důkazní účinky ve formě (právních?) domněnek zpravidla považuje za příliš silné. Takové domněnky nezapadají do důkazní systematiky, se kterou německé právo před nařízením eIDAS pracovalo. Podle Jandta by unijní právo nemělo vytvářet právní domněnky, ale mělo by nechat na vnitrostátním právu, jak unijní právní pojmy do své důkazní systematiky zařadí.

Podle Roßnagela vnitřně koherentní není ani důkazní škála v rámci samotného nařízení eIDAS. Důkazní domněnky spojené s kvalifikovanou elektronickou pečetí nejsou přítomny u kvalifikovaného elektronického podpisu, ačkoli možnosti zneužití jsou vyšší, neboť není jasně vázána k žádné fyzické osobě.[237] Dále kritizuje, že čl. 35 odst. 2, čl. 41 odst. 2 a čl. 43 odst. 2 nejsou podle něj pouze domněnkou pravosti důkazního prostředku *(Echtheit eines Beweismittels)*, nýbrž také existencí skutečnosti *(Vorliegens von Tatsachen)*, což dosud v Německu bylo vyhrazeno pouze veřejným listinám.[238] Pod existující skutečnosti zde Roßnagel zřejmě řadí původnost dat (že byly

[235] DONÁT, J. – MAISNER, M. – PIFFL, R. *Nařízení eIDAS : komentář.* Praha: C. H. Beck, 2017, s. 167.
[236] Dumortier in LODDER, A. R. – MURRAY, A. D. (eds)., cit. dílo, s. 282.
[237] ROSSNAGEL, A. Neue Regeln für sichere elektronische Transaktionen. *Neue Juristische Wochenschrift*. 2014, s. 3686–3692, s. 3692.
[238] ROSSNAGEL, A. Neue Regeln ..., cit. dílo, s. 3692.

vytvořeny původcem) opatřených kvalifikovanou pečetí, správnost data a času (že data existovala v daném čase) v případě kvalifikovaného časového razítka a odeslání dat identifikovaným odesilatelem (že data byla odeslána odesilatelem) v případě kvalifikované služby elektronického doporučeného doručování. Za nepochopitelnou považuje domněnku integrity dat (tj. nezměněnosti dat) podle čl. 43 odst. 2 eIDAS, neboť v právním textu eIDAS nespatřuje žádnou záruku toho, že ke změně dat nemohlo dojít kdykoli po přenosu dat, aniž by si změny někdo všiml nebo byla prokazatelná.[239]

6.16 Potíže nařízení eIDAS

V této části jsou probírány ty rysy nařízení, které autor považuje za problematické. Buď se jedná o oblasti nařízením neupravené vůbec, ačkoli by si úpravu zasloužily, anebo o oblasti upravené nařízením nedostatečně.

6.16.1 Chybějící horizont podepisující osoby a spoléhající se osoby

Vlastnostem vlastnoručního podpisu je podrobněji věnována kapitola 4.1 výše. Podpis je prvotně důležitý pro podepisující osobu a pro osobu (protistranu), která se na podpis spoléhá, považuje ho za projev vůle podepisující osoby a listiny jím stvrzené případně drží pro potřeby dokladování třetí straně nebo pro potřeby dokazování v soudním či správním řízení. Podepisující a spoléhající osoby jsou hlavní subjekty, z jejichž pohledu má existence podpisu smysl, neboť stvrzuje právní jednání mezi nimi. Jsou to ony, které jsou vystaveny rizikům z právního vztahu mezi sebou.

Jakékoli právně-technické řešení, které se snaží nahradit vlastnoruční podpis v elektronickém světě, by se pochopitelně mělo snažit poskytnout aspoň některé funkce (4.2) vlastnoručního podpisu, ideálně všechny. Současně by mělo být navrhováno tak, aby neustále drželo na zřeteli oba tyto subjekty a jim imanentní zájmy. Jsou to totiž právě tyto subjekty, které se nakonec rozhodnou, zda budou legislativou předložené právně-technické řešení v právním styku mezi sebou využívat, anebo nikoli.

Tento přístup z nařízení eIDAS ani z procesu jeho přijímání nelze vysledovat. Nařízení je soustředěné na služby vytvářející důvěru, na jejich poskytovatele a na dohled nad poskytovateli. Ostatní pojmy mají pouze pilířovou úpravu (6.2.1).

Pokud je v něčem nařízení vůči těmto podepisující a spoléhající osobě „vstřícné“, tak v tom, že jim na první pohled zjednodušuje potřebu orientace. Subjektům

[239] ROSSNAGEL, A. Neue Regeln ..., cit. dílo, s. 3692.

dostačuje vybrat si některého (spíše kvalifikovaného) poskytovatele služeb vytvářejících důvěru. Podepisující osoba musí využít služby takového poskytovatele, který vydává kvalifikovaný certifikát pro elektronický podpis. Pravidelně s certifikátem od něj bude přebírat i QSCD.[240] K vytvoření elektronického podpisu může využít jakoukoli platformu a jakoukoli aplikaci. Spoléhající se osoba pak může využít služeb poskytovatele, který poskytuje službu ověřování platnosti elektronického podpisu. Z hlediska nařízení se oba subjekty zdají být poskytovateli „obsloužené" a zbaveny starostí. Různorodé technické a potažmo právní potíže ale mohou snadno vyvstat. Srov. 6.15.7.

6.16.2 Vynechání vazby na smysly a vůli podepisující fyzické osoby

Z hlediska vytváření elektronického podpisu jsou vrcholem nařízení požadavky na kvalifikovaný elektronický podpis (článek 2 bod 12), který je vytvářený QSCD (článek 2 bod 23). Srov. 6.10. Jak již však úvod nařízení avizuje v bodu odůvodnění 56, *„nařízení by nemělo zahrnovat celé systémové prostředí, ve kterém se tyto prostředky využívají"* a *„z certifikační povinnosti [by měly být] vyloučeny aplikace pro vytváření podpisů"*. Druhá zde uvedená věta začíná alibistickým zdůvodněním: *„Jak je podrobně uvedeno v příslušných [technických] normách"*. Bod odůvodnění 56 je skutečně v nařízení proveden důsledně. V celém nařízení nenalezneme žádný požadavek na:

- systémové prostředí,
- aplikace vytvářející elektronický podpis,
- předložení (typicky zobrazení) obsahu transakce před vytvořením podpisu,
- věrné předložení obsahu transakce před vytvořením podpisu,
- vědomé seznámení se podepisující osoby s obsahem transakce,
- vědomost o závaznosti obsahu a o uzavření transakce.

Prakticky jediný požadavek v nařízení jdoucí tímto směrem je bod 2 v příloze II: *„Kvalifikované prostředky pro vytváření elektronických podpisů nesmějí měnit podepisovaná data ani bránit tomu, aby byla tato data předložena podepisující osobě před vlastním podepsáním."* Zákaz bránit předložení však je značně odlišný od spíše potřebného požadavku zajištění předložení (zobrazení, přehrání apod.). Požadavek nezměnění podepisovaných dat v QSCD není požadavkem na jejich nezměnění v aplikaci vytvářející podpis nebo v systémovém prostředí.

[240] V případě podpisů na dálku bude přebírat údaje nebo vazbu umožňující vzdálené ovládání QSCD.

Jelikož nařízení eIDAS tyto „samozřejmé“ požadavky ani neuvádí, následně nestanoví ani subjekty, které za jejich zajištění odpovídají. Tuto nepřehlédnutelnou mezeru v souvislosti s bodem odůvodnění 56 zmiňuje, byť nikoli tak podrobně, např. i Dumortier: „soud nebo expert se budou muset zabývat více záležitostmi, než jen certifikátem a zařízením pro vytváření podpisu“.[241]

Důsledkem absence výše uvedených požadavků je, že nařízení neobsahuje ani ustanovení, že kvalifikovaný elektronický podpis zakládá právní domněnku, že obsah v podepsaných datech je projevem vůle podepsané osoby (srov 6.15.6 a 6.15.11). Nejedná se zde pouze o reflexi možností technických útoků (6.15.7), jako o naprostou rezignaci na byť jen formulování potřebných požadavků.

Jediným normativním požadavkem by pak byla definice elektronického podpisu prostého, kterým jsou data, která „podepisující osoba používá k podepsání“ (srov. 6.4). *Z použití pro podepsání* by poté bylo nutné implikovat veškeré v seznamu výše uvedené požadavky. To se však autorovi zdá být příliš extenzivním výkladem a požadavky proto považuje za nařízením neupravené.

6.16.2.1 Implementace požadavků vnitrostátním právem?

Chybějící požadavky podle autora lze implementací nařízení ve vnitrostátním právu teoreticky doplnit. Body odůvodnění, jakož i normativní část nařízení tyto požadavky totiž zcela opomíjejí. Body odůvodnění i normativní část pak mlčí i o možnosti vnitrostátní implementace takových požadavků, tj. ani je výslovně neuvádí, ale ani nevylučují. Lze je dokonce považovat vesměs za oblast mimo oblast působnosti.

Pro možnost vnitrostátní implementace hovoří pak zásady právní jistoty a legitimního očekávání, což jsou zásady práva EU, které jsou závazným pramenem unijního práva, jež má vyšší právní sílu než nařízení. Členský stát pak může přikročit k vnitrostátní implementaci vlastně právě proto, aby splnil požadavky řádné implementace unijního nařízení.

Proti zvláštní vnitrostátní implementaci hovoří pět důvodů:

1. Možnost rozporu se zásadou vnitřního trhu (článek 4 eIDAS).
2. Omezení subjektů veřejného sektoru podle článku 27 odst. 1 až 3 eIDAS, zejména odst 3: *„Členské státy nesmějí v případě přeshraničního využívání on-line služby poskytované subjektem veřejného sektoru vyžadovat*

[241] Dumortier in LODDER, A. R. – MURRAY, A. D. (eds)., cit. dílo, s. 281.

elektronický podpis s vyšší zárukou bezpečnosti než kvalifikovaný elektronický podpis."

3. Účel nařízení je vytvořit jednotnou právní úpravu a technicky kompatibilní prostředky a služby pro elektronické podpisy elektronických transakcí.
4. Požadavky mohou být jen nerealisticky splnitelné.
5. Nevhodně provedená implementace může být horší než žádná. Může být vhodné nechat řešení vzejít až z praxe a soudních sporů, které uváží zcela individuální fakta případů bez omezení nevhodnými pravidly legislativy.

Důvodům 1 a 3 je třeba čelit tím, že případně navržená právní ustanovení budou představovat spíše vnější přídavné doplnění jednotné úpravy v nařízení eIDAS než rozpor s ní.

Důvod 2 lze vyřešit, jelikož čl. 27 odst. 3 eIDAS se týká pouze přijímání QES subjekty veřejného sektoru. Na opačný vertikální vztah ani na vztahy horizontální čl. 27 odst. 3 eIDAS nedopadá (srov. 6.14.2). Další možnosti přídavných požadavků, například na jednoznačnou identifikaci, jsou již rovněž popsány výše v 6.14.2.

Na důvody 4 a 5 je třeba brát velký zřetel. Autor je v zásadě názoru, že bez zahrnutí možností zavést do kvalifikovaných certifikátů omezení použití (srov. 6.16.9, 6.16.10) by se mělo k úpravě přistupovat jen velmi opatrně a zejména nezávadět důkazní domněnky.

Důvody 1 až 5 nejsou překážku pro to, aby dodatečné požadavky členský stát nepřikázal subjektům svého veřejného sektoru. Dokonce by je přikázat měl, neboť jimi vytvářené dokumenty v mnoha státech budou mít charakter veřejné listiny a budou nadány presumpcí správnosti.

Požadavky by se uplatňovaly u subjektů veřejného sektoru aj. orgánů veřejné moci pouze při jejich vlastním vytváření elektronických podpisů, resp. pečetí a nepředstavovaly by žádné omezení pro jejich protějšky, ať již vnitrostátní, nebo přeshraniční. Činnost subjektů veřejného sektoru, zejména veřejné správy a orgánů veřejné moci, je v pravomoci členského státu (zásada správní autonomie) a je to členský stát, který má eminentní zájem na tom, aby jeho vlastní veřejná správa, soudy aj. orgány veřejné moci byly při vytváření elektronických podpisů dostatečně chráněny. Takové předpisy mohou mít i povahu vnitřních předpisů v rámci veřejné správy.

Již zcela bez právních omezení vycházejících z eIDAS je možné doplnění požadavků na elektronické transakce mezi subjekty veřejného sektoru jednoho členského státu, pokud nedochází k přesahům této komunikace navenek, ať již vůči jedincům, či přeshraničním protějškům. Tyto systémy jsou vyloučené z působnosti nařízení eIDAS v důsledku čl. 2 odst. 2 eIDAS.

6.16.2.2 Implementace požadavků smluvně?

Názor autora na tuto otázku je, že smluvní doplnění požadavků je možné. Nařízení eIDAS nijak nevylučuje ani neomezuje (čl. 2 odst. 3 eIDAS) smluvní svobodu ve vztazích soukromého práva ohledně formy, ve které spolu budou subjekty v rámci soukromého práva jednat, včetně požadavků na úroveň zajištění formy. Subjekty si tedy mohou sjednat libovolné požadavky na zajištění vzájemné komunikace, včetně požadavků, které vysoce překračují požadavky např. na QES nebo na QSCD, popř. i formu se zajištěním, která vůbec neodpovídá či nesleduje hlavní metodiku podle nařízení eIDAS.

Při formulaci takových smluv je nicméně vhodné dbát na realističnost zajištění požadavků, zejména pak určit odpovědnost za zajištění požadavků každou ze stran, přiměřeně zvážit rizika a úměrně tomu nastavit celé obchodní procesy i jejich technické, personální, fyzické a organizační zajištění. Nerealistická ustanovení lze napadat odkazy na vyšší hodnoty práva (srov. 6.15.7), ochranu slabší strany apod.

6.16.3 Chybějící povinnosti podepisující osoby (pečetící osoby)

V nařízení není podepisující osobě výslovně předepsána vůbec žádná povinnost. Do úvahy připadá přitom řada povinností, které se pro podepisující osobu snad zdají být až samozřejmé, ale jejichž právní charakter povinnosti tak může být zpochybňován.

Na základě nařízení lze možná implikovat, že někdo by měl zajistit předpoklady splnění některých právních norem. Tak kupř. požadavek čl. 26 písm. c) eIDAS implikuje, že by měl existovat někdo, kdo zajistí splňování tohoto požadavku (v modalitě „může“). Touto osobou může, ale nemusí být nutně podepisující osoba. Z existence požadavku lze ale vyvodit i to, že by se podepisující osoba o udržení své výhradní kontroly zřejmě měla snažit. Otázkou však bude, zda si jednak této nejasné povinnosti vůbec bude jen na základě znění čl. 26 eIDAS vědoma, jednak zda má praktické schopnosti vůči jí použitým zařízením ji prosazovat.

Pravdivost údajů v certifikátu. Podepisující osoba (budoucí) by již ve fázi žádosti o certifikát měla žádat jen o vložení takových údajů ke své osobě, které jsou pravdivé k datu žádosti. Je to bezpochyby právě ona, kdo si je nejlépe vědom, které údaje o ní platí. Většina poskytovatelů služeb sice bude mít postupy ověřování vkládaných údajů, ale ty mohou mít různou úroveň zajištění ověřování pravosti. Rovněž tak všechny jiné subjekty, které žadateli o certifikát potvrzují nějaké údaje, by měly být zavázány k tomu, aby potvrzovaly jen pravdivé a aktuálně platné údaje. Výjimkou mohou být veřejné listiny a jejich ekvivalenty v právních řádech členských států. Dojde-li po vystavení certifikátu časem ke změně platnosti údajů, mělo by být zřejmé, zda je něčí povinností žádat u poskytovatele o zneplatnění certifikátu, v němž jsou údaje stále uvedeny, a strany spoléhající se na certifikát je proto dále také považují za platné. Měly by být zřejmé právní následky, pokud tak učiněno není. Účelem nařízení eIDAS je prostředkovat důvěru mezi dvěma osobami pro elektronické transakce, a to i přeshraničně. Tj. mezi osobami, které se navzájem nemusely nikdy fyzicky setkat, které mohou hovořit různými jazyky, na něž se vztahuje různé místní právo. Je-li spoléhající se osoba uvedena v omyl ohledně údajů nebo znaků podepisující osoby, které jsou uvedeny v jejím certifikátu, mohou jí vzniknout různé právní nároky, a to i přímo vůči podepisující osobě. Její procesní postavení zejména v rámci přeshraničního právního styku je však fakticky slabé. Bylo by mnohem vhodnější, aby povinnosti podepisující osoby byly jednak uvedeny explicitně, jednak založeny *erga omnes*, tj. i vůči poskytovateli služeb, který by pak vlastně byl jakýmsi preventivním a typicky i místně přítomným prosazovatelem povinností podepisující osoby co do obsahu certifikátu, který vydává. Za stávajícího znění eIDAS kupř. spoléhající se straně nikdo explicitně neodpovídá za údaje nebo znaky i v kvalifikovaném certifikátu pro elektronický podpis, které sice platily v době vystavení certifikátu, ale později platné být přestaly, nejsou již správné či pravdivé. Tyto certifikáty se často vydávají s platností až na 3 roky. Poskytovatel však za jejich zneplatnění odpovědný explicitně není, podepisující osoba není povinna mu změny stavu platnosti údajů či znaků hlásit. Z eIDAS dokonce neexistuje ani jednoznačná povinnost poskytovatele zneplatnit certifikát, pokud jej o to požádá sama podepisující osoba. Všechny tyto okolnosti mohou tak být upraveny jen smluvně ve vztahu mezi podepisující osobou a poskytovatelem služeb. Z hlediska spoléhající se strany není taková úprava optimální. Smlouvy poskytovatelů s podepisující osobou se mohou navzájem i značně lišit, a to i případ od případu v rámci jednoho poskytovatele a jedné jeho služby. Z hlediska

právní jistoty a časové náročnosti v praxi je zcela odlišné být nucen analyzovat u každého došlého elektronického podpisu smlouvu, kterou snad podepisující osoba uzavřela se svým poskytovatelem, nebo se moci spolehnout na jednotnou evropskou právní úpravu. Z právního hlediska je pak situace i mnohem nepříznivější v tom ohledu, pokud spoléhající se strana má vymáhat po podepisující se osobě konkrétní povinnosti, které jí byly založeny jen smlouvou s jiným subjektem, totiž s poskytovatelem.

Péče o zařízení používaná k vytvoření elektronického podpisu. Pro vytvoření elektronického podpisu, včetně jeho kvalifikované verze, je nutné, aby podepisující osoba používala a ovládala technická zařízení s určitou náležitou péčí. Ve zjednodušené systematice se jedná o QSCD, o systémové technické prostředí a o aplikaci vytvářející elektronický podpis. V případě QES vytvářených na dálku může existovat mírně jiné dělení. Podepisující osobě by měla být uložena povinnost aspoň základní bezpečnostní péče o tato zařízení. Současně je však jasné, že některé laické osoby ji nebudou schopny zajistit. Povinnosti péče by měl mít i zaměstnavatel podepisující osoby nebo subjekt v podobném postavení, pokud vlastní nebo provádí správu zařízení.

Bezpečnostní incidenty. Bezpečnostní incidenty je schopna zpozorovat zpravidla pouze podepisující osoba. Podepisující osoba by měla mít povinnost bezodkladně hlásit poskytovateli bezpečnostní incidenty, které zjistí, a všechny, které jí zjistitelné jsou, mezi což náleží ztráta kontroly nad QSCD, zejména když má fyzickou podobu (čipovou kartu, token) a drží jej, ať již se jedná o obyčejnou ztrátu, nebo o krádež. Tyto povinnosti by měl mít i zaměstnavatel podepisující osoby nebo subjekt v podobném postavení, pokud spravuje technické prostředky podepisující osoby.

Pečetící osoba. Přiměřeně podobné potíže chybějící úpravy povinností v eIDAS platí i pro pečetící osobu. Rozdíl právního hodnocení může spočívat v tom, že pečetící osoba je osobou právnickou, u níž právo může shledat vyšší schopnosti kvalifikace nebo schopnost jejího zajištění. V tomto ohledu je situace strany spoléhající se na kvalifikovanou (zaručenou) elektronickou pečeť pravděpodobně mírně lepší než v případě spoléhání se na kvalifikovaný (zaručený) elektronický podpis.

Při absenci explicitní úpravy povinností podepisující ev. pečetící osoby v eIDAS mohou soudy v případě sporů mít tendenci hledat základ povinností například v obecném mimosmluvním deliktním právu. Vzhledem k tomu, že u valné většiny podepisujících osob se bude jednat o osoby laické z hlediska bezpečnosti informačních

technologií, právní jistota vyvozování takových povinností je jen malá. Bude se též lišit případ od případu podle rozhodného právního řádu. Mírně vyšší nároky lze klást na právnické osoby jako pečetící osoby. Nevýhodou zde zase je, že nařízení eIDAS nijak nestanoví povinnost organizačně a úkolově rozložit nakládání se zaručenou nebo kvalifikovanou elektronickou pečetí mezi fyzické osoby, zaměstnance apod. Pravděpodobným důsledkem toho ale bude, že myslitelné povinnosti budou spíše přičítány přímo právnické osobě samotné.

Implementace vnitrostátním právem. Vzhledem k výše zmíněným potížím právní jistoty spoléhající se strany by autor považoval za správné, aby uvedené povinnosti podepisující osoby byly implementovány aspoň vnitrostátním právem. Povinnosti je však třeba stanovit tak, aby byly realistické z hlediska průměrné osoby.

Při stanovení povinností je třeba brát ohled i na to, že nařízení eIDAS ponechává velmi široké pole pro rozmanitost služeb vytvářejících důvěru. Povinnosti by měly být stanoveny tak, aby tuto rozmanitost neodůvodněně nezúžily. Některé povinnosti by měly být uloženy i zaměstnavatelům apod. subjektům (srov. výše 6.16.8).

V případě pečetící osoby samotné nařízení eIDAS nepřímo připouští, že může existovat určitá vnitrostátní implementace. Podle bodu odůvodnění 60 eIDAS poskytovatelé vydávající kvalifikované certifikáty pro elektronické pečetě *„by měli zavést nezbytná opatření, aby byli schopni určit totožnost fyzické osoby zastupující právnickou osobu, které je kvalifikovaný certifikát pro elektronickou pečeť poskytován, je-li tato identifikace nezbytná na vnitrostátní úrovni v soudním nebo správním řízení"*.

Bod odůvodnění se zde pravděpodobně odvolává na to, že v rámci soudních nebo správních řízení mohou existovat zvláštní případy procesní subjektivity právnické osoby, jako tomu je například i v ČR, kdy za právnickou osobu jedná pouze jeden její zástupce, například pouze jeden člen statutárního orgánu. Správnímu úřadu nebo soudu pak musí být zřejmé, o kterého zástupce se jedná. Navržený postup, totiž že totožnost fyzické osoby zástupce bude známa pouze poskytovateli služby, však pravděpodobně soudy ani správní orgány neuspokojí. Autorovi se zdá mnohem správnější, aby poskytovatel služeb vždy věděl a ověřil, které fyzické osobě vydává kvalifikovaný certifikát pro elektronickou pečeť.

6.16.4 Chybějící povinnosti spoléhající osoby (ověřování platnosti...)

Nařízení nestanoví výslovně žádné zvláštní povinnosti ani spoléhající se osobě. Především není nikde v nařízení výslovně uložena spoléhající se osobě nebo spoléhající se straně povinnost ověřovat zaručený (AdES) nebo kvalifikovaný elektronický podpis (QES) či zaručenou (AdESeal) nebo kvalifikovanou elektronickou pečeť (QESeal).

Dle názoru autora je přesto z nařízení eIDAS vyložitelná povinnost či potřeba spoléhající se osoby provést ověření platnosti QES nebo QESeal, ev. AdES nebo AdESeal, kdykoli chce mít spoléhající se osoba možnost se na právní ustanovení nařízení eIDAS spolehnout. Plyne to ze systematického výkladu, výše provedeného v 6.11 o ověřování platnosti a v 6.15.2 o objektivitě existence digitálních objektů.

Provádění nutných činností spoléhající se osobou nebo stranou je nicméně i pak nařízením upraveno nedostatečně. O jejich podstatě a podrobnostech obsahu mohou vznikat četné nejasnosti, popřípadě i spory.

6.16.4.1 Nejednoznačnosti systému ověřujícího platnost podpisu

Na rozdíl od absence požadavků na aplikaci vytvářející podpis je v eIDAS přítomen požadavek na určité vlastnosti aplikace ověřující platnost podpisu. Podle čl. 32 odst. 2 eIDAS *„Systém použitý k ověření platnosti kvalifikovaného elektronického podpisu musí poskytovat spoléhající se straně řádný výsledek postupu ověření platnosti a umožňovat jí zjistit jakékoli problémy týkající se bezpečnosti."*

Není však řečeno, kdo za zajištění funkce odpovídá. Je to vývojář (výrobce) systému? Spočívá-li systém pouze v programovém vybavení, bude zcela běžné, že jej vývojář bude poskytovat s licencí s úplným omezení odpovědnosti za škodu *„AS IS"*.

Lze tak pravděpodobně předpokládat, že odpovědnost za zajištění funkcí systému často zbude na samotné spoléhající osobě, která však systém běžně nevytváří.

Za zmínku též stojí, že ani k srpnu 2017 Komise zatím nevydala prováděcí akt podle čl. 32 odst 3 a čl. 40 eIDAS o technických normách, jejichž vyhovění by presumovalo vyhovění postupu podle čl. 32 odst. 1 eIDAS.

K výše uvedeným požadavkům na systém je nutné upozornit, že ověřující systém nemůže zjistit všechny problémy týkající se bezpečnosti na straně podepisujícího (srov. 6.16.2; vazba na vůli apod.), ale pouze takové, které vyplývají

z ověřování shody podpisu nebo z ověřování certifikátu, certifikační cesty a výskytu v důvěryhodném seznamu.

6.16.5 Chybějící ověřování platnosti zaručeného elektronického podpisu

Jak upozorňuje např. Rossnagel,[242] v nařízení se sice nachází článek 32 o postupu pro ověřování kvalifikovaného elektronického podpisu (QES), chybí však obdobná (nebo stejná) úprava pro určení pravidel pro ověřování zaručeného elektronického podpisu. To by nemuselo na první pohled být tolik na závadu, jelikož těžiště nařízení spočívá v úpravě kvalifikovaného elektronického podpisu.

Nařízení nicméně stanoví pro všechny případy vystavování kvalifikovaných certifikátů, i pro případ vystavení kvalifikovaného elektronického časového razítka, použití právě zaručeného elektronického podpisu nebo zaručené elektronické pečetě.

Ověřit QES tedy nelze, nejsou-li pravidla pro ověření zaručeného elektronického podpisu nebo pečetě, čímž je potvrzen kvalifikovaný certifikát podepisující osoby.

Do úvahy připadá použití výkladového pravidla *a maiori ad minus*.[243] Je-li nějaký postup dostatečně dobrý pro ověření QES, pak by stejný postup (či těsná analogie) měl být dostačující i pro ověření zaručeného elektronického podpisu.

Pro praxi ale nelze vyloučit, že pro ověření zaručeného elektronického podpisu budou případně stanovena pravidla mírně měkčí, zejména třeba v úrovni technických norem a jejich konkrétních odkazů na certifikační politiky poskytovatelů apod. Takové postupy mohou být jako pod-postup součástí například postupu podle čl. 32.

Z výkladového pravidla užitečného účinku lze pouze dovodit, že nějaký rozumný postup pro ověřování zaručených elektronických podpisů existovat musí, jinak by celé nařízení eIDAS v této oblasti bylo zbytečné.

6.16.6 Chybějící právní úprava pro elektronické podpisy vytvářené na dálku

Bod odůvodnění 52 deklaruje, že pro případ vytváření elektronického podpisu na dálku by poskytovatel, který vytváření zajišťuje, měl *„používat **důvěryhodné systémy** a **produkty** zahrnující **zabezpečené kanály** pro elektronickou komunikaci, a zajistit tak*

[242] ROSSNAGEL, A. Neue Regeln ..., cit. dílo, s. 3690.

[243] Na základě dostupné literatury nelze jednoznačně rozhodnout, zda tento logický argument je přípustný v rámci unijního práva, přinejmenším některé argumenty logického výkladu se však v unijním právu příležitostně používají. Navíc použití argumentu se zdá být poměrně přesvědčivé.

spolehlivost prostředí, v němž jsou elektronické podpisy vytvářeny, a zaručit, že je toto prostředí používáno pod výlučnou kontrolou podepisující osoby" (zvýraznil autor).

Používání zabezpečených kanálů ani podmínka zajištění spolehlivosti prostředí, v němž jsou elektronické podpisy vytvářeny, však v normativní části nařízení stanoveny vůbec nejsou. Shodně Roßnagel i Dumortier. Formulaci v bodu odůvodnění pak lze považovat spíše za popis principu, nikoli však za podrobností realizace. Za jejich absence je možné tyto požadavky pouze implikovat z požadavků na zaručený elektronický podpis a na QES. Implikace pochopitelně přináší menší právní jistotu pro podepisující i spoléhající osobu. Chybějící podrobná úprava může ale být výhodou z hlediska flexibility vůči budoucímu technickému pokroku a může poskytovatelům služeb ponechávat větší šíři možností tvorby služby.

Při absenci úpravy v normativní části je nutné pro případ vytváření elektronických podpisů na dálku vyvodit výše citované požadavky z bodu odůvodnění 52 výkladem užitečného účinku, zejména z článku 26 písm. c) eIDAS. Má-li podepisující osoba mít výhradní kontrolu nad daty pro vytváření elektronického podpisu (s vysokou mírou přesvědčení), přičemž tato data pro vytváření elektronického podpisu spravuje poskytovatel služeb a jsou uložena v té části QSCD, kterou drží a spravuje poskytovatel, pak je to možné pouze tehdy, pokud ani poskytovatel sám není schopen použít data pro vytváření elektronického podpisu. Toho není schopen jen tehdy, jestliže tato data pro vytváření elektronického podpisu jsou uložena v zašifrované podobě, anebo přístup k jejich použití uvnitř jednotky (část QSCD) podléhá autentizačnímu postupu, přičemž ani poskytovatel není schopen sám data pro vytváření elektronických podpisů dešifrovat nebo potvrdit autentizační postup namísto podepisující osoby. Obdobně toho nesmí být schopna ani žádná jiná třetí osoba, která by k této části zařízení QSCD získala fyzický nebo elektronický přístup.

Mají-li ale být data pro vytváření elektronického podpisu podepisující osoby použita při vytváření podpisu, musí být aspoň na krátkou dobu dešifrována nebo uvolněna autentizačním postupem. Má-li být udržena výhradnost kontroly podepisující osobou, je to možné jen tehdy, pokud ze zařízení, které podepisující osoba skutečně drží, používá a ovládá a které obsahuje určité údaje buď charakteru dešifrujících klíčů, nebo klíče pro vzdálené uvolnění autentizačního postupu, je vytvořen bezpečný kanál (ev. bezpečná cesta) a celek prostředku QSCD vytváří ono zmíněné spolehlivé prostředí, v němž jsou podpisy vytvářeny. Bez použití bezpečného kanálu by uvedené

údaje mohly být zachyceny některým subjektem odposlouchávajícím síťovou komunikaci, popř. i samotným poskytovatelem, čímž by se porušila podmínka výhradnosti kontroly.

V zásadě by se zde mělo hovořit o tom, že QSCD je funkčně i hmotně rozděleno na dvě části. Jednu drží a spravuje poskytovatel, druhá je přítomna v zařízení, které drží, používá a ovládá podepisující osoba. Části mohou mít různou formu hardwaru, softwaru či firmwaru.

V praxi přesto může být sporné, které vlastnosti zařízení, jež drží, používá a ovládá podepisující osoba, ještě spadají pod podmínky kladené na QSCD a které již spadají pod aplikaci vytvářející podpis nebo pod systémové prostředí, jež nařízení eIDAS neupravuje. Určitou jistotu snad vnese oznámení technických norem, které podle čl. 29 odst. 2 eIDAS vydá Komise.

V mezidobí však výrobci takových systémů postupují podle alternativních postupů hodnocení bezpečnosti produktů informačních technologií podle čl. 30 odst 3 písm. b) eIDAS, který má používat *„srovnatelné úrovně bezpečnosti"* a který subjekt určený členským státem k provádění certifikace QSCD oznámí Komisi.

Dále podle bodu odůvodnění 52 eIDAS *„V případě kvalifikovaného elektronického podpisu vytvořeného pomocí prostředku pro vytváření elektronických podpisů na dálku by se měly použít požadavky stanovené v tomto nařízení, které jsou použitelné na kvalifikované poskytovatele služeb vytvářejících důvěru."* V normativní části tomu odpovídá, že vytváření elektronických podpisů podle čl. 3 bod 16 písm. a) eIDAS spadá pod definici služby vytváření důvěry. Autor se však nedomnívá, že by bod odůvodnění 52 vylučoval, že službu elektronického podpisu vytvářeného na dálku lze poskytovat i jen jako nekvalifikovanou, tj. pouze při dodržení čl. 19 eIDAS.

V nařízení pak nejsou uvedeny zvláštní podmínky pro kvalifikované poskytovatele, které by při poskytování takové činnosti měl plnit. Bude-li poskytovatel službu vytváření elektronického podpisu na dálku poskytovat jako kvalifikovanou službu, budou se na něj vztahovat jen obecné povinnosti kvalifikovaného poskytovatele služeb dle čl. 24 eIDAS.

Další povinnosti lze možná vůči poskytovateli služeb implikovat výkladem užitečného účinku z požadavků na QSCD, které se nachází v čl. 29 a v příloze II eIDAS a z požadavků čl. 24 odst. 2 písm. e) eIDAS, že *„používá důvěryhodné systémy*

a produkty, které jsou chráněny proti pozměnění, a zajišťuje technickou bezpečnost a spolehlivost procesů, které podporují". Povinnosti poskytovatele zde lze podřadit pod zajišťování technické bezpečnosti a spolehlivosti procesů. Pojmem (důvěryhodného) produktu se rozumí *„technické zařízení nebo programové vybavení či jejich příslušné součásti, které jsou určeny k používání pro poskytování služeb vytvářejících důvěru"* (čl. 3 bod 21 eIDAS). V případě podpisů vytvářených na dálku se přinejmenším část QSCD, ve které jsou uložena data pro vytváření elektronických podpisů podepisující osoby, musí považovat za produkt, ev. za důvěryhodný systém, které poskytovatel k poskytování dané služby využívá.

Výše uvedený výklad potvrzuje, že právní úprava vytváření elektronických podpisů na dálku v normativní části nařízení skutečně chybí, což může způsobovat právní nejistotu. Současně však je ukázáno, že obsah citovaného bodu odůvodnění lze z normativní části aspoň v jisté úrovni abstrakce výkladem vyvodit, a to jako normativní požadavky nařízení.

V praxi se mohou vyskytovat řešení, která příliš dobrou faktickou bezpečnost zajišťovat nebudou, přičemž slabým článkem může být zejména to zařízení, které drží, používá a ovládá podepisující osoba. V praxi se ale naopak mohou vyskytnout i řešení, jejichž bezpečnost bude značně vysoká a v některých ohledech bude i překonávat bezpečnost založenou na čipových kartách jako QSCD. Praktickou nevýhodou bude vždy potřeba konektivity k tomu, aby elektronický podpis bylo vůbec možné vytvořit.

Jednou z dalších možných právních otázek je, zda v případě elektronického podpisu vytvořeného na dálku se jedná o elektronický podpis podepisující osoby anebo o elektronický podpis poskytovatele, který právně zastupuje podepisující osobu.

Veškerá systematika pojmů a znění ustanovení v eIDAS je vytvořeny tak, že by se jednoznačně mělo jednat o první možnost. Nejvýznamnějších důvodů lze zmínit několik. Nařízení kupř. nikde neupravuje druhou možnost zastupování. Do kvalifikovaných certifikátů pro elektronický podpis se podle přílohy I písm. c) vkládá jméno podepisující osoby nebo její pseudonym. Rovněž reformulace podmínky pro zaručený elektronický podpis, nyní v článku 26 písmeno c) eIDAS, totiž že je vytvořen pomocí dat pro vytváření elektronických podpisů, *„která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou"*, by systematicky měla vést k výkladu, že se jedná o vlastní podpis podepisující osoby.

6.16.7 Odložení počátku platnosti a pozastavení platnosti certifikátu

Nejjednodušší model certifikátů vydávaných podle užívaných technických norem[244] stanoví, že v samotném certifikátu se nachází interval platnosti „od–do". Tak je tomu i v případě eIDAS. Podle přílohy I písm. e) nebo podle přílohy III písm. e) musí kvalifikovaný certifikát obsahovat *„označení začátku a konce doby platnosti certifikátu"*. Certifikát běžně má platnost rok, dva, tři, výjimečně i déle. Nejjednodušší model dále připouští, že certifikovaný subjekt, nebo někdo jiný, může kdykoli požádat o zneplatnění certifikátu. Původní doba platnosti „od–do" je tedy kdykoli omezitelná na straně „do", certifikát může vyjít z platnosti dříve. Pro možnost udržení ověření platnosti certifikátu na straně spoléhající osoby má uvedený model zásadní dopad v tom, že souhrn elektronicky podepsaných dat s elektronickým podpisem dostačuje opatřit jediným časovým razítkem. Dostačuje, pokud jej vytvoří až sama spoléhající osoba v okamžiku, když provádí první ověření elektronického podpisu. Časové razítko zde dosvědčuje, že podpis s podepsanými daty existoval dříve, než došlo k zneplatnění nebo expiraci certifikátu. S využitím jediného časového razítka je model robustní. Uvedené zhruba řečeno platí bez ohledu na to, zda se používá řetězový model, ulitový model nebo hybridní model pro ověřování platnosti (srov. 6.11.1.3).

Nařízení eIDAS však připouští složitější režimy činnosti poskytovatelů.

Nařízení v čl. 28 odst. 4 hovoří o *„počáteční aktivaci" (initial activation)*. Počáteční aktivace je termín odlišný od začátku *„počátku platnosti"*. Umožňuje poskytovateli aktivaci odložit a do doby aktivace stav certifikátu vést jako neexistující. Záleží zde na správnosti provedení postupu aktivace, aby QSCD nemohl být v žádném případě použit dříve, než dojde k aktivaci kvalifikovaného certifikátu. Jestliže tomu tak je, což ovšem nařízení eIDAS svými ustanoveními nezaručuje, bude k udržení ověření platnosti dostačovat shodný postup jako v případě nejjednoduššího modelu výše. Režim podle čl. 28 odst. 4 eIDAS platí i pro přeshraniční styk, tj. v celé EU.

Druhý zvláštní režim nabízí nařízení v čl. 28 odst. 5, který dává možnost *„dočasného pozastavení platnosti kvalifikovaných certifikátů" (temporary suspension)*. Taková možnost je výhodná například v době odjezdu na několikatýdenní dovolenou, při které by pro podepisující osobu nebylo praktické zajišťovat si dohled nad QSCD. Kvalifikovaný certifikát na dobu pozastavení pozbývá platnost a jeho stav pozastavení musí být indikován od poskytovatele i navenek vůči spoléhající se osobě. Kdykoli

[244] Zpravidla se jedná o technické normy X.509 v3 nebo některý jejich profil.

v obecné době platnosti „od–do“, která je uvedená v certifikátu, mohou tedy nastat další časové intervaly pozastavení, během nichž je vytvoření podpisu neplatné. Model s pozastavením má zásadní dopad na potřebu zcela jiného způsobu vytváření QES. Ten by měl být opatřen dvěma časovými razítky v časech „před + po“, které určují přesněji dobu vytvoření podpisu a ta nespadá do žádného intervalu pozastavení. Podle bodu odůvodnění 53 je režim pozastavování jedním ze zavedených operativních postupů v některých členských státech. Článek 28 umožňuje, aby členský stát implementoval nařízení tak, že svým vnitrostátním právem stanoví podrobnější pravidla pro pozastavování platnosti kvalifikovaných certifikátů. Dovolení pozastavení platnosti je či bylo by devastujícím z hlediska *jednotnosti* obsahu používaných formátů QES v případném přeshraničním styku, jakož i z hlediska postupů ověřování platnosti. Spoléhající osoby musí zjišťovat, zda kvalifikovaný certikát nepochází od poskytovatele služeb, který postupuje podle práva členského státu, jenž pozastavování umožňuje, a zda tuto možnost využívá. Pokud tomu tak je, měl by vyžadovat systém dvou časových razítek a jiný systém ověření. To pochopitelně vede k technické fragmentaci, ale následně i k fragmentaci tržní, kterou se jinak právě nařízení eIDAS snaží překonat.

Ustanovení článku 28 odst. 5 eIDAS působí jako kompromis při vytváření textu nařízení mezi více členskými státy, které dříve používaly, resp. nepoužívaly pozastavení platnosti certifikátu. Potíže dovolené fakultativní možnosti nejsou ale zanedbatelné.

Ze znění čl. 28 odst. 5 eIDAS *„Členské státy mohou stanovit vnitrostátní pravidla..." („Member States may lay down national rules...“)* autor odvozuje, že jedním z možných výkladů je, že taková vnitrostátní pravidla by měla být použitelná pouze pro vnitrostátní provoz, a nikoli přeshraničně. V praxi by však zřejmě i takové vnitrostátní ostrovy nakonec vytvářely technické a právní obtíže i navenek.

6.16.8 Chybějící úprava vztahu zaměstnavatel–zaměstnanec

Mnoho případů užití (kvalifikovaných, zaručených) elektronických podpisů nevzniklo spontánně ze zájmu fyzických osob se elektronicky podepisovat, ale je výsledkem příkazu legislativy v některé agendě veřejného práva. Jedná se o použití ve vertikálních vztazích.

Na jedné straně se pak nacházejí obchodní společnosti aj. soukromé subjekty, které musí provádět některé agendy za pomoci elektronického podpisu, na straně druhé subjekty veřejného sektoru nebo orgány veřejné moci (úřad). Obě strany komunikace

však spojuje to, že za společnost, resp. za úřad jedná fyzická osoba, a to i formou svého kvalifikovaného elektronického podpisu. Společné rysy jsou:

- technické prostředky pořizuje, zajišťuje a spravuje zaměstnavatel,
- podepisující fyzická osoba nemá zájem o jiné využití pro své vlastní účely,
- zaměstnavatel chce mít kontrolu nad kvalifikovaným certifikátem.

Technické prostředky zahrnují zařízení QSCD, systémové prostředí, aplikaci vytvářející podpis a jiné prostředky, například síťové, dostupné služby vytvářející důvěru atd. Do správy však spadají i vnitřní organizační postupy, včetně například způsobů zaškolení apod. Podepisující fyzická osoba nemá vliv na volbu technologií, na zajištění jejích vlastností, typicky ani odbornost, ani pravomoc o nich rozhodovat. Tomu ale ne zcela odpovídá právní úprava, a to i v nařízení eIDAS, podle níž se ve všech těchto případech stále jedná o (elektronický) podpis dané fyzické osoby.

Je-li zaměstnanec v tomto postavení, nařízení eIDAS nestanoví, zda za zajištění požadavků na všechny technické prostředky odpovídá zaměstnavatel, anebo stále zaměstnanec, popř. jiná třetí osoba. Jak je uvedeno výše, systémové prostředí a aplikace vytvářející podpis nejsou zahrnuty do regulace eIDAS, tudíž za jejich provedení rozhodně neodpovídá poskytovatel služeb vytvářejících důvěru.

Pro zaměstnance tak vzniká faktická nejistota o tom, zda zaměstnavatel zajistil technické prostředí skutečně tak, že jeho vytváření podpisu je dostatečně chráněno proti padělání. Právní nejistota zde spočívá v tom, zda takovou povinnost zaměstnavatel měl. Jakékoli elektronické transakce vytvořené pomocí dat pro vytváření podpisu zaměstnance budou stále přičítány prvotně jemu jako fyzické osobě. Takové podpisy mohou potvrdit i elektronické transakce v jeho soukromé sféře, mimo původně zamýšlené užití v rámci společnosti nebo úřadu.

Určitá nejistota vzniká i na straně zaměstnavatele. Ten chce mít možnost zneplatnit certifikát vydaný svému zaměstnanci, pokud dojde ke změně funkce zaměstnance anebo pokud ukončí svůj pracovní poměr, popř. i z jakýchkoli dalších možných důvodů (např. bezpečnostní incident zachycený zaměstnavatelem).

6.16.9 Chybějící účelové omezení použitelnosti certifikátu

Příloha I DirES o požadavcích na kvalifikované certifikáty v písm. i) připouštěla uvést *„případně omezení oblasti použitelnosti certifikátu"*. Příloha II eIDAS obdobnou

možnost neuvádí. Podle článku 28 odst. 2 eIDAS *„Kvalifikované certifikáty pro elektronické podpisy nepodléhají žádným závazným požadavkům, které přesahují požadavky stanovené v příloze I."* Uvedené zřejmě znamená, že členský stát nesmí v rámci implementace nařízení požadovat po poskytovatelích žádné další přídavné požadavky nad rámec přílohy I.

Podle článku 28 odst. 3 eIDAS však *„Kvalifikované certifikáty pro elektronické podpisy mohou obsahovat další zvláštní atributy, které nejsou povinné. Těmito atributy nesmějí být dotčeny interoperabilita a uznávání kvalifikovaných elektronických podpisů."* Uvedené znamená, že poskytovatel může dobrovolně nabízet vložení atributů, které nejsou uvedeny v příloze I. Běžně se zřejmě bude jednat zejména o různá pole, jako jsou adresa subjektu nebo název organizace, v níž je podepisující osoba zaměstnána, může být uvedena adresa její elektronické pošty apod.

Může se však jednat i o atributy, které budou představovat omezení použitelnosti certifikátu. Omezení použitelnosti by nemělo znamenat dotčení uznávání, neboť tato podmínka je povinností spoléhající strany neodmítnout přeshraniční certifikát. Zde však se omezení použitelnosti individuálně dovolává podepisující osoba až na základě obsahu certifikátu a nedochází k apriornímu odmítnutí jeho uznání spoléhající stranou.

Otázkou je, zda obsažené omezení použitelnosti certifikátu bude srozumitelné spoléhající se straně. Zejména v přeshraničním styku může být potíží i jazyk vyjádření omezení. Měly by se proto používat spíše takové atributy, které jsou obsaženy v technických profilech norem, a programové prostředky by pak mohly, a proto i měly, být schopné spoléhající se osobě význam omezení sdělit v jazyce uživatelského prostředí.

Autor je proto názoru, že při dodržení výše uvedených podmínek nařízení vložení atributu s významem omezení použitelnosti kvalifikovaného certifikátu pro elektronický podpis umožňuje. Relativní složitost provedených úvah a vynětí možnosti z povinných součástí certifikátu v příloze II. však snižuje právní jistotu ohledně toho, že stejný výklad budou zaujímat i jiné osoby.

6.16.10 Chybějící finanční omezení použitelnosti certifikátu

Příloha I DirES o požadavcích na kvalifikované certifikáty v písm. j) připouštěla uvést *„případně omezení hodnot transakcí, pro něž lze certifikát použít"*. Příloha II eIDAS obdobnou možnost neuvádí. Je otázka, zda se toto omezení v DirES nemělo

vztahovat pouze na omezení odpovědnosti poskytovatele certifikačních služeb. Dle čl. 6 odst. 3 DirES *„Členské státy zajistí, aby poskytovatel mohl v kvalifikovaném osvědčení určit omezení pro jeho použití, pokud tato omezení mohou být známá třetím osobám. Poskytovatel neodpovídá za škody vyplývající z použití kvalifikovaného osvědčení, které přesahuje v něm uvedená omezení."*

V německém právu transponujícím DirES však příloha I byla transponována v § 7 odst. 1 bod 7. SigG tak, že kvalifikovaný certifikát mohl obsahovat *„údaje, které omezují užití podpisového klíče na určité použití podle povahy nebo rozsahu"*.[245]

Němečtí poskytovatelé certifikačních služeb pak uvedené omezení peněžní či finanční použitelnosti kvalifikovaného certifikátu umožňovali vkládat. Tato možnost byla využita a ze sporné situace vznikl judikát. Vzhledem k důležitosti, kterou této otázce autor přisuzuje, a protože tento text se jinde nezabývá platným právem v Německu před nařízením eIDAS, je tato kauza podrobně popsána bezprostředně níže.

6.16.10.1 BFH, 18. 10. 2006 – XI R 22/06: finanční omezení certifikátu

Shodou okolností se jednalo o vůbec první rozsudek[246] jednoho z vrchních soudů v Německu ve věci kvalifikovaného elektronického podpisu. Rozhodoval Spolkový finanční dvůr [*Bundesfinanzhof* – (BFH)], který je nejvyšším spolkovým soudem pro záležitosti daní a cel. Podstatou rozsudku[247] je rozhodnutí otázky, zda je platné použít QES, jehož kvalifikovaný certifikát obsahuje finanční omezení, v konkrétním případě na hodnotu pouhých 100 €, pro účel podpisu úkonu podání žaloby na Finanční soud [Finanzgericht – (FG)]. Prvoinstanční soud FG podání žaloby pro nedostatek náležitostí QES a následně i formy odmítl přijmout. Žalobce podal revizní odvolání k BFH. Bundesfinanzhof vyložil podstatu otázky: *„...peněžní omezení se vztahuje pouze na přímé finanční transakce (např. příkazy k převodu nebo jiné peněžní obchody) ... (např. koupě) ..."*[248] Druhou případně spornou otázkou bylo, zda pro účely platného podání žaloby nevadí, že QES nebyl vyhotoven právě pro dokument žaloby, ale byl jím opatřen celý e-mail, popsaný v rozsudku jako „kontejner", který kromě žaloby obsahoval i další dokumenty. Podpis QES byl proveden přes celý tento kontejner, se všemi dokumenty

[245] *„Angaben darüber, ob die Nutzung des Signaturschlüssels auf bestimmte Anwendungen nach Art oder Umfang beschränkt ist."*

[246] FISCHER-DIESKAU, S. – HORNUNG, G. Erste höchstrichterliche Entscheidung zur elektronischen Signatur. *Neue Juristische Wochenschrift*, 60. Jg. (2007), Heft 40, 2007, s. 2897–2899.

[247] BFH, 18. 10. 2006 – XI R 22/06. Dostupné z: <http://lexetius.com/2006,3265> nebo <http://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BFH&Datum=18.10.2006&Aktenzeichen=XI+R+22%2F06>.

[248] BFH, 18. 10. 2006 – XI R 22/06, R. 35. Dostupné z: <http://lexetius.com/2006,3265>.

včetně žaloby. Bundesfinanzhof se vyslovil: *„… podstatný je smysl souvislosti mezi textem a podpisem; tento smysl souvislosti existuje i při ‚podpisu kontejneru'…"*[249] Konsekventně BFH rozhodnutí FG zrušil a věc vrátil FG k vyřízení.

Zajímavý je ovšem i kontext použité argumentace obou stran sporu, který lépe vyjeví právní i skutkovou podstatu záležitosti. Zdůvodnění obou soudů vyvolalo i rozsáhlou následnou diskusi.

Původně nepřijatou žalobu na FG podával zplnomocněný advokát jako zástupce svého klienta. Soud FG původní žalobu nepřijal v zásadě z toho důvodu, že jím používaný software „EGVP-Programm" podpis neověřil jako platný,[250] přičemž se tak stalo právě kvůli přítomnosti uvedeného „peněžního omezení 100 €" v souvisejícím kvalifikovaném certifikátu. Soud BFH používal stejný software a ani v jeho případě se platnost podpisu na původní žalobě u FG ověřit nepodařilo.[251]

Při skutkové rekapitulaci BFH uvedl, že se jednalo o atribut peněžní omezení *(Attribut: Monetäre Beschränkung)* poskytovatele Datev, který ve svém informačním popisu k němu uvádí: „Údaj Vám umožňuje uvést horní finanční hranici nasazení certifikátu" [eine finanzielle Obergrenze beim Einsatz des Zertifikats anzugeben].[252] Ohledně pojmu atribut stejný popis uvádí, že se jedná o vlastnost *(Eigenschaft)*, postavení *(Stellung)* nebo omezení *(Beschränkung)*.[253]

Žalobce i při podání stížnosti na BFH zdůrazňoval, že omezení 100 € považoval za relevantní pouze v případě závazkových smluv *(schuldrechtlichen Verträge)*, nikoliv však pro podání žaloby, kterou podával z titulu procesního zmocnění svým klientem. S tímto úkonem nemají být spojeny žádné finanční závazky. Omezení pochází z jiné oblasti práva a mělo ho chránit před zneužitím v této oblasti.[254] Navíc k úhradě případných nákladů řízení je povinen klient, a nikoli jeho advokát.[255]

Další linie argumentace vedl žalobce přes to, že podle judikátu GmS-OGB 1/98 má vlastnoruční podpis zajišťovat autorství *(Urheberschaft)* a vyjádření vůle *(Äußerungswillen)*. První instance ale měla požadovat hodnotově neomezenou garanční

[249] BFH, 18. 10. 2006 – XI R 22/06, R. 39. Dostupné z: <http://lexetius.com/2006,3265>.
[250] BFH, 18. 10. 2006 – XI R 22/06, R. 35. Dostupné z: <http://lexetius.com/2006,3265>.
[251] Z rozsudku není patrné, zda sama revizní žaloba byla podána tradiční písemně papírovou formou, nebo rovněž elektronicky se stejným kvalifikovaným certifikátem s tím, že BFH ověřil QES ještě jinak.
[252] BFH, 18. 10. 2006 – XI R 22/06, R. 35. Dostupné z: <http://lexetius.com/2006,3265>.
[253] Toto slučování atributů s omezeními nepokládá autor za vhodné.
[254] BFH, 18. 10. 2006 – XI R 22/06, R. 12. Dostupné z: <http://lexetius.com/2006,3265>.
[255] BFH, 18. 10. 2006 – XI R 22/06, R. 17. Dostupné z: <http://lexetius.com/2006,3265>.

funkci (7 vlastností podpisu, srov. 4.2) QES, které podle žalobce ale stejně nejsou vyjádřeny v požadavcích autentizace a identifikace v SigG.[256] Požadavky na vlastnosti podpisu jsou dle něj přehnané, o čemž svědčí možnosti telegrafického a telefaxového podání žaloby. Požadavky na procesní formu nemají být samoúčelné a rozhodující pro připuštění písemnosti má být, zda je osvědčené autorství a vůle.[257]

Žalovaný uváděl, stejně jako v první instanci, že peněžní omezení vykládá tak, že „z podání nesmí vyplývat žádné finanční následky, které by přesahovaly hranici 100 €." Takové náklady ale mohly případně žalujícího snadno postihnout, zejména pokud by své jednání skutečně neměl pokryté platnou plnou mocí. Navíc se domnívá, že by finanční omezení mělo chránit oba subjekty, tj. i zastoupeného. Kromě toho žalující měl možnost vyjádřit omezení použití certifikátu na oblast své profesionální činnosti *(berufliche Tätigkeit)*, ale neučinil tak.[258] Nasazení QES pak má mít 7 funkcí: uzavírací, zachovávací, indentifikační, pravostní, ověřovací, důkazní a varovací.[259]

Vůči tomuto střetu argumentací BFH v zásadě uvedl pouze dvě úvahy. První bylo zjištění, že jiní poskytovatelé certifikačních služeb mají jinak formulovaný obsah atributu „peněžní omezení". Například u BNotK „... zákazník je může zapsat, pokud chce se svým elektronickým podpisem vykonávat finanční transakce jen do jisté výše." Obdobně jej mají definované i PCS Deutsche Post a D-Trust.[260] Druhou úvahou je přiklonění se k tomuto popisu, jak již je uvedené výše ve shrnutí, že „... peněžní omezení se vztahuje pouze na přímé finanční transakce (... příkazy k převodu ... jiné peněžní obchody ... koupě)".[261]

6.16.10.2 Ohlasy

Prakticky všichni hodnotící zdůrazňovali, že rozsudek měl nejen ryze právní význam, ale jednalo se i o právně-politickou otázku vstřícnosti justice vůči elektronickým dokumentům. Proto byla věnována značná pozornost již rozhodnutí první instance FG [262] a BFH rozhodoval za stavu, kdy mohl mít k dispozici i několik

[256] BFH, 18. 10. 2006 – XI R 22/06, R. 10–11. Dostupné z: <http://lexetius.com/2006,3265>.
[257] BFH, 18. 10. 2006 – XI R 22/06, R. 14–15. Dostupné z: <http://lexetius.com/2006,3265>.
[258] SKROBOTZ, J. FG Münster: Unzulässige Klageerhebung mit verwendungsbeschränkter Signatur, *Multimedia und Recht*. 2006, s. 638–639.
[259] SKROBOTZ, J., cit. dílo, s. 639.
[260] BFH, 18. 10.2006 – XI R 22/06, R. 34. Dostupné z: <http://lexetius.com/2006,3265>.
[261] BFH, 18. 10.2006 – XI R 22/06, R. 35. Dostupné z: <http://lexetius.com/2006,3265>.
[262] Např. se zmiňují další 3 články in SKROBOTZ, J., cit. dílo, a FISCHER-DIESKAU, S. – HORNUNG, G. *Erste ...,* cit. dílo, s. 2897.

článků ohlasů na prvoinstanční rozhodnutí. Všichni proto rozsudek BFH v tomto ohledu přivítali. Ohledně ryze právní dimenze a odůvodnění rozsudku však pochyby byly.

Skrobotz obecně lituje, že rozsudek nepomohl rozřešit akademickou otázku, zda neplatný je podpis sám, nebo celé vyjádření. Kritizuje nerozlišování atributů a omezení soudem. Konečně nesouhlasí ani s „mantrou" soudů, že QES je funkčním ekvivalentem vlastnoručního podpisu, ani s tím, že by písemná forma užívaná procesním právem byla založena na funkcích listin, neboť je připuštěn i počítačový fax. Skrobotz by zřejmě dal přednost snížení procesních požadavků.[263] Nicméně zřejmě přivítal, že se soud nevyslovil ve prospěch omezení jako krytí dalekosáhlých následků jednání. Dle něj není totiž ani jasné, zda by bylo možné použít stejný certifikát např. pro koupi zboží za 99 €, neboť nelze vyloučit, že kupujícímu nevzniknou vyšší náklady třeba v důsledku úroků z prodlení, prodávajícímu vzniká povinnost plnit, která za nepříznivých okolností rovněž může vést k vyšším nákladům, než je prodejní cena.[264]

Autoři Fischer-Dieskau a Hornung[265] nejsou zcela spokojeni se zdůvodněním BFH z toho důvodu, že se domnívají, že hlavním důvodem uspokojení žalobce mělo být to, že v daném případě nepřicházelo překročení hranice 100 € při běžném průběhu věci v úvahu, nemělo se protivit „objektivnímu horizontu příjemce". Argumentace „rozvinutím problémů do následných nákladů" by se dle nich neměla používat, neboť řešení neobvyklých situací spadá pod obecnou úpravu náhrady škod apod.

Soudní výklad vztahování se peněžního omezení pouze na „přímé finanční transakce" pak dle nich znamená, že zákonodárcem poskytnutá ochrana majitele podpisového klíče se v jiných, méně bezprostředních případech ztratí. Ochranu „peněžním omezením" přitom považují za jednu ze základních metod, která se užívá.

Uvádějí, že pro advokáty, stejně jako pro jiná povolání, je důležité oddělit osobní sféru od profesní, na kterou v jejich případě mají sjednané pojištění. Jako vhodnější pro tyto případy však považují omezení podle druhu *(nach Art)*.

Jak naznačeno již výše, autoři se nedomnívají, že by se peněžní omezení mělo vykládat jako částka potenciální výše odpovědnosti. Ta v daném případě hrozí v případech, pokud by advokát jednal bez plné moci nebo provedl jiné porušení povinností mandatáře. Jak autoři uvádějí, tyto povinnosti a odpovědnost z nich má ale

[263] SKROBOTZ, J., cit. dílo.
[264] SKROBOTZ, J., cit. dílo, s. 638.
[265] FISCHER-DIESKAU, S. – HORNUNG, G. *Erste ...,* cit. dílo, s. 2898–2899.

advokát v každém případě, nezávisle na daném podání, se kterým nesouvisí. V dané souvislosti považují závěr první instance (FG) za perverzi práva, neboť omezení, které mělo advokáta chránit, bylo ve výsledku použito proti němu. Právě nepřijetí žaloby zde založí vznik odpovědnosti advokáta vůči klientovi. Dalším důvodem jim je, že vymáhání odpovědnosti, například formou náhrady škody, považují za základní právní jistotu stran, do které by nemělo být zasahováno.

Autoři dále na základě studia příruček softwaru EGVP před a po rozsudku uváději,[266] že výrobce EGVP zareagoval na rozsudek BFH tím, že přestal případná omezení v kvalifikovaných certifikátech vůbec zkoumat, a jako ověřené tedy projdou všechny podpisy, byť by certifikát obsahoval např. omezení dle druhu znemožňující procesní použití v rámci justice. Kritizují to, neboť soud jako příjemce dle nich není nově schopen rozpoznat přítomnost omezení. Účelem omezení je pro ně především ochrana majitele podpisového klíče, která je tak vyřazena.

6.16.10.3 Hodnocení

Použitá argumentace soudu, který se pokusil o objektivizaci významu „peněžního omezení“ z jeho používání ostatními poskytovateli, na jednu stranu dává jakýsi smysl nalézt jedno společné měřítko pro právo, na straně druhé z platného práva SigG a SigV vůbec nijak nevyplývalo, že různí PCS nemají mít možnost vyjadřovat význam omezení naprosto různě, vzájemně nezávisle, a tím i soutěžit o zákazníky. Je možné, že někteří zákazníci by dali přednost široce pojatému „peněžnímu omezení“, zatímco jiní naopak jen zcela úzkému. Autor je názoru, že pokud soud chtěl použít úzký výklad omezení, neměl se odvolávat na jiné poskytovatele, o jejichž certifikát se nejednalo, ale měl provést analýzu použitelnosti úzkých a širokých omezení z hlediska právní praxe a až na jejím základě případně dovodit, že široké omezení neposkytuje dobrý smysl (což zůstává otevřené). V tomto smyslu autor souhlasí se stanoviskem Fischer-Dieskau a Hornunga, že je otázka, zda peněžní omezení má být skutečně vykládáno takto úzce a zda to někdy nepovede k nežádoucí ztrátě ochrany. Na druhé straně s nimi nesouhlasím ohledně toho, že by se peněžní omezení mělo vykládat pouze jako náklad jednající osoby a nezahrnovat celkovou nominální výši uvedeného obchodu, zde možných procesních nákladů žaloby. Obdobně by tomu bylo třeba v případě zprostředkovatele, který by při peněžním omezení 100 € například hodlal uzavírat obchody ve výši 1000 € s tím, že jeho účast na zisku i ztrátě je např. pouze 8 %,

[266] FISCHER-DIESKAU, S. – HORNUNG, G. *Erste ...,* cit. dílo, s. 2899.

a jeho rizika tak jsou dostatečně pokryta. Podklad pro tuto úvahu pochází spíše z koncepce čelení rizikům odpovídajícími protiopatřeními než z výlučně právních úvah, které se dle druhu právního vztahu asi přeci jen mohou případ od případu lišit. Jestliže někdo provádí jednání, v jehož důsledku mohou vzniknout nějaké náklady, byť rozdělené mezi více osob, měl by používat technologie a organizační opatření, které přiměřeně kryjí celou částku, o niž se jedná, a nikoli jen částku připadající na něj osobně.

Jinou přijatelnou a možnou úvahou soudu by bylo, že není užit obrat „finanční omezení“, ale „peněžní omezení“, které proto těsně souvisí s penězi, a týká se tedy jen takového jednání, jehož esenciálií je peněžní platba. Tato argumentace však použita nebyla.

Z diskursu plyne, že význam omezení částkou není nijak zvlášť jasný. Každé právní jednání může dříve nebo později mít za následek finanční důsledky. Vhodnější by bylo, aby omezení byla prvotně uváděna dle druhu jednání a omezení částkou bylo použito případně jako druhotný parametr takových jednání.

Výklad peněžního omezení by se dle názoru autora měl vztahovat na běžnou nominální hodnotu záležitosti při běžném vývoji. Výjimkou snad mohou být jednání, která mají vyšší míru běžného rizika. Určení peněžního vyjádření hodnoty procesních úkonů může být problematické, obdobně jako například tzv. pákové obchody na burze.

Autor si dovede představit i použití omezení omezující odpovědnost za škodu nebo jinou podobnou odpovědnost, ale takové by se nemělo nazývat peněžní omezení.

Pro samotné Německo nicméně uvedený judikát měl především právně politický význam. Advokáti aj. podatelé po něm mohou provádět procesní úkony s certifikáty obsahujícími obecné peněžní omezení 100 €. Postup a zdůvodnění soudu budí dojem, že hledal nejmenší možnou míru vyjádření se, která by mu umožnila případ rozhodnout, zřejmě ve prospěch žaloby, a přitom diskurs pro budoucnost jakkoli neuzavřít.

6.16.11 Chybějící zjištění totožnosti podepisující osoby

Nařízení eIDAS neupravuje žádné případy, kdy je poskytovatel služeb vytvářejích důvěru povinen jinému subjektu sdělit osobní údaje o podepisující osobě, které vystavil kvalifikovaný certifikát pro elektronický podpis. V něm se podle

přílohy I písm. c) eIDAS může nacházet o podepisující osobě tak málo informací, jako je pouze *„jméno podepisující osoby nebo pseudonym"*.

V kvalifikovaném certifikátu pro elektronický podpis se podle přílohy I písm. f) však musí nacházet *„identifikační číslo certifikátu, které musí být jedinečné pro daného kvalifikovaného poskytovatele služeb vytvářejících důvěru"*. Jelikož podle čl. 24 odst. 2 písm. h) eIDAS kvalifikovaný poskytoval *„po přiměřenou dobu, i poté, co ukončil svou činnost kvalifikovaného poskytovatele služeb vytvářejících důvěru, eviduje a zpřístupňuje veškeré příslušné informace týkající se dat, která vydal a obdržel, zejména pro účely poskytnutí důkazů v soudním a správním řízení"*, měl by tyto informace o totožnosti, místě bydliště, čísle průkazů apod. mít dostupné.

Na základě nařízení eIDAS není kupř. spoléhající se strana, ani po osvědčení vážného právního zájmu, oprávněna po poskytovateli služeb žádat sdělení více údajů o totožnosti podepisující osoby, například i pro účely možnosti vznesení žaloby vůči podepisujícímu apod. Poskytovatelé služeb by zřejmě vyhověli pouze takovým žádostem, které v rámci práva členského státu, jímž se řídí, jim takové povinnosti stanoví, např. v souvislosti s právní úpravou v oblasti trestního práva, povinnosti součinnosti s orgány činnými v trestním řízení, součinnosti s obecnými soudy apod. Nesjednocení procesní úpravy každopádně znamená, že si spoléhající strany v přeshraničním styku budou jen málo jisté, zda, jak rychle a za jakých procesních podmínek jsou informace o totožnosti podepisující osoby vůbec získatelné.

Bylo by zřejmě vhodné, aby členské státy zavedly aspoň v rámci implementace eIDAS úpravu, která by nějaké vhodné možnosti připouštěla. Při jejich vytváření je zřejmě třeba dbát ohled i na čl. 23 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016, obecného nařízení o ochraně osobních údajů (GDPR).

6.16.12 Chybějící úprava biodynamických podpisů

Nařízení eIDAS ignoruje, že jedním z druhů provedení (4.5) elektronického podpisu je *vii. biodynamická verze vlastnoručního podpisu*. Tento bude v systematice nařízení eIDAS odpovídat pouze elektronickému podpisu prostému (6.4). Ani ve verzi směrnice DirES tento druh nesplňoval požadavky na zaručený elektronický podpis, protože v praxi[267] nemohl být běžně proveden pomocí zařízení, které by podepisující osoba mohla mít pod svou výhradní kontrolou. V nařízení eIDAS se však možnost

[267] Vlastnoruční podpisy na podpisové plošinky používají například komerční poštovní kurýři.

vyhovění definici ještě více vzdálila, neboť nařízení pro vytvoření zaručeného elektronického podpisu předpokládá použití dat pro vytváření elektronického podpisu.

Jedním z důvodů, proč byl biodynamický podpis opomenut, může být to, že nařízení se jako unijní předpis soustřeďuje na přeshraniční elektronické transakce a chce přispět ke zvýšení důvěry v tomto kontextu. Přeshraniční elektronické transakce se však typicky budou provádět na dálku a výsledek záznamu o biodynamickém podpisu by v takovém případě přinesl jen malou přidanou důvěru mezi stranami, které se předem vůbec nemusí znát. Dokumenty takto podepsané se rovněž obtížně předávají nebo postupují třetí straně, má-li být zachována ověřitelnost podpisů. S ohledem právě na tyto potřeby je příklon k druhu provedení pomocí *viii. digitálního podpisu* v nařízení eIDAS pochopitelný. Uvedený stav navíc znamená, že v rámci vnitrostátní legislativy lze v případě potřeby snadno vytvořit úpravu vhodnou právě pro biodynamické podpisy, protože je možné se vyhnout rozporu s nařízením eIDAS.

6.16.13 Podregulace

Nařízení vůbec neobsahuje dostatečnou úpravu nařízením upraveného předmětu působnosti, a to zejména v oblasti dle čl. 1 písm. c) eIDAS (jen „pilířovitý" právní rámec pro elektronické podpisy, elektronické pečeti...). Částečně podregulovaná je i oblast služeb vytvářejících důvěru (kap. III eIDAS) a elektronického dokumentu (kap. IV eIDAS). Tyto nedostatky jsou zmiňovány průběžně v celé této kapitole v rámci dílčích témat. Podregulace snižuje právní jistotu. Její dosažení naopak mělo být cílem nařízení, aby se i přeshraničně vytvářela důvěra mezi stranami elektronických transakcí. Průběžně jsou navrhovány možnosti aspoň dodatečné nápravy vnitrostátní implementací nařízení, pokud přichází do úvahy. Podrobněji k fenoménu např. v 6.2.1. Jedno z možných vysvětlení tohoto stavu je zmíněno v 6.17.

6.16.14 Chybějící stanovení sad kryptografických algoritmů a parametrů

Bod odůvodnění číslo 8 rozhodnutí Komise (EU) 2016/650 zmiňuje, že pro spolehlivou ochranu proti padělání, jak vyžaduje příloha II odst. 1 písm. c) nařízení eIDAS, je nezbytným předpokladem bezpečnosti certifikovaného produktu použití vhodných kryptografických algoritmů, délek klíčů a hašovacích funkcí. Konstatuje však: *„Vzhledem k tomu, že tato problematika nebyla harmonizována na evropské úrovni, měly by se členské státy společně dohodnout na kryptografických algoritmech,*

délkách klíčů a hašovacích funkcích, které se v oblasti elektronických podpisů a pečetí mají používat."

Lze podotknout, že členské státy nemají v rámci nařízení eIDAS stanoven žádný závazný způsob dohadování se a zejména výsledného stanovení kryptografických sad a jejich parametrů. Bude tedy záležet především na jejich dobré vůli.

6.16.15 Nerozlišení míry automatizace elektronického podpisu

Při provádění elektronických transakcí, při provádění jejich završení formou elektronického podpisu, existují v zásadě tři možné scénáře:

1. podepisující osoba vytváří jeden podpis *individuálně*;
2. podepisující osoba vytváří podpisy *dávkově*, v jedné dávce jedním pokynem k vytvoření se jednotlivě podepíše každý dokument z předem dané sady (dávky) dokumentů nebo dat určených k podpisu;
3. podpisy vytváří *automat (elektronický agent),* bez přímého dohledu podepisující osoby, průběžně od okamžiku do uvedení do chodu, podle předem daných a nastavených pravidel.

Jen první scénář odpovídá tradičnímu postupu vytváření vlastnoručního podpisu.

V druhém scénáři jsou všechny podpisy vytvořeny automaticky, velmi rychle jeden po druhém. Během jednotek sekund lze tak podepsat i jednotky tisíc dokumentů. Od třetího případu se liší tím, že pečlivá podepisující osoba zde stále má v principu možnost provést předem systematické nebo namátkové kontroly dokumentů, které hodlá podepisovat, zda obsahují předpokládaný obsah. Scénář snad připomíná situaci, kdy podepisující osobě připraví stoh dokumentů k vlastnoručnímu podpisu sekretářka nebo jiný spolehlivý spolupracovník. Podepisující jednotlivé dokumenty spíše nečte, ale jen podepisuje, možnost čtení však má. Místo sekretářky zde podepisující zpravidla spoléhá na určitý výpočetní systém, který dokumenty (data k podpisu) připravil.

Ve třetím scénáři podepisující (vhodněji řečeno podepsaná) osoba obsah dokumentu předem vůbec nemá předložen, nemá možnost jej mít předložen. Zcela spoléhá na spolehlivou činnost automatu, právně někdy zvaného elektronický agent. Případy dva a tři spojuje spoléhání se na výpočetní systém, ve třetím případě je ale míra spolehnutí se vyšší.

Nařízení eIDAS uvedené tři scénáře výslovně nerozlišuje.

6.17 Hypotéza ovlivnění francouzským právem

V této části kapitoly se zabýváme jednou z možností, proč mohl vzniknout tak nepochopitelně strohý koncept nařízení eIDAS.

Ukazuje se, že samotné nařízení eIDAS je mnohem sebenosnější a dostatečnější právní úpravou v zemích, jako jsou Francie, Belgie a některé další státy EU (Maďarsko, Itálie, Lucembursko, Nizozemsko, Polsko, Rumunsko a Španělsko),[268] ovlivněné francouzskou deliktní civilistikou z *Code civil* podle jeho konceptu pochybení *(faute)*, nebo ve Spojeném království s deliktním právem z *common law* (tzv. *torts*), než je tomu v zemích se středoevropskou právní kulturou, ovlivněnou Rakouskem a Německem, do níž náleží i ČR.

Jinak řečeno, mezerovité a do podrobností nedotažené nařízení eIDAS může v uvedených státech i bez podrobného doplnění vnitrostátním právem regulovat na základě dobré technické praxe a spojení s technickými normami vyhlašovanými Komisí, podle obecných principů práva a soudní ochrany, které v těchto zemích platí a existují, zatímco např. v ČR a zřejmě ani v Německu tomu tak nebude.

Důsledkem je, že k dosažení zhruba stejného významu a rozsahu regulace nařízením eIDAS pro ČR, jako u zmíněných států, by bylo třeba jeho doplnění buďto dlouhou řadou podrobných ustanovení, nebo stručnějšími abstraktními pravidly.

Je-li tomu tak, pak by metodické kontroly (např. ČR) na případný rozpor s právem EU měly být revidovány. Metodika se totiž prvořadě soustřeďuje na snahu nepřidávat ani „neubírat“[269] žádné další právní normy k prostému textu norem unijního práva, což se ovšem děje bez vzájemného srovnání celkového účinku evropského právního předpisu v různých zemích EU.

6.17.1 Soukromoprávní delikty v právu Francie, Belgie aj. států s Code civil

Francouzskou civilně deliktní regulaci vystihuje vyjádření, že francouzské „právo soukromoprávní odpovědnosti nejen umožňuje chránit již uznávaná práva proti narušitelům, ale rovněž přispívá ke vzniku a ochraně **práv teprv vznikajících**, zatím neuznávaných. Vytváří metodu **doplňování a vylepšování** právního systému a jeho

[268] Ovlivnění zemí u soukromoprávních deliktů je bráno pode VAN DAM, C. *European Tort Law.* 2nd edition, Oxford University Press, 2013, s. 9.

[269] „Ubírání“ by se technicky provádělo též přidáváním nebo ponecháním právních norem, které by potlačovaly právo EU, jeho účel nebo smysl, aniž by s ním byly v přímém zřetelném rozporu, a tudíž by zůstaly aplikačně použitelné.

aktualizace“.[270] Důvodem jsou zejména dvě více než 200letá ustanovení francouzského občanského zákoníku (Code civil):

„Čl. 1382 Jakékoli jednání člověka, které způsobuje škodu jinému, zavazuje osobu, jejímž pochybením k ní došlo, aby ji napravila.

Čl. 1383 Každý je odpovědný nejen z důvodu svého jednání, ale ale i z důvodů své nerozvážnosti nebo nedbalosti." [271]

Pro přiznání odpovědnosti za škodu jsou, na rozdíl od práva ČR, ve Francii poté nutné jen tři předpoklady: existence škody, pochybení[272] *(faute)* a kauzální vztah mezi pochybením a škodou. Chybí požadavek protiprávnosti, neboť je částečně skryt právě v pojmu pochybení. Současně někdy pochybení *(faute)* obsahuje i zavinění ve smyslu českého práva, ale neshoduje se ani s ním a nemusí být ani vždy přítomno v našem smyslu slova zavinění, jazykovém ani právním.

Právě institut pochybení je klíčový pro avizovanou flexibilitu. Francouzské soudy a nauka definují *pochybení (faute)* jako „chybu v chování měřenou proti standardu rozumného člověka“.[273] Standard chování sice může být stanoven v některém zákonu, ale nemusí! V druhém případě může být „pochybení založeno na porušení nepsané předem existující povinnosti. *Nepsané povinnosti* mohou být *odvozeny* z nařízení, morálky, zvyků a **z technických norem.**“[274]

Rozpracovanými široce používanými referenčními standardy pro nepsané povinnosti jsou dále též chování „dobrého otce rodiny *(le bon père de famille*, *bonus pater familias)*, spravedlivého a opatrného člověka *(l'homme droit et avisé)*, nebo dobrého profesionála *(le bon professionnel)*.“[275]

---

[270] VINEY, G. – VAN GERVEN, W. – LEVER, J. – LAROUCHE, P. *Cases, Materials and Text on National, Supranational and International Tort Law.* Hart Publishing 2000. Zvýraznění přidal autor.

[271] Art 1382 C.civ: „Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrive, à le réparer“.
Art 1383 C.civ: „Chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence“.
Citace podle díla z poznámky pod čarou Chyba: zdroj odkazu nenalezen, s 2. V aktuálním číslování Code civil se jedná o články 1240 a 1241.

[272] V českých právních textech bývá *faute* překládána jako *zavinění*, v tomto textu autor užívá *pochybení*.

[273] British Institue of International and Comparative Law: *Introduction to French tort law*, dostupné z: <http://www.biicl.org/files/730_introduction_to_french_tort_law.pdf>; navštíveno 4/2016.

[274] VAN DAM, C., cit. dílo, s. 57. Zdůraznění přidáno autorem.

[275] VAN DAM, C., cit. dílo, s. 57.

Technické normy, spravedlivý a opatrný člověk i dobrý profesionál následně vytváří poměrně hustou síť povinností, aniž by musely být všechny objeveny a zapsány dlouho předem.

Při přijímání jakékoli legislativy v oblasti informačních technologií je značnou potíží snaha současně jak oblast právně normativně upravit, tak i nezabránit možnosti rozvoje technologií petrifikací právě stávajícího stavu, který může být praxí i záhy překonán.

Při tomto požadavku a existenci institutu *faute* je pak francouzský nebo belgický právník[276] vždy ve velkém pokušení načrtnout jen velmi strohou právní úpravu, k níž budou víceméně paralelně a částečně až nezávisle přijímány technické normy, s tím svým očekáváním, že právě technické normy samotné a činnost profesionálů zaručí implikaci i právních povinností pro jednání osob, které se zařízeními, jež z přijatých technických norem vycházejí, přijdou do styku a používání.

V současném středoevropském pojetí práva včetně právního řádu ČR stejný přístup fatálně selže, neboť technická norma v něm není pramenem práva a nemůže založit jakoukoli povinnost, a tedy ani právo bez toho, aby právo danou povinnost předem dostatečně určitě nestanovilo samo a technické normě nesvěřilo ev. jen její podrobnější provedení.

I když francouzské soudy mají tradičně být jen *ústy zákonodárce*, a tedy *automatem na rozsudky* v jednotlivém případě, právě v oblasti mimosmluvních soukromoprávních deliktů zákonodárce rezignoval na dokonalou úpravu všech povinností předem a svěřil jejich rozpoznávání ze života společnosti do úvahy a rozvoje práva soudům.

Oproti tomu ve středoevropském pojetí mají soudy velmi omezenou pravomoc i v tomto případě, slouží spíše k upřesňování práva než k právotvorbě, která je vyhrazena parlamentu.

6.17.2 Soukromoprávní delikty v právu Anglie

V právu Anglie a Walesu ve Spojeném království jsou soukromoprávní delikty charakteru náhrady škody nebo jiné újmy rozptýleny po tzv. *torts*. Ty se vyvinuly historicky zejména v oblasti *common law*, částečně ale i *equity*, z jednotlivých druhů

[276] Z průběhu přijímání nařízení eIDAS lze velmi pravděpodobně skutečně soudit na zvýšenou přítomnost a aktivitu osob, které pocházejí z frankofonního území EU.

žalob. Různé *torts* jsou vůči sobě značně fragmentované, nikdy nedošlo k vytvoření úplně jednotné systematizace naukou pro všechny delikty společně jednoduše proto, že inkrementální postup tvorby práva anglickými soudy neměl důvod vytvářet jednotné spojení. Hovoří-li nauka o tom, že francouzský systém spíše honoruje poškozeného, anglické právo soukromých mimosmluvních deliktů spíše brání extenzivním možnostem bezbřehých žalob.

V pivotním druhu *torts*, tedy v případě nedbalostního deliktu *(tort of negligence)*, existují tři podmínky: povinnost péče *(a duty of care)*, porušení této povinnosti a následná škoda.[277] Filtrem, oproti francouzskému právu řádově mnohem těsnějším, je již **povinnost péče**. Tu lze přiznat podle třístupňového testu kauzy *Caparo*:[278] i) poškození musí být přiměřeně předvídatelné, ii) musí panovat určitá blízkost *(proximity)* mezi žalobcem a žalovaným, iii) přiznání povinnosti péče musí být férové, spravedlivé a přiměřené. Pro asymetrické situace plyne povinnost péče spíše alternativně podle případu *Hedley Byrne*, zvaného též *předpoklad odpovědnosti*,[279] který dnes stanoví podmínky: i) žalovaný má z jistého úhlu pohledu určitou výhodu nad žalovaným, jako zvláštní dovednost nebo znalost; ii) žalobce na ní spoléhal a toto spolehnutí muselo být přiměřené; iii) nelze ji vyloučit vzdáním se práva; iv) předpoklad a spolehnutí se typicky, ne však nutně, vyplynou z přímého kontaktu mezi žalobcem a žalovaným.

Poté, co žalobce dokáže, že žalovaný mu dle výše uvedených kritérií byl povinen poskytnout povinnost péče, je třeba prokázat druhý krok, tedy že ji porušil. K tomu je třeba stanovit v závislosti na všech okolnostech případu **standard péče**. Zde se již podobně jako ve Francii jedná o právně nepsaná pravidla, jejich zjišťování či stanovení z praxe je ale právní otázkou *(question of law)*. Prokázání skutečného jednání žalovaného je faktickou otázkou *(question of fact)*, tedy důkazem skutkové podstaty. Z jejich srovnání vyplyne, zda byl standard péče v daném případě porušen.[280]

Ačkoli je tedy britský soudce omezen testy povinnosti péče, standard péče již zjišťuje v zásadě shodně jako francouzský soudce z celé ustálené praxe společnosti, tedy i z technických specifikací, technických norem a praxe profesionálů. Uživatelé

[277] VAN DAM, C., cit. dílo, s. 102.
[278] VAN DAM, C., cit. dílo, s. 105.
[279] VAN DAM, C., cit. dílo, s. 106.
[280] British Institue of International and Comparative Law: *Introduction to English Tort Law*, s. 2. Dostupné z: <http://biicl.org/files/763_introduction_to_english_tort_law.pdf>; navštíveno 4/2016,

informačních technologií následně nemohou tuto praxi ignorovat, ale jsou jí potenciálně vázáni i právně.

V oblasti *torts* i v jiných oblastech *common law* jsou pak k dispozici i dlouhé seznamy různých podmínek, testů a zásad, které nyní má anglické právo a anglický soudce k dispozici pro případ předkládání a řešení sporů z oblastí, jež dosud právně nebyly řešeny. Systém tak sice neposkytuje optimální právní jistotu, slušnou šanci na férové a spravedlivé řešení potenciálního sporu však ano.

6.17.3 Soukromoprávní delikty v právu ČR

Právo ČR vychází z ústavních maxim, čl. 2 odst. 4 Ústavy ČR: *„Každý občan může činit, co není zákonem zakázáno, a nikdo nesmí být nucen činit, co zákon neukládá.“* a čl. 4 odst. 1 Listiny základních práv a svobod: *„Povinnosti mohou být ukládány toliko na základě zákona a v jeho mezích a jen při zachování základních práv a svobod.“*

Uvedená dvě pravidla znamenají, že v ČR *není právních povinností*, které neukládá zákon nebo které nevznikají uložením na základě zákona a v jeho mezích, tj. buď podzákonnými právními předpisy, nebo smluvně. Kromě kulturního dědictví právního pozitivismu ze středoevropské oblasti práva, která byla rozvinuta zejména Rakouskem a Německem již na sklonku 18. a později v 19. století, jsou uvedená ústavní pravidla i ochranou práv osob před recidivou totalit z 20. století, ale i před různou úřední šikanou či i jen nešikovností opět nově se rozvíjející státní správy a samospráv po roce 1989. Konsekventně, ani v novém občanském zákoníku nebylo možné volit přiznání náhrady škody jinak než v souvislosti s povinnostmi uloženými zákonem nebo na jeho základě.

Technické normy nejsou v ČR považovány za pramen práva. Závaznost konkrétní technické normy musí navazovat na povinnosti stanovené předem v některém právním předpisu a být stanovena výslovně nebo aspoň dostatečně určitě v právní normě. Dostatečným příkazem rozhodně není pouhá nenormativní poznámka pod čarou. V ČR došlo v 90. letech ke značnému uvolnění závaznosti technických norem, což do značné míry souvisí se zavedením tržního prostředí a potřebou hospodářské soutěže, která není omezována technickou normalizací. Technické normy zpravidla stále představují určitou technickou praxi, nikoli však nutně nejrozvinutější nebo nejlepší. Potřeba normalizace úplně nezaniká, zejména v oblasti IT však je saturována tzv.

komerčními konsorcii různých výrobců, kteří pro potřeby kompatibility a interoperability svých produktů a služeb vyvíjí specifikace v různých oborech činnosti. Ukládat používání specifikací pocházejících z komerčních konsorcií naráží na obtíže základní legitimity v demokratické společnosti, byť za jistých okolností a podmínek se i k tomu někdy přistupuje, zpravidla jako k nevýlučné možnosti.

V ČR není pramenem práva ani obyčejové právo.[281]

Náhrada škody pro případ mimosmluvní nedbalosti vychází z § 2910 obč. zák., který v první větě stanoví odpovědnost za zaviněný zásah do absolutního práva a v druhé větě za zaviněné porušení ochranného účelu právní normy.[282] Čisté ekonomické ztráty se lze domoci spíše přes ustanovení věty druhé. Porušené absolutní právo nebo právní norma musí být stanoveny v některém právním předpise. Nejsou-li vyjádřeny, náhrada škody nevzniká, ledaže je ještě aplikovatelný generální prevenční § 2900 obč. zák., který vyjadřuje prastarou zásadu nikomu neškodit *(neminem laedere)*, ovšem velmi zúženým způsobem. Z ekonomických hodnot chrání pouze vlastnictví a rozhodně nepokrývá všechny možnosti čisté ekonomické ztráty.[283] Právně i skutkově bude předem vždy nejasné rozhodování o tom, zda nedbalost uživatele vznikne při *aktivním jednání*, nebo zda bude spíše považována za *opomenutí*. V případě opomenutí není § 2900 aplikovatelný vůbec. Spornými budou pravděpodobně i omezení *okolnostmi případu* a *zvyklostmi soukromého života*, jejichž absence opět může úplně zabránit použití § 2900.

Souhrnně lze uzavřít následovně. Bez stanovení právních povinností souvisejících s oblastí vztahů spadajících pod nařízení eIDAS v rámci implementace nařízení nebudou v této oblasti vztahů v ČR mezi podepisujícím a ověřujícím efektivně uplatnitelné soukromoprávní sankce druhu náhrady škody, zejména směřující k náhradě čisté ekonomické ztráty.

Některé soukromoprávní postihy umožní odpovědnost výrobců produktů za škodu vůči uživatelům produktů podle § 2939 a násl. obč. zák., byť by si i tyto vztahy zasloužily podrobnější rozvinutí při implementaci nařízení, neboť činnost bezpečnostních produktů v IT nespočívá pouze ve funkci, ale i v odolnosti vůči narušení funkcí a útokům na funkce. Soukromoprávní postih je umožněn v rámci některých

[281] Výjimkou je mezinárodní právo veřejné, které zde však není předmětem diskursu.
[282] Bezouška in HULMÁK, M. a kol. *Občanský zákoník VI. Závazkové právo. Zvláštní část (§ 2055–3014). Komentář.* 1. vydání. Praha: C. H. Beck, 2014, s. 1539–1540.
[283] Bezouška in HULMÁK, M. a kol., cit. dílo, s. 1515.

vztahů uživatelů k poskytovatelům služeb vytvářejících důvěru, s právní úpravou obsaženou v samotném nařízení eIDAS.

6.17.4 Nestejnost významu samotného nařízení eIDAS

Závěr o tom, že vnitrostátní implementací nedoplněné nařízení eIDAS bude mít v právním řádu zemí, jako je zmíněná Francie, Belgie a dalších 7 států s vlivem deliktní úpravy *Code civil*, jakož i v právním řádu Anglie, úplně jiný regulativní účinek, než když se zcela shodně nedoplní v právu ČR, je nyní nabíledni.

Lze říci, že regulační metoda nařízení eIDAS, spočívající jen ve velmi lehké právní normalizaci a značně spočívající na normalizaci technické, má svoji eleganci a účinnost, byť i tak je asi kritizovatelná (srov. průběžně tuto kapitolu), ale jen ve výše uvedených zemích, tedy rozhodně mimo ČR nebo Německo.

7. Implementace nařízení eIDAS v právu Německa

Německé úřady i zákonodárce zůstali během přijímání nařízení eIDAS, ale i po jeho vyhlášení v roce 2014, podivuhodně pasivní. Německo zůstalo zcela nepřipraveno na účinnost podstatné části nařízení, týkající se služeb vytvářejících důvěru, která nastala 1. 7. 2016. Německý zákon SigG i vyhlášky SigV zůstaly dále platné, ačkoli je zjevné, že terminologie zákona není navázána na nařízení a jeho četná ustanovení se musí nacházet v konfliktu s nařízením (např. již v úvodních částech definice pojmů, jako je elektronický podpis nebo kvalifikovaný elektronický podpis). Řešení těchto konfliktů, při aplikační přednosti evropského práva, není často nijak zjevné a způsobuje značnou právní nejistotu.

7.1 eIDAS-Durchführungsgesetz – referentský návrh

Teprve 18. října 2016 vydalo Spolkové ministerstvo hospodářství a energetiky (BMWE)[1] první verzi návrhu prováděcího zákona k eIDAS (eIDAS-Durchführungsgesetz), tzv. referentský návrh,[2] a rozeslalo jej k připomínkám centrálním aj. úřadům, jakož i odborným místům. Znění referentského návrhu je obtížné u BMWE nalézt, je však k dispozici u některých subjektů,[3] které k němu následně podávaly připomínky formou stanovisek (Stellungnahme). Dohledatelná jsou stanoviska těch subjektů, která byla zveřejněna na internetu. Připomínky přitom měly být podávány do 1. 11. 2016 (sic), jak zmiňuje např. stanovisko[4] spolku TeleTrusT, které sdružuje subjekty v oblasti bezpečnosti informačních technologií.

Jinak řečeno, na nařízení eIDAS vydané v Úředním věstníku EU dne 28. srpna 2014, s účinností částí týkajících se služeb vytvářejících důvěru od 1. 7. 2016, reaguje BMWE až 26 měsíců od vydání a 4 měsíce po účinnosti dané části eIDAS; dotazovaným stranám přitom nechá na vyjádření lhůtu pouhých dvou týdnů.

---

1 Bundesministeriums für Wirtschaft und Energie.

2 Referentenentwurf des Bundesministeriums für Wirtschaft und Energie: Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG.

3 Dostupné z: <https://www.cr-online.de/referentenentwurf-eldas-vo.pdf>; navštíveno 8. 8. 2016.

4 TeleTrusT: Stellungnahme zum „Referentenentwurf des 'eIDAS – Durchführungsgesetzes'" des Bundesministeriums für Wirtschaft und Energie, Berlin, 1. 11. 2016. Dostupné z: <https://www.teletrust.de/fileadmin/docs/publikationen/stellungnahmen/2016/161101-TeleTrusT-Stellungnahme_zum_BMWi-Referentenentwurf_eIDAS-Durchf%C3%BChrungsgesetz.pdf>; navštíveno 8. 8. 2017.

Situace budí dojem, že BMWE se aktivizovalo až někdy na jaře 2016, tedy v době, kdy se již nezadržitelně blížila účinnost části nařízení eIDAS a začaly na něj ve větší míře proudit dotazy ohledně kolizí SigG s eIDAS.[5]

Reakce na referentský návrh by si zasloužily samostatné sebrání a zhodnocení, neboť zřejmě představují cennou zpětnou vazbu praxe k problematice. Níže zmiňujeme pouze dvě nejvýznamnější.

7.1.1 Dobrozdání k referentskému návrhu – A. Roßnagel

Z právního pohledu má prvořadou důležitost dobrozdání prof. A. Roßnagela[6] z univerzity v Kasselu. V sofistikovaném stanovisku se snaží upozornit na hlavní problematicky palčivé části nařízení eIDAS a možnosti jejich řešení v německém právu. V úvodním zdvořilostně laděném prvním bodu návrh zákona vítá, neboť přispívá k právní jistotě, přizpůsobuje německou systematiku práva elektronického podpisu právním termínům z nařízení eIDAS, vytváří prostor tvorby práva v zákonné rovině. V druhém bodu upozorňuje, že požadavky eIDAS na přístupnost pro handikepované osoby mohou vyžadovat explicitní upřesnění. Těžiště dobrozdání ale zřejmě leží až v následujících bodech.

Ve třetím bodu se věnuje vztahu práva evropského a národního v případě evropského nařízení, jakým je i předpis eIDAS. Upozorňuje na možnosti, kdy navzdory aplikační přednosti nařízení je možné přijímat či aplikovat právo národní. Tento diskurs je zásadní, neboť až na jeho základě vzniká určitý prostor pro právotvorbu národního zákonodárce.

Ve čtvrtém bodu upozorňuje, že např. pojmy odbornosti *(Fachwissen)* a spolehlivosti *(Zuverlässigkeit)* jsou v nařízení neurčité a je možné je v německém právu konkretizovat např. podle dosavadní úpravy v SigG.

V pátém bodu upozorňuje, že eIDAS se nezabývá tím, jak zajistit dlouhodobý výsledek služeb vytvářejících důvěru, což dosud zajišťoval § 17 SigV.

---

[5] Uvedenou situaci nelze hodnotit jinak, než že ve spolkové administrativě buď neexistovaly odborné osoby ani útvary, které by přijetí evropského nařízení eIDAS sledovaly, byť i jen následně po jeho vydání. Pokud existovaly, pak zřejmě s nedostatkem pravomoci k jednání, byť i jen na úrovni vyvolání včasné přípravy prováděcího zákona.

[6] ROSSNAGEL, A. *Entwurf eines eIDAS-Durchführungsgesetzes – Verbändeanhörung*, Universität Kassel, Fachbereich Wirtschaftswissenschaften, Fachgebiet Öffentliches Recht, Umwelt- und Technikrecht, 31. Oktober 2016. Dostupné z: <https://www.uni-kassel.de/fb07/fileadmin/datas/fb07/5-Institute/IWR/Ro%C3%9Fnagel/Ro%C3%9Fnagel_Stellungnahme_zum_Referentenentwurf_VDG.pdf>; navštíveno 8. 8. 2017.

V šestém bodu se Roßnagel snaží zajistit exkluzivní požadavky na elektronické podpisy používané notáři, neboť nařízení eIDAS požadavky na bezpečnost podpisů snižuje. Podle něj je zapotřebí, aby aspoň pro notářské činnosti, zejména pro notářské zápisy, byly zajištěny vyšší úrovně bezpečnosti elektronického podpisu, než jsou podle eIDAS, což dle jeho právního názoru je možné. Rovněž se domnívá, že nařízení eIDAS se aplikačně neuplatňuje na ryze vnitrostátní skutkové podstaty, např. na úřední vyjádření a soudní jednání.

Konečně v posledním, sedmém bodu se zabývá důkazními účinky. Kvůli výše již zmíněnému snížení požadavků na bezpečnost dochází až k takovému výkladu, že tam, kde evropský právní předpis hovoří o domněnce *(Vermutung)*, je v německé důkazní systematice adekvátní hovořit pouze o důkazu *prima facie (Anscheinsbeweis)*, který je mnohem snáze vyvratitelný.

7.1.2 Stanovisko k referentskému návrhu – KosIT

Právně i technicky relevantní jsou mnohé připomínky koordinačního místa pro IT-standardy KosIT.[7] Kupříkladu v bodě 3 upozorňuje „S úžasem jsme vzali na vědomí, že v návrhu zákona Vertrauensdienstegesetz chybí jakékoli zmocnění k vydávání nařízení, které by odpovídalo současnému úseku I č. 1.2 Přílohy 1 SigV. Rádi bychom přitom dali najevo, že německý katalog algoritmů tak jako dříve považujeme za nutný.“ Výsledkem zřejmě je zmínka v § 2 odst. 2 VDG, že určení algoritmů a jejich parametrů zůstává v působnosti úřadu BSI, ovšem na základě jiných německých zákonů, než které vychází z evropského nařízení eIDAS.

Stanovisko v bodě 1 upozorňuje na to, že ačkoli návrh zákona předpokládá vkládání různých atributů do kvalifikovaných certifikátů, v současném znění technické normy EN 319 412-2 existuje mezera, neboť tyto druhy atributů neprofiluje. Německý standard CommonPKI pak nemá přeshraniční platnost. Atributy o zastoupení pak považuje za problematické, neboť mají značně menší trvanlivost než identifikační údaje, rolí úřadů pak není běžně přezkoumávat vztahy zastoupení mezi zaměstnavatelem a zaměstnancem, resp. úřady by byly nuceny nést riziko spoléhání se na tento údaj.

[7] Koordinierungsstelle fur IT-Standards (KosIT): *Stellungnahme zum Referentenentwurf eines eIDAS-Durchführungsgesetzes*, Bremen, den 1. 11. 2016. Dostupné z: <http://www.bmwi.de/Redaktion/DE/Downloads/Stellungnahmen/Stellungnahmen-elDAS-VO/stellungnahme-bremen.pdf?__blob=publicationFile&v=4>.

Stanovisko dále upozorňuje na potřebu nejasnosti ověřovacího modelu: „Specifikace ETSI Standards a zejména ETSI norma EN 319 102-1 V1.1.1 2016 dovolují použít ulitový model, ale i řetězový model, takže ověřování podle obou modelů je možné.“ Použití řetězového *(Kettenmodell)* nebo ulitového *(Schalenmodell)* modelu by pak dle KosIT mělo být jen na rozhodnutí podepisující osoby nebo spoléhající osoby. Tento názor se autorovi zdá chybný, neboť eIDAS stanoví určitá pravidla pro ověřování platnost v čl. 32 eIDAS a prozatím užívaná zmíněná technická specifikace nemůže být právně nadřazena evropskému nařízení. Komise zatím podle čl. 32 odst. 3 eIDAS nevyhlásila žádné technické normy pro účel ověřování platnosti.

7.2 eIDAS-Durchführungsgesetz – zákonodárný proces

Spolková vláda schválila svůj návrh[8] dne 29. března 2017.

Ve Spolkové radě (Bundesrat) byl návrh[9] zveřejněn 31. března 2017 jako návrh zákona spolkové vlády (tisk 266/17).[10] Dne 2. 5. 2017 k němu Výbor pro vnitřní záležitosti a Právní výbor při zaujaly stanovisko výborů,[11] obsahující jen několik spíše cizelačních doporučení, zatímco Výbor pro práci, integraci a sociální politiku se připomínek zdržel. Dne 12. 5. 2017 Spolková rada schválila usnesením[12] návrhy ze stanoviska výborů jako své vlastní.

Do Spolkového parlamentu (Bundestag) byl vládní návrh podán jako tisk 18/12494[13] dne 24. 5. 2017. Součástí vládního návrhu je i protivyjádření (Gegenäußerung der Bundesregierung) spolkové vlády v příloze 4 (Anlage 4) vůči stanovisku Spolkové rady, v němž odmítá navrhované změny a vysvětluje své důvody.

V první poradě *(Erste Beratung)* dne 1. 6. 2016 byl návrh přikázán čtyřem výborům.[14] Výbor pro průmysl a energetiku se svým závěrečným doporučením

[8] Dostupné z: <http://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2017/20170329-zypries-digitale-signatur-spart-kosten-und-ist-sicher.html>; navštíveno 8. 8. 2017.

[9] Dostupné z: <http://www.bundesrat.de/bv.html?id=0266-17>; navštíveno 8. 8. 2017.

[10] Bundesrat Drucksache 266/17 von 31. 3. 2017, Gesetzentwurf der Bundesregierung. Viz URL výše, nebo též u Bundestag na <http://dipbt.bundestag.de/dip21/brd/2017/0266-17.pdf>; navštíveno 8. 8. 2017.

[11] Bundesrat Drucksache 266/1/17 von 02.05.2017, Empfehlungen der Ausschüsse; viz URL výše.

[12] Bundesrat Drucksache 266/17 (Beschluss) von 12.05.17, Stellungnahme des Bundesrates; viz URL výše.

[13] Deutscher Bundestag, 18. Wahlperiode, Drucksache 18/12494 von 24.05.2017, Gesetzentwurf der Bundesregierung... Dostupné z: <http://dip21.bundestag.de/dip21/btd/18/124/1812494.pdf>; navštíveno 8. 8. 2017.

[14] *„Überweisungsvorschlag: – Ausschuss für Wirtschaft und Energie (f) – Ausschuss für Recht und Verbraucherschutz – Ausschuss für Verkehr und digitale Infrastruktur – Ausschuss Digitale Agenda“* v Deutscher Bundestag Stenografischer Bericht 237. Sitzung Berlin, Donnerstag, den 1. Juni 2017, Plenarprotokoll 18/237. Dostupné z:

a zprávou[15] vyjádřil dne 21. 6. 2017. Výbor navrhl jen drobné doplnění návrhu, přičemž shrnul i výsledky hlasování ostatních přikázaných výborů. Ve všech ostatních výborech došlo ke schválení buď původního návrhu, resp. s navrženou změnou, proti byla vždy frakce *Bündnis 90/Die Grünen*, zpráva však neuvádí její důvody.

Dne 22. 6. 2016 byly vládní návrh a výše uvedené doporučení výboru projednány ve sloučené druhé i třetí poradě[16] zároveň. Ve znění s návrhem výboru byl hlasy vládních frakcí (*Regierungsfraktionen*, tj. zřejmě stran *CDU/CSU* a *SPD*) a frakce *Die Linke* zákon přijat, zatímco frakce *Bündnis 90/Die Grünen* hlasovala proti. V žádné ze tří porad nedošlo k plenárnímu vystoupení žádného poslance.

Spolkové radě bylo zpětně přijetí zákona oznámeno 23. 6. 2017 tiskem 518/17,[17] se lhůtou k vyjádření se do 14. 7. 2017. Spolková rada vyslovila 7. 7. 2017 souhlas se zákonem[18] a současně i usnesení,[19] že schválené znění zákona *„vyhovuje článku 108 odstavci 5 základního zákona“*.

7.2.1 eIDAS-Durchführungsgesetz – vydání

Prováděcí zákon *eIDAS-Durchführungsgesetz*[20] byl vydán v německé spolkové sbírce zákonů dne 28. července 2017 a účinnosti nabyl den poté, tj. 29. července 2017. S jeho účinností byl zrušen i dosud platný zákon SigG a k němu příslušná vyhláška SigV. Prováděcí zákon sestává z řady částí. Jeho nejvýznamnější částí je první část, kterou se přijímá Vertrauensdienstegesetz, zkratka VDG (srov. 7.3).

<http://dipbt.bundestag.de/dip21/btp/18/18237.pdf#P.24070>; navštíveno 8. 8. 2017.

15 Deutscher Bundestag, 18. Wahlperiode, Drucksache 18/12833 von 21.06.2017, Beschlussempfehlung und Bericht des Ausschusses für Wirtschaft und Energie (9. Ausschuss) zu dem Gesetzentwurf der Bundesregierung ... – Drucksache 18/12494. Dostupné z: <http://dip21.bundestag.de/dip21/btd/18/128/1812833.pdf>.

16 Deutscher Bundestag Stenografischer Bericht 240. Sitzung Berlin, Donnerstag, den 22. Juni 2017, Plenarprotokoll 18/240, s. 24533. Dostupné z: <https://dip21.bundestag.de/dip21/btp/18/18240.pdf#P.24533>.

17 Bundesrat Drucksache 518/17, dostupné z: <http://www.bundesrat.de/bv.html?id=0518-17>.

18 Bundesrat Stenografischer Bericht 959. Sitzung Berlin, Freitag, den 7. Juli 2017, Plenarprotokoll 959, s. 374. Dostupné z: <https://www.bundesrat.de/SharedDocs/downloads/DE/plenarprotokolle/2017/Plenarprotokoll-959.pdf>.

19 Bundesrat Drucksache 518/17 (Beschluss) von 07.07.17, Beschluss des Bundesrates. Dostupné z: <http://www.bundesrat.de/bv.html?id=0518-17>; navštíveno 8. 8. 2017.

20 Gesetz zur Durchführung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Durchführungsgesetz); Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 52, ausgegeben zu Bonn am 28. Juli 2017. Dostupné z: <http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s2745.pdf>; navštíveno 8. 8. 2017.

7.2.2 eIDAS-Durchführungsgesetz – změny zákonů

Články 2 až 11 eIDAS-Durchführungsgesetz jsou novelizační ustanovení, kterými se nahrazují dosavadní využití pojmů digitálních objektů a související, jak byly dosud upraveny v SigG a v SigV, za formulace, které pojmově odpovídají novému nařízení eIDAS, popř. jeho prováděcímu zákonu VDG (srov. níže). Autor takové úpravy označuje jako ustanovení využívající nařízení eIDAS. Jde rovněž o implementační úpravu německého práva.

Změny postihly např. právní předpisy De-Mail-Gesetz (čl. 3), Personausweisgesetz (čl. 4), Personausweisverordnung (čl. 5), Abgabenordnung (čl. 6), Vergabeverordnung Verteidigung und Sicherheit (čl. 7), Vergabeverordnung (čl. 8), Sektorenverordnung (čl. 9), Konzessionsvergabeverordnung (čl. 10). Dalších 46 právních předpisů je novelizováno ve 46 odstavcích čl. 11 (Folgeänderungen). Většina změn je formální, spočívají například ve vyškrnutí vazby *„podle Signatursgesetz"*. Některé předpisy jsou novelizovány více, z důležitých to je například v čl. 11 odst. 15 změna Zivilprozessordnung v jeho § 371a, která je ovšem podstatná (srov. níže). Dle čl. 11 odst. 27 byl upraven i BGB, ovšem jen vyškrnutím *„podle Signatursgesetz"*.

7.3 Zákon o službách vytvářejících důvěru (VDG)

Zákon o službách vytvářejících důvěru (*Vertrauensdienstegesetz*, dále jen „VDG"[21]) je obecným implementačním zákonem nařízení eIDAS v Německu. Dle § 1 VDG upravuje provádění předpisů nařízení eIDAS.

Zákon se však nevztahuje na právní předpisy, které upravují použití určitých služeb vytvářejících důvěru a jimi využívaných produktů. Takovým zákonem by mohl být například De-Mail-G (De-Mail-Gesetz), jímž upravená služba De-Mail by mohla v Německu být kandidátem na kvalifikovanou službu elektronického doporučeného doručování. Dalšími možnými příklady jsou jiné zákony, které dovolují nebo přikazují využití určitého kvalifikovaných digitálních objektů z eIDAS.

Níže jsou probrány hlavní body úpravy ve VDG.

[21] Zkratka VDG je oficiální německou zkratkou pro Vertrauensdienstegesetz. V plné citaci: „Vertrauensdienstegesetz vom 18. Juli 2017 (BGBl. I S. 2745), das durch Artikel 2 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist."

7.3.1 Institucionálně kompetenční zmocnění

V zákonu VDG se určuje působnost zastupovat německý stát pro různé úlohy a oblasti předpokládané v nařízení eIDAS. Podle § 2 odst. 1 VDG se činnost *orgánu dohledu (Aufsichtsstelle)* rozděluje mezi dva subjekty, a to podle druhu služby vytvářející důvěru. Pro služby vytvářející důvěru podle čl. 3 bodu 16 písm. a) a c) eIDAS je orgánem dohledu *Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen* (dále jen „Bundesnetzagentur"), pouze pro služby podle čl. 3 bodu 16 písm. b), tj. služby autentizace internetových stránek, je orgánem dohledu *Bundesamt für Sicherheit in der Informationstechnik* (dále jen „BSI"). V § 2 odst. 2 VDG se zdůrazňuje, že výše uvedené přiřazení působnosti pro Bundesetzagentur se nedotýká působností BSI dle jiných německých zákonů, zejména stanovení technických norem, hodnocení bezpečnostních algoritmů a jejich parametrů, stanovení předpisů a hodnocení technických norem pro nasazování služeb vytvářejících důvěru v digitalizačních plánech odpovídajících odborných zákonů. V § 4 VDG se určují další podrobnosti činnosti orgánu dohledu nad poskytovateli služeb vytvářejících důvěru a v § 5 VDG jsou stanoveny povinnosti součinnosti (obecného) poskytovatele služeb vytvářejících důvěru vůči orgánu dohledu, v rámci prokazování dodržování povinností stanovených nařízením eIDAS.

Úřad BSI je dle § 2 odst. 3 VDG určen i jako *vnitrostátní orgán pro bezpečnost informací*, kterému se dle čl. 19 odst. 2 eIDAS hlásí bezpečnostní incidenty.

Subjektem, který zřizuje, udržuje a zveřejňuje důvěryhodné seznamy, je podle § 9 VDG též Bundesnetzagentur.

Určené subjekty certifikující bezpečnost produktů informačních technologií (zkušebny) jsou podle VDG dvojího druhu. *Veřejným subjektem* je dle § 17 odst. 4 VDG úřad BSI. *Soukromé subjekty* jmenuje Bundesnetzagentur na návrh organizace, přičemž jejich schopnosti ověřuje akreditační orgán podle německého akreditačního zákona. Dokud Komise nevydá akty v přenesené pravomoci podle čl. 30 odst. 4 eIDAS, stanoví potřebná kritéria německé úřady v souladu s § 17 VDG.

V § 20 VDG je upraveno zmocnění spolkové vlády vydat k VDG prováděcí nařízení *(Rechtsverordnung)*.

7.3.2 Přídavné atributy v kvalifikovaných certifikátech

Dle § 12 VDG lze do kvalifikovaných certifikátů pro elektronické podpisy nebo pro elektronické pečeti vkládat další atributy (znaky) subjektu.

Na žádost žadatele lze zařadit údaje o plné moci žadatele od třetí osoby k jejímu zastupování; údaje týkající se úředního, zaměstnaneckého nebo zvláštního vztahu k osobě žadatele; další údaje týkající se osoby. Údaje o plné moci k zastoupení smí být vloženy pouze s doloženým souhlasem třetí osoby. Úřední, zaměstnanecké nebo zvláštní údaje smí být vloženy jen s potvrzením příslušného místa. Další osobní údaje se vkládají na žádost dotyčného. Jsou-li výše uvedené zvláštní atributy vkládány do certifikátu, v němž je uveden namísto jména pseudonym, je k tomu nutné doložení výslovného souhlasu buď uvedené třetí osoby, nebo příslušného místa.

Výše uvedené se přiměřeně použije i pro kvalifikované certifikáty pro elektronické pečeti. V nich lze uvést i atribut pro vztah zastoupení uvnitř žádající právnické osoby, pokud je tento zastupitelský vztah vůči poskytovateli doložen.

Dle § 12 odst. 3 VDG si tedy lze představit i kvalifikovaný certifikát pro elektronickou pečeť, který je vystaven na právnickou osobu, avšak je v něm vyznačen atribut jejího zastupování, tzn. že případné údaje o fyzické osobě by měly význam určení osoby, zástupce, který jménem právnické osoby jedná. Způsob tohoto použití by bylo ještě vhodné ověřit nezávisle na znění VDG.

7.3.3 Povinnost poučení o bezpečnostních opatřeních a právních účincích

Podle § 13 odst. 1 bod 1 VDG má kvalifikovaný poskytovatel služeb vytvářejících důvěru povinnost poučit uživatele služby o *„opatřeních, která jsou nezbytná k tomu, aby přispívala k bezpečnosti nabízených kvalifikovaných služeb vytvářejících důvěru a jejich hodnověrnému používání, a přitom poukazovat na odpovídající informační možnosti, zejména na informační propozice výrobce produktů pro kvalifikované služby vytvářející důvěru a na informační propozice orgánů dohledu"*. Kvalifikovaný poskytovatel má rovněž za povinnost poučit uživatele o tom, že bezpečnostní hodnota kvalifikovaných elektronických podpisů, pečetí nebo elektronických časových razítek se v čase snižuje a má se ošetřit opatřením pro dlouhodobé udržení důkazu (srov. 7.3.4). Má je též poučit o právních účincích kvalifikovaných služeb vytvářejících důvěru.

Německý zákonodárce povinnost poučení v zásadě podřadil jako konkretizační implementaci povinnosti seznámení s podmínkami služby, které je stanoveno podle čl. 24 odst. 2 písm. 1) nařízení eIDAS.

Autor se domnívá, že právě tato poučovací povinnost do značné míry nahrazuje explicitní stanovení povinností podepisující nebo spoléhající osoby. Podle § 272 odst. 2 BGB *nedbale jedná*, *„kdo na pečlivost potřebnou ve styku nebere zřetel"*.[22] Poučení má za následek, že by si i dříve neznalý uživatel již měl být vědom pečlivosti potřebné ve styku při použití kvalifikovaného elektronického podpisu. Dojde-li pak k nedodržení pečlivosti, je takové jednání z pohledu práva nedbalé. Záleží poté na tom, zda nedbalost je dostatečným právním důvodem pro nepříznivé právní následky. Zřejmě tomu tak bude tehdy, pokud by podepisující nebo spoléhající osoba namítala omyl vůle, například nedostatek vědomí k vyjádření *(Erklärungsbewußtsein)*, jak již rozebráno výše v 5.2.2. Zde je dle judikatury BGH rozhodná právě nedbalost. Nejednala-li osoba nedbale, a přesto mohlo k omylu vědomí vyjádření věrohodně dojít, bude právní jednání nicotné. Jednala-li nedbale, bude její právní jednání platné a nezbývá jí, než ho rozporovat dle § 119 an. BGB, s čímž ale souvisí i její povinnost k náhradě škody dle § 122 BGB. V jiných případech německé soukromé deliktní právo obecně vyžaduje kromě znaku *zavinění*, jako je uvedená nedbalost, i znak *protiprávnosti*,[23] která by se musela zvlášť nalézt. Možnost rozporovatelnosti právního jednání bez povinnosti náhrady škody by byla, pokud by omyl byl vyvolán lstivým klamem dle § 123 BGB (srov. 3.2.4).

Za platnosti předchozí německé úpravy platila navíc ještě povinnost dle § 6 bod. 2 SigV utajovat přístupový PIN. V případě nedbalostního úniku této přístupové informace a při jednání bez srozumění s držitelem podpisového klíče sice držitel nebyl zavázán jako právně jednající osoba, ale byl spoléhající se osobě povinován k náhradě škody podle povinností ochrany *(Schutzpflichten)*, a to buď dle § 280 odst. 1 BGB v rámci smluvního vztahu, nebo ve spojení s § 311 BGB v rámci vztahu předsmluvního.[24]

---

[22] *„Fahrlässig handelt, wer die im Verkehr erforderliche Sorgfalt außer Acht läßt."*

[23] ELISCHER, D. Protiprávnost – co je jejím zdrojem v soukromém právu? *Časopis pro právní vědu a praxi* č. 4/2016, s. 501–526, s. 505.

[24] EINSELE, D. *BGB § 126a Elektronische Form*. Rn. 21. In: SÄCKER, J. (ed.) *Münchener Kommentar zum Bürgerlichen Gesetzbuch: BGB Band 1: Allgemeiner Teil §§ 1–240, ProstG, AGG*. 7. Auflage. München: C. H. Beck, 2015. Dostupné z: <https://beck-online.beck.de/>.

7.3.4 Dlouhodobé udržení důkazu

Dle § 15 VDG se v případě potřeby mají kvalifikovaně elektronicky podepsaná, pečetí nebo elektronickým časovým razítkem opatřená data nově chránit předtím, než klesne jejich bezpečnostní hodnota. Mají se k tomu použít *vhodná opatření*, která musí odpovídat stavu techniky. Ustanovení neurčuje, o jaký druh opatření se má jednat. Nevztahuje se však pouze na kvalifikovaný digitální objekt upravený v nařízení eIDAS, ale vyžaduje se chránit celek, tj. například podepsaná data a jejich kvalifikovaný elektronický podpis dohromady.

7.3.5 Odvolání kvalifikovaného certifikátu

V § 14 VDG je podrobnější úprava podmínek odvolání *(Widerruf)* kvalifikovaného certifikátu, než je v eIDAS. V kontextu německého VDG zde budeme hovořit o odvolání, v rámci českého právního řádu se užívá pojem zneplatnění, který se ale zdá být významově naprosto shodný.

Podle § 14 odst. 1 VDG musí kvalifikovaný poskytovatel služeb dosud platný kvalifikovaný certifikát bezodkladně odvolat zejména tehdy, pokud to požaduje osoba, které byl vydán; pokud byl z hlediska příloh I, III nebo IV eIDAS vystaven na základě nesprávných (falešných) údajů; pokud ukončuje svoji činnost; nebo skutečnosti nasvědčují, že kvalifikovaný certifikát byl zfalšován nebo není dostatečně odolný proti falšování, nebo použitý kvalifikovaný prostředek pro vytváření elektronických podpisů (pečetí) vykazuje bezpečnostní nedostatek. Jiné důvody odvolání lze stanovit smluvně. Skutečnost falešných údajů ve vydaném certifikátu se může vyznačit jako důvod odvolání.

Pokud kvalifikovaný certifikát obsahuje zvláštní atributy, může odvolání kvalifikovaného certifikátu požadovat i třetí osoba, jež vydala souhlas s atributem o svém zastoupení a právo k zastoupení zaniklo nebo bylo odvoláno, nebo příslušné místo, které potvrdilo přídavný atribut, přičemž pominuly podmínky pro uvedení takového údaje.

Odvolání kvalifikovaných certifikátů může nařídit i orgán dohledu, pokud dojde k ukončení činnosti poskytovatele, nebo došlo k výše uvedeným možnostem zfalšování kvalifikovaného certifikátu či bezpečnostního nedostatku prostředku.

7.3.6 Další záležitosti

VDG obsahuje i další úpravy. V § 8 VDG jsou upraveny záležitosti ochrany dat. V § 7 VDG se nachází pravidla pro bezbariérovost služeb, tj. pro postižené osoby. V § 16 VDG jsou podrobnosti plánu ukončení činnosti. V § 18 VDG se upravuje způsob hodnocení v souvislosti s kvalifikovanou službou elektronického doporučeného doručování v souvislosti s odpovídající německou úpravou v De-Mail-G. V § 19 VDG jsou určeny sankce za porušení povinností podle VDG nebo eIDAS.

7.4 Novelizace § 371a Zivilprozessordnung

Dle čl. 11 odst. 15 eIDAS-Durchführungsgesetz byl změněn § 371a odst. 1 věta druhá ZPO: *„Dojem pravosti vyjádření předloženého v elektronické formě, který spočívá na ověření platnosti kvalifikovaného elektronického podpisu podle článku 32 nařízení (EU) č. 910/2014 ... může být otřesen jen takovými skutečnostmi, které zakládají vážné pochybnosti, že vyjádření bylo provedeno odpovídající osobou."*

V § 371a ZPO se upravuje *důkazní síla elektronických dokumentů*. Dle prvé věty § 371a odst. 1, která zůstala nezměněna, *„Soukromé elektronické dokumenty, které jsou opatřeny kvalifikovaným elektronickým podpisem, se přiměřeně řídí předpisy ohledně důkazní síly soukromých listiny."*

Nová úprava druhé věty sleduje původní smysl úpravy, který se ovšem odvolával na Signatursgesetz. Tak jako dříve i nyní má QES v rámci soukromé listiny pouze povahu důkazu *prima facie (Augenschein, Anscheinsbeweis)*.

Tím německý zákonodárce potvrzuje, že čl. 25 odst. 2 eIDAS nemá charakter právní normy, která by byla závazná pro důkazní hodnocení QES, ale že využívá bodu odůvodnění 22 eIDAS, že je na členském státu stanovit důkazní účinky, nestanoví-li nařízení eIDAS jinak. Německý zákonodárce tedy míní, že nařízení eIDAS důkazní účinky QES nestanoví. Pro soukromé listiny vlastnoručně podepsané se užívá odlišná úprava v § 440 odst. 2 ZPO, popř. navazující § 441 a § 442 ZPO. Současně touto novelou sepisovatel návrhu zákona vyhověl aspoň částečně jednomu z podnětů Roßnagela (srov. 7.1.1).

7.5 Souhrn

Německá implementace eIDAS byla přijata o rok pozdě.

Za chybu německé implementace autor považuje, že VDG obecně nerecipuje digitální objekty a služby vytvářející důvěru z eIDAS do německého práva. Německý zákonodárce zde zaujímá pozici, jako by unijní nařízení buď mělo přímou působnost ve všech oblastech německého práva, nebo je dána aplikací působnosti nařízení. Právně platná bude spíše druhá možnost (srov. 6.3), což může vést k nepřehlednosti německého uživatele práva.

Za klady implementace lze považovat, že zákonodárce konkretizoval odvolání kvalifikovaného certifikátu (§ 14 VDG), které je v eIDAS upraveno jen příliš obecně. Zmiňuje i dlouhodobé udržení důkazu (§ 15 VDG), povinnost poučení uživatele (§ 13 VDG), zakládá přídavné atributy (§ 12 VDG). S přídavnými atributy je spojeno i právo osob, které s nimi vyslovily souhlas nebo je potvrzovaly, aby mohly žádat o zneplatnění.

Nejasné zůstává, zda mezi jiné atributy vkládané na žádost žadatele bude moci zůstat omezení použitelnosti certifikátu podle druhu a podle finančního omezení.

Je však zřejmé, že například atribut o právu zastoupení je natolik právně významným atributem, že doplnění volitelných atributů dle čl. 28 odst. 3 eIDAS, zde členským státem, rozhodně není pouze formální.

V důkazní rovině obsahuje ZPO velmi podrobnou úpravu důkazních účinků, a to i důkazních účinků kvalifikovaného elektronického podpisu z eIDAS. ZPO ale neupravuje důkazní účinky zaručené ani kvalifikované elektronické pečeti, ponechává je tedy zřejmě ve znění eIDAS, ať již soudy zhodnotí význam obsažených domněnek jakkoli.

8. Implementace nařízení eIDAS v ČR

V této kapitole je pojednáno o implementačním předpisu nařízení eIDAS v ČR.

8.1 Implementace adaptačním zákonem

V ČR bylo nařízení eIDAS v částech mimo svou kap. II, tj. pro předmět úpravy dle čl. 1 písm. b) a c) eIDAS, zatím implementováno zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce (dále jen „ZSVD" nebo „adaptační zákon") a změnovým zákonem č. 298/2016 Sb. (dále jen „změnový zákon"). Níže jsou uvedena implementační ustanovení podle svého druhu, jak jsou rozlišována naukou práva EU.[1] Derogovaným ustanovením je věnována zvláštní část níže. Jak uvádí i důvodová zpráva,[2] oblast nařízení neupravují žádné mezinárodní smlouvy, jimiž je ČR vázána.[3] Není třeba přijímat opatření vůči mezinárodním smlouvám.

8.2 Adaptivně-recepční ustanovení

Recepce nařízení eIDAS pro právní jednání v právním řádu ČR se provádí v § 5–11 ZSVD. Stejná ustanovení budou ze ZSVD též adresáty práva ČR zřejmě nejčastěji čtena a vykládána. Jedná se o úpravu obecnou, zákon ZSVD ani nařízení eIDAS nebrání tomu, aby zákonodárce v dílčím případě přijal úpravu zvláštní.

8.2.1 Právní jednání veřejnoprávního podepisujícího

V § 5 písm. a) ZSVD je legislativní zkratkou určen pojem *„veřejnoprávního podepisujícího"*, kterým je

- *„stát,*
- *územní samosprávný celek,*
- *právnická osoba zřízená zákonem nebo*
- *právnická osoba zřízená nebo založená státem, územním samosprávným celkem nebo právnickou osobou zřízenou zákonem"* (rozčlenil autor).

Tyto subjekty jsou veřejnoprávním podepisujícím bez ohledu na právní podstatu jednání, které samy provádí nebo které se provádí vůči nim. Může tedy jít o právní

[1] KRÁL, R. *Nařízení ES z pohledu jejich vnitrostátní aplikace a implementace*. Praha: C. H. Beck, 2006.

[2] Důvodová zpráva ZSVD, Sněmovní tisk 763, Parlament ČR, PS 2013–2017. Dostupné z: <http://www.psp.cz/sqw/historie.sqw?o=7&T=763>; navštíveno 10/2017.

[3] Důvodová zpráva ZSVD, s. 24.

jednání veřejnoprávní povahy i soukromé právní jednání. Důvodem dle důvodové zprávy[4] je, aby u těchto subjektů nedocházelo k špatným vyhodnocením povahy podepisovaného právního jednání, zajištění jednotnosti výkonu spisové služby,Chyba: zdroj odkazu nenalezen ale i celounijní akceptovatelnosti podpisů.[5]

Dle § 5 písm. b) ZSVD se však pravidla § 5 ZSVD použijí i na osoby nespadající pod pojem *„veřejnoprávního podepisujícího"*, pro právní jednání *„při výkonu své působnosti"*. Takovými osobami mohou být i soukromoprávní subjekty, jsou-li nadány výkonem působnosti, tj. zřejmě zejména výkonem veřejné správy pro vrchnostenské jednání. Jednají-li tyto subjekty soukromoprávně, pravidla § 5 ZSVD a potažmo ani § 6 ZSVD (pro jednání vůči nim) se jich netýkají. [6]

Podepisuje-li tedy veřejnoprávní podepisující elektronický dokument, kterým právně jedná, musí podle § 5 ZSVD použít pouze *„kvalifikovaný elektronický podpis"* (QES).[7] Navíc musí podle § 11 odst. 1 ZSVD opatřit *„podepsaný elektronický dokument kvalifikovaným elektronickým časovým razítkem"* (QTS).[8]

Jedná se o obecné ustanovení, zvláštní zákon může stanovit druh elektronického podpisu odlišně.

Autor zde v § 5–10 ZSVD použitý pojem *elektronický dokument* vykládá ve smyslu definice v eIDAS (srov. 6.15.11). Důvodem je systematická souvislost digitálních objektů s elektronickým dokumentem, které nařízení eIDAS předpokládá, resp. předpokládalo zejména ve svém návrhu od Komise. Důvodem je i to, že dle § 1 ZSVD je předmět zákona upravován *„v návaznosti na přímo použitelný předpis Evropské unie"*, tj. nařízení eIDAS. Konečně i důvodová zpráva sama vykládá,[9] že pojmy nařízení eIDAS zákon znovu nedefinuje, ale přejímá je z nařízení, přičemž mezi pojmy používanými zákonem výslovně zmiňuje i elektronický dokument. Autor zde upozorňuje, že pojem *elektronického dokumentu* podle eIDAS je poměrně široký a v konkrétních případech použití právního předpisu ČR může být podepisovaný obsah

[4] Důvodová zpráva ZSVD, s. 34.

[5] Důvodová zpráva ZSVD (s. 34) uvádí celounijní akceptovatelnost podepsaných dokumentů. Jak je uvedeno v textu výše (srov. 6.15.11, 6.14), uznávání elektronických dokumentů nařízení eIDAS bez dalšího nestanoví. Přeshraniční uznávání QES je však jednou z podmínek, které bude třeba splňovat.

[6] Dle důvodové zprávy (s. 34) byly subjekty v § 5 ZSVD stanoveny tak, aby jednak korespondovaly s okruhem tzv. veřejnoprávních původců podle § 3 a § 63 zák. č. 499/2004 Sb., o archivnictví a spisové službě, kteří též mají i povinnost vést spisovou službu, a jednak podle kritéria možného statusu subjektu jako nositele veřejné moci a jeho orgánů jako vykonavatelů veřejné moci.

[7] Dle § 19 odst. 1 ZSVD lze do půlky září 2018 namísto QES dle § 5 ZSVD použít i $AdES_{QC}$.

[8] Dle § 19 odst. 5 ZSVD lze do půlky září 2018 namísto QTS dle § 11 ZSVD použít elektronické časové razítko vydané kvalifikovaným poskytovatelem služeb vytvářejících důvěru.

[9] Důvodová zpráva k ZSVD, s. 31.

vymezen úžeji. V takovém případě má zvláštní úprava práva ČR přednost, pojem elektronického dokumentu z eIDAS by však měl být dostatečně obecný, byť je méně obecný než *data* (srov. 6.15.11).

Předepsaná kombinace digitálních objektů, tj. QES a QTS, zaručuje střednědobou možnost ověření platnosti QES podle čl. 32 nebo 33 eIDAS a jejich vytvoření je pro veřejnoprávní podepisující dobře realizovatelné. Znění § 11 odst. 1 ZSVD autor vykládá tak, že se časovým razítkem QTS má opatřit spojení elektronického dokumentu a jeho podpisu QES, nikoli tedy například samotný QES.

Požadavek § 11 ZSVD není v rozporu s požadavky nařízení eIDAS, neboť pouze zvyšuje požadavky na právní jednání veřejnoprávních podepisujících. Není tedy ani například v rozporu s čl. 27 odst. 3 eIDAS, ani v rozporu s čl. 25 odst. 2 a 3 eIDAS.

8.2.1.1 Pečetění veřejnoprávním podepisujícím

V § 8 ZSVD se stanoví obecné podmínky použitelnosti institutu elektronické pečeti namísto elektronického podpisu.

Elektronickou pečeť má veřejnoprávní podepisující[10] použít, *„nestanoví-li jiný právní předpis jako náležitost právního jednání obsaženého v dokumentu podpis nebo tato náležitost nevyplývá z povahy právního jednání"*. Je mu pak přikázáno zapečetit *„dokument v elektronické podobě kvalifikovanou elektronickou pečetí."* (QESeal).[11] Navíc musí podle § 11 odst. 2 ZSVD opatřit *„zapečetěný elektronický dokument kvalifikovaným elektronickým časovým razítkem"* (QTS).[Chyba: zdroj odkazu nenalezen]

Autor spatřuje určitou nevhodnost příkazu použití QESeal v tom případě, pokud veřejnoprávní podepisující má jednat automatickým či převážně automatickým způsobem. V takovém případě by se mu jako adekvátnější jevilo povolení použití např. $\text{AdESeal}_{\text{QC}}$, jelikož dosažení úrovně QESeal nepovažuje v tomto případě za zcela jistě dosažitelné. Veřejnoprávní podepisující pak mohou být postaveni před nemožnou podmínku. Ta se však odrazí v tom, že takové vlastnosti budou požadovat po svých dodavatelích. Jimi dodaná řešení však nakonec nemusí podmínku jistě splnit, což může být důvodem napadení daného právního jednání, a to na úkor veřejnoprávního podepisujícího, tedy potažmo státu.

[10] A *„jiná právnická osoba, jedná-li při výkonu své působnosti"*. Subjekt je zde vztažen na právnickou osobu zřejmě z toho důvodu, že přikázaný druh elektronické pečeti může vytvořit pouze pečetící osoba, tj. osoba právnická.

[11] Dle § 19 odst. 2 ZSVD lze do půlky září 2018 namísto QESeal (žádanou i např. dle § 8 ZSVD) použít elektronickou značku podle zákona č. 227/2000 Sb. nebo $\text{AdESeal}_{\text{QC}}$.

Další otázkou je, zda a proč vůbec stanovit obecnou povinnost použít elektronickou pečeť, navíc v úrovni QESeal, pouze na základě výše uvedené podmínky. Autorovi by se zdálo vhodnější takovou povinnost stanovit zvláštními zákony případ od případu.

Rovněž je použita zde obtížně vyložitelná dvojice pojmů *dokument* v hypotéze a *dokument v elektronické podobě* v dispozici právní normy. Pár budí dojem, jako by v hypotéze měl být předpokládán dokument coby právní skutečnost splnitelná papírovou listinnou podobou dokumentu anebo obecnou představou „dokumentu", zatímco v dispozici se má jednat o dokument téhož druhu a obsahu v elektronické podobě. Ustanovení § 8 ZSVD však nemůže být obecným příkazem pro veřejnoprávní podepisující vytvářet takové hypotetické dokumenty i v elektronické podobě v rámci veřejnoprávních vztahů, neboť by zejména neobstálo vůči čl. 2 odst. 2 Listiny.[12] Dovolení elektronické formy jednání pro veřejnoprávního podepisujícího v rámci veřejného práva musí být dle autora výslovné nebo aspoň dostatečně určité v některém zákonu ČR. Nařízení eIDAS takový příkaz rovněž neobsahuje. Autor proto nevykládá § 8 ZSVD jako obecné umožnění ani jako příkaz pro jednání dokumentem v elektronické podobě pro veřejnoprávní podepisující ve vztazích veřejného práva, ale takové modality by očekával ve zvláštním zákoně, včetně možnosti přikázat druh elektronické pečeti, který se v takovém případě má přesně použít.

Do úvahy by tedy QESeal připadala spíše pro soukromé právní jednání veřejnoprávního podepisujícího, kde však může představovat významnou překážku, je-li takové jednání prováděno prostředky výpočetní techniky vytvořenými před vznikem nařízení eIDAS nebo neberoucím ohled na nařízení eIDAS.

Celkově má autor znění § 8 ZSVD za málo podařené. Možná jde i důsledek toho, že institut pečeti nemá v ČR čerstvou právní tradici nebo jasný vzor použití.

Důvodová zpráva vykládá smysl § 8–10 ZSVD tak, že: „Dále se stanoví povinnost veřejného sektoru pečetit jím produkované elektronické dokumenty, které nejsou podepsány elektronickým podpisem, eventuálně jeho alternativami (např. fikcí podpisu podle § 18 odst. 2 zákona č. 300/2008 Sb.)."[13] Uvedená fikce podpisu se však uplatňuje pouze ve vztahu a směru jednání vůči subjektům veřejného sektoru, nikoli při jejich vlastním jednání. Účelem § 8 ZSVD však zřejmě dle důvodové zprávy má být:

[12] Listina základních práv a svobod, ústavní zákon č. 2/1993 Sb. ve znění ústavního zákona č. 162/1998 Sb.

[13] Důvodová zpráva ZSVD, s. 36.

„Tím bude zajištěno, že u veškerých elektronických dokumentů veřejného sektoru bude **zajištěna autenticita** (platnost elektronických podpisů a pečetí bude ‚prodloužena' kvalifikovaným elektronickým časovým razítkem), což umožní jejich dlouhodobou využitelnost (mj. takový dokument bude možné autorizovaně konvertovat).“[14] A rovněž: „Současně nebude potřeba ve zvláštních zákonech nadále uvádět technicistní ustanovení o pečetění dokumentů či jejich opatřování elektronickým časovým razítkem.“[15] Aby mohl platit tento výklad a vzhledem k tomu, že se důvodová zpráva nijak nevymezuje k pojmům *dokument* a *dokument v elektronické podobě*, je zřejmě nutné oba tyto výskyty slova dokument vykládat, jako by místo nich byl obrat *elektronický dokument*, tj. pojem z nařízení eIDAS. Ani výklad důvodové zprávy neuvádí, že by ustanovení znamenalo dovolení elektronické podoby jednání. Povinné stanovení pečetění veškerých nepodepisovaných elektronických dokumentů veřejného sektoru autor stále považuje za sporné. Některá jednání veřejného sektoru totiž nemusí mít stanoven způsob autentizace právě proto, jelikož způsob či proces vydání takové informace není dostatečně zajištěn a má například jen ryze orientační a nezávaznou povahu. Bude-li nyní veřejný sektor takové výstupy potvrzovat elektronickou pečetí QES, může v příjemci vyvolat jednak dojem, že takový proces se v pozadí nachází, jednak vyvolat i vznik legitimního očekávání, které však následně může být zklamáno.

8.2.2 Veřejnoprávní jednání vůči veřejnoprávnímu podepisujícímu

Podle § 6 odst. 1 ZoSDV *„podepisuje-li se elektronický dokument, kterým se právně jedná vůči veřejnoprávnímu podepisujícímu … v souvislosti s výkonem [jeho] působnosti."*[16], pak *„k podepisování elektronickým podpisem lze použít pouze uznávaný elektronický podpis"* (tj. $AdES_{QC}$ nebo QES).

Ustanovení se tedy použije pouze tehdy, když se právně jedná v dovolené elektronické podobě, tj. elektronickým dokumentem, a je-li náležitostí jednání elektronický podpis. Musí se jednat o jednání v souvislosti s veřejnoprávní působností. Zjevným účelem je, aby byla zajištěna určitá úroveň ověření totožnosti podepisující osoby, která vždy musí mít kvalifikovaný certifikát pro elektronický podpis. Podepisující osoba si však nemusí pořizovat QSCD, aby mohla vytvářet QES. Nevyžaduje se ani použití žádného časového razítka. Takové časové ověření a zajištění ověřitelnosti platnosti podpisu si může provést veřejnoprávní podepisující po příjmu

[14] Důvodová zpráva ZSVD, s. 36. Zvýraznil autor.
[15] Důvodová zpráva ZSVD, s. 36.
[16] Nebo *„vůči jiné osobě v souvislosti s výkonem jejich působnosti"*.

podepsaného elektronického dokumentu. Jedná se o obecné ustanovení, zvláštní zákon může stanovit druh elektronického podpisu odlišně.

8.2.2.1 Pečetění vůči veřejnoprávnímu podepisujícímu

Dle § 9 ZSVD, *„pečetí-li se elektronický dokument, kterým se právně jedná vůči veřejnoprávnímu podepisujícímu"*[17], pak *„k pečetění elektronickou pečetí lze použít pouze uznávanou elektronickou pečeť"* (tj. $AdESeal_{QC}$ nebo QESeal).

Ustanovení je zřejmě třeba vykládat tak, že pokud právní řád ČR připouští jednání elektronickým dokumentem vůči subjektu charakteru veřejnoprávního podepisujícího, jehož náležitostí je elektronická pečeť, pak se musí použít uznávaná elektronická pečeť.

Není třeba zřejmé, zda pokud by elektronický dokument byl potvrzen například podpisem QES a navíc byla připojena například elektronická pečeť jen AdESeal, pokud by to bylo z hlediska daného právního předpisu právně nadbytečné, zda by AdESeal měla být důvodem k odmítnutí jednání. Autor je názoru, že spíše nikoli. Obecně by ale pro předcházení sporům doporučil, aby v případě pečetění vůči veřejnoprávním podepisujícím byly vždy používány uznávané elektronické pečetě.

8.2.3 Soukromé právní jednání

Dle § 7 ZSVD, *„podepisuje-li se elektronický dokument, kterým se právně jedná jiným způsobem než způsobem uvedeným v § 5 nebo § 6 odst. 1"* (tj. jiným než od nebo vůči veřejnoprávnímu podepisujícímu, podrobně srov. výše), pak *„k podepisování elektronickým podpisem lze použít zaručený elektronický podpis, uznávaný elektronický podpis, případně jiný typ elektronického podpisu"*.

Mezi jiný způsob jednání náleží zřejmě zejména soukromé právní jednání. Dovolené druhy podpisu jsou AdES, uznávaný podpis ($AdES_{QC}$ nebo QES) nebo *„případně jiný typ elektronického podpisu"*, tj. i elektronický podpis prostý.

Jednají-li veřejnoprávní podepisující a soukromý subjekt v rámci soukromého právního jednání vůči sobě navzájem, neplyne jim dle názoru autora jen z § 5 a § 6 ZSVD povinnost jednat vůči sobě navzájem v písemné podobě. Pokud však povinnost písemné podoby nebo elektronické podoby s elektronickým podpisem ukládá pro dané právní jednání některý zákon nebo se k některé z těchto podob rozhodnou strany na

[17] Nebo *„vůči jiné osobě v souvislosti s výkonem jejich působnosti"*.

základě vzájemné dohody, pak i pro soukromé právní jednání musí veřejnoprávní podepisující použít QESChyba: zdroj odkazu nenalezen a QTSChyba: zdroj odkazu nenalezen podle § 5 ZSVD. Podpis protějšího soukromého subjektu však spadá pouze pod § 7 ZSVD, protože není ani veřejnoprávním podepisujícím (§ 5 ZSVD), ani nejedná vůči veřejnoprávnímu podepisujícímu v souvislosti s výkonem jeho působnosti (§ 6 ZSVD).

V ostatních případech stran soukromého jednání dostačuje pro každou ze stran podle § 7 ZSVD k podepisování elektronickým podpisem v zásadě jakýkoli druh elektronického podpisu z nařízení eIDAS, tedy i elektronický podpis prostý. Srov. 9.4.

8.2.3.1 Pečetění v rámci soukromého právního jednání

Dle § 10 ZSVD, *„pečetí-li se elektronický dokument, kterým se právně jedná jiným způsobem než způsobem uvedeným v § 8 nebo § 9 odst. 1"* (tj. jiným než od nebo vůči veřejnoprávnímu podepisujícímu, podrobně srov. výše), pak *„k pečetění elektronickou pečetí lze použít zaručenou elektronickou pečeť, uznávanou elektronickou pečeť, případně jiný typ elektronické pečeti"*. Lze tedy použít i elektronickou pečeť prostou. Pro více srov. např. 10.3.3 níže.

8.3 Doplňovací a konkretizační ustanovení

V této části jsou zmíněna ustanovení ZSVD, která mají charakter doplnění nebo konkretizace nařízení eIDAS. Autor tyto druhy striktně nerozlišuje, protože konkretizační ustanovení má někdy současně i charakter doplnění. Zcela přesně by se ustanovení měla zřejmě rozlišovat podle primárního účelu, který mají. Nicméně to asi není zcela nutné, pokud nedochází k námitce rozporu s nařízením eIDAS. Autor u žádného ustanovení v této části zmíněné takový rozpor neshledává.

8.3.1 Ověření platnosti $AdES_{QC}$ a $AdESeal_{QC}$

Podle § 12 ZSVD se na ověřování platnosti $AdES_{QC}$ a $AdESeal_{QC}$ mají obdobně použít ustanovení čl. 32 odst. 1 písm. a) až e), g) a h) eIDAS. Vynecháno je tedy písm. f) s požadavkem na vytvoření pomocí QSCD. Adekvátní by zřejmě bylo i přikázání obdobného použití čl. 32 odst. 2 eIDAS, které však v ZSVD výslovně chybí. Oproti ověřování podpisu QES podle čl. 32 odst. 1 bude obecně mnohem vyšší potíž s ověřením požadavku čl. 32 odst. 1 písm. h) eIDAS, který se týká splnění požadavků na AdES podle čl. 26 eIDAS. V případě QES je do značné míry zajišťuje právě QSCD.

Není zřejmé, a to ani z ZSVD, podle čeho se má požadavek hodnotit, když potvrzení o použití QSCD, a tím potažmo i o plnění čl. 26 eIDAS, chybí.

ZSVD neurčuje, kdy se ověřování platnosti má provádět. Dle autora tedy platí obecná teze, že by spoléhající osoba měla provádět (technické) ověření platnosti elektronického podpisu nebo pečeti kdykoli, když se aktuálně nebo v budoucnosti bude chtít na daný elektronický podpis spolehnout právně (srov. 6.11, 6.15.2 a 6.16.4).

Důležité je, že § 12 ZSVD se nepoužije na AdES nebo AdESeal, jimiž jsou potvrzované kvalifikované certifikáty, popř. kvalifikovaná elektronická časová razítka, od kvalifikovaných poskytovalů služeb vytvářejících důvěru. Ty se tedy ověřují jinak, zřejmě vůči důvěryhodnému seznamu.

8.3.2 Písemná forma smlouvy s poskytovatelem služeb

Dle § 2 ZSVD *„kvalifikovaný poskytovatel služeb vytvářejících důvěru poskytuje kvalifikovanou službu vytvářející důvěru na základě písemné smlouvy"*. Požadavek je převzat ze zrušeného ZEP jako osvědčená praxe. Dle důvodové zprávy může být v listinné i elektronické podobě, přičemž projevy vůle stran nemusí být na témže dokumentu.[18]

8.3.3 Uchovávání dokumentace kvalifikovaným poskytovatelem služeb

V § 3 ZSVD se upravují navíc povinnosti poskytovatele uchovávat dokumenty *související* s některými službami vytvářejícími důvěru. Pojem *dokument* jde zřejmě v kontextu § 3 ZSVD vykládat široce, popř. podle ustanovení zákona č. 499/2004 Sb., o archivnictví a spisové službě, aby zahrnoval elektronické i listinné podoby, zřejmě i xerokopie dokladů, ale případně i elektronická *data* nebo *údaje*, jak pro případ vydaných digitálních objektů poskytovatelem, tak pro případ, že poskytovatel přijímá potvrzení v elektronické podobě, která mají spíše charakter dat než dokumentu. Výše uvedený výraz „související" je nutné chápat jako velmi abstraktní a extenzivně vykládaný. Zřejmě musí nahradit dříve mnohem explicitnější výčet v § 6 odst. 5 ZEP.

Základní doba uchovávání je 10 let, poté dalších 15 let uchovávání údajů identifikačního druhu. Obecně má kvalifikovaný poskytovatel s dokumenty zacházet podle zákona upravujícího archivnictví a spisovou službu, nestanoví-li eIDAS nebo

[18] Důvodová zpráva ZSVD, s. 31.

ZSVD jinak. Uvedená ustanovení nahrazují § 6 odst. 6 ZEP, který byl částečně též podrobnější a explicitnější.

Podle důvodové zprávy je účelem těchto povinností uchovávání mít k dispozici důkazy pro případná správní nebo soudní řízení.

8.3.4 Předání dokumentace v případě ukončení činnosti poskytovatele

V § 4 ZSVD se konkretizuje či doplňuje předání dokumentace v případě ukončení činnosti kvalifikovaného poskytovatele. Nepřevezme-li dokumentaci jiný kvalifikovaný poskytovatel, musí ji předat Ministerstvu vnitra a to ji dle § 13 odst. 5 ZSVD musí převzít.

8.3.5 Zneplatnění kvalifikovaného certifikátu na pokyn Ministerstva vnitra

V § 13 odst. 2 ZoVSD se stanoví pravomoc Ministerstva vnitra udělit poskytovateli služeb pokyn ke zneplatnění kvalifikovaného certifikátu, pokud je důvodné podezření, že kvalifikovaný certifikát (i) byl padělán, (ii) vydán na základě nepravdivých údajů nebo (iii) používaný prostředek pro vytváření elektronických podpisů/pečetí vykazuje bezpečnostní nedostatky. Jedná se o nahrazení § 15 ZEP. Chybí zneplatnění v případě ukončení činnosti poskytovatele.

8.3.6 Vedení seznamu certifikátů kvalifikovaných poskytovatelů

Navíc k zveřejňování důvěryhodných seznamů má Ministerstvo vnitra pravomoc i povinnost dle § 13 odst. 4 ZoVSD vést seznam certifikátů, na jejichž základě kvalifikovaní poskytovatelé (i) podepisují zaručeným elektronickým podpisem anebo (ii) pečetí zaručenou elektronickou pečetí, a to buď vydané kvalifikované certifikáty (pro elektronické podpisy, elektronické pečeti), nebo vydaná kvalifikovaná elektronická časová razítka. Tento seznam certifikátů se zveřejňuje způsobem umožňujícím dálkový způsob.

Účelem pravděpodobně je mít na úrovni ČR k dispozici způsob zveřejňování certifikátů nezávislý na unijním institutu důvěryhodných seznamů. Je též možné, že požadavek byl do ZSVD zařazen jako nahrazení § 9 odst. 1 písm. d) ZEP.

8.3.7 Zmocnění Správy základních registrů

V § 14 ZSVD se nachází zmocnění Správy základních registrů *„poskytovat služby vytvářející důvěru, a to i jako hospodářskou činnost"*. Správa základních registrů

je *správní úřad*, který je zřízen zákonem č. 111/2009 Sb. Dle jeho § 6 je podřízen Ministerstvu vnitra, je účetní jednotkou a je součástí rozpočtové kapitoly Ministerstva vnitra. Jeho hlavním účelem i působností je být správcem informačního systému základních registrů. Z § 14 ani § 15 ZSVD není patrné, proč zákonodárce toto zmocnění do zákona vložil. Umožnění hospodářské činnosti se zdá být obsaženo navíc, pokud by některá dílčí činnost měla okrajově hospodářskou povahu.

ZSVD nestanoví ani nevylučuje, zda úřad má poskytovat *kvalifikované* služby vytvářející důvěru. V § 15 ZSVD je obsažena úprava pro zvláštní službu vytvářející důvěru,[19] jejíž předmět nesmí spočívat v certifikátech pro elektronické podpisy, elektronické pečeti ani autentizaci internetových stránek. Prakticky takové certifikáty by mohly být vydávány pro účel *autentizace osob* (resp. *identifikace osob*), ev. pro šifrování obsahu. Z § 15 odst. 2 až 4 ZSVD se zdá, že by Správa základních certifikátů mohla vydávat autentizační certifikáty pro fyzické osoby nebo právnické osoby, které by se používaly v rámci některého systému identifikace, nejspíše též v rámci nových verzí elektronických občanských průkazů. V případě fyzické osoby by zvláštní položkou takových certifikátů mohl být *„agendový identifikátor fyzické osoby pro agendu vydávání certifikátů"* [§ 15 odst. 2 písm. d) bod 2 ZSVD]. Této domněnce nasvědčuje i část dvacátá zák. č. 298/2016 Sb., která mění zákon č. 328/1999 Sb., o občanských průkazech, a přidává do něj ustanovení § 16 odst. 9, že *„Správa základních registrů zajišťuje autentizaci držitele občanského průkazu uvedeného v § 2 odst. 2 písm. a) a vydává za tímto účelem identifikační certifikáty občanského průkazu."* Dle stejné části je přidána i úprava informačního systému pro autentizaci, jehož správcem je stanovena právě Správa základních registrů.

Ustanovení § 14 a § 15 ZSVD se nenacházela v původním návrhu vládního zákona, podaného do Poslanecké sněmovny. Nejsou ani uvedena a vysvětlena v důvodové zprávě.

8.4 Institucionálně-kompeteční ustanovení

V § 13 ZSVD se stanoví působnost Ministerstva vnitra jednak jako orgánu dohledu (čl. 17 eIDAS), jednak jako subjektu, který vede a vydává důvěryhodné seznamy (čl. 22 eIDAS). V ZSVD však chybí stanovení kompetence, který orgán ČRje

[19] Taková není uvedena v nařízení eIDAS. Vnitrostátní právo smí upravovat takové zvláštní služby, ale nemají přeshraniční status služby vytvářející důvěru podle eIDAS.

oprávněn zastupovat stát dle čl. 31 odst. 1 eIDAS pro účel oznamování provedení nebo zániku certifikace QSCD/ QSealCD vůči Komisi.

8.5 Sankční a procesní ustanovení

V § 16 a § 17 ZSVD se nachází sankční úprava přestupků fyzických, právnických a podnikajících fyzických osob. Stanoví se veřejnoprávní sankce pro případy výslovně uvedených případů porušení povinností, které jsou odvozeny z povinností uložených v nařízení eIDAS nebo ZSVD.[20] V závislosti na druhu přestupku lze za přestupky uložit pokutu až 2 miliony Kč. Podle důvodové zprávy[21] byla maximální výše pokut snížena, neboť dle ustálené judikatury nemá být ani zákonná výše maximálních pokut likvidační. Výše sankce pak byla stanovena na základě možné způsobené škody a aby sankce byly „přiměřeně přísné, odrazující a efektivní a plnící tak preventivně represivní funkci správního trestání".[22] Vyšší částky pokut by též mohly ohrozit zájem poskytovatelů na tento trh vstoupit. Podle § 18 ZSVD přestupky projednává Ministerstvo vnitra.

8.6 Využití

V návaznosti na ZSVD bezprostředně následující zákon č. 298/2016 Sb. obsahuje zřejmě 64 novelizací zákonů, v nichž se promítá nová terminologie ze ZSVD. Pochopitelně se jedná zejména o předpisy veřejného práva.

8.7 Důkazní účinky

Adaptační zákon ZSVD neobsahuje žádnou úpravu, která by doplňovala důkazní účinky digitálních objektů oproti tomu, jak jsou stanoveny nařízením eIDAS. Přitom dle bodu odůvodnění 22 eIDAS *„je na vnitrostátním právu, aby vymezilo právní účinky služeb vytvářejících důvěru, nestanoví-li se v tomto nařízení jinak"*. Ohledně důkazních účinků budou tedy při uplatňování nařízení eIDAS v právu ČR platit pouze důkazní účinky stanovené v samotném nařízení eIDAS (srov. 6.15), avšak pouze v oblasti vztahů spadajících do pravomocí přenesených na EU a do nařízením sobě vyhrazené působnosti. Důkazní účinky digitálních objektů stanovené v eIDAS se například vůbec neuplatní v případě hodnocení důkazů v rámci trestních řízení (srov. 6.3.4).

[20] Autor nerešeršoval, zda ZSVD sankčně pokrývá všechny možné porušení povinností v eIDAS a ZSVD.
[21] Důvodová zpráva ZSVD, s. 20.
[22] Důvodová zpráva ZSVD, s. 20.

Významné důkazní účinky má QESeal (srov. 6.15.8), zatímco pro QES platí z hlediska důkazního účinku jen stejné pravidlo zákazu hrubé diskriminace (srov. 6.15.6), jaké platí i pro elektronický podpis prostý. V ČR se rámci většiny případů procesní úpravy tedy podpisy AdES, $AdES_{QC}$ i QEC budou posuzovat podle zásady volného hodnocení důkazů, stejně jako i pečetě AdESeal a $AdESeal_{QC}$. Na rozdíl od elektronického podpisu prostého však tyto další druhy elektronického podpisu a pečetí mají určité autentizační vlastnosti a zpravidla též existuje postup ověření (technické) platnosti daného druhu podpisu či pečeti, tj. zjištění jejich vlastní autenticity. V případě pro QES např. dle čl. 32 eIDAS. Při stejné důkazní zásadě volného hodnocení důkazů budou tedy podpisy a pečetě vyšší úrovně zpravidla hodnoceny výrazně přesvědčivěji.

Autor je v zásadě názoru, že zejména pro QES by se měla uplatňovat *skutková domněnka* (srov. 9.4.1), že z ověření technické platnosti QES plyne pravost (původnost) a integrita podepsaných dat. Vzhledem k jejich obsahu a podmínkám vytvoření pak většinou bude plynout i skutková domněnka projevu vůle, zachycené podepsanými daty, té fyzické osoby, jejíž podpis QES je přítomen. Vyvrátit tyto skutkové domněnky by ale mělo být jednodušší než důkazem opaku. Ať již poukazem na okolnosti vytvoření podpisu, nebo na jiné okolnosti, které vytvoření podpisu QES předcházely nebo po něm následovaly a které vzbuzují pochybnosti o tom, že je daný podpis pravý. Pro nižší úrovně podpisů $AdES_{QC}$ nebo AdES platí přiměřeně totéž s tím, že se důkazní přesvědčivost snižuje, popř. se snižuje v určitých aspektech, v nichž jsou slabší vlastnosti daného druhu podpisu nebo jeho technického provedení, které má podpis dokazovat. Srov. např. funkce a důkazní účinky vlastnoručního podpisu v případě AdES (6.5.1.1 a 6.15.4). Vzácně mohou být důkazní vlastnosti i vyšší, pokud skutečné technické provedení takové vlastnosti vykazuje.

V nařízení eIDAS je stanovena vysoká i důkazní hodnota QTS (srov. 6.15.9) a též služby kvalifikovaného doporučeného doručení (srov. 6.15.10), které však zatím v ČR nejsou provozovány. Ke kritice toho, aby domněnky z eIDAS byly považovány za právní domněnky, však srov. též kritiku RoßnagelaChyba: zdroj odkazu nenalezen (6.15.12).

Jediným případem, kdy vnitrostátní právo stanoví vyšší důkazní účinek, je případ *veřejné listiny* (srov. 9.2).

8.8 Opomenutá implementační ustanovení

V této části je uveden přehled oblastí, které autor považuje za v ZSVD opomenuté. Přehled může využít zákonodárce pro úvahy o doplnění implementace nařízení eIDAS nebo právníci, kteří sepisují smlouvy nebo vnitřní předpisy v oblasti elektronického podpisu.

8.8.1 Kryptografická schémata – působnost, způsob určení

V ZSVD a potažmo zřejmě v celém českém právním řádu chybí zmocnění k tomu, aby někdo stanovil kryptografická schémata pro digitální objekty upravené v eIDAS, zejména pro jejich kvalifikované verze. Chybí tedy nejen působnost, ale i způsob určení takových sad, dílčích kryptografických algoritmů a jejich parametrů.

Za účinnosti DirES byla nejurčitěji schémata určena v příloze č. 1 vyhlášky č. 366/2001 Sb., která byla účinná do srpna 2006. Určitá zmínka se později ještě vyskytovala v příloze vyhlášky č. 496/2004 Sb., o elektronických podatelnách, účinné do 30. 6. 2012.

Požadavky na kryptografická schémata tedy nyní zřejmě budou pro český právní řád vyplývat jen značně nepřímo, například z požadavků v odst. 1 písm. c) přílohy II eIDAS na kvalifikované prostředky pro vytváření elektronických podisů, že *„data pro vytváření elektronického podpisu nelze odvodit a že elektronický podpis je ... spolehlivě chráněn proti padělání"*. Z toho, že kvalifikovaný poskytovatel služeb vytvářejích důvěru prošel auditem a odevzdal výslednou zprávu o posouzení shody orgánu dohledu podle čl. 20 odst. 1 eIDAS, že tato zpráva byla analyzována orgánem dohledu dle čl. 17 odst. 4 písm. b) eIDAS s pozitivním výsledkem tak, že poskytovateli služeb byl udělen statut kvalifikovaného poskytovatele, resp. kvalifikované služby dle čl. 17 odst. 4 písm. g) eIDAS a byl zapsán do důvěryhodného seznamu podle čl. 20 odst. 3 a čl. 22 eIDAS, lze implikovat, že poskytovatel používá dostatečně silná kryptografická schémata, která výše uvedený požadavky splňují.

Německá implementace výslovně ponechala stanovení technických norem, hodnocení bezpečnostních algoritmů a jejich parametrů dle § 2 odst. 2 VDG v působnosti úřadu BSI (srov. 7.3.1).

8.8.2 Ověřování totožnosti a zvláštních znaků

Ustanovení v čl. 24 odst. 1 eIDAS výslovně předpokládá, že vnitrostátní právo konkretizačně upravuje způsob ověřování totožnosti a zvláštních znaků fyzické osoby nebo právnické osoby, které se vydává kvalifikovaný certifikát, pokud je kvalifikovaný poskytovatel ověřuje přímo.

V § 6 odst. 5 písm. c) zákona č. 227/2000 Sb., o elektronickém podpisu, (dále „ZEP") byla kvalifikovanému poskytovateli uložena povinnost v rámci dokumentů uchovávat i *„kopie předložených osobních dokladů podepisující osoby nebo dokladů, na jejichž základě byla ověřena identita označující osoby"*. Z uvedeného následně plynulo oprávnění poskytovatele požadovat pro ověření identity více dokladů totožnosti současně, jakož i možnost vytvářet a ukládat jejich kopie. V českém právním řádu se sice dříve nacházely a i nyní nacházejí veřejnoprávní úpravy ověřování totožnosti například pro případ legalizace (notářsky[23] či úředně[24] ověřený podpis), ty však nedosahovaly uvedené úrovně ověření, ani pro situaci ověřování totožnosti poskytovatelem služeb nebyly aplikovatelné, neboť se zde v zásadě jedná o soukromoprávní vztah mezi poskytovatelem a jeho zákazníkem. Nově tedy bude záležet především na smluvních podmínkách poskytovatele, tj. na soukromé právní dohodě mezi poskytovatelem služeb a osobou, jejíž totožnost a znaky se ověřují. To poskytuje spoléhající se osobě poměrně málo právní jistoty o úrovni ověření totožnosti a zvláštních znaků, tj. i o míře ověření údajů, které následně jsou uvedeny v certifikátu.

Německý VDG rovněž neupravuje obecné ověřování totožnosti. Upravuje však podrobněji ověřování přídavných atributů (srov. 7.3.2), které lze do certifikátu vkládat.

8.8.3 Povinnost zneplatnění certifikátu na žádost

Není výslovně stanovena povinnost poskytovatele zneplatnit certifikát alespoň na žádost subjektu, jehož jméno (ev. pseudonym) nebo název jsou v certifikátu uvedeny. Chybí výslovně stanovená povinnost uvádět pravdivé údaje a možnost zneplatnění pro nepravdivost. Jiné subjekty, např. zaměstnavatel nebo subjekt potvrzující údaje, nemají výslovnou možnost ze zákona žádat o zneplatnění certifikátu. Takové povinnosti byly dříve výslovně upraveny v § 6a odst. 3 a 4 ZEP.

[23] Ustanovení § 64 zákona č. 358/1992 Sb., notářský řád.
[24] Ustanovení § 12 písm. e) zákona č. 21/2006 Sb., o ověřování.

Takové povinnosti mohou poskytovateli plynout z obecných pravidel prevence újmy (škody). Nedopadal by ně něj ale zřejmě § 2900 obč. zák., neboť se nejedná o konání. Např. dle Paška[25] pro jednání omisivní lze v rámci prevence škody uplatnit pouze § 2901–2903 obč. zák. Do úvahy pak připadá povinnost poskytovatele zakročit dle § 2901 obč. zák., neboť mezi zvyklosti soukromého života zneplatňování certifikátu na žádost certifikované osoby náleží a bývá běžně vyžadováno, poskytovatel má kontrolu nad nebezpečnou situací možností zneplatnit certifikát i to odůvodňuje povaha poměru. Povinnost by vyplývala i z druhé věty § 2901 obč. zák., neboť poskytovatel může zneplatněním snadno odvrátit újmu, a to s minimálními náklady. Žadatel o zneplatnění nicméně musí tvrdit, popř. i dokladovat možnost hrozby vzniku škody. Jeho právní jistota je tím snížena. Potřebnou povinnost poskytovatele zneplatnit certifikát na žádost je nutné nově hledat zejména ve smluvních podmínkách.

Ve srovnání s českou implementací se v § 14 VDG upravují možnosti zneplatnění certifikátu nejen výslovně, ale i podrobně. Možnost žádat zneplatnění pak má nejen osoba, pro kterou byl certifikát vydán, ale i třetí osoby, které vyjádřily souhlas s vyjádřením atributu, jenž je v certifikátu uveden (srov. 7.3.5).

8.8.4 Subjekt zastupující ČR pro oznamování QSCD/QSealCD

V čl. 31 eIDAS nařízení předpokládá existenci subjektu, který za členský stát oznamuje vůči Komisi provedení nebo zánik certifikace QSCD/QSealCD. V zákoně ZSVD se subjekt nestanoví. Jeho jednání nespadají pod činnost orgánu dohledu.

8.8.5 Elektronický podpis „dat" nerecipován

V ZSVD chybí jakákoli recepce vytváření elektronických podpisů nebo elektronických pečetí vůči (elektronickým) datům. Veškeré obsažené recepce se týkají pečetění nebo podepisování elektronických dokumentů, a nikoli dat. K rozdílu mezi pojmy *data* a *elektronický dokument*, oba dle nařízení eIDAS, srov. 6.15.11. Pro praxi nemusí být toto opomenutí zcela zásadní, neboť na mnoho situací bude aplikovatelné nařízení eIDAS bez recepce ZSVD přímo, popř. soudy mohou aplikovat zákonnou analogii. Určité potíže by mohly vzniknout v rámci veřejného práva, kde analogie v neprospěch nevrchnostenské strany řízení zásadně není přípustná.

[25] Pašek in PETROV, J. – VÝTISK, M. – BERAN, V. a kol. *Občanský zákoník: komentář*. Praha: C. H. Beck, 2017, s. 2822.

Německá implementace nerecipuje nařízení v tomto ohledu vůbec (srov. 7.5), což autor považuje spíše za slabinu německé implementace.

8.8.6 Další

V ZSVD zřejmě chybí v § 1 vhodnější vymezení úpravy předmětu zákona. V předmětu by měly být uvedeny jednak obecné požadavky na digitální objekty [upravené v eIDAS podle čl. 1 písm. c) eIDAS[26]], jednak obecné využití těchto digitálních objektů v právním řádu ČR (obecný recepční charakter ZSVD). Tento charakter totiž mají zejména § 5–11 ZSVD a dále § 19 (přechodná ustanovení) ZSVD. Ačkoli v § 1 není takový předmět ZSVD uváděn, je autor názoru, že výskyt uvedených ustanovení je natolik výslovný, že znění § 1 písm. b) je nutné vykládat extenzivně, jako uvedený předmět obsahující. Extenzivnost výkladu lze odůvodnit například samotným názvem nařízení eIDAS, který jej popisuje jako dichotomii či spojení předmětu o *„elektronické identifikaci"* a o *„službách vytvářejících důvěru"*, obojí pro *„pro elektronické transakce"*. Důvodem pro toto pojetí je i důvodová zpráva ZSVD, která podřazuje četné digitální objekty z eIDAS pod služby vytvářející důvěru.[27]

8.9 Derogace a změny pojetí

Adaptační zákon zrušil s účinností od 19. 9. 2016 zákon č. 227/2000 Sb., o elektronickém podpisu („ZEP"), který dříve upravoval náležitosti elektronického podpisu. V této části jsou zmíněna zrušená ustanovení ZEP, která autor považuje za právně významná, a je komentováno, zda a jak jsou nahrazena nařízením eIDAS a adaptačním zákonem ZSVD. Pokud tyto dva předpisy nepokrývají derogovaná ustanovení, došlo k derogaci výslovné úpravy a často i ke snížení právní jistoty.

V takovém případě lze právní úpravu někdy vyvodit z jiných ustanovení uvedených předpisů, popř. z obecných pravidel nebo zásad právního řádu, které se autor níže též snaží identifikovat a vyložit. Autor zcela nevylučuje, že v právním řádu lze nalézt i jiné uplatnitelné obecné nebo zvláštní pravidla a zásady, stejně ovšem i takové, které budou naopak působit protichůdně.

Přehled by měl sloužit pro uvědomění si změn a současného právního stavu v uvedených oblastech. Může ho využít zákonodárce při úvahách o doplnění

[26] A nikoli jen předmět § 1 písm. b) ZSVD odpovídající čl. 1 písm. b) eIDAS.

[27] Důvodová zpráva ZSVD, s. 13: „Cílem regulace je adaptace národního právního řádu na část nařízení eIDAS týkající se služeb vytvářejících důvěru."

implementace nařízení eIDAS, ale i právníci, kteří nyní sepisují smlouvy nebo vnitřní předpisy v oblasti elektronického podpisu.

8.9.1 Právní domněnka seznámení se s obsahem

Podle § 3 odst. 1 ZEP platilo: *„Datová zpráva je podepsána, pokud je opatřena elektronickým podpisem. Pokud se neprokáže opak, má se za to, že se podepisující osoba před podepsáním datové zprávy s jejím obsahem seznámila."* Druhá věta představuje vyvratitelnou právní domněnku o seznámení se s obsahem datové zprávy před podepsáním. Z existence elektronického podpisu může soud usuzovat, že se podepisující osoba s obsahem datové zprávy před podpisem seznámila, že obsah schvaluje a podle významu obsahu buď vyjadřuje v datové zprávě svoji vůli, anebo potvrzuje určité skutečnosti v datové zprávě uvedené. Alternativně může mít její podpis i význam jiného tzv. „komitmentu" (srov. 4.7).[28]

V nařízení eIDAS právní domněnka seznámení se s podepisovaným obsahem před podepsáním není vyjádřena pro žádný druh elektronického podpisu, ale ani pro elektronickou pečeť. Seznámení se s obsahem není vyjádřeno ani jako normativní požadavek pro žádný druh elektronického podpisu (srov. 6.16.2).

Z požadavku definice elektronického podpisu prostého, že jej *„podepisující osoba používá k podepsání"*, lze vyvodit, že v běžných situacích by se podepisující osoba zřejmě měla snažit seznámit s podepisovaným obsahem, resp. s podepisovanými daty. V běžné situaci příjemce však nebude dostatečně jisté, zda u podepisující osoby panovala běžná situace. Jednak nařízení eIDAS neklade žádné požadavky na aplikaci vytvářející podpis (srov. 6.16.2), jednak bude záležet na míře automatizace vytváření podpisu (srov. 6.16.15), jednak na druhu komitmentu (srov. 4.7), který podpis vyjadřuje. Je-li podpis vytvářen jako dávkový podpis, podepisující osoba se spíš s jednotlivým obsahem neseznámila. Je-li vytvářen jako podpis automatický, je jisté, že se s jednotlivým obsahem předem neseznámila. Má-li pak například podpis komitmenty potvrzení přijetí, potvrzení odeslání nebo potvrzení doručení dat, je naopak spíše pravděpodobné, že se s obsahem, resp. s daty, neseznámila.

8.9.2 Právní domněnka projevu vůle

Dle § 3a odst. 2 ZEP platilo: *„Pokud označující osoba označila datovou zprávu, má se za to, že tak učinila automatizovaně bez přímého ověření obsahu datové zprávy*

[28] Některé aplikace vytvářející podpis umožňují vyjádřit druh *komitmentu* jako součást podpisu.

a vyjádřila tím svou vůli." Ustanovení obsahuje tři právní domněnky. Poslední je právní domněnkou o vyjádření vůle v označené datové zprávě.

Lze se ptát, zda ZEP kryl tyto vyslovené právní domněnky požadavky, tj. zda zákonné normativní požadavky dávají vzniknout bezpečnostnímu modelu, který by následně dovoloval je stanovit. Dle autora byla otázka této kongruence[29] diskutabilní. V ČR se k vytváření podpisu nepožadoval bezpečný prostředek pro vytváření podpisů (SSCD). Z hlediska požadavků na používané prostředky proto byl vrcholem požadavek na zaručený elektronický podpis v § 2 písm. b) bod 3 ZEP, že *„byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou"*. V rámci širšího výkladu pod tyto prostředky mohlo spadat nejen bezpečné úložiště dat pro vytváření podpisu, ale i systémové prostředí a aplikace vytvářející podpis. V praxi byl celek velmi často představován jen osobním počítačem. Citovaná definice ohledně prostředků vyslovuje pouze předpoklad schopnosti udržení kontroly nad nimi. Nezpůsobilý by tedy byl prostředek, který možnost takové kontroly vůbec neposkytuje, kupř. jeho činnost je nahodilá, nespolehlivá, snadno narušitelná. Způsobilý je ale prostředek, který udržení takové kontroly poskytuje. Typicky každý takový prostředek ale vyžaduje, aby byly dodrženy potřebné postupy jeho nasazení, správy a použití. Zákon ZEP i směrnice DirES mlčely o tom, kdo má tyto postupy zajišťovat. To mohlo být zejména sporné tehdy, pokud dané prostředky byly používány v rámci výkonu zaměstnání, tj. podepisující osoba byla zaměstnancem nebo osobou v obdobném vztahu. Prostředky pak totiž bývaly pořizovány zaměstnavatelem, jejich nasazení a správa často zajišťovány správcem, kterým buď byl jiný zaměstnanec, někdy ale i externí správcovská společnost, dodávající tyto činnosti jako své služby.

Je zřejmé, že citovaný požadavek výhradní kontroly by neměl smysl, kdyby podepisující osoba neměla pro podpis relevantní prostředky pod svou výhradní kontrolou aspoň v okamžiku vytváření podpisu. V tomto smyslu tedy dle autora vyplývaly povinnosti pro podepisující osobu, ale i pro jiné subjekty, které ovlivňovaly chod těchto prostředků, aby výhradní kontrolu podepisující osoby zajistily. Fakticky i právními dohodami, které rozdělovaly odpovědnost tak, aby byla stanovena najisto. Další právní povinnosti obsahoval ZEP pro podepisující osobu explicitně.

[29] Jako *kongruenci* mezi právními požadavky a právními domněnkami označuje požadovaný vztah například Jandt.

V nařízení eIDAS právní domněnka projevu vůle není vyjádřena pro žádný druh elektronického podpisu, ale ani pro elektronickou pečeť.

V případě vlastnoručních podpisů považuje Polčák právní domněnku projevu vůle za obyčejové pravidlo,Chyba: zdroj odkazu nenalezen o kterém není nutné pochybovat (srov. 4.1). Z definice elektronického podpisu prostého, že jej *„podepisující osoba používá k podepsání"*, by se pak mohlo soudit, že i v jeho případě se má užít stejné obyčejové pravidlo. V § 565 obč. zák. větě druhé se vyjadřuje obdobná domněnka pravosti a správnosti soukromé listiny, pokud se užívá proti osobě, která ji zjevně podepsala, ev. proti jejímu právnímu nástupci, zejména dědici. Dle autora jsou takové právní domněnky bez dalšího použitelné pouze v těch případech, kdy scénář vytvoření elektronického podpisu je v elektronické realitě zajištěně[30] zcela stejný jako v případě vlastnoručního podpisu, tedy že podepisující osoba věrně vidí[31] podepisovaný obsah a vědomě k němu vytváří elektronický podpis. Jelikož nařízení eIDAS nestanoví požadavky na zajištění bezpečnosti systémového prostředí ani aplikace vytvářející elektronický podpis, domněnku lze uplatnit tehdy, když podepisující osoba nepopírá, že výše předpokládaný scénář nastal, nebo je to dokázáno jinak. V jiných případech může dojít ke sporu o to, čeho si podepisující osoba byla či nebyla vědoma během operace vytváření svého elektronického podpisu. Pro více srov. 9.4.1.

8.9.3 Soulad s originálem (integrita)

V § 4 (Soulad s originálem) ZEP bylo ustanovení: *„Použití zaručeného elektronického podpisu nebo elektronické značky zaručuje, že dojde-li k porušení obsahu datové zprávy od okamžiku, kdy byla podepsána nebo označena, toto porušení bude možno zjistit."* Ustanovení bylo nejasné. Není formulované tak, aby se dalo považovat za právní domněnku. Vyloží-li se jako normativní požadavek na zaručený elektronický podpis nebo elektronickou značku, pak se ale jedná o redundantní požadavek, neboť takový již byl vyjádřen v § 2 písm. b) bod 4 ZEP pro zaručený elektronický podpis nebo v § 2 písm. c) bod 3 ZEP pro elektronickou značku.

Ustanovení se vztahuje pouze na interval od podpisu nebo označení do okamžiku ověřování. Nevyjadřuje se o původnosti datové zprávy, nevztahuje ji

[30] Požadavek zajištěnosti je podstatný. Zahrnuje nejen požadavky na QSCD, ale i na systémové prostředí a na aplikaci vytvářející elektronický podpis. Zajištění má charakter nejen funkční, ale i záruk bezpečnosti implementace.

[31] Popřípadě jí je prezentován jinými lidskými smysly.

k totožnosti podepisující nebo označující osoby ani k jejich vůli nebo z hlediska pravosti vůle (nepodsunutí obsahu).

V nařízení eIDAS není právní domněnka zachování integrity datové zprávy, tj. dat v terminologii eIDAS, uvedena pro žádný druh elektronického podpisu. Je však vyjádřena pro kvalifikovanou elektronickou pečeť. Pro ni jsou stanoveny domněnka správnosti původu dat a domněnka integrity dat (srov. 6.15.8). Význam těchto domněnek je však německou naukou zpochybňován (srov. závěr 6.15.8 a srov. 6.15.12).

V praxi se pravděpodobně bude možné setkat s tím, že integrita podepsaných dat bude dedukována z faktu existence zaručeného nebo kvalifikovaného elektronického podpisu. Integrita je totiž definičním požadavkem dle čl. 26 písm. d) eIDAS na zaručený elektronický podpis. Jakkoli může být tato dedukce běžně spolehlivá, bude plynout pouze deduktivně a nikoli jako důkazní pravidlo z právního předpisu.

8.9.4 Povinnosti podepisující osoby

Podle § 5 odst. 1 písm. a) ZEP podepisující osoba byla povinna: *„zacházet s prostředky, jakož i s daty pro vytváření zaručeného elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití"*. Toto ustanovení bylo mírně nejasné. ZEP znal *„prostředky, které podepisující osoba může udržet pod svou výhradní kontrolou"* [§ 2 písm. b) bod 3], *„prostředek pro vytváření elektronických podpisů"* [§ 2 písm. s)] a *„data pro vytváření elektronických podpisů"* [§ 2 písm. n)].

Zřejmě je systematicky třeba vyložit, že *„daty pro vytváření zaručeného elektronického podpisu"* je třeba mínit *„data pro vytváření elektronických podpisů"* dle § 2 písm. n) ZEP, v terminologii PKI tzv. soukromý klíč. Jelikož prostředky byly v § 5 odst. 1 písm. a) ZEP zmíněny v plurálu, zřejmě se jednalo o všechny prostředky využívané k vytvoření podpisu, tedy dle § 2 písm. b) bod 3 i dle § 2 písm. s) ZEP.

ZEP zde tedy povinnosti vyplývající z § 2 písm. b) bod 3 o zajištění výhradní kontroly uložil jako povinnost zacházení podepisující osobě. Je otázka, zda to bylo adekvátní. Pochyby jsou jednak o schopnostech průměrně podepisující osoby, jednak o rozdělení odpovědnosti v případě používání prostředků zaměstnavatele.

Podle § 4 odst. 1 obč. zák. platí: *„Má se za to, že každá svéprávná osoba má rozum průměrného člověka i schopnost užívat jej s běžnou péčí a opatrností"* a navíc platí, že *„to každý od ní může v právním styku důvodně očekávat"*. Znění tohoto

ustanovení není jasné. Úvodní část budí dojem, že se jedná o právní domněnku. Právní domněnka se však vyslovuje o skutkovém stavu. Ze schopnosti nelze implikovat povinnost. Ještě méně jasná je část očekávání běžné péče a opatrnosti.

Bez ohledu na § 4 odst. 1 obč. zák. autor zná plně svéprávné fyzické osoby, které v oblasti výpočetní techniky jsou schopné se dopouštět těžkých chyb jejího ovládání. Očekávat od nich, že budou schopné udržet plnou kontrolu či výhradní kontrolu nad svými prostředky, je nerealistické. Stejně nerealistické je předpokládat, že správným zacházením s náležitou péčí zajistí předejití neoprávněného použití. Takové osoby pochopitelně učiní nejlépe, pokud si prostředky a certifikát pro vytváření elektronického podpisu nebudou vůbec pořizovat. Proto by je k jejich pořizování ani neměl nikdo nutit, a to ani zákonnými předpisy, ani v rámci funkcí v zaměstnání.

Podle § 5 odst. 1 písm. b) ZEP byly podepisující osoby dále povinny: *„uvědomit neprodleně poskytovatele certifikačních služeb, který vydal kvalifikovaný certifikát, o tom, že hrozí nebezpečí zneužití jejích dat pro vytváření zaručeného elektronického podpisu"*. Komplementárně k tomu měl kvalifikovaný poskytovatel certifikačních služeb dle § 6a odst. 3 ZEP povinnost *„neprodleně zneplatnit certifikát, pokud o to držitel, podepisující osoba nebo označující osoba požádá, nebo pokud ho uvědomí, že hrozí nebezpečí zneužití jejich dat pro vytváření elektronických podpisů nebo elektronických značek, nebo v případě, že byl certifikát vydán na základě nepravdivých nebo chybných údajů"*. Další povinnosti podepisující osoby jí byly uloženy v rámci povinností držitele certifikátu (srov. 8.9.6).

V nařízení eIDAS nejsou uvedeny žádné povinnosti podepisující osoby. To je v tomto textu i předmětem kritiky (srov. 6.16.3). Jednou z hypotéz tohoto stavu je možnost, že návrh nařízení eIDAS sepisoval někdo, kdo byl profesně ovlivněn francouzskou koncepcí deliktního práva (srov. 6.17).

Při derogaci výše zmíněných výslovných ustanovení plynou určité povinnosti pro podepisující osobu jen z obecných zásad soukromého práva a ustanovení občanského zákoníku. Tak v případě bezpečnostního incidentu by se zřejmě uplatnilo především ustavení o prevenci škody dle § 2903 obč. zák., které požaduje, aby zakročil ten, komu újma hrozí, jejím odvrácením přiměřeným způsobem. Povinnost zakročení vzniká i v případě ohrožení jiných osob dle § 2901 obč. zák., neboť existuje určitá

možnost kontroly jejich ohrožení. Takovým zakročením jistě v obou případech je žádost o neprodlené zneplatnění certifikátu vůči poskytovateli (srov. 8.8.3).

Pravidla o zacházení s prostředky a daty pro vytváření elektronického podpisu s náležitou péčí se z ustanovení o prevenci újmy vyvozují podstatně obtížněji. Snad je lze implikovat z výše uvedených prevenčních ustanovení pro případ bezpečnostního incidentu. Existují-li povinnosti pro případ bezpečnostního incidentu, měla by osoba, u které může nastat, postupovat přiměřeně takovým způsobem, aby k němu nedošlo.

Zvláštností kupř. německého SigG a SigV bylo, že ani tyto právní předpisy neupravovaly povinnosti podepisující osoby. Poskytovatel služeb však měl při vydání kvalifikovaného certifikátu povinnosti provést vůči ní určitá poučení. Podepisující osoba tak byla minimálně informována o tom, co je správná praxe a pečlivost v případě používání jí vydaných podpisových prostředků. Obdobně tomu je dle § 13 odst. 1 bod 1 VDG. Porušení správné praxe, tj. pečlivosti potřebné ve styku, je následně nedbalým jednáním, což má za právní následek to, že podepsaná osoba sice může namítat omyl své vůle a potažmo neplatnost[32] svého právního jednání, ovšem bude odpovídat za škodu. Německá právní úprava v případě právního jednání nepotřebuje explicitní protiprávnost, ale zřejmě již dostačuje poučení o potřebné pečlivosti ve styku. Podrobněji v 7.3.3.

8.9.5 Povinnosti spoléhající osoby

V ZEP neměla spoléhající se osoba, tj. osoba spoléhající se na elektronický podpis, výslovně stanoveny žádné povinnosti. V rámci § 5 odst. 2 ZEP však vystupovala jako *„ten, komu vznikla škoda"* a komu bylo uloženo provést *„veškeré úkony potřebné k tomu, aby si ověřil, že zaručený elektronický podpis je platný a jeho kvalifikovaný certifikát nebyl zneplatněn"*. Sankcí za nesplnění byla ztráta možnosti vymáhat odpovědnost za škodu (spolu)způsobenou podepisující osobou. Tuto škodu mohla podepisující osoba (spolu)způsobit například tím, že by dle § 5 odst. 2 ZEP (srov. 8.9.4 výše) neprodleně neuvědomila o hrozbě zneužití poskytovatele. Této odpovědnosti se mohla podepisující osoba zprostit, pokud neprodleně uvědomila poskytovatele o hrozbě zneužití a ten provedl zneplatnění certifikátu podepisující osoby. Pokud spoléhající se osobě došla zpráva s elektronickým podpisem po tomto zveřejnění, měla objektivní možnost zjistit stav zneplatnění certifikátu. Pokud ověření platnosti

[32] V kontextu německého práva „nicotnost" *(nichtigkeit)*.

certifikátu spoléhající osoba neprovedla a spolehla se na elektronický podpis, nebyl by podpis podepisující osoby ani považován za platný, ani by spoléhající se osoba neměla právo po podepisující osobě právo vyžadovat náhradu škody, kterou utrpěla. Musí se snažit zjistit škůdce nebo škodu snést.

V nařízení eIDAS nejsou výslovně uvedeny žádné povinnosti spoléhající osoby, ev. spoléhající se strany. To je v tomto textu předmětem kritiky (srov. 6.16.4).

Dle názoru autora je nicméně z nařízení eIDAS vyložitelná povinnost či potřeba spoléhající se osoby provést ověření platnosti QES nebo QESeal, ev. AdES nebo AdESeal, kdykoli chce mít spoléhající se osoba možnost se na právní ustanovení nařízení eIDAS spolehnout. Uvedené plyne ze systematického výkladu nařízení, provedeného výše v 6.11 (ověřování platnosti) a v 6.15.2 (objektivita existence digitálních objektů). Bez provedení ověření platnosti si spoléhající osoba vůbec nemůže být jista, že jí došlý nebo držený digitální objekt představuje právní pojem z eIDAS. Nařízení k ověření platnosti poskytuje hrubá kritéria v čl. 32 a čl. 33, která se dle čl. 40 používají přiměřeně podobně i v případě QESeal.

8.9.6 Povinnosti držitele certifikátu

Dle § 2 písm. g) ZEP držitelem certifikátu se rozuměla *„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"*.

Držitel certifikátu byl pomocný pojem ZEP, který sloužil k tomu, aby bylo možné určit subjekt, který o vydání certifikátu žádal. Žadatelem a následně držitelem mohla být nejen podepisující osoba sama, ale mohl jím být i subjekt odlišný, například její zaměstnavatel (právnická osoba, organizační složka státu). I když kvalifikovaný certifikát byl stále v rámci metodiky DirES vydáván na fyzickou osobu, přes institut držitele certifikátu měl držitel k tomuto certifikátu stanovena zvláštní práva, zejména právo žádat bez udání důvodu o jeho zneplatnění dle § 6a odst. 3 ZEP.

Dle § 5b ZEP pak držitel certifikátu byl *„povinen bez zbytečného odkladu podávat přesné, pravdivé a úplné informace poskytovateli certifikačních služeb ve vztahu ke kvalifikovanému certifikátu a ve vztahu ke kvalifikovanému systémovému certifikátu"*. Držitel certifikátu byl povinen tyto informace udávat zejména v okamžiku žádosti o certifikát a zřejmě i na případné vyžádání později.

V nařízení eIDAS, stejně jako v DirES dříve, se institut držitele certifikátu nepoužívá. Nařízení neobsahuje ani odpovídající povinnost podávat *přesné, pravdivé a úplné informace* tím, kdo o certifikát žádá. Povinnost podávat pravdivé informace, pokud možno též přesné a úplné, však lze v českém právním řádu implikovat z povinnosti jednat v právním styku poctivě, stanovené v § 6 odst. 1 obč. zák. Obsahem pojmu poctivost je mj. „čestnost, upřímnost, ... ohled na zájmy druhé strany, vlastní důvěryhodnost..."[33] Nevýhodou jen takto vyvozené povinnosti může být, že žadatel bude udávat informace jen přibližně správné s tou výmluvou, že si nebyl jist, jaká přesnost či úplnost je požadována.

V německém VDG není povinnost uvádění pravdivých údajů rovněž výslovně stanovena. V § 12 VDG se však pro zvláštní atributy, uváděné do kvalifikovaných certifikátů pro elektronické podpisy a pečeti, stanoví požadavky na svolení dotčených osob a prokázání jejich souhlasu (srov. 7.3.2). Společně s ověřením totožnosti by tak měla být dostatečně zajištěna správnost údajů v daném kvalifikovaném certifikátu.

8.9.7 Derogace elektronické značky

Elektronická značka byla do ZEP dodatečně přidaný právní pojem. Dle § 3a odst. 2 ZEP a z existence označené datové zprávy platily tři právní domněnky, že označující osoba jejím vytvořením: *„tak učinila [i] automatizovaně [ii] bez přímého ověření obsahu datové zprávy a [iii] vyjádřila tím svou vůli"*. Automatizované vytvoření proto striktně normativně není znakem elektronické značky, nicméně přesto jej bylo možné dedukovat z uvedeného ustanovení právních domněnek. Dle § 2 písm. f) ZEP označující osobou může být: *„fyzická osoba, právnická osoba nebo organizační složka státu"*. Z kombinace těchto aj. ustanovení ZEP plyne, že elektronická značka sloužila pro automatizované *„označování"*, které bylo přičitatelné třem druhům výše uvedených subjektů a po technické stránce mělo charakter digitálního podpisu, tedy stejné techniky jako zaručený elektronický podpis. Související termíny a požadavky víceméně stínovaly požadavky na zaručený elektronických podpis, popř. uznávaný elektronický podpis. Český zákonodárce užil zvláštní termíny zřejmě proto, aby nedošlo ke kolizi s pojmy DirES.

[33] Pipková H. in PETROV, J. – VÝTISK, M. – BERAN, V. a kol. *Občanský zákoník. Komentář.* 1. vydání. Praha: C. H. Beck, 2017, s. 31.

V nařízení eIDAS se výslovně neurčuje institut, který by sloužil pro automatizované vytváření. V tomto textu je dovozeno, že podle eIDAS lze pro automatizované vytváření použít AdES nebo AdESeal (srov. 6.6.4).

Implementační předpisy, zejména ZSVD, nestanoví v ČR náhradu za elektronickou značku. Tato zdrženlivost je pravděpodobně vhodná, neboť český implementační předpis by se snadno mohl dostat do rozporu s výkladem nařízení.

8.9.8 Derogace povinné akreditace poskytovatele služeb

V nařízení eIDAS ani v ZSVD se již nepoužívá režim akreditace poskytovatele služeb, používaný v ZEP. Jedná se o důsledek toho, že směrnice DirES v případě poskytovatele kvalifikovaných certifikátů nevyžadovala apriorní kontrolu činností poskytovatele. Národní transpozice DirES proto pravidelně využívaly čl. 3 odst. 7 DirES, který umožňoval používání elektronických podpisů *„ve veřejném sektoru podmínit případnými doplňujícími požadavky"*. Zcela pravidelně členské státy sahaly po přídavném režimu akreditace poskytovatele služeb, aby ho podrobily předběžné kontrole, čímž mezi členskými státy vznikly právní rozdíly i technologické nekompatibility. V nařízení eIDAS je předběžná kontrola kvalifikovaných poskytovatelů služeb již předepsána.

Režim dobrovolné akreditace poskytovatele není nařízením eIDAS vyloučen. Úroveň zajištění činnosti mohla být v praxi u akreditovaných poskytovatelů vyšší, než je u nynějších kvalifikovaných poskytovatelů v rámci eIDAS. Režim akreditace poskytovatele služeb asi nyní nebude dále běžný. Na úrovni práva EU zřejmě nepřináší poskytovateli přidanou výhodu.

8.9.9 Režim poskytovatele služeb a dohled nad ním

V ZEP byla obsažena poměrně podrobná úprava činnosti poskytovatelů a dohledu nad nimi, zejména v případě akreditovaných poskytovatelů certifikačních služeb. Ta je nyní zrušena a nahrazena úpravou v eIDAS. Činnost poskytovatelů a dohled nad nimi byl v ČR rovněž upraven několika vyhláškami.

Úprava v eIDAS je jen z počtu právních norem stručnější. Viz též konstatování Roßnagela nebo Jandta (6.2.1), že nařízení nepředstavuje úplnou harmonizační úpravu v oblasti služeb vytvářejících důvěru. Je proto téměř jisté, že úprava v eIDAS není zcela dostatečně podrobná nebo bude místy mezerovitá i v oblasti činnosti poskytovatelů

a dohledu nad nimi. Podstatné však je, že kontrola poskytovatelů služeb vytvářejících důvěru, kteří vydávají kvalifikované certifikáty, se stále provádí před započetím provozu služby, tedy stejně jako dříve u akreditovaných poskytovatelů certifikačních služeb podle ZEP.

Nyní případně chybějící úprava se musí ošetřit buď smluvně, nebo být založena na výkladu obecných právních zásad nebo pravidel z právního řádu ČR. Je však mimo záměr a rozsah tohoto textu provádět přesnou analýzu činností poskytovatelů služeb a dohledu nad nimi. Skutečně užitečná analýza by si vyžadovala samostatnou studii a součinnost orgánu dohledu i poskytovatelů služeb.

8.9.10 Změna pojetí uznávaného elektronického podpisu

Dle § 11 odst. 3 písm. a) ZEP se uznávaným elektronickým podpisem rozuměl *„[i] zaručený elektronický podpis založený na [ii] kvalifikovaném certifikátu vydaném [iii] akreditovaným poskytovatelem certifikačních služeb a [iv] obsahujícím údaje, které umožňují jednoznačnou identifikaci podepisující osoby"*.

Tento uznávaný elektronický podpis měly používat jednak subjekty odvozené od státu mezi sebou, jednak se měl užívat i ve vertikálních vztazích navzájem,[34] a to pro oba směry komunikace.

Ve srovnání s QES z eIDAS byl uznávaný podpis dle ZEP volnější v tom smyslu, že nepožadoval použití *„prostředku pro bezpečné vytváření elektronických podpisů"* (tj. SSCD), čímž se požadavek [i] relaxoval pouze pro úroveň AdES. Naopak byly zdůrazněny požadavky pro jednoznačnou identifikaci podepisující osoby, kterých se týkaly všechny požadavky [ii], [iii] a [iv]. K akreditaci [iii] výše, k [iv] níže.

Nařízení eIDAS nestanoví, který druh elektronického podpisu má stát a jeho orgány používat pro jaké účely. Pouze stanoví, že jeho subjekty veřejného sektoru nesmí pro využívání on-line služeb, který poskytují, přeshraničně vyžadovat vyšší úroveň podpisu než QES. Předepisují-li státy svým vnitrostátním právem pro určité on-line služby veřejného sektoru nižší úrovně elekronického podpisu, než je QES, měly by přeshraničně uznávat stejné nebo vyšší úrovně. Pro právní řád ČR obecně stanoví druhy použitelných podpisů pro různé účely adaptační zákon ZSVD.

[34] Ustanovení § 11 ZoEP bylo několikrát novelizováno. Jednalo se mj. zřejmě o důsledek toho, že správní právo má tradiční potíž definovat subjekty veřejné správy pozitivním způsobem.

Uznávaný elektronický podpis je nově definován v § 6 odst. 2 ZSVD jako *„zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis nebo kvalifikovaný elektronický podpis"* a slouží pro jednání vůči veřejnoprávnímu podepisujícímu subjektu, který není veřejnoprávním podepisujícím (ani jinou osobou při výkonu veřejnoprávní působnosti).

8.9.11 Derogace jednoznačné identifikace

V § 11 ZEP se v různých obměnách ustanovení v různých časových zněních zákona vyskytoval požadavek na jednoznačnou identifikaci. Nařízení eIDAS nestanoví v příloze I jednoznačnou identifikaci jako povinnou náležitost kvalifikovaného certifikátu pro elektronický podpis. Konsekventně adaptační zákon ZSVD jednoznačnou identifikaci neobnovil.

Požadavek jednoznačné identifikace v § 11 ZEP působil až kuriozní potíže. Na jednu stranu byl zřejmě obrazem potřeby či aspoň požadavků části úřadů státní správy, která si uvedenou úpravu v § 11 ZEP vymohla. Identifikátor pak byl dokonce předmětem úpravy téměř samostatné vyhlášky.[35] Na stranu druhou se správní úřady zřejmě nebyly schopné shodnout na tom, který z nich by potřebný identifikátor spravoval pro všechny další úřady a jak by poskytoval související osobní údaje dalším úřadům, což neřešila ani uvedená vyhláška. Certifikovaným fyzickým osobám byl v praxi vkládán do jejich kvalifikovaného certifikátu nejčastěji identifikátor MPSV,[36] na základě jejich soukromoprávního souhlasu, ačkoli účel měl být veřejnoprávní. Tato zvláštní situace pak panovala skoro celou dobu účinnosti ZEP, tedy asi 15 let.

Dle autora je právně i po účinnosti nařízení eIDAS možné požadovat jednoznačnou identifikaci při komunikaci s orgány veřejné moci. Takový požadavek ale nesmí již být součástí požadavků na kvalifikovaný nebo zaručený elektronický podpis, může ale být jiným požadavkem na podání. V praxi poskytovatelů pak pochopitelně je dosažitelné, aby buď do kvalifikovaného certifikátu pro elektronický podpis, nebo do atributového certifikátu, který by byl navázaný na kvalifikovaný certifikát pro elektronický podpis, byl vložen potřebný jednoznačný identifikátor. V současnosti nepředstavuje podstatný problém ani správa takového identifikátoru, neboť ho lze vytvořit jako zvláštní agendový identifikátor fyzické osoby (AIFO) v rámci systému

[35] Vyhláška č. 212/2012 Sb. o struktuře údajů, na základě kterých je možné jednoznačně identifikovat podepisující osobu...

[36] Identifikátor Ministerstva práce a sociálních věcí.

základních registrů. Pro uvedené by pochopitelně byla potřebná zákonná úprava, určující i subjekt veřejné správy, který by uvedený AIFO zprostředkoval poskytovatelům služeb. Možná ale bude účelnější vyzkoušet, zda si úřady neporadí i bez existence jednoznačné identifikace při přijímání elektronických podpisů.

Požadavek jednoznačné identifikace s pomocí identifikátoru MPSV kupodivu zůstal zachován v katastrální vyhlášce (srov. 5.1.5.2), a to jako požadavek na ověření pravosti uznávaného elektronického podpisu. Elektronický podpis se zde nachází typicky na soukromé písemnosti či listině, jejíž právní účinky ovšem závisí na provedení intabulace listiny katastrálním úřadem. Použití identifikátoru MPSV, spojené s následným získáním dalších údajů o totožnosti (adresa, rodné číslo apod.) z informačního systému MPSV zde umožňuje katastrálnímu úřadu získat ověřitelně informace o podepisující osob. Požadavek na přítomnost identifikátoru MPSV tak skutečně má spíše charakter doplnění dalších ověřitelných informací o podepisující osobě, než aby byl požadavkem na náležitosti samotného kvalifikovaného elektronického podpisu, takže se zřejmě jedná o úpravu, která je souladná s nařízením eIDAS, byť by zápis požadavku rozhodně měl být formulován odlišně a nikoli jako ověření pravosti podpisu. Kritičtější však je, že na rozdíl od úředně ověřeného podpisu vlastnoručního „ověření pravosti" v případě uznávaného elektronického podpisu katastrálnímu úřadu vůbec neposkytuje srovnatelný důkaz o pravosti podpisu podepsané osoby (srov. 11.7.3.4), provedeném úřadem.

8.9.12 Omezení užití certifikátu (oblast použitelnosti, finanční)

Dle § 12 odst. 1 písm. i) ZEP mohly být součástí kvalifikovaného certifikátu volitelně údaje o tom, zda se *„používání kvalifikovaného certifikátu omezuje podle povahy a rozsahu jen pro určité použití"*. Dle § 12 odst. 1 písm. i) ZEP mohlo být součástí kvalifikovaného certifikátu volitelně *„omezení hodnot transakcí, pro něž lze kvalifikovaný certifikát použít"*. Dle § 12 odst. 2 ZEP uvedená omezení podle odstavce 1 písm. i) a j) ale musela být zjevná třetím stranám.

Uvedená omezení odpovídají omezením z přílohy I písm. i) DirES *„omezení oblasti použitelnosti" (limitations on the scope of use*, *Beschränkungen des Geltungsbereichs)* a písm. j) *„omezení hodnot transakcí" (limits on the value of transactions*, *Begrenzungen des Wertes der Transaktionen)*, které byly volitelnou součástí kvalifikovaného certifikátu. Ze znění samotné přílohy I směrnice DirES nebylo

patrné, koho měla tato omezení chránit. Zda podepisující osobu, nebo poskytovatele certifikačních služeb, který kvalifikovaný certifikát vydal. Podle čl. 6 (Odpovědnost) odst. 3 a 4 DirES se však mělo jednat o omezení odpovědnosti poskytovatele za škodu pro případ *„omezení pro ... použití" (limitations on the use*, *Beschränkungen für die Verwendung)* a *„mezní hodnoty transakcí" (a limit on the value of transactions*, *eine Grenze für den Wert der Transaktionen)*, přičemž ale omezení musela být rozeznatelná třetími stranami. Nicméně i indikace omezení poskytovatele by zřejmě měla vliv na spoléhající se osobu, jak dalece by byla ochotna se na certifikát spolehnout.

Nařízení eIDAS v čl. 28 odst. 1 stanoví, že *„kvalifikované certifikáty pro elektronické podpisy musí splňovat požadavky stanovené v příloze I"*, a odst. 2, že tyto certifikáty *„nepodléhají žádným závazným požadavkům, které přesahují požadavky stanovené v příloze I"*. V příloze I již žádná možnost uvádět omezení není zmíněna.

Čl. 28 odst. 3 eIDAS nicméně stanoví výjimky. Dané certifikáty *„...mohou obsahovat další zvláštní atributy, které nejsou povinné. Těmito atributy nesmějí být dotčeny interoperabilita a uznávání kvalifikovaných elektronických podpisů."* Dovolení není vztaženo k úrovni členského státu, jako např. čl. 28 odst. 5 eIDAS. Znamená to, že výjimky z obsahu certifikátů zřejmě mohou stanovit jednotliví poskytovatelé služeb. Obsah kvalifikovaného certifikátu podle přílohy I eIDAS rozhodně nevyčerpávává položky, které se v kvalifikovaných certifikátech běžně vyskytují. Význam polí, vkládaných poskytovateli podle jejich certifikačních politik, však bude stanoven těmito politikami, nebo technickými normami, na které se odvolávají. Pro jejich právní význam může být potřeba interpretace, která nemusí být jednoznačná.

Nařízení eIDAS pak stále umožňuje omezit odpovědnost poskytovatelů. Poskytovatel ale musí podle čl. 24 odst. 2 písm. d) eIDAS o omezeních ještě před uzavřením smluvního vztahu jasně informovat osobu, která chce jeho službu využít, jakož i o přesných podmínkách používání služby. Aby poskytovatelé neodpovídali za *„škody způsobené využíváním služeb nad rámec uvedených omezení"*, musí dle čl. 13 odst. 2 eIDAS být *„omezení rozpoznatelná pro třetí osoby"*. Podrobně účel omezení vysvětluje bod odůvodnění 37 eIDAS. Omezení mají snižovat finanční rizika poskytovatelů. Informace o omezeních mají být *„zahrnuty v podmínkách poskytované služby, nebo jinými rozpoznatelnými prostředky"*. Je pozoruhodné, že nařízení eIDAS zvažuje potřeby poskytovatelů služeb, ale nevěnuje se potřebám koncových uživatelů, tj. podepisující osoby a spoléhající se osoby.

Německá implementace eIDAS v § 12 VDG zavádí explicitně tři druhy atributů (údajů), které lze do kvalifikovaných certifikátů pro elektronické podpisy a pečeti vkládat (srov. 7.3.2). Potvrzuje se tím, že rozšiřování atributů dle čl. 28 odst. 3 eIDAS je možné, zde na úrovni členského státu.

Zda bude možné do kvalifikovaných certifikátů vkládat atributy charakteru omezení použitelnosti certifikátu, v souladu s úpravou v čl. 28 odst. 3, resp. čl. 38 odst. 3 eIDAS, ukáže zřejmě až čas a praxe. Právně se taková možnost stala významně obtížnější, neboť jejich přítomnost již není v příloze I, resp. v příloze III eIDAS výslovně uváděna.

9. Právní jednání s elektronickým podpisem v ČR

V této kapitole je pojednáno o některých možnostech právního jednání s elektronickým podpisem dle právního řádu ČR v době po účinnosti ZSVD.

9.1 Poznámky k legislativní technice

V této části je uvedeno několik poznámek k legislativní technice, která byla použita v zákonech č. 297/2016 Sb. (ZSVD) a č. 298/2016 Sb. („změnový zákon“).

9.1.1 Modularita (zejména vůči veřejnému právu)

Důvodová zpráva zákona ZSVD uvádí, že jedním z cílů jeho pojetí je odstranit nadbytečné formulace v jiných zákonech, pokud se odvolávají na digitální objekty ze ZSVD, popř. eIDAS. Tato snaha je záslužná! Dosavadní úprava byla kvůli podstatě veřejného práva silně fragmentovaná, a v důsledku toho pro právního laika nepřehledná. Obecně by bylo žádoucí mít napříč veřejným právem jednotnou modulární právní úpravu, která by umožňovala provádět podání, resp. přijímat doručování od orgánů veřejné moci co nejjednotnějším způsobem ve všech typech řízení. Dle názoru autora se však tento cíl zdařil pouze částečně nebo některé právní obraty mohou vyvolávat právní nejistotu o svém významu. Oboje je dokumentováno níže.

9.1.2 Obrat „účinky vlastnoručního podpisu“

Ve změnovém zákoně č. 298/2016 Sb. se v několika případech používá obrat *„podepsaného způsobem, se kterým zvláštní právní předpis **spojuje účinky vlastnoručního podpisu**"* (zvýraznil autor) s tím, že připojená poznámka pod čarou pak vždy odkazuje současně na *„§ 18 odst. 2 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů"* a na *„§ 6 odst. 1 zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce“*.

Úmyslem normotvůrce zřejmě bylo jedním uvedeným obratem postihnout obě uvedené možnosti citované v poznámce pod čarou.

Zatímco odkaz na § 18 odst. 2 zákona č. 300/2008 Sb. považuje autor za korektní příklad případu, kdy zvláštní předpis stanoví účinek vlastnoručního podpisu, v § 6 odst. 1 ZSVD tomu tak není! V § 6 odst. 1 ZSVD se pouze dovoluje používání $AdES_{QC}$ nebo QES k podepisování *elektronickým podpisem* při jednání vůči veřejnoprávnímu podepisujícímu. V tomto kontextu účinek vlastnoručního podpisu

stanoví pouze čl. 25 odst. 2 nařízení eIDAS, a to pouze pro QES. Nařízení má však působnost danou zásadou přenesených pravomocí a vlastní vymezené působnosti. V případě ryze vnitrostátního jednání pak nemusí existovat vůbec žádný právní předpis, který by pro QES stanovil účinek vlastnoručního podpisu. Poznámky pod čarou nejsou součástí normativního textu, přesný systematický výklad je pak právě uvedený, totiž že možný je buď QES, anebo vůbec žádný elektronický podpis.

Je však možné, že soudy a úřady budou používat historický výklad indikovaný poznámkou pod čarou, tj. pro účel ustanovení, v nichž se obrat nachází, hledět na § 6 odst. 1 ZSVD tak, jako kdyby se zde i vyslovoval účinek vlastnoručního podpisu, a přijímat jak QES, tak $AdES_{QC}$. Lze snad říci, že účelem ustanovení s citovaným obratem je možnost, aby elektronický podpis ve vztahu k elektronickému dokumentu nahrazoval náležitost vlastnoručního podpisu ve vztahu k listinnému podání,[1] a v tomto smyslu tedy má (v jiném kontextu) účinek *jako* vlastnoruční podpis, přičemž připuštěny jsou dvě možnosti provedení elektronického podpisu. Tento výklad je pro praxi vstřícnější a snad i prakticky přiměřenější.

9.1.3 Obrat „zajišťujícím integritu, případně původ dat"

Ve změnovém zákoně č. 298/2016 Sb. se v několika případech nahrazuje dřívější obrat *„označené uznávanou elektronickou značkou"* za nový *„zabezpečen způsobem zajišťujícím integritu, případně původ dat"*.

Nový obrat znamená, že způsob nemusí zajišťovat původ dat (jen „případně"), což je vlastnost, kterou elektronická značka poskytovala. Zda je ztráta zajištění původu dat vhodná, je věcí uvážení, autor se domnívá, že obecně spíše nikoli. Obrat neuvádí, v jaké míře zajištění vlastností mají být vlastnosti provedeny.

Z hlediska digitálních objektů, které poskytuje nařízení eIDAS, lze proto požadavek zajistit zaručeným elektronickým podpisem, zaručenou elektronickou pečetí nebo jejich vyššími verzemi. Jak je uvedeno výše, pro automatizovaně vytvářené verze se hodí zejména AdES nebo AdESeal, popř. jejich varianty založené na kvalifikovaném certifikátu.

Požadavek integrity dat však lze rovněž zajistit kvalifikovaným elektronickým časovým razítkem (čl. 42 eIDAS) a též službou elektronického doporučeného doručování (čl. 3 bod 36 eIDAS).

[1] Podobnou právní normou byl definován účinek QES ve čl. 5 odst. 1 směrnice DirES.

Z hlediska důkazních účinků jsou nejpřesvědčivější domněnky stanoveny pro kvalifikovanou elektronickou pečeť (QESeal, čl. 35 odst. 2 eIDAS, srov. 6.15.8) a pro službu kvalifikovaného elektronického doporučeného doručování (čl. 43 odst. 2 eIDAS, srov. 6.15.10). Podle autora však není jisté, že QESeal lze platně vytvořit v případě automatizovaného vytváření pečeti.

Nelze vyloučit, že požadavek integrity dat lze splnit i jinými prostředky, které v nařízení eIDAS vůbec nejsou upraveny.

Autor si není jist, zda výše uvedený rozptyl možností realizace požadavků je ideální jak z hlediska právní jistoty, tak z hlediska kompatibility technických implementací. Pokud je účelem nahradit *uznávanou elektronickou značku* ze ZEP, pak by autor měl tendenci nahradit její použití rovnocenně pomocí $AdES_{QC}$ nebo $AdESeal_{QC}$ s tím, že podepisující nebo pečetící osoba si může vybrat, v rámci možností své právní subjektivity.

9.1.4 Kompetence Ministerstva vnitra

Dle části třetí zákona č. 298/2016 Sb. se mění kompetenční zákon č. 2/1969 Sb., a to v § 12 odst. 1 písm. n). Dle nového znění Ministerstvo vnitra je ústředním orgánem státní správy pro vnitřní věci, zejména pro: *„… n) elektronickou identifikaci a služby vytvářející důvěru“*.

Kompetence se zjevně odvolává na znění nařízení eIDAS. Striktně vyloženo, digitální objekty, jako elektronický podpis, elektronická pečeť, nejsou službou vytvářející důvěru. Buď se změní znění ustanovení, anebo se ustanovení kompetence bude vykládat široce, jako zahrnující použití výše uvedených digitálních objektů, ve vnitřních věcech. Ustanovení nahradilo dřívější kompetenci Ministerstva vnitra pro elektronický podpis.

9.1.4.1 Derogace dřívějších změnových zákonů

V § 20 ZSVD je pochopitelně zrušen zákon č. 227/2000 Sb. (ZEP) a rovněž vyhlášky č. 378/2006 Sb. a č. 212/2012 Sb., které ZEP prováděly. V bodech 2. až 16. jsou pak zrušeny různé změnové zákony, kterými se v průběhu let 2002 až 2014 upravovalo využívání digitálních objektů ze ZEP v různých jiných právních předpisech. Smyslem těchto derogací zřejmě je jakoby vrátit stav platného práva do stavu, než se tyto změnové zákony staly účinné. Je možné mít určité pochybnosti o tom, zda tento

způsob derogací poskytuje dostatečnou právní jistotu. Je totiž možné, že platné právo bylo změněno v dotčených ustanoveních dodatečně ještě nějak jinak.

Odstranění změn zavedených změnovými zákony čistě mechanicky reverzním způsobem pak může vést k tomu, že se z právního řádu odstraní jiné části, než které do něj původní změnový zákon přidal. Diskurs o případně vhodnějším způsobu derogací nicméně přesahuje účel tohoto textu.

9.2 Pozadí zpracování listin u veřejnoprávních původců

Elektronické dokumenty vydávané orgány veřejné moci mají někdy charakter veřejné listiny. Taková listina může často být opatřena, v souladu se ZSVD, kvalifikovaným elektronickým podpisem a kvalifikovaným elektronickým časovým razítkem. Veřejné listiny se těší *presumpci správnosti*.

Je důležité pochopit, že tato presumpce není založena pouze na přítomnosti obou digitálních objektů z eIDAS, ale především na tom, že u veřejnoprávního původce existuje systém spisové služby, v jehož rámci jsou originály listin v případě pochyb dohledatelné. Tato část proto představuje určitý úvod do toho, jak se u veřejnoprávních původců s listinami a spisy zachází a zda systém představuje dostatečnou záruku pro výše uvedenou presumpci správnosti.

Pro pochopení systematiky stávající úpravy v právním řádu ČR je třeba mírně historické ohlédnutí. Platí zhruba, že nejméně cca do roku 2000 byly téměř všechny veřejnoprávní agendy prováděny jen za pomoci tradičních papírových listin. Jen příležitostně vznikaly elektronizované ostrůvky některých agend, jako např. bylo nahlížení do neautentizovaných výpisů z obchodního rejstříku apod. Někde existovaly vnitřní informační systémy, ale rozhraní směrem k účastníkům řízení bylo stále jen listinné. Při jednání vůči úřadům aj. orgánům veřejné moci musely soukromoprávní subjekty jednat pouze klasickou listinnou podobou. Listiny se typicky podávaly na podatelny úřadů fyzickou návštěvou nebo posílaly poštou. Za této situace byly dominantními právními předpisy různé procesní řády, jako např. obecně zákon o správním řízení[2] nebo občanský řád soudní.[3] Správa listin a spisů se zřejmě řídila vnitřními předpisy státní správy, činnost archivů se řídila stručným zákonem ČNR

[2] Zákon č. 71/1967 Sb., o správním řízení.
[3] Zákon č. 99/1963 Sb., občanský soudní řád, v tehdejším znění.

o archivnictví.[4] Pravidla o listinné komunikaci byla proto soustředěna do výše uvedených procesních řádů, k nimž mohla existovat případně zvláštní úprava.[5]

V prvních letech nového milénia již sice úřady začaly být schopné používat webové stránky pro informační účely, tím ale jejich schopnosti zpravidla i končily. Prvním systematičtějším impulsem pro elektronizaci veřejné správy, popř. soudnictví se stala směrnice DirES a její česká transpozice v zákoně č. 227/2000 Sb., o elektronickém podpisu (tj. ZEP). Zákon nicméně řešil pouze elektronické podpisy, nikoli elektronickou komunikaci ani elektronické dokumenty. Dalším krokem proto byla snaha využít systém internetové elektronické pošty, který byl v komerčním styku ustálený nejméně od roku 1995. V návaznosti na novely ZEP se veřejnoprávním subjektům v r. 2004 přikázalo zřizování elektronických podatelen,[6] které měly být schopny přijímat zprávy elektronické pošty, popř. je i od veřejnoprávních subjektů odesílat. Výše uvedené procesní řády (správní řád, občanský soudní řád aj.) byly tehdy doplněny o možnost přijímat (podání) a odesílat (doručování) elektronickou verzi písemnosti ev. *datové zprávy* (pojem ZEP pro podepsaný obsah) *na elektronickou adresu*, podepsané uznávaným elektronickým podpisem, což se technicky provádělo internetovou elektronickou poštou a na straně veřejnoprávních subjektů bylo prostředkováno jejich elektronickými podatelnami. Reálný úspěch těchto předpisů byl nevalný. Úřady dále vedly téměř veškerou svou agendu papírově, došlých elektronicky podepsaných elektronických zpráv bylo velmi málo, úřady si je tiskly a dále zpracovávaly v tradiční listinné formě. Na jednu stranu úřady neměly žádnou vlastní iniciativu se elektronizovat, na straně druhé zbývalo velmi mnoho materie, která vůbec nebyla právně a potažmo ani organizačně nebo technicky řešena.[7] Ryze po technické stránce by

---

[4] Zákon České národní rady č. 97/1974 Sb., o archivnictví.

[5] Například tehdy zákon č. 337/1992 Sb., o správě daní a poplatků.

[6] Vyhláška č. 496/2004 Sb., o elektronických podatelnách, a nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb.

[7] K roku 2006 existovaly zhruby tyto potíže (některé přetrvávají dodnes): stanovení řádného podepisování, právní následky v případě „půjčení" jiné osobě, povinnosti ověřování platnosti podpisu a právní následky technické neplatnosti, přesná metoda ověřování platnosti (časová razítka, certifikační cesta...), řešení odpovědnosti po dobu poshovění, dlouhodobá archivace, nestanovení povinnosti veřejnoprávním subjektům elektronicky právně jednat, mnoho paralelních úprav téměř shodného významu v procesních předpisech, nejednotný způsob odvolávání se na pojmy ze ZoEP, neimplementovaný požadavek na jednoznačnou identifikaci, chybějící užší výběr ze sad kryptografických schémat, chybějící formáty pro elektronické podpisy, chybějící formáty pro elektronické dokumenty, neupravení přikládání příloh podání od třetích osob, neupravení konverzí mezi papírovou a elektronickou formou, neupravení přeposílání stejnopisů podání v elektronické podobě jiným účastníkům řízení, neupravení předávání a postupování spisů s elektronickými dokumenty, požadavky na harmonizaci vzhledu uživatelského rozhraní při vytváření podpisu, přesnější stanovení způsobu nahrazení písemné formy formou elektronickou, přesné stanovení druhu

bylo potřeba jednoznačně stanovit několik desítek technických specifikací, k čemuž nedocházelo ani úrovni ČR, ale ani na úrovni EU.

V roce 2004 byl přijat nový správní řád, zákon č. 500/2004 Sb. (dále jen „spr. řád"), který do sebe sice nepřímo pojal možnost komunikace prostřednictvím elektronických podatelen, fakticky ale zvrat nepřinesl. Téhož roku byl přijat i nový zákon č. 499/2004 Sb., o archivnictví a spisové službě (dále jen „zák. o archivnictví"), ale ani ten neznamenal přelom, protože spisy se stále vedly především papírově.

Ze systémového hlediska tehdy *spisová služba* byla jen organizací činností[8] nad dokumenty a spisy. Na dokumenty se sice v rámci spisové služby umisťují různé pomocné značky a poznámky vyřizujících osob, nicméně vlastní obsah dokumentů, až na výjimky, jako jsou pravidla pro uvádění jednacích čísel, je určen činností původce a právními předpisy upravujícími jeho činnost; pravidla spisové služby do něj nezasahují.

---

elektronických podpisů, chybějící referenční aplikace pro vytváření a pro ověřování elektronického podpisu...

[8] **Klasická spisová služba stručně:** dokument vytvořený vnějším subjektem nebo i některou součástí určeného původce dorazí do *podatelny* příjemce (určeného původce), kde je opatřen podacím razítkem, je mu přiděleno číslo jednací a jeho přijetí je zaevidováno v *podacím deníku*. Dokument je přidělen odpovídajícímu oddělení nebo pověřené osobě k vyřízení (předání se rovněž eviduje v podacím deníku). Pro více dokumentů ke stejné věci se vytváří tzv. *spis*, dokumenty v něm shromážděné mají mít stejné jednací číslo až na pořadové číslo ve spisu. Během vyřizování věci je spis „otevřený". Pokud je postup vyřizování složitější, může se vyřizování provádět a evidovat namísto podacího deníku pomocí *jednacího plánu* (má vlastnosti nadmnožiny podacího deníku). *Vyřízením spisu* se rozumí vyhotovení a podpis závěrečného rozhodnutí (nebo jiné formy vyřízení) a jeho vypravení přes *výpravnu* (ta může být součástí podatelny). Je-li předepsáno doručení do vlastních rukou, zpět došlá doručenka se rovněž zařadí do spisu. Po vyřízení spisu nastává tzv. *uzavření spisu*, přičemž se zkontroluje přítomnost všech dokumentů a jejich označení tzv. *spisovými znaky* (indikuje typ dokumentu podle jeho obsahu), *skartačními znaky* (A-archiv, S-stoupa, V-výběr) a *skartačními lhůtami*. Tyto znaky jsou na dokument povinny uvádět vyřizující osoby (zaměstnanci) již dříve. Celý spis se rovněž označí skartačním znakem a lhůtou, jež se převezmou ze skartačního znaku/lhůty dokumentu, jímž bylo provedeno vyřízení spisu. Uzavřený spis se předá na uložení do *spisovny*, kde se běžně nachází až do doby skartace. Pokud je předepsáno velmi dlouhé zachování spisu, může určený původce vytvořit tzv. *správní archiv*, do něhož se po určité době spisy předávají ze spisovny (jako do meziskladu). Životnost spisu a dokumentů u určených původců končí po uplynutí vyznačené *skartační lhůty* ve *skartačním řízení*. Skartaci organizuje za původce *skartační komise*, která probere spisy určené ke skartaci, rozhodne o zařazení spisů označených V do kategorie A nebo S, sestaví *skartační návrh* a zašle ho příslušnému archivu (tj. externí instituci). Archivář z archivu posoudí návrh i spisy, provede případné přeřazení mezi kategoriemi A a S a podepíše *protokol o skartačním řízení*, který teprve umožňuje znehodnotit dokumenty kategorie S. Dokumenty typu A přebírá příslušný archiv jako tzv. archiválie a potvrzuje převzetí v tzv. *protokolu o předání archiválií*.
Zákon a prováděcí předpisy rozebírají výše uvedené pojmy a činnosti poměrně podrobně (např. určují stavebně-technické a bezpečnostní náležitosti spisoven a správních archivů), přesto představují pouze základní kostru správy dokumentů u určených původců. Kvůli rozdílům činnosti si podrobnosti vedení spisové služby má každý určený původce upravit podrobně vnitřním předpisem – *Spisovým a skartačním řádem* (dnes zván jako *Spisový řád*). Jeho součástí je i *spisový a skartační plán*, který obsahuje seznam typů dokumentů roztříděných do věcných skupin s vyznačenými spisovými znaky, skartačními znaky a skartačními lhůtami.

Zde je třeba si uvědomit, že papír jako základ tradiční listiny je univerzální nosič, který umožňuje zachycení velmi různorodých informací, jež ani nemusí být vytvořeny a na papír naneseny současně, ani nemusí pocházet od jediné osoby. Kromě vlastního potřebného obsahu listiny se jedná především o umístění autentizačních prvků, jako jsou vlastnoruční podpisy, popř. úřední razítka. Dalšími pak jsou již zmíněné různé pomocné značky podle metodiky spisové služby nebo pro účely archivace. Podstatné je, že kromě různých vrstev fyzické a organizační bezpečnosti spisů a dokumentů, ať již na úřadech, nebo později v archivech, jsou další bezpečnostní funkce, tj. autentizační prvky, přítomny již přímo na dokumentu a k jejich dlouhodobému zachování (i stovky let[9]) dostačuje zcela pasivní skladování spisů za definované teploty, vlhkosti a čistoty. V tomto smyslu je proto zák. o archivnictví koncipován tak, že jeho základní jednotkou ukládané informace je dokument. Podle § 2 písm. e) zák. o archivnictví se *dokumentem* pro účely daného zákona rozumí *„každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, ať již v podobě analogové či digitální, která byla vytvořena původcem nebo byla původci doručena"*.

Pojem je skutečně definován pro účely především archivnictví, aby bylo možné potenciálně archivovat jakýkoli informační artefakt, který původce vytvořil nebo mu byl doručen. Definice se proto nijak zvlášť nezabývá tím, jaké mají dokumenty autentizační prvky. Předpokládá se, že ty případně předepisují zvláštní zákony. V rámci zák. o archivnictví existují jen zcela obecná pravidla pro vyhotovování a podepisování dokumentu,[10] popř. si veřejnoprávní původci mají stanovit podrobnější pravidla v rámci svého spisového řádu nebo jiného vnitřního předpisu.

Jen obecně rámcová úprava nakládání s dokumenty, obsažená v zák. o archivnictví , je dostatečná pro tradiční papírové listiny. Pro digitální dokumenty dostačuje tehdy, pokud se nekladou požadavky na právní význam, na důkazní přesvědčivost apod. Existence jakéhokoli digitálního dokumentu je totiž nesamozřejmá už sama o sobě. Jedná se jen o určitou posloupnost bitů, která bez dalšího může být kdykoli změněna libovolným způsobem. Jakýkoli systém, který nakládá s digitálním dokumentem, musí především zajistit jeho neporušitelnost (*integritu*). K tomu již je ale zapotřebí informace přídavná k dokumentu, která musí být určitým způsobem k dokumentu udržována. Rovněž *autentizační* informace mohou mít charakter přídavné

[9] Správní praxe vyžaduje různě dlouhé doby uchování. Pro běžná správní řízení dostačuje zpravidla 10 let. Dlouhá bývá potřeba uchování dokumentace budov. Ještě dlouhodobější je potřeba dokumentace míst se zátěží pro životní prostředí, kde se dosahují až stovky let.

[10] Ustanovení § 16 a § 17 vyhl. č. 259/2012 Sb., o podrobnostech výkonu spisové služby.

informace k dokumentu. Kvůli těmto požadavkům by úprava pro nakládání s elektronickými dokumenty měla explicitně obsahovat ustanovení, která by tyto přídavné *digitální objekty* rozeznávala, stanovila jejich funkce či vlastnosti a stanovila, přinejmenším v úrovni cílů, závazné provedení a nakládání s takovými digitálními objekty.

Rovněž je nově třeba zcela jiná kvalita evidenčních pomůcek v rámci spisové služby. V tradičním listinném provedení spisů, pokud by došlo k havárii elektronizovaných evidenčních pomůcek, vždy zbývaly samotné spisy ve fyzickém provedení, dostatečně autentické, na jejichž základě bylo možné evidenční pomůcky obnovit. V elektronickém provedení dokumentů však může být problematické spisy a dokumenty lokalizovat, dojde-li ke kolapsu odkazovacích systémů. Dále je v případě elektronických dokumentů zapotřebí zajistit i to, aby odkazy evidencí nevedly na podvržené dokumenty. Nedostačuje mít navržen sofistikovaný systém vícenásobného způsobu řazení, ale je třeba, aby jak provedení systému, tak datová reprezentace byly odolné proti záměrnému útoku na systém evidencí. Ze samotného textu zák. o archivnictví takové vlastnosti neplynou.

Pro další podrobnosti o zpracování dokumentů je vhodné konzultovat díla[11] z oblasti spisové služby. Obecně je však při používání či navrhování právních předpisů v oblasti spisové služby a archivnictví třeba mít na vědomí, že zejména spisová služba by měla být koncipována tak, aby během celé doby uchovávání elektronických dokumentů i elektronických spisů byla zajištěna kontrolovatelnost platnosti zaručených a kvalifikovaných elektronických podpisů a pečetí. Vnitřní konverze do výstupního formátu mohou být nutné z hlediska snadné práce s informacemi, pro důkazní funkce je však žádoucí mít zachovány i originální formáty dokumentů a podpisů nebo pečetí, včetně zajištění jejich kontrolovatelnosti. V opačném případě budou soudy budoucnosti řešit otázky o tom, zda při vnitřní konverzi před desítkami let nedošlo ke ztrátě autenticity dokumentu nebo podpisu, jak kvalitní byly postupy konverze nebo jak důvěryhodní a pečliví byli zaměstnanci, kteří je prováděli a osvědčovali. Tyto otázky budou zpětně v podstatě neřešitelné. Je lepší jim předejít správnými metodikami, aby nemusely vůbec vzniknout.

[11] Např. KUNT, M. – LECHNER, T. *Spisová služba.* 2., aktualizované vydání. Praha: Leges, 2017.

9.3 Veřejnoprávní jednání s elektronickým podpisem – podání

V této části probereme tři předpisy (správní řád, soudní řád správní a občanský soudní řád) z oblasti veřejného práva a v jejich rámci vždy podání.[12]

Zabývat se budeme tím, jak se v rámci těchto jednání má uplatnit elektronický podpis. V právním řádu se pochopitelně nachází řada dalších[13] veřejnoprávních předpisů, které upravují další řízení a jejich požadavky mohou být odlišné. Jak uvádí i důvodová zpráva ZSVD, některé předpisy pro některé druhy jednání elektronický podpis výslovně nevyžadují. Tak tomu je např. u „žádostí o informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, nebo u podnětů podle zákona č. 500/2004 Sb., správní řád".[14]

Účelem popisu zde však není podat vyčerpávající přehled veřejnoprávní elektronické komunikace, nýbrž pouze jejich nejvýznamnějších obecných vzorů.

9.3.1 Infrastrukturní okruhy právních předpisů

V ČR platí tři základní okruhy právních předpisů, které se týkají elektronických dokumentů a elektronických podpisů ve veřejnoprávní oblasti:

- Nařízení eIDAS a jeho adaptační zákon ZSVD v části pro digitální objekty odvozené od elektronického podpisu.
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů (dále jen „ZEÚ").
- Zákon č. 499/2004 Sb., o archivnictví a spisovové službě (dále jen „zák. o archivnictví ").

Tyto tři okruhy právních předpisů lze považovat za „obecně infrastrukturní" v tom smyslu, že upravují problematiku obecně napříč celou veřejnou správou, popř. veřejnou mocí, bez ohledu na dílčí oblast práva, resort, druh úřadu.

Systematicky je třeba úpravu těmito třemi okruhy hodnotit jako poměrně nesourodou. Každý okruh řeší jen dílčí potřebu, a to ze svého úhlu pohledu.

K těmto třem okruhům se zřejmě přidá ještě zákon č. 250/2017 Sb., o elektronické identifikaci, účinný od 1. 7. 2018. Právní charakter jednání s využitím

[12] O druhém hlavním druhu jednání, kterým je *rozhodnutí*, jež přijal správní orgán, nebo *rozsudek* soudu, z důvodu omezení rozsahu textu bohužel pojednáno není.
[13] Typicky budou novelizovány ve změnovém zákoně č. 298/2016 Sb.
[14] Důvodová zpráva ZSVD, s. 35.

identifikace dle tohoto zákona však budou muset též případně stanovit zvláštní předpisy.

9.3.2 Možnosti technické komunikace

Z hlediska technologického existují dnes tři hlavní možnosti elektronické komunikace v rámci veřejného práva.[15] Všechny jako podklad konektivity využívají službu sítě internet. Nad touto vrstvou existují typově tři další možné druhy služeb. První je elektronická pošta podle internetových specifikací. Druhou je systém datových schránek. Třetí jsou webové portály, které umožňují přijímat podání pro různé zvláštní, ale i obecné druhy agendy (typicky Finanční správa ČR, Česká správa sociálního zabezpečení atd.). Třetí druh se zpravidla specializuje na příjem specifických formulářů, tj. umožňuje s různou mírou interaktivity formulář na stránkách vytvářet, kontrolovat a nakonec i podat. Funkce takových portálů musí být předjímána a upravena v resortních právních předpisech veřejného práva. Webový portál navázaný na obecnou elektronickou podatelnu se však spravuje podle obecných správních předpisů.

9.3.2.1 Výklady fikce podání v ZEÚ

Druhou uvedenou možnost v ČR upravuje zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů (dále jen „ZEÚ“). Hlavním důvodem vytvoření systému datových schránek bylo mít elektronický způsob doručování, tj. od orgánů veřejné moci[16] vůči účastníkům řízení, který by prokazoval doručení a jeho datum a čas. Tyto funkce nebyla internetová elektronická pošta schopna plnit, doručení nastávalo pouze tehdy, když jej adresovaný účastník řízení sám zpětně potvrdil. Ten na tom často nemusel mít zájem, pouze se tak předem dozvěděl doručený obsah a případně obstruoval i následný pokus o doručení poštou. Datové schránky se *povinně* zřídily pro orgány veřejné moci (§ 6 odst. 1 ZEÚ) na straně jedné a na straně druhé pro mnohé právnické osoby (§ 5 odst. 1 ZEÚ) a dále pro advokáty, statutární auditory, daňové poradce a insolvenční správce (§ 4 odst. 3 ZEÚ), jakožto zvláštní profese, jejichž náplň činnosti často obsahuje zastupování jiných subjektů, a to zejména vůči státním orgánům. Jiné subjekty, např. fyzické osoby, mohou o zřízení datové schránky požádat dobrovolně. Datové schránky tedy mají různé režimy činnosti a funkcionality, podle toho, o jaký druh subjektu se jedná. Ke každé datové schránce se též zřizuje jeden nebo více přístupových účtů, každý pro jednu fyzickou osobu, která získá přístupové údaje. Jedna a táž fyzická osoba může mít přístupové údaje pro více

[15] Nejsou zde zmiňovány vnitřní infrastruktury uvnitř veřejné správy nebo mezi státními orgány.
[16] Jak je pojem určen legislativní zkratkou v § 1 ZEÚ.

datových schránek.[17] Datové schránky umožňují kromě doručování i provádění úkonů vůči orgánům veřejné moci, tj. zejména činění různých podání. Pro přístup do datové schránky v nejjednodušší úrovni zabezpečení dostačuje jako autentizace pouze přihlašovací jméno a heslo, které tvoří takzvané přístupové údaje, což je z hlediska uživatele velmi levné i snadné. Jádrem funkce systému datových schránek je posílání datové zprávy.[18] Ve směru od orgánů veřejné moci k výše uvedeným účastníkům se jedná o doručování, ve směru od účastníků směrem k orgánům veřejné moci se jedná o elektronické úkony charakteru podání. Pro tuto funkci je v § 18 odst. 2 ZEÚ stanovena právní fikce, že *„Úkon učiněný ... prostřednictvím datové schránky má **stejné účinky** jako **úkon učiněný písemně a podepsaný** ..."* (zvýraznil autor). ZEÚ je v této části napsán jako obecně doplňující úprava podávání vůči orgánům veřejné moci, ať je v právním řádu ČR obsažena kdekoli. Vůči těmto dílčím úpravám, roztroušeným po právním řádu ČR, pak ZEÚ bude běžně vždy v roli *lex specialis*.[19]

Autor běžně zastává výklad (I), že obraty *„písemně"* a *„podepsaný"* dle něj především byly a jsou přímo navázány na stejné pojmy ve správním řádu (srov. níže). Podle autora je proto pak třeba jimi rozumět *„v listinné (papírové) podobě"* a *„s vlastnoručním podpisem"*, což autorovi plyne především z historického výkladu ZEÚ ve vztahu k správnímu řádu v době, kdy byl ZEÚ přijímán, a z toho faktu, že normotvůrci se prvotně jednalo o pokrytí podání ve správních řízeních. Správní řád byl tedy prvořadým zákonem, který se ZEÚ snažil doplňovat jako *lex specialis*, a to doslovně. V § 18 odst. 2 ZEÚ zákon prováděl hned dvojí fikci. První fikcí je, že odesilatel (subjekt, do jehož datové schránky se uživatel přihlásil) je původcem podání, a to v úrovni myšleného připojení podpisu. Druhou fikcí je proměna podoby, co se týče obsahu i podpisu. Z elektronické podoby se provádí proměna na tradiční listinnou podobu a přihlašovací autentizace (login/heslo) a elektronický podpis prostý (stisk tlačítka odeslání) jsou přeměněny na vlastnoruční podpis.

Podání učiněné datovou schránkou vůči orgánu veřejné moci (nikoli doručení v opačném směru), ačkoli tedy technologicky má elektronickou podobu, resp. využívá elektronické prostředky, se pak z hlediska příjmu orgánem veřejné moci ocitne ve stejném právním režimu jako tradiční podání v listinné podobě opatřené vlastnoručním

[17] Může mít například tři účty a troje přístupové údaje, je-li např. členem statutárního orgánu bytového družstva, statutárního orgánu obchodní společnosti a nakonec i pro svou vlastní schránku fyzické osoby.

[18] Datová zpráva je zde pojem ZEÚ.

[19] Jiný vztah, tj. aby jiný zákon byl zvláštní úpravou vůči ZEÚ, bývá výjimečný.

podpisem. ZEÚ tedy umožňuje elektronické podávání přes datové schránky, aniž by se úprava zvláštního procesního předpisu veřejného práva vůbec musela měnit proti stavu před nástupem internetu, jak existovala řekněmě cca v roce 1993. V tomto smyslu na podání učiněné podle § 18 odst. 2 ZEÚ pak skutečně lze hledět i jako na takové, které stanoví účinek rovnocenný vlastnoručnímu podpisu (srov. 9.1.2).

V praxi dílčí předpisy veřejného práva určitou úpravu podání v elektronické podobě obsahují, neboť v mezidobí existovaly snahy implementovat komunikaci prvním (elektronická pošta) a třetím druhem (webový portál). To může v praxi vyvolávat potíže výkladu, neboť podání přes datové schránky pak je někdy chápáno za podání v elektronické podobě.

Výše uvedený výklad autora bohužel totiž není v praxi jediný. Mnoho osob začalo vycházet při substituci z jiné cílové situace. Někdy se uvažuje výklad (II), totiž že podání bylo a zůstává v elektronické podobě a autentizace přístupu do schránky je právní fikcí dle § 18 odst. 2 ZEÚ převedena na vyhovující elektronický podpis, tj. na *uznávaný elektronický podpis*. Tento výklad zastává například Nejvyšší soud ve svém čerstvém stanovisku: „Elektronický dokument, který byl zaslán prostřednictvím datové schránky odesílatele ... se považuje – jak vyplývá z ustanovení § 18 odst. 2 zákona o elektronických úkonech – za podepsaný, tj. má z hlediska jeho podpisu stejné právní účinky jako elektronický dokument v podobě datové zprávy podepsaný uznávaným elektronickým podpisem.“[20] Ve stanovisku je pak i opakováno: „elektronické podání učiněné prostřednictvím datové schránky osoby, pro niž byla tato datová schránka zřízena, má stejné právní účinky jako elektronické podání podepsané uznávaným elektronickým podpisem této osoby.“[21] Odtud se výklad následně rozšířil i do judikátu(ů) Nejvyššího správního soudu.[22] Autor tento výklad považuje za ahistorický a rovněž v rozporu s vícenásobným výskytem obratu *„podepsaného způsobem, se kterým zvláštní právní předpis spojuje účinky vlastnoručního podpisu"* ve změnovém zákoně (podrobně srov. 9.1.2), který bývá pravidelně přes poznámkový aparát vázán právě na § 18 odst. 2 ZEÚ. Pokud by ale podpis fingovaný ISDS měl být považován jen za uznávaný elektronický, pak uznávaný elektronický podpis, definovaný v ZSVD, účinky vlastnoručního podpisu obecně nemá, a konsekventně by pak podání podle § 18 odst. 2

[20] Stanovisko pléna Nejvyššího soudu ze dne 5. 1. 2017 k podáním činěným v elektronické podobě a k doručování elektronicky vyhotovených písemností soudem, prováděnému prostřednictvím veřejné datové sítě, sp. zn. Plsn 1/2015, s. 7, odst. 18.

[21] Stanovisko NS Plsn 1/2015, s. 13, odst. 39.

[22] Rozsudek Nejvyššího správního soudu ze dne 7. 9. 2017, sp. zn. 7 As 221/2017 - 40, odst. 25.

ZEÚ, tedy přes ISDS, nebylo možné všude tam, kde změnový zákon klade podmínku výše citovaným obratem. Zákon ZSVD totiž uznávaný elektronický podpis pouze připouští pro použití za elektronický podpis v případech určitých předvídaných situací. Jinou námitkou může být, že pokud nedochází k fingování změny podoby, z elektronické na listinnou, charakter písemnosti má zřejmě i původní podávaný elektronický dokument, pročež ale odpadá důvod fingování vůbec. Existence části zákonného pravidla o právní fikci přestane vůbec poskytovat smysl. Používání výkladu II nicméně nevadí, dokud vede na to, že se elektronický úkon (podání) považuje za platný.

Obecně by ještě byl možný výklad (III), dle nějž cílově substituovaným stavem by byly pouze obecné výrazy doslovně, tj. *„písemně"* a *„podepsaný"* bez výkladu. U takového podání by tedy platily oba znaky ve své abstraktní rovině, aniž by se určovalo, o jakou fyzickou podobu se jedná. To je současně i slabinou výkladu. Výhodou naopak je, že se z hlediska aplikace jedná o výklad velmi extenzivní, který umožňuje odůvodnit splnění podmínek formy i podpisu pro velmi mnoho situací i podob provedení.

Bez ohledu na výklady I, II, a III platí výjimka ze závěru v § 18 odst. 2 ZoEU, která vylučuje použití výše diskutované právní fikce: *„…ledaže jiný právní předpis nebo vnitřní předpis požaduje společný úkon více z uvedených osob"*. Protože k účtu datové schránky se může přihlásit a datovou zprávu odeslat pouze jedna fyzická osoba, nelze přihlašování využít pro vícenásobné podepsání. Pak se ani jedna ze dvou výše uvedených právních fikcí z § 18 odst. 2 ZEÚ neuplatní, neuplatní se ani žádný z jejích možných výkladů I, II, III, jedná se o podání v elektronické podobě, k jehož potvrzení jsou zapotřebí uznávané elektronické podpisy více uvedených osob.[23]

9.3.3 Přijímané formáty dokumentů veřejnoprávními (určenými) původci

Podle § 64 odst. 1 zák. o archivnictví musí určení původci zajistit v případě digitálních dokumentů jejich příjem alespoň v datových formátech stanovených jako *výstupní datové formáty*, anebo jako *formáty* dokumentů, které jsou *výstupem z autorizované konverze dokumentů*. Výstupní datové formáty *dokumentů v digitální podobě* jsou stanoveny v § 23 vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby:

[23] Z důvodové zprávy ZEÚ: „v takovém případě úkonu učiněnému prostřednictvím datových schránek účinky podepsaného dokumentu nepřiznávají a je třeba použít zaručený elektronický podpis."

- statické texty vč. statických obrazů: *PDF/A* (ISO 19005);
- statické obrazové: *PNG* (ISO/IEC 15948), *TIF/TIFF* (revize 6 – nekomprimovaný), *JPEG/JFIF* (ISO/IEC 10918);
- dynamické obrazové (video): *MPEG-2* (ISO/IEC 13818), *MPEG-1* (ISO/IEC 11172), *GIF*;
- zvukové (audio): *MP2* (MPEG-2 Audio Layer II), *MP3* (MPEG-2 Audio Layer III), *WAV* (Waveform audio format), *PCM* (Pulse-code modulation);
- databáze: *XML* (Extensible Markup Language Document), přičemž popis jeho struktury musí být pomocí schématu XML nebo Document Type Definition (DTD);
- metadata: *XML* (Extensible Markup Language Document);[24]
- jiný fakultativní datový formát (dle § 23 odst. 8 vyhl. č. 259/2012 Sb.).

Formáty výstupu obsaženého v datové zprávě jsou obsaženy v příloze č. 1 bod 4 k vyhlášce č. 193/2009 Sb., o stanovení podrobností provádění *autorizované konverze dokumentů*, a je jimi jediný formát:

- *PDF verze 1.7 a vyšší* (Portable Document Format).

Jiné formáty pro příjem může případně stanovit jako povinné již jen zvláštní předpis veřejného práva.[25]

Formáty PDF a PDF/A[26] jsou současně též jediné formáty, které jsou schopny v sobě bez dalšího zahrnout informace o zaručeném elektronickém podpisu, tj. sloužit jako společný kontejner pro podepsaný obsah i pro zaručený elektronický podpis, včetně případných dalších digitálních objektů, jak se používají v rámci formát podpisů **PAdES**. Další formáty **XAdES** a **CAdES**, vyhlášené prováděcím rozhodnutím Komise (EU) 2015/1506, tuto vlastnost nemají. Ačkoli podle čl. 27 odst. 5 eIDAS jsou subjekty veřejného sektoru povinny všechny tyto tři formáty uznávat, žádný obecnější český právní předpis je zřejmě nezmiňuje ani je nerecipuje adaptační zákon ZSVD.

---

[24] Podle schématu XML pro výměnu dokumentů a jejich metadat mezi elektronickým systémem spisové služby stanoveného národním standardem. Nebo podle schématu XML pro vytvoření datového balíčku SIP stanoveného národním standardem, který obsahuje metadata podle schématu XML pro zaznamenání popisných metadat uvnitř datového balíčku SIP stanoveného národním standardem.

[25] Činí tak například § 72 odst. 3 zák. č. 280/2009 Sb., daňový řád, ve znění pozdějších předpisů. Formát a struktura dat jsou pak zveřejněné správcem daně na webové stránce: <https://adisepo.mfcr.cz/adistc/adis/idpr_pub/epo2_info/popis_struktury_seznam.faces>. Tento zvolený způsob právní úpravy v daňovém řádu je sice flexibilní, ale poskytuje jen málo právní jistoty ohledně toho, jaký formát dat se přijímá.

[26] V tomto případě od verze PDF/A-2, normované v ISO 19005-2:2011.

Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby, používá zastaralou terminologii ZEP, který již byl zrušen, nevzala na vědomí účinnost eIDAS. Přenosu a potažmo příjmu přes systém datových schránek může bránit pro něj právně stanovený výčet přenášených formátů dokumentů.[27] Ani v tomto seznamu nejsou uvedeny formáty PAdES, XAdES a CAdES, které musí uznávat a potažmo zřejmě i přijímat subjekt sektor veřejného sektoru podle nařízení eIDAS.[28] Veřejnoprávní původce nicméně může dle § 23 odst. 8 vyhl. č. 259/2012 Sb. přijímat jiné fakultativní formáty, přičemž informace podle § 3 odst. 3 vyhl. č. 259/2012 Sb. zveřejní na své úřední desce, nezřizuje-li ji, pak na svých internetových stránkách, přičemž uvádí *„f) přehled dalších datových formátů dokumentů obsažených v datové zprávě, ve kterých veřejnoprávní původce přijímá dokumenty v digitální podobě, včetně jejich technických, popřípadě jiných parametrů"*.

Má-li být přijímaný elektronický dokument elektronicky podepsán, pak je ale otázka formátu elektronického podpisu nevynechatelná. Bohužel není zcela jednoznačně zodpověditelná. Pokud subjekt veřejného sektoru při poskytování svých on-line služeb přijímá zaručené elektronické podpisy, pak musí uznávat formáty PAdES, CAdES a XAdES, které dle čl. 27 odst. 5 eIDAS vyhlásila Komise. V důsledku

---

[27] Příloha č. 3 k vyhlášce č. 194/2009 Sb. o stanovení podrobností užívání a provozování informačního systému datových schránek:

„I. Přípustné formáty datové zprávy dodávané do datové schránky: a) **pdf** (Portable Document Format); b) **PDF/A** (Portable Document Format for the Long-term Archiving); c) **xml** (Extensible Markup Language Document); d) fo/zfo (602XML Filler dokument); e) html/htm (Hypertext Markup Language Document); f) odt (Open Document Text); g) ods (Open Document Spreadsheet); h) odp (Open Document Presentation); i) txt (prostý text); j) rtf (Rich Text Format); k) doc/docx (MS Word Document); l) xls/xlsx (MS Excel Spreadsheet); m) ppt/pptx (MS PowerPoint Presentation); n) **jpg/jpeg/jfif** (Joint Photographic Experts Group File Interchange Format); o) **png** (Portable Network Graphics); p) **tif/tiff** (Tagged Image File Format); q) **gif** (Graphics Interchange Format); r) **mpeg1/mpeg2** (Moving Picture Experts Group Phase 1/Phase 2); s) **wav** (Waveform Audio Format); t) **mp2/mp3** (MPEG-1 Audio Layer 2/Layer 3); u) isdoc/isdocx (Information System Document) verze 5.2 a vyšší; v) edi (mezinárodní standard EDIFACT, standardy ODETTE a EANCOM pro elektronickou výměnu obchodních dokumentů – EDI); w) dwg (AutoCAD DraWinG File Format) verze 2007 a vyšší; x) shp/dbf/shx/prj/qix/sbn/sbx (ESRI Shapefile); y) dgn (Bentley MicroStation Format) verze V7 a V8; z) gml/gfs/xsd (Geography Markup Language Document).

II. Formáty uvedené v bodu I jsou přípustnými formáty datové zprávy dodávané do datové schránky, obsahují-li odpovídající příponu. Příponou se rozumí vnější znak formátu datové zprávy, který umožňuje programovému vybavení určení typu datového souboru.

III. Formát uvedený v bodu I písm. c) [tj. **xml**] je přípustným formátem datové zprávy dodávané do datové schránky, odpovídá-li veřejně dostupnému XSD schématu publikovanému příjemcem datové zprávy."

(autor tučně zvýraznil ty formáty, které je určený původce povinen přijímat vždy).

[28] Čl. 27 odst. 5 eIDAS ve spojení s prováděcím rozhodnutím Komise (EU) 2015/1506.

toho by takový veřejnoprávní původce tedy měl povinně přijímat i formát **p7s** (pro CMS a CAdES) a **XML** (XAdES) pak i mimo kontext databází a metadat. Jedná se zde spíše o formát dat než o formát dokumentu. Rovněž provozuje-li elektronickou podatelnu, pak je zřejmě nucen přijímat zprávy elektronické pošty. Ty mohou být opět podepsány formátem **p7s**, popř. původce přijímá i formáty reprezentující *celou zprávu* internetové elektronické pošty. Příjem těchto formátů je pak implikovaně nutný.

Neposkytuje-li on-line služby ani nepřijímá elektronickou podatelnou, pak na základě výše uvedeného bude přesto smysluplné přijímat aspoň formát formáty **PDF** nebo **PDF/A**, obsahující podpis dle PAdES.

9.3.3.1 Přijímané formáty dokumentů soudy

Dle Stanoviska[29] pléna Nejvyššího soudu ze dne 5. 1. 2017, sp. zn. Plsn 1/2015, (níže v této části jen „stanovisko NS“ nebo „stanovisko“) lze přijímat pouze dokumenty formátu PDF, PDF/A, DOC, DOCX, XLS, XLSX, ZFO, TXT a RTF, popřípadě podání může též být v těle datové zprávy. Stanovisko NS[30] zde vychází z instrukce Ministerstva spravedlnosti ze dne 17. 4. 2013, č. j. 133/2012-OD-ST, kterou se upravuje jednotný postup podatelny při příjmu a ověřování datových zpráv a dokumentů v nich obsažených.

Jedná se tedy jen o podmnožinu formátů určenýchChyba: zdroj odkazu nenalezen v příloze č. 3 vyhlášky č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek.

Ze stanoviska NS je důležitá vstřícnost, že obálku, kontejner apod. zaobalení datové zprávy, ať je posílána sítí internet, datovými schránkami nebo jinak, považuje za součást podání. To je podstatné, protože zaručený elektronický podpis nebo autentizační informace systému datových schránek se mohou nacházet právě na úrovni této obálky, a nikoli až jednotlivých dokumentů, které jsou součástí podání uvnitř obálky. Stanovisko takový elektronický podpis kontejneru či obálky dovoluje považovat za platné z hlediska podání a uvádí, že neplatí analogie s tradičním papírovým podáním, kde je obálka oddělitelná a její podpis neznamená podpis podání.[31]

---

[29] Stanovisko pléna Nejvyššího soudu ze dne 5. 1. 2017 k podáním činěným v elektronické podobě a k doručování elektronicky vyhotovených písemností soudem, prováděnému prostřednictvím veřejné datové sítě, sp. zn. Plsn 1/2015.

[30] Stanovisko NS Plsn 1/2015, s. 3.

[31] Stanovisko NS Plsn 1/2015, s. 4–5 (body 12.–15.), 10–11 (bod 29.–31.).

Stanovisko nicméně považuje zřejmě za ideální: „uznávaným elektronickým podpisem by ... měl být opatřen především ten elektronický dokument, který obsahuje vlastní podání toho, kdo činí písemné podání jako procesní úkon“[32] a „tato část datové zprávy se považuje za perfektní elektronické podání učiněné tou osobou, která k němu připojila svůj uznávaný elektronický podpis“.[33]

Stanovisko též uvádí, že dle § 42 odst. 1 o. s. ř. lze podání v elektronické podobě učinit pouze prostřednictvím veřejné datové sítě. Za tuto považuje aktuálně síť internet a v jejím rámci pak služby internetové pošty, systému datových schránek nebo webové rozhraní elektronické podatelny. Odmítá proto přípustnost podání v elektronické podobě pomocí technických nosičů, jako jsou CD, DVD, USB flash disky apod.[34]

9.3.4 Odesílané formáty dokumentů veřejnoprávními (určenými) původci

V obecném veřejném právu dle autora chybí jednoznačné stanovení formátů dokumentů, které mohou veřejnoprávní původci odesílat jako jednotlivé dokumenty.

V zák. o archivnictví se sice vyskytuje pojem tzv. *výstupních datových formátů*, ale význam není sebevysvětlující ze slov. Podle § 65 odst. 5 zák. o archivnictví má určený původce povinnost převést digitální dokumenty do výstupního datového formátu při uzavření spisu. Po této operaci následuje typicky uložení spisu ve spisovně, kde spis leží, než se dosáhne času skartačního řízení. Účelem výstupního formátu zde tedy je, aby dokument byl ve formátu, v němž bude ležet ve spisovně a odkud ho bude později po skartačním řízení případně schopen přijmout archiv.

Tomu odpovídá i § 23 odst. 1 vyhl. č. 259/2012 Sb., dle které se jím má rozumět *„a) datový formát výstupu z elektronického systému spisové služby"*, což zjevně slouží výše uvedenému účelu, tj. pro výstup každého digitálního dokumentu ze stavu otevřeného spisu ve spisové službě do stavu uzavřeného spisu ve spisovně. Souhlasně s tím se jím rozumí i *„b) datový formát dokumentu ukládaného ve spisovně, která je součástí elektronického systému spisové služby"*. Je-li tedy elektronická spisovna součástí *elektronického systému spisové služby*, přesto má v rámci operace uzavření spisu dojít uvnitř daného systému ke změně do výstupního datového formátu. Konečně se jím rozumí i *„c) datový formát pro předávání do digitálního archivu"*, k čemuž dochází po uplynutí skartační doby.

---

[32] Stanovisko NS Plsn 1/2015, s. 9 (bod 26.).
[33] Stanovisko NS Plsn 1/2015, s. 10 (bod 28 písm. b).
[34] Stanovisko NS Plsn 1/2015, s. 3, odst. 9.

Jak je uvedeno výše, veřejnoprávní původce může fakultativně přijímat i jiné formáty elektronických dokumentů. Je skutečně možné, že pro účely některých odborných řízení mohou být vhodné jiné digitální formáty (např. dwg pro AutoCAD). Dokumenty v nich mohou být vedeny, dokud je spis (nebo vyřizovaný dokument) vedený v otevřeném stavu. Po uzavření dokumentu se i takový zvláštní formát musí převést na výstupní datový formát.

Odpověď na otázku, v jakém formátu mohou tedy veřejnoprávní původci odesílat jednotlivé dokumenty, se tedy řídí tím, jaké formáty digitálních dokumentů přijímají adresáti. Jsou-li adresáty veřejnoprávní původci, srov. výše 9.3.3. Je-li však náležitostí elektronického dokumentu i vůči nim elektronický podpis, pak se podle § 5 ZSVD musí jednat o QES (8.2.1) a podle § 11 musí být opatřen QTS (6.7.1). Ani ZSVD však nestanoví, v jakém formátu se má vytvořit elektronický podpis nebo v jakém má být elektronický dokument. Vzhledem k tomu, že dle čl. 27 odst. 5 eIDAS Komise vyhlásila formáty PAdES, CAdES a XAdES jako povinně uznávané, je smysluplné se uchýlit k jednomu z těchto formátů, ačkoli zde nejsou povinné. Jelikož pak soubory používané pro CAdES a XAdES nejsou mezi povinně přijímanými,[35] zbývají pouze formáty **PDF** nebo **PDF/A**, obsahující vnitřně QES a QTS ve formátu PAdES.

Existuje-li mezi konkrétními veřejnoprávními původci dohoda, pravděpodobně si mohou zasílat data nebo elektronické dokumenty i v jiných formátech. Zvláštní právní úprava může rovněž stanovit odlišně.

9.3.5 Přijímané formáty dokumentů soukromoprávnímu subjekty

Dle názoru autora v právním řádu ČR chybí obecná povinnost soukromoprávních subjektů, aby přijímaly elektronické dokumenty v jakémkoli určitém formátu. Stanovení této povinnosti zřejmě chybí i v rámci veřejnoprávních vrchnostenských vztahů.

Veřejné právo ČR obecně nestanoví povinnost soukromoprávních subjektů přijímat úkony úřadů nebo orgánů veřejné moci v elektronické podobě. Výjimkou je ZEÚ, který přikazuje mnohým právnickým osobám a některým dalším subjektům povinné zřízení a zpřístupnění datové schránky. Souhlasně se ZEÚ byly poté upraveny různé procesní řády. Takovým subjektům se pak doručuje přednostně do jejich datové schránky, přičemž § 17 odst. 1 věta druhá ZEÚ obsahuje pouze jedinou podmínku,

[35] Formát XML je pouze pro databáze a metadata.

„umožňuje-li to povaha dokumentu". Jelikož ZEÚ nehovoří o tom, zda se povaha má chápat abstraktně, tj. bez ohledu na listinnou či elektronickou formu, lze se domnívat, že povahu dokumentu je třeba hodnotit i s ohledem na zvolitelný formát elektronického dokumentu. S odvolávkou na tuto podmínku by soukromoprávní subjekt zřejmě mohl namítat nedoručení, pokud by byl použit jakkoli nezvyklý formát elektronického dokumentu. Z výstupních formátů tak kromě PDF jsou obecně přijatelné zřejmě ještě PNG, JPEG a GIF, neboť tyto bývají zobrazitelné obecným prohlížečem internetových stránek, který je stejně nutný pro příjem datových zpráv přes obecné webové rozhraní datových schránek. Ostatní neuvedené formáty, zejména MP2, MP3, WAV, PCM a XML, již nelze považovat za univerzálně zpracovatelné a prezentovatelné.

Ze samotného charakteru příkazu doručování do datových schránek lze implikovat, že daní adresáti mají povinnost si zajistit do nich přístup, což zpravidla činí pořízením vlastní výpočetní techniky a přístupu k internetu. Lze stejně implikovat, že mají i povinnost si pořídit software na „čtení" těch formátů elektronických dokumentů, které jim orgány veřejné moci zasílají? Autor je názoru, že to implikovat *spíše nelze*.

Úřady a orgány veřejné moci naštěstí používají téměř výhradně formát PDF, pro který je k dispozici „zdarma" prohlížeč Adobe Reader. Tento prohlížeč je k dispozici pro dost výpočetních platforem (Windows od XP až 10, Mac OS 10, Android), od r. 2014 není však k dispozici např. pro Linux. Pro tento operační systém jsou aspoň zatím dostupné alternativní softwary, rovněž zdarma. Ve faktické rovině lze připustit, že pokud si již subjekt pořídil výpočetní prostředek, má možnost si nainstalovat i některý software „čtečky" PDF.

Další potíží ovšem je, že elektronické dokumenty pocházející od veřejnoprávních původců, mají být podle § 5 ZSVD podepsány pomocí QES a podle § 11 ZSVD opatřeny QTS. Formát podpisu v rámci PDF nebo PDF/A je zřejmě opět jediný použitelný. Jelikož pak žádný předpis právního řádu ČR nepředepisuje způsob ověření platnosti, je použitelný pouze obecný postup dle čl. 32 eIDAS (srov. 6.11.2), jehož výklad je pouze přibližný. Software Adobe Reader nebo jiné čtečky PDF nemusí ale nutně provádět ověření platnosti podle tohoto postupu ani se uživateli negarantuje, že se takový postup používá.[36]

[36] Například v produktu Adobe Acrobat Reader DC Verze 2018.009.20044 na Windows 10 se způsob ověřování nastavuje v: Úpravy – Předvolby – Podpisy – Digitální podpis – Ověření <Další..>

Autor se proto domnívá, že pokud soukromoprávní subjekty přijímají od veřejnoprávních podepisujících elektronické dokumenty, je to spíše záležitost jejich souhlasu, v zásadě soukromoprávní povahy, týkající se formátu dokumentu, formátu elektronického podpisu i vágního způsobu ověření platnosti elektronického podpisu. Výše uvedenými úvahami je zřejmě zdůvodnitelné přijímání formátu PDF, ale ani to není dle autora zcela právně samozřejmé.

9.3.6 Kryptografická schémata

V rámci eIDAS není obsaženo pověření pro stanovení kryptografických schémat, která se mají používat pro účel kvalifikovaných nebo zaručených elektronických podpisů. Nejsou proto stanoveny ani žádným prováděcím aktem eIDAS. Pověření neobsahuje ani ZSVD pro právní řád ČR. V něm tedy nyní nejsou nijak právně výslovně stanovena kryptografická schémata.

Požadavky na teoretické vlastnosti kryptografických schémat sice lze v principu vyvodit z obecných požadavků např. na QSCD v eIDAS, prakticky ale takové vývody budou diskutabilní (srov. 8.8.1). Kromě jejich kryptologických vlasností je především třeba se vzájemně sjednotit na společném užívání. V ČR nyní budou užívaná kryptografická schémata dána zejména tím, jaká budou použita v kvalifikovaných certifikátech, vydávaných kvalifikovanými poskytovateli služeb vytvářejících důvěru, jejichž postupy jsou ověřené auditními zprávami a orgánem dohledu. Nařízení eIDAS ale přikazuje i přeshraniční uznávání QES s kvalifikovanými certifikáty vydanými v jiných členských státech. Právně vzniklá situace neposkytuje dobrou právní jistotu, že všude v EU budou používána vhodná kryptografická schémata, ani obranu proti tomu.

9.3.7 Technické možnosti podání

Pro podání v elektronické podobě vůči správním úřadům si lze představit nejméně šest jeho skutkových provedení:

1. Sken listinné podoby (vč. vlastnoručního podpisu) zaslaný elektronickou poštou (bez uznávaného elektronického podpisu).
2. Zpráva elektronické pošty (bez uznávaného elektronického podpisu).
3. Elektronický dokument zaslaný elektronickou poštou (bez uznávaného elektronického podpisu).
4. Elektronický dokument zaslaný přes ISDS (bez uznávaného elektronického podpisu) oprávněnou osobou.

5. Elektronický dokument podepsaný uznávaným elektronickým podpisem, zaslaný přes ISDS.
6. Elektronický dokument podepsaný uznávaným elektronickým podpisem, zaslaný elektronickou poštou.

Níže budeme hodnotit, jaká provedení jsou právně možná v různých řízeních.

9.3.8 Správní řád (podání vůči správnímu úřadu)

Dle první věty § 37 odst. 4 spr. řádu[37] *„Podání je možno učinit písemně nebo ústně do protokolu anebo v elektronické podobě."* Původní znění (od přijetí zákona do 30. 6. 2012) závěru této věty přitom bylo: *„... anebo v elektronické podobě podepsané zaručeným elektronickým podpisem."* Od 1. 7. 2012 do 18. 9. 2016 pak bylo účinné toto znění závěru věty: *„... anebo v elektronické podobě podepsané uznávaným elektronickým podpisem."* Ustanovení této věty nikdy nebylo a ani nyní není ideální, neboť se nedrží v právní teorii ČR používané terminologie, v níž *písemnost* je technologicky neutrální pojem, který může být splněn podobou listinnou i elektronickou. V tomto správném smyslu používá pojem *písemnost* § 19 odst. 1 spr. řádu, ovšem pro případ doručování. Slovo *písemně* v § 37 odst. 4 spr. řádu znamená dle autora *„písemně v listinné podobě"* a obrat *v elektronické podobě* znamená dle autora *„písemně v elektronické podobě"*. V dřívějších zněních (do 18. 9. 2016) byla tato dichotomie zcela markantní.[38]

Optimálně formulované není ani vznesení požadavku na přítomnost podpisu na podání. Ten plyne především z poslední věty § 37 odst. 2 spr. řádu, dle níž *„Podání ... musí obsahovat podpis osoby, která jej činí."* Jen z tohoto ustanovení však nelze dovozovat, zda a jak se požadavek podpisu vztahuje na výše zmíněnou elektronickou podobu. Tento požadavek dříve (do 18. 9. 2016) plynul ze závěru výše citované první věty § 37 odst. 4 spr. řádu, a to na zaručený nebo uznávaný elektronický podpis. Jelikož nyní v § 37 spr. řádu není nikde výslovně uveden požadavek na elektronický podpis, např. u zmíněné elektronické podoby, není možné možné hladce aplikovat § 6 odst. 1 ZSVD ohledně *„podepisování elektronickým podpisem"*. To je paradoxní výsledek přijetí ZSVD a jeho doprovodného změnového zákona č. 298/2016 Sb.[Chyba: zdroj odkazu nenalezen]

[37] Zákon č. 500/2004 Sb. ve znění pozdějších předpisů. Autor uvádí znění účinné od 1. 7. 2017.

[38] Vypuštění slov závěru věty: *„podepsané uznávaným elektronickým podpisem"* je obsažené v čl. XLV změnového zákona č. 298/2016 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce...

V druhé větě § 37 odst. 4 spr. řádu je však nyní uvedeno, že podání je možné učinit i pomocí *„jiných technických prostředků, zejména prostřednictvím ... veřejné datové sítě bez použití podpisu"*. Nepoužití podpisu v rámci těchto prostředků však má za následek, dle stejné věty, nutnost podání do 5 dnů „potvrdit" způsobem podle věty první § 37 odst. 4 spr. řádu, výše citované. Z toho zřejmě lze dovodit, že podpis je náležitostí všech citovaných způsobů, tj. i podání v elektronické podobě. Z podstaty podoby podání pak lze dovodit, že elektronickou podobu podání bude třeba potvrdit elektronickou podobou podpisu, tj. elektronickým podpisem. Následně již lze použít § 6 odst. 1 ZSVD, tj. dovodit, že pro podání se musí použít uznávaný elektronický podpis ($AdES_{QC}$ anebo QES). Podání v provedení **6** je tedy platným podáním v elektronické podobě dle věty první § 37 odst. 4 spr. řádu.

Možnost podání provedením **4** pak běžně vyplývá z § 18 odst. 2 ZEÚ, kdy se uplatní fikce podání písemně (tj. listinné podoby) a fikce podepsání (tj. vlastnoručního podpisu), opět tedy dojde ke splnění podání podle věty první § 37 odst. 4 spr. řádu. Ústavní soud jasně vyslovil,[39] že provádí-li úkon osoba oprávněná dle výslovně určeného § 8 odst. 1 ZEÚ a soud její podání odmítne s odkazem na absenci elektronického podpisu, zasáhne pro extrémní rozpor s principy spravedlnosti, přepjatý formalismus a porušení práva na spravedlivý proces.[40] Dle autora se zde jedná o zřejmou nezákonnost a porušení principů právního státu, které Ústavní soud nezmínil zřejmě jen proto, že nebyly přímo namítány v dotyčné ústavní stížnosti.

Diskurs se v tomto případě vede ale ohledně toho, zda oprávněnými osobami jsou pouze osoby dle § 8 odst. 1 až 4 ZEÚ, nebo i osoby pověřené dle § 8 odst. 6 ZEÚ. Dle judikátu čj. 8 As 89/2011 se Nejvyšší správní soud vyslovil, že: „úkon učiněný prostřednictvím datové schránky osobou oprávněnou či osobou pověřenou, která doložila své pověření, má podle § 18 odst. 2 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, stejné účinky jako úkon učiněný písemně a podepsaný, proto nemusí být podepsaný elektronickým podpisem ve smyslu zákona č. 227/2000 Sb., o elektronickém podpisu, ani jej není třeba potvrzovat písemným podáním shodného obsahu či předložením jeho originálu dle § 37 odst. 2 věty druhé s. ř. s."[41] Judikát je citován i v novější judikatuře[42] z roku 2016. Uvedená judikatura by tedy znamenala, že pověřená osoba musí navíc *doložit své pověření k podání* –

[39] Nález Ústavního soudu sp. zn. II.ÚS 3042/14 ze dne 19. 1. 2016 (N 7/80 SbNU 81).
[40] Sp. zn. II.ÚS 3042/14, cit. dílo, body 38 až 39.
[41] Rozsudek Nejvyššího správního soudu ze dne 17. 2. 2012, čj. 8 As 89/2011 - 31.
[42] Rozsudek Nejvyššího správního soudu ze dne 29. 3. 2016, čj. 8 Afs 179/2015 - 47.

provedení úkonu. Pokud by se však vzalo za rozhodující stanovisko NS, pověření pověřené osoby vyplývá již z toho, že jí osobou oprávněnou § 8 odst. 1 až 4 ZEÚ byla přidělena možnost „posílat zprávy“,[43] pověření je tak možné implikovat a není nutné ho dokládat. Zmíněné judikáty se týkají podání ke správním soudům a stanovisko NS se týká podání k soudům obecně, nikoli tedy podání ve správním řízení. Vyšší soudy, zejména Ústavní soud, mají tendence ochraňovat osoby, činící úkony pomocí datových schránek.

Provedení **1**, **2** a **3** bude třeba považovat za podání v elektronické podobě, ovšem bez uznávaného elektronického podpisu. Je tedy třeba ve smyslu druhé věty § 37 odst. 4 spr. řádu je potvrdit do pěti dnů podáním stejného znění, a to buď písemně v listinné podobě s vlastnoručním podpisem, v provedení **4** nebo **6**, ev. ústně do protokolu.

Podání **5**, je-li elektronický dokument podepsán uznávaným elektronickým podpisem stejné osoby, jakou je osoba přistupující do datové schránky odesilatele, nečiní potíže. Lze je shodně uznat jako podání provedením **4** nebo jako podání provedením **6**.

Potíže mohou vyvstat ve dvou případech. První možná potíž vyvstává u podání provedením **5**, pokud se liší osoba elektronicky podepsaná od osoby, která do datové schránky měla přístup a datovou zprávu podala a odeslala. Zde se autor jednoznačně přiklání k řešení použitému ve stanovisku NS jako právní věta III. pro podání[44] soudům, tj. poukázat na to, že fikce podpisu se neuplatní, je-li již podání uznávaným elektronickým podpisem opatřeno. Dle autora je dále vhodné vzít v potaz, že ISDS jako systém má charakter spíše komunikační, tj. služby pro přenos datové zprávy, než jako univerzálně použitelný nástroj, který by autentizoval původce (podepisující osobu) jakékoli možné listiny. Do datových zpráv ISDS budou navíc nutně příležitostně přikládány dokumenty listin i jiných původců, než je subjekt, pro který byla datová schránka zřízena. Nemá smysl zbavovat tyto listiny v elektronické podobě jejich důkazního účinku nebo jiných právních vlastností jen z toho důvodu, že jsou přepravovány pomocí ISDS. Právní fikce dle § 18 odst. 2 ZEÚ by měla mít charakter spíše pomocný, jako usnadňující a úsporný nástroj u těch subjektů, kteří si prostředky pro vytváření uznávaného elektronického podpisu nechtějí pořizovat.

[43] Stanovisko NS Plsn 1/2015, odst. 43, odůvodnění právní věty IV., s. 15.
[44] Stanovisko NS Plsn 1/2015, právní věta III. a její odůvodnění, s. 13–14.

Druhou potíží je provedení **4**, provedené z datové schránky (právnické) osoby, která má zpřístupněno více osob oprávněných k přístupu do této datové schránky, včetně ev. tzv. osob pověřených, přičemž příjemci není zřejmé, která z nich podání provedla, má k dispozici pouze údaj o „odesílající" datové schránce. Dle autora zde z platného práva ani z existující judikatury není způsob řešení nijak zvlášť jasný nebo jednoznačný. Je pochopitelně možné řešení ve smyslu stanoviska NS, probírané níže (srov. 9.3.9).

Souhrnně lze uzavřít, že úkon podání v elektronické podobě ve správním řízení je běžně optimální provádět včetně použití uznávaného elektronického podpisu a pro přepravu použít ISDS. Důvodem je, že úřady zvyklé na přítomnost aspoň nějakého „podpisu" příležitostně zamítají podání, které jím není vybaveno, zatímco podání s uznávaným podpisem přijímají prakticky vždy. Opatření elektronickým podpisem též pomůže vyřešit situace, pokud by došlo k nesouladu mezi osobou, která podání chce učinit, a parametry datové schránky, která byla použita pro provedení podání.

Použití ISDS pak poskytuje výhodu jistoty dodání co do adresáta i času. Časem podání je podle již ustáleného výkladu okamžik dodání do datové schránky adresovaného úřadu.[45] To může nastat nejvýše v řádově desítkách minut od podání. Je lhostejné, kdy se do této datové schránky adresáta poté přihlásí úředník nebo jeho systém spisové služby, který dodané zprávy vybírá automaticky. Oproti tomu při dodání na elektronickou adresu internetové pošty pošty záleží na skutečném provozu systému elektronické podatelny, kdy a jak potvrdí příjem internetové poštovní zprávy. Existují úřady, které potvrzují přijetí prakticky okamžitě, zatímco jiní adresáti vybírají poštu až ráno před pracovní dobou.

9.3.9 Občanský soudní řád (podání vůči soudu)

Podle § 42 odst. 1 občanského soudního řádu (o. s. ř.[46]) je možné podat písemné podání. Toto písemné podání se zde činí třemi způsoby, a to sice v *„listinné nebo elektronické podobě prostřednictvím veřejné datové sítě nebo telefaxem"*.

V § 42 odst. 4 o. s. ř. jsou stanoveny obecné náležitosti podání, včetně toho, že *„musí být podepsáno a datováno"*. To se snadno provede pro první způsob, tj. pro

[45] Rozsudek Nejvyššího správního soudu ze dne 15. 7. 2010, 9 Afs 28/2010 – 79.
POLČÁK, R. Okamžik doručení do datové schránky. *Revue pro právo a technologie*. 2010, roč. 1, č. 2, s. 22–24.

[46] Zákon č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů. Autor uvádí znění účinné v 11/2017.

listinnou podobu.

Podle druhé věty § 42 odst. 4 o. s. ř. ale *„povinnost podpisu a datování se nevztahuje na podání v elektronické podobě podle zvláštního právního předpisu"*. Takové podání v elektronické podobě vůči soudu upravuje zřejmě jediný zvláštní předpis, a to sice ZEÚ (zák č. 300/2008 Sb.[47]), který je též zde zmíněn v poznámce pod čarou. Podle § 18 odst. 2[48] ZEÚ: *„Úkon učiněný ... prostřednictvím datové schránky má stejné účinky jako úkon učiněný písemně a podepsaný ... "* Dikce *písemně* a *podepsaný* je přizpůsobena správnímu řádu, i v kontextu občanského soudního řádu by ale dle autora měla znamenat listinnou podobu a vlastnoruční podpis (srov. výklady I, II a III v 9.3.2.1). Výše citovaná druhá věta § 42 odst. 4 o. s. ř. zbavuje takové podání i povinnosti datování, neboť čas podání bude patrný z ISDS. Uvedená úprava pokrývá provedení **4** a případně **5**.

Podle § 42 odst. 2 o. s. ř. *„Písemné podání obsahující návrh ve věci samé učiněné ... v elektronické podobě je třeba nejpozději do 3 dnů doplnit předložením jeho originálu, případně písemným podáním shodného znění."* Předložení *originálu* připadá do úvahy v případě provedení **1** (sken listiny s podpisem), popř. dříve též u telefaxu. Obrat *písemným podáním* zde zřejmě míří na způsob podání v listinné podobě s vlastnoručním podpisem. Například provedení **2** a **3** je možné vytisknout, vlastnoručně podepsat a podat.

Podle § 42 odst. 3 o. s. ř. platí: *„V případě podání v elektronické podobě podepsaného způsobem, se kterým zvláštní právní předpis spojuje účinky vlastnoručního podpisu, se nevyžaduje doplnění podání předložením jeho originálu podle odstavce 2."* Zde je použit výše probíraný obrat *účinky vlastnoručního podpisu* (srov. 9.1.2), včetně pozn. pod čarou s odkazem jednak na § 18 odst. 2 zákona č. 300/2008 Sb. a jednak na § 6 odst. 1 ZSVD. Jak již je uvedeno výše, § 18 odst. 2 ZEÚ finguje účinky podpisu, ale i písemného podání. Jeho použití se zdá přijatelné a opět řeší provedení **4** a **5**. Použití § 6 odst. 1 ZSVD je značně problematičtější (srov. 9.1.2), ale tolerantně je vykládáme jako připuštění podpisů $AdES_{QC}$ nebo QES, a řeší provedení **6** i **5**. Jak je vidno, nalezli jsme řešení všech šesti provedení podání v elektronické podobě, v některých případech i vícenásobné. Stejně jako výše ve

[47] Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů. Autor uvádí znění účinné v 11/2017.

[48] Nadpis § 18 je „Provádění úkonů vůči orgánům veřejné moci prostřednictvím datové schránky".

správním řízení, je i v případě občanského soudního řádu nutné provedení **1**, **2** a **3** podat dodatečně znovu.

Stanovisko NS považuje podání dle § 42 odst. 2 o. s. ř. za *podání ve věci samé*, tj. takové, kterými se „disponuje řízením (žaloba, její zpětvzetí či změna, odvolání, dovolání apod.)“.[49] Tato podání lze učinit dle stanoviska v elektronické podobě bez potřeby jejich doplnění, pokud byla učiněna prostřednictvím datových schránek nebo podepsána uznávaným elektronickým podpisem.[50] Za doplnění podání *„předložením jeho originálu, případně písemným podáním shodného znění"* stanovisko NS považuje podání v listinné podobě podepsané vlastnoručním podpisem (ev. i úředně ověřeným, pokud se to vyžaduje) anebo „doručení originálu nebo písemného podání shodného znění v elektronické podobě s uznávaným elektronickým podpisem nebo prostřednictvím ISDS“.[51]

Ostatní podání než podle čl. § 42 odst. 2 o. s. ř. označuje stanovisko NS za *jiná podání.* Tato jiná podání lze podle stanoviska NS učinit v elektronické podobě bez potřeby jejich doplnění, i když nebyla učiněna prostřednictvím ISDS ani podepsána uznávaným elektronickým podpisem.[52]

V praxi může vzniknou otázka, jak z pohledu práva hodnotit podání, které je učiněno pomocí datové schránky a současně opatřeno elektronickým podpisem. Zejména kritickou pak bude situace *odlišné totožnosti odesilatele a podepsané osoby*. Stanovisko situaci řeší tak, že v případě, když podání v elektronické podobě je podepsáno uznávaným elektronickým podpisem, pak i když bylo učiněno prostřednictvím datové schránky, nepoužije se tzv. fikce podpisu podle § 18 odst. 2 ZEÚ.[53] Toto pravidlo řeší i možnou situaci kolize. Za osobu činící podání bude považována osoba podepsaná uznávaným elektronickým podpisem. Důvodem je mj. i to, že pokud je podpis obsažen, byť elektronický, nemá smysl uplatňovat jeho zákonnou fikci.

Pokud však podání bude podepsáno nižší úrovní elektronického podpisu, než je uznávaný elektronický podpis, stanovisko stále považuje podání za učiněné danou podepsanou osobou, ovšem nyní se již jedná o podání v elektronické podobě, které

[49] Stanovisko NS Plsn 1/2015, s. 8.
[50] Stanovisko NS Plsn 1/2015, s. 8.
[51] Stanovisko NS Plsn 1/2015, s. 8.
[52] Stanovisko NS Plsn 1/2015, s. 8.
[53] Stanovisko NS Plsn 1/2015, s. 13 (právní věta III.), s. 13–14 (odst. 38.–39.).

nesplňuje požadavky § 42 odst. 2 a 3 o. s. ř., a proto musí být doplněno ve lhůtě 3 dnů výše uvedeným způsobem. Za příklad takového podání je uveden obyčejný sken podání, na kterém je uveden vlastnoruční podpis jiné osoby, než z jejíž datové schránky byl odeslán (např. z datové schránky advokáta).[54]

9.3.9.1 Podání datovou schránkou právnické osoby

Stanovisko NS řeší navíc ještě jednu zvláštní situaci, která vzniká v případě procesních úkonů právnických osob. Za právnickou osobu jedná (zastupuje) dle čl. 21 odst. 1 písm. a) o. s. ř. v jedné věci zásadně pouze jeden *„člen statutárního orgánu"* (srov. závěr části 10.1), což má v řízení napomáhat prosazení teorie projevu vůle, tedy zásady, že každý procesní úkon je „nutno posuzovat podle toho, jak byl navenek projeven" a ani podstatný omyl jednajícího nepovede k jinému posouzení jednání.[55] Jednání jedinou osobou pak napomáhá tomu, aby nedocházelo k rozporům ve vyjádření různých osob. Jelikož však „z informací v datové zprávě přitom nevyplývá, která konkrétní fyzická osoba učinila daný procesní úkon prostřednictvím datové schránky",[56] přijímající soudy nejsou schopny kontrolovat, zda úkon provedl potřebný člen statutárního orgánu.

Stanovisko NS však vychází této procesní potřebě a současně použitelnosti ISDS vstříc druhou právní větou IV: „Je-li osobou, pro kterou byla zřízena datová schránka, právnická osoba, má ... procesní úkon učiněný prostřednictvím datové schránky stejné účinky jako procesní úkon, který za právnickou osobu písemně učiní a podepíše osoba oprávněná jednat za právnickou osobu podle příslušného procesního předpisu."[57]

Uvedené znamená, že procesní úkon vůči soudu může provést kterákoli z osob, která má přístup do datové schránky právnické osoby. Dle citované právní věty bude písemnost projevu a podpisu přičtena právě té osobě, která je za právnickou osobu oprávněná jednat. To se uplatní i v případě, že úkon odeslala pověřená osoba dle § 8 odst. 6 ZEÚ. Stanovisko NS je zde názoru, že „je ... na oprávněné osobě, které byla zřízena datová schránka, aby při nastavení tohoto pověření vzala v úvahu důsledky, jež s sebou pro ni nese (vzhledem k ‚fikci podpisu') postup pověřené osoby plynoucí z ustanovení § 18 odst. 2 zákona o elektronických úkonech". Autor na jednu stranu chápe, že vstřícnost je žádoucí, aby nedocházelo k odmítání procesních podání, trpících

[54] Stanovisko NS Plsn 1/2015, s. 14, odst. 41.
[55] Stanovisko NS Plsn 1/2015, s. 17, odst. 53.
[56] Stanovisko NS Plsn 1/2015, s. 16, odst. 49.
[57] Stanovisko NS Plsn 1/2015, s. 14 (právní věty IV.).

jen malou vadou. Na druhé straně se autor domnívá, že pověření podle § 8 odst. 6 ZEÚ bude často právnickou osobou udělováno pro potřebu běžné komunikace se správními úřady svým zaměstnancům, zatímco komunikace v občanském soudním řízení může chtít být ponechána v pravomoci statutárního orgánu atp.

Dle první věty IV. stanoviska NS se však obecně úkon a podpis přičítá té osobě, „pro kterou byla zřízena datová schránka", a nikoli té osobě, která se přihlásila do datové schránky. Vhodná reakce na toto právní posuzování by měla vést k opatrnosti při pověřování osob dle § 8 odst. 6 ZEÚ, což ale paradoxně způsobí, že o to méně se bude ISDS používat.

Uvedených potíží s fikcemi podpisu se lze též, byť jen částečně, zbavit tím, že se každé podání elektronicky podepisuje. Fikce se pak neuplatní.

9.3.10 Veřejnoprávní podání – souhrn

Výše uvedené odstavce dokládají, že ačkoli veřejné právo zjevně využívání elektronických dokumentů a jejich elektronických podpisů předpokládá a ačkoli se někdy mohou těšit i presumpci správnosti veřejných listin stejně jako listinná (papírová) podoba, je v právním řádu ČR úprava jejich používání a nakládání s nimi v mnoha ohledech nedotažena, nebo se přinejmenším jeví nejasná.

Nejsou najisto stanoveny formáty elektronických dokumentů, které se mají používat, nejsou stanoveny nebo jednoznačně recipovány formáty zaručených elektronických podpisů z nařízení eIDAS, není jednoznačně stanoven ani plně recipován z nařízení eIDAS postup ověřování a potvrzování platnosti elektronických podpisů. Není ani jasně stanoveno, kdy vždy se mají elektronické podpisy ověřovat, zda a jak se má podporovat dlouhodobé zachování ověřitelnosti platnosti elektronického podpisu jednotlivých dokumentů. Nejsou jednoznačně stanovena kryptografická schémata schopná zajistit potřebné vlastnosti kvalifikovaných elektronických podpisů.

Oblast elektronizace spisů a jejich následné archivace je stále pouze ve vývoji a není zřejmé, zda skutečně používané technické postupy zajišťují celkovou bezpečnost a autenticitu digitálních dokumentů ve stejné úrovni, jako tomu dříve bývalo v případě tradičních papírových dokumentů. Právě tato úroveň bezpečnosti a autenticity záznamů však zřejmě stojí za presumpcí správnosti veřejných listin.

9.4 Soukromé právní jednání s elektronickým podpisem

V kapitole věnované teorii (srov. 5.1) již byly vyjádřeny obecné předpoklady, za nichž je možné provést soukromé elektronické právní jednání v ČR.

Podepisování v oblasti soukromého práva je upraveno v § 7 ZSVD. Dle něj *„podepisuje-li se elektronický dokument, kterým se právně jedná jiným způsobem než způsobem uvedeným v § 5 nebo § 6 odst. 1."*, pak *„k podepisování elektronickým podpisem lze použít zaručený elektronický podpis, uznávaný elektronický podpis, případně jiný typ elektronického podpisu."* Uvedené právní jednání jiným způsobem zahrnuje soukromé právní jednání. Oproti tomu uvedený jiný typ elektronického podpisu zahrnuje i elektronický podpis prostý z eIDAS.

K této situace se autor již vyjádřil,[58] a to zejména v závěru článku.[59] Autor považuje připuštění elektronického podpisu prostého pro platné právní jednání v písemné formě za určité ohrožení osob, které takto budou jednat, neboť pro elektronický podpis vyhovují prakticky všechny druhy techniky (srov. 4.5) elektronických podpisů, tedy i tzv. *click-wrap* podpis. Jak autor výše uvádí, některé výklady § 561 a § 562 obč. zák. (srov. 5.1.5) sice představují určitou možnost námitek proti právě uvedenému připuštění pouze elektronického podpisu prostého z eIDAS, v praxi však bude zatím převládat výklad druhý, dle kterého elektronický podpis prostý recepcí v ZSVD z eIDAS možný je. Jediná ochrana takto údajně podepsané osoby již spočívá pouze v nemožnosti důkazního použití většiny druhů techniky (srov. 4.5), neboť nemají ani autentizační (pravostní) funkci. Takový důkaz autenticity musí být zajištěn něčím dalším, než je pouze samostatný elektronický podpis.[60]

Dovolení elektronického podpisu prostého pro splnění písemné formy právního jednání se nezdá vhodné ani s ohledem na třetí osoby, pokud vůči nim má být dané právní jednání dokladováno v rámci běžného právního styku při realizaci práva.

Pro další diskurs tématu v tomto textu viz též části 5.1.3, 5.1.5 a 6.4.

9.4.1 Důkazní účinek QES, ev. $AdES_{QC}$, v soukromém právu

Jak je uvedeno již výše, autor je názoru, že nařízení eIDAS nestanoví důkazní účinek pro jím upravené druhy elektronických podpisů, a to ani pro QES dle čl. 25 odst.

[58] KMENT, V. Nahradí elektronický podpis prostý ten tradiční vlastnoruční? *Bulletin advokacie*. 2016, č. 12, s. 31–35.
[59] KMENT, V. Nahradí ..., cit. dílo, s. 35.
[60] KMENT, V. Nahradí ..., cit. dílo, s. 34–35.

2 eIDAS. Tento názor vyslovoval již ihned po publikaci nařízení v září 2014.[61] V tomto textu je doložen stejný výsledek jednak podrobným výkladem nařízení eIDAS (např. 6.15.6 a 6.15.12), jednak stejného názoru je RoßnagelChyba: zdroj odkazu nenalezen (7.1.1) a nakonec i německý zákonodárce při své implementaci nařízení (srov. 7.4). Jelikož ZSVD důkazní účinky neupravil, jsou elektronické dokumenty s podpisem QES zřejmě ve všech druzích řízení v českém právním řádu ponechány v režimu volného hodnocení důkazů. Tyto důkazní účinky jsou částečně již probírány výše v 8.7.

V analýze nařízení eIDAS výše je uvedeno, že neupravuje řadu náležitostí (6.16), které by bylo vhodné mít upraveno. Tyto náležitosti nejsou upraveny ani v ZSVD (srov. 8.8 a 8.9). Ve druhé větě § 565 obč. zák. je zakotvena právní domněnka: *„Je-li soukromá listina použita proti osobě, která listinu zjevně podepsala, … má se za to, že pravost a správnost listiny byla uznána.“*

Tato právní domněnka vyžaduje hlubší analýzu[62] a dle autora se hodí zejména pro případ tradičních papírových listin a vlastnoručních podpisů. Je diskutabilní, zda je uplatnitelná pro případy elektronických listin s elektronickým podpisem. Autor by ji v žádném případě neuplatnil pro ty elektronické podpisy prosté, které nemají autentizační funkci.

I v případě elektronických podpisů QES by autor spíše než touto právní domněnkou situaci hodnotil pomocí tzv. skutkových domněnek.[63] Skutkové domněnky jsou podle Macura zkušenostní věty,[64] které jsou založeny na běžném průběhu nebo souvislosti mezi jevy, kdy z jednoho prokazatelného jevu lze běžně usuzovat na druhý. Dle Macura skutkové domněnky naprosto nejsou v rozporu s volným hodnocením důkazů, ale je tomu přesně naopak. Slouží k tomu, aby posuzování skutkových otázek nebylo u soudce otázkou libovůle,[65] ale aby se s nimi vypořádával systematicky. Právní domněnka není podle Macura nic jiného než zkušenostní domněnka povýšená na zákon. Právně pak rozdíl mezi nimi spočívá v tom, že právní domněnku je nutné vyvrátit důkazem opaku, zatímco pro vyvrácení zkušenostní domněnky dostačuje jen podstatné zpochybnění.[66]

---

[61] KMENT, V. Evropské ..., cit. dílo, s. 34–35.
[62] Autor má takovou analýzu rozpracovánu, ale vzhledem k rozsahu textu zde pro ni není prostor.
[63] MACUR, J. Právní a skutkové domněnky při dokazování listinou v civilním soudním řízení. *Právní rozhledy*. 2001, č. 2, s. 60–64.
[64] Dle Macura mezi pojmy *zkušenostní věta* a *skutková domněnka* není kvalitativní rozdíl. In MACUR, J. Právní ..., cit. dílo, s. 63.
[65] MACUR, J. Právní ..., cit. dílo, s. 64.
[66] MACUR, J. Právní ..., cit. dílo, s. 63–64.

Dle autora lze na základě kladného ověření platnosti QES dle čl. 32 eIDAS použít skutkovou domněnku, že (i) se jedná o podpis pravý. Z pravosti podpisu pak lze použít další jednotlivé skutkové domněnky, že (ii) původcem podepsaných dat (elektronického dokumentu) je podepsaná osoba,[67] že (iii) podepsaná data jsou úplná a neporušená, že obsah podepsaných dat (elektronického dokumentu) buď (iv) vyjadřuje vůli podepsané osoby, nebo že (v) jimi podepsaná osoba ověřila pravdivost podepsaného obsahu v datech (elektronickém dokumentu). Domněnka (ii) bývá někdy označována jako původnost či pravost, popř. autenticita listiny, domněnky (iv) a (v) jako správnost či pravdivost, domněnka (iii) jako neporušenost či integrita.

Domněnku (ii) kupř. stanovil německý zákonodárce v § 371a odst. 1 ZPO (srov. 7.4) jako důkaz *prima facie*. Domněnky (iii) nebo (iv) se běžně užívají např. v německém právu jako tzv. důkazní pravidla *(Beweisregeln)*, byť zde se Macur vyjadřuje o tradičních papírových listinách.[68]

Důvodem pro výše uvedené skutkové domněnky autorovi je i to, vedle statistické četnosti, že podpisy jako QES představují z bezpečnostního hlediska vrchol toho, jak ještě běžně elektronicky právně jednající osoba může zabezpečit původnost svého vyjádření v elektronických dat (elektronickém dokumentu). Jestliže by neměly být přiznávány výše uvedené skutkové domněnky podpisům QES, tím spíše nelze považovat za důkazně přesvědčivé elektronické záznamy z mnoha jiných elektronických systémů.

Na druhé straně v tomto textu výše se nachází mnoho upozornění, že právní rámec nařízení eIDAS ani jeho implementace v ZSVD nepokrývá mnoho záležitostí, které usnadňují vznik pochyb o správnosti výše uvedených skutkových domněnek. Tyto pochyby by však neměly být vznášeny jen jako obecně možné, ale měly by být zkoumány v jednotlivých případech jako skutkové otázky samostatně s tím, že by měla být uplatněna vysvětlovací povinnost důkazním břemenem nezatížené strany v maximální možné míře. Možnost vyvrácení každé domněnky je třeba hodnotit s ohledem na konkrétní okolnosti případu.

V zásadě podobné skutkové domněnky by měly platit i v případě podpisu $AdES_{QC}$ s tím, že některé vnitřní předpoklady skutkových domněnek zde zřejmě budou vyvratitelné průměrně snadněji.

---

[67] Tj. osoba uvedená v kvalifikovaném certifikátu, na němž je QES založen.
[68] MACUR, J. Právní ..., cit. dílo, s. 62.

K důkaznímu účinku dalších digitálních objektů z eIDAS již výše v 8.7 a 6.15.

10. Elektronické právní jednání právnických osob (ČR)

Text obsahově završíme touto kapitolou o elektronickém právním jednání právnických osob, zejména podle právního řádu ČR, přičemž se soustředíme na soukromé právní jednání a na to, jak při něm lze případně využít digitální objekty nebo služby vytvářející důvěru, upravené v nařízení eIDAS.

10.1 Jednání za právnickou osobu zástupci (fyzickými osobami)

I v případě, že právní nauka určitého právního řádu vyznává teorii reality, je zásadně zapotřebí, aby právnická osoba právně jednala prostřednictvím fyzických osob, a to právně stanoveným způsobem. Tím spíše to platí tehdy, když právní úprava a následně i teorie spíše vychází z teorie fikce, jak tomu je, aspoň při prvním přiblížení k textu občanského zákoníku, nyní v ČR. Je třeba fyzických osob jako zástupců právnické osoby.

Podle § 161 obč. zák. o jednání za právnickou osobu: *„Kdo právnickou osobu zastupuje, dá najevo, co ho k tomu opravňuje, neplyne-li to již z okolností. Kdo za právnickou osobu podepisuje, připojí k jejímu názvu svůj podpis, popřípadě i údaj o své funkci nebo o svém pracovním zařazení."*

Jedná-li se o funkci ve vedení právnické osoby, spočívá zmíněné oprávnění jednak na abstraktním aktu, jednak na konkrétním ustavení fyzické osoby do funkce, předpokládané prvním abstraktním aktem. Abstraktním aktem bývá u právnických osob soukromého práva zakládací listina (nadace, ústav...), zakladatelská listina (jednočlenná obchodní korporace), společenská smlouva (obchodní korporace), stanovy (společenství vlastníků...), vzácněji pořízení pro případ smrti (nadace, ústav...). V případě právnických osob veřejného práva nese zpravidla označení statut. Uvedené abstraktní akty musí splňovat požadavky právního řádu, kterým se řídí i celý postup zakládání a vzniku právnické osoby. Občanský zákoník tento abstraktní akt označuje za zakladatelské právní jednání (§ 163 obč. zák.). Fyzické osoby se ustavují do funkce postupem, který abstraktní akt též stanoví a předpokládá. Orgán, jehož členové zastupují právnickou osobou navenek, se běžně nazývá statutární orgán, a to i v případě, že se pro něj používá zvláštní právní označení jako představenstvo, výbor aj. Podle § 163 obč. zák. *„Statutárnímu orgánu náleží veškerá působnost, kterou zakladatelské právní jednání, zákon nebo rozhodnutí orgánu veřejné moci nesvěří jinému orgánu právnické*

osoby." Současně platí, že člen statutárního orgánu může zastupovat právnickou osobu dle § 164 odst. 1 obč. zák. *„ve všech záležitostech"*.

Členové statutárního orgánu mohou právnickou osobu zastupovat kolektivně více členy současně, nebo ji může zastupovat každý jeho člen samostatně. Dle § 164 odst. 2 obč. zák.: *„Neurčí-li zakladatelské právní jednání, jak jeho členové právnickou osobu zastupují, činí tak každý člen samostatně."* Alternativně *(a contrario)* zakladatelské právní jednání tedy může stanovit společné jednání členů statutárního orgánu. Je-li to v určitém jednotlivém případě nepraktické, dovoluje § 164 odst. 2 obč. zák., že *„člen právnickou osobu [může] zastoupit jako zmocněnec samostatně, jen byl-li zmocněn k určitému právnímu jednání"*. Zmocnění se tedy musí týkat určitého právního jednání.

Pro právní jistotu třetích osob jsou zřízeny a vedeny veřejné rejstříky právnických osob, do kterých se dle § 120 odst. 1 obč. zák. pro právnickou osobou zapisuje i *„jméno a adresa bydliště nebo sídla každého člena statutárního orgánu spolu s uvedením způsobu, jakým tento orgán právnickou osobu zastupuje, a údajů o dni vzniku nebo zániku jejich funkce"*. Tento zápis ve veřejném rejstříku chrání třetí osobu nejen v otázce toho, zda vůči němu jedná správná fyzická osoba za právnickou osobu, ale i před vnitřními aj. vadami tvorby vůle právnické osoby. Podle § 162 obč. zák.: *„Zastupuje-li právnickou osobu člen jejího orgánu způsobem zapsaným do veřejného rejstříku, nelze namítat, že právnická osoba nepřijala potřebné usnesení, že usnesení bylo stiženo vadou, nebo že člen orgánu přijaté usnesení porušil."* Třetí osoba je tedy chráněna i v případě překročení vnitřního oprávnění členem statutárního orgánu, tzv. jednáním *ultra vires*. Uvedené se nemusí nutně uplatnit v případě, že třetí osoba si je překročení oprávnění nebo jiných zmíněných nedostatků vědoma, neboť tím může být porušena povinnost jednat poctivě dle § 6 odst. 1 obč. zák. a zákaz těžení ze svého nepoctivého činu dle § 6 odst. 2 obč. zák.

Druhým, odlišným způsobem zastupování za právnickou osobu dle výše citovaného § 161 obč. zák. je případ, když je právnická osoba zastupována svými *zaměstnanci*, například prodavačem v prodejně. V tomto případě oprávnění spočívá v § 166 odst. 1 obč. zák., že *„Právnickou osobu zastupují její zaměstnanci v rozsahu obvyklém vzhledem k jejich zařazení nebo funkci; přitom rozhoduje stav, jak se jeví veřejnosti."* Právním podkladem, který zaměstnance opravňuje za právnickou osobu jednat, je jeho zaměstanecký poměr, tj. typicky pracovní smlouva. Z hlediska třetích

osob je však nerozhodné, zda tento zaměstnanecký smluvní vztah řádně existuje, popř. zda není překročeno stanovené oprávnění zastupovat, v jeho rámci určené, pokud z toho, jak se jeví veřejnosti a co je obvyklé vzhledem k zařazení nebo funkci, se zastoupení jeví jako oprávněné. Výjimkou by obdobně jako výše byly situace, pokud třetí osoba o překročení oprávnění ví a došlo by tak k porušení povinnosti poctivosti.

Chce-li právnická osoba omezit nebo vymezit zástupčí oprávnění svých zaměstnanců, může tak učinit i svými vnitřními předpisy. Vůči třetí osobě však má účinky jen, *„muselo-li jí být [omezení zástupčího oprávnění z vnitřního předpisu] známo"* (§ 166 odst. 2 obč. zák.).

Občanský zákoník ještě připouští zastoupení právnické osoby *běžným členem* právnické osoby anebo *členem orgánu nezapsaného* do veřejného rejstříku. Pro tato zastoupení platí dle § 166 odst. 1 obč. zák. obdobně to, co je stanoveno o zastoupení právnické osoby zaměstnancem, tj. jak je již uvedeno výše.

Celkově lze platnou českou právní úpravu shrnout tak, že právnickou osobu zastupují především členové statutárního orgánu a zaměstnanci. Zatímco oprávnění a způsob jednání členů statutárního orgánu jsou navenek osvědčeny obsahem veřejného rejstříku, u zaměstnanců je pro rozsah zastoupení rozhodující zařazení nebo funkce a stav, jak se jeví veřejnosti.

Řidčeji mohou obdobně jako zaměstnanci zastupovat právnickou osobu i její běžní členové nebo členové orgánu nezapsaného do veřejného rejstříku, jehož činnost ale běžně bude upravena v zakladatelském právním jednání. Vymáhání nepřekročení zástupčího oprávnění právnickou osobou je záležitostí odpovědnosti soukromoprávní, ale případně i trestněprávní.

Odlišně je jednání právnické osoby stanoveno v *procesním právu*. Zákon č. 99/1963 Sb., občanský soudní řád, nebyl přeformulován z hlediska koncepce či terminologie zastupování a stále hovoří o jednání za právnickou osobu. Tento rozdíl terminologie však není podstatný. V uvedeném procesním řádu se především jedná o určitost právního jednání vůči soudu, které je dosaženo tím, že za právnickou osobu nakonec v téže věci jedná (zastupuje) současně vždy pouze jediná fyzická osoba (§ 21 odst. 5 o. s. ř.), a nikoli například dvě nebo tři, které by před soudem, nebo ve vyjádření vůči němu, hlasovaly o svém stanovisku nebo se vyjadřovaly navzájem odlišně a soud by musel vyhodnocovat i případné rozpory. Za právnickou osobu proto jedná

(zastupuje) podle čl. 21 odst. 1 písm. a) o. s. ř. jeden *„člen statutárního orgánu"*, běžně jím je *„předseda statutárního orgánu"*, ale může jím být i jiný *„člen, který tím byl pověřen"*. Je-li předsedou či pověřeným členem jiná právnická osoba, pak *„jedná vždy fyzická osoba, která je k tomu touto právnickou osobou zmocněna nebo jinak oprávněna"*. V § 21 odst. 1 o. s. ř. jsou uvedeny ještě další možnosti stanovení jednající fyzické osoby. Zájmy takové jednající fyzické osoby nesmí být v rozporu se zájmy právnické osoby, za kterou by měla jednat (§ 21 odst. 1 o. s. ř.). Oprávnění za právnickou osobu se musí soudu prokázat (§ 21 odst. 5 o. s. ř.).

Ve *správním řízení* se úprava jednání právnické osoby v § 30 odst. 1 spr. řádu (Úkony právnické osoby) blanketně odkazuje na úpravu v občanském soudním řádu: *„Jménem právnické osoby činí úkony ten, kdo je k tomu oprávněn v řízení před soudem podle zvláštního zákona"*, kterým je míněn právě občanský soudní řád. I pro správní řízení pak podle § 30 odst. 2 spr. řádu platí, že *„v téže věci může za právnickou osobu současně činit úkony jen jedna osoba"*.

Uvedené procesní úpravy občanského soudního řádu a správního řádu mají jako zvláštní zákon přednost před úpravou v zakladatelském právním jednání, které se tedy uplatní pouze hmotněprávně. Pro použití ISDS srov. též část 9.3.9.1.

10.2 Jednání (právnické osoby) elektronickým agentem

Již koncem 90. let se začaly vyskytovat elektronické systémy, které byly schopny určité obsluhy svých protějšků, jež by dříve spadala do obchodní komunikace mezi (obchodní) společností a jejím zákazníkem. V internetové praxi z nich vznikly zejména tzv. elektronické obchody (on-line shopy, e-shopy), v právní praxi se jim říkalo a dosud říká různě. V anglosaských zemích bývají zváni jako elektroničtí agenti, přičemž použitelná je například definice dle čl. 2 odst. 6 UETA[1], že *„**‚Elektronický agent'** znamená počítačový program nebo elektronický nebo jiný automatický prostředek použitý nezávisle pro úplné nebo částečné vyvolání akce nebo odpovědi na elektronické záznamy nebo činnosti, bez dohledu nebo činnosti jednotlivce."* V Německu je považovali za elektronický systém, převážně softwarové povahy *(Softwareprogramm)*, „který může pro uživatele vyřešit určité úlohy a přitom vykazovat znaky určitého stupně inteligence, které mu umožňují své úkoly řešit částečně autonomně a se svým prostředí smysluplným způsobem interagovat."[2] Takový

[1] *Uniform Electronic Transactions Act (1999),* cit. dílo. Zvýraznil autor.
[2] CORNELIUS, K. Vertragsabschluss durch autonome elektronische Agenten. *Multimedia und Recht*.

agent může mít různé vlastnosti reaktivity, proaktivity, činění vývodů (rozhodování) a komunikačních schopností.[3] Poté, co tyto systémy překročily pouhou hranici poskytování informací a začaly být využívány pro uzavírání smluv, právní nauka i praxe se pokoušely zjistit, jak jejich činnost právně popsat či zařadit.

Prvním zvažovaným právním vzorem bylo *zastoupení*. Elektronický agent by zde fungoval jako skutečný „agent", až na to, že by nedisponoval lidským substrátem. Od tohoto pojetí se muselo ustoupit,[4] neboť u zástupce se předpokládá vlastní vůle, kterou elektronický agent nedisponuje. Institut též předpokládá odpovědnost či ručení za překročení zástupčího oprávnění, kterých elektronický agent též není schopen.

Další možností bylo považovat je za *posla*. Zde by bylo výhodou, že poslíček nemusí být, dle německého práva, dokonce ani svéprávný, jím doručené vyjádření vůle svéprávného vystavitele bude platné a účinné. Právo zde však předpokládá, že poslíček nijak nemění obsah přenášeného vyjádření, což opět neodpovídá situaci.[5]

Nabídka každému (Angebot an jedermann, *ad incertas personas)* by byla analogií používanou u prodejních a služebních (např. čistič bot) automatů, při níž se využívá toho, že automat má v sobě vyjádření vůle předem hotové a uložené. Ani tato analogie však nevystihuje podstatně vyšší složitost elektronických agentů, kteří jsou schopni interakce s jiným okolím, zajišťováním zásob apod.[6] Další odlišností je, že agent je schopen úpravy nabídky na míru podle adresáta jednání, omezenému okruhu adresátů apod.[7]

Jednou z dalších možností, kvůli níž byla do tohoto textu informativně zařazena část o podmínkách právního jednání (2.2.3.1), by bylo považovat za právní jednání (vyjádření vůle) původní nastavení výpočetní techniky, v jehož rámci by veškeré její nastavení bylo považovatelné právě za podmínky právního jednání. Takový koncept by teoreticky možný byl. Pro právníky by však nebyl srozumitelný, protože kromě podmínek odkládacích a rozvazovacích by museli vstřebat různé smyčky a mnoho jiných abstraktních počítačových operací, systémů a modelů mnoha úrovní, které jsou

2002, roč. 8, č. 6, s. 353–358, s. 354.

3 CORNELIUS, K., cit. dílo, s. 353.

4 CORNELIUS, K., cit. dílo, s. 354.

5 CORNELIUS, K., cit. dílo, s. 355.

6 CORNELIUS, K., cit. dílo, s. 354.

7 DRENSKA, M. *Die rechtlichen Aspekte des elektronischen Handels in Bezug auf den Vertragsabschluss*. Dissertation. Augsburg: Juristischen Fakultät der Universität Augsburg, 2006, s. 16.

v zásadě předmětem zcela odlišné a samostatné lidské profese, totiž softwarového inženýrství. Koncept by byl obtížně vstřebatelný i ze strany protějšku, který by musel sám vyhodnotit, zda všechny podmínky (tj. počítačový program) jsou splněny, tj. zda právní jednání může nastat, zda nastává. Proto se za právní jednání považují až případná vlastní sdělení či interakce elektronického agenta, který již příslušné zadané podmínky, určené programátory, nastavením a nasazením, zpracoval a vydal. Takovému právnímu jednání se například říká *počítačové vyjádření (Computererklärung)*, čímž se naznačuje, že obsah takového jednání je zhruba takový, jako kdyby jej činila lidská osoba vyjádřením vůle *(Willenserklärung)*. To příjemci i umožňuje takové vyjádření hodnotit prakticky stejně, nemusí se přizpůsobovat vnitřním systémům, jazyku a metodám výpočetní techniky, resp. jen v malé míře.

Nauka i praxe pak dovodila, že takové vyjádření je právním jednáním *(Willenserklärung)* té osoby, která stojí na konci řetězce.[8] Jedná se přitom o tu osobu, která k nasazení, nastavení, ev. naprogramování elektronického agenta dala podnět, z jejíhož popudu a vůle se všechny uvedené činnosti provádí. Této osobě je pak jednání elektronického agenta přičítáno *(zurechnen)*.

Tak např. dle nedávného rozsudku BGH (2012): „Nikoli počítačový systém, nýbrž osoba, která jej využívá jako komunikační prostředek, poskytuje vyjádření [vůle]: obsah vyjádření se přitom neurčuje podle toho, jak jej automatický systém předpokládaně vykládá a zpracovává, ale podle toho, jak mu lidský adresát na základě dobré víry [nach Treu und Glauben] a zvyklostí provozu může rozumět."[9]

Ke stejnému závěru došlo dříve platné právo v ČR, když se v např. v § 3a odst. 2 ZEP stanovilo, že v případě označení elektronickou značkou o označující osobě platí právní domněnka: *„že tak učinila automatizovaně bez přímého ověření obsahu datové zprávy a vyjádřila tím svou vůli"*.

Nezávislou otázkou je, za co se má považovat jednání protějšku elektronického agenta. V případě běžných elektronických obchodů jím bývá uživatel webového rozhraní, které elektronický obchod poskytuje. Uživatel běžně postupuje klikáním na odkazy (hyperlinky), klikáním na tlačítka, vyplňováním formulářů. Drenska je názoru,

[8] HÄRTING, N., cit. dílo, s. 103.

[9] Rozsudek BGH z 16. 10. 2012 (*Online-Flugbuchung*), citace z MÜLLER-HENGSTENBERG, C. D., KIRN, S. Intelligente (Software-)Agenten: Eine neue Herausforderung unseres Rechtssystems – Rechtliche Konsequenzen der „Verselbstständigung" technischer Systeme. *Multimedia und Recht*. 2014, č. 5, s. 307–313, s. 308.

že v běžných případech se u něj bude jednat jen o šíření tohoto jednání, tj. o pouhé elektronické právní vyjádření[10] (srov. 5.2.1.1) spočívající v přenosu. Nevylučuje však, že uživatel též může používat na své straně složitější výpočetní systém, a pak i v jeho případě se může jednat o činnost prostřednictvím elektronického agenta, tj. i jeho systém bude poskytovat počítačové vyjádření.

Pro úplnost podotkněme, že při využití elektronického agenta může docházet k četným faktickým potížím, pochybením a omylům, ať na straně jeho provozovatele, anebo protějšího uživatele, které jsou právně důležité. Těmito právními otázkami se zde nezabýváme. Prakticky je pochopitelně vhodné takové případy co nejvíce vyloučit.

Chceme se ale zabývat tou otázkou, jak zjistit, *kdo je původcem, resp. osobou, která se za provozem elektronického agenta nachází,* případně *komu se jeho činnost má právně přičítat*. Elektronického agenta může nasadit a provozovat osoba fyzická i osoba právnická. Nás zde zajímá druhý případ. Výše uvedená analýza jednání právnické osoby podle českého právního řádu vyjevuje, že za právnickou osobu jednají zásadně její zástupci. Otázkou pro nás zde pak proto je, zda při jednání elektronického agenta za právnickou osobu dostačuje určit pouze to, o kterou právnickou osobu se jedná, nebo je třeba navíc určit i některou fyzickou osobu, která právnickou osobu zastupuje, ať již se jedná o člena či členy statutárního orgánu, nebo o zaměstnance.

Tuto odpověď by mělo poskytovat právo. Pro uvádění konkrétní fyzické osoby hovoří určitá praktičnost, popř. i možnost vyvozování individuální odpovědnosti.

Proti uvádění mohou existovat četné jiné důvody. Nasazení a provozování elektronického agenta za právnickou osobu je zřídkakdy předmětem činnosti jediné fyzické osoby, ale spíše spolupráce celé řady osob různých odborností a jednání, jejichž podíl na výsledku může být velmi různorodý. Na činnosti se mohou podílet programátoři, navrhovatelé logiky činnosti, grafického vzhledu různých součástí, autoři popisů položek a způsobu stanovení cen. Systém může být průběžně doplňován. V rámci systému může docházet i k dílčí komunikaci skutečných osob (chaty, fóra). Výsledná vnější činnost či projevy elektronického agenta jsou proto mnohem spíše výslednicí vnitřního rozhodnutí o obchodním vedení právnické osoby než jednáním jakéhokoli jednotlivého zástupce za společnost navenek. Zřejmě by bylo možné připisovat uzavřené obchody formálně určité fyzické osobě, ale stejně zřejmě by tato situace neodpovídala dobře realitě.

[10] DRENSKA, M., cit. dílo, s. 13.

Zákazník by pak mohl mít tendenci se obracet právě na danou uvedenou fyzickou osobu, která by se mohla stát beznadějně přetíženou, ačkoli má provozovatel v rámci elektronického agenta kupř. vytvořen systém obsluhy nebo podpory zákazníků, který je schopen bez potíží zákazníky kapacitně obsloužit.

Určení a zveřejňování takto určené fyzické osoby by vůči ní mohlo v rámci právnické osoby vést buď ke zvýhodnění, nebo naopak znevýhodnění. Právnická osoba má běžně zájem především obchodovat pod svým vlastním jménem a budovat si vztahy se zákazníky i dodavateli tak, aby fluktuace zaměstnanců nebyla důležitá a aby přetrvávaly vztahy i v případě, že dojde ke změnám členům statutárních orgánů. Čím více se jedná o společnost kapitálového charakteru, tím více je třeba upřednostňovat zájmy vlastníků, a nikoli například vytvářet z některých fyzických osob nenahraditelné formální provaděče právního jednání.

V rámci soukromoprávních vztahů se rovněž neuplatňuje veřejná moc, tzv. vrchnostenská, u níž je vhodné zajistit znalost o fyzické osobě, která ji skutečně provádí, aby byla kontrolovatelná.

10.3 Jednání právnické osoby provozující elektronický obchod

V této části se budeme zabývat tím, jak právnická osoba může jednat prostřednictvím elektronického agenta, kterým je jí provozovaný elektronický obchod.

10.3.1 Smlouvy distanční a se spotřebiteli v právu EU

Právem, které pokrývá odpověď na naši hlavní otázku, totiž zda je třeba uvádět fyzickou osobu zastupující právnickou osobu, anebo nikoli, je prvotně právo EU. Z práva EU jsou pak relevantní zejména legislativní akty týkající se ochrany spotřebitelů, distančního uzavírání smluv a provozu v prostředí e-commerce.

Právo EU se ochraně spotřebitelů věnuje již od roku 1985.[11] Předpisem, který již mj. reaguje na vznik internetu a zvýšené možnosti přeshraničního prodeje, je směrnice 97/7/ES[12] ze dne 20. května 1997 o ochraně spotřebitele v případě smluv uzavřených na dálku (9 stran textu ve věstníku). Zákonodárci postřehli, že *„zavádění nových*

[11] Směrnice 85/577/EHS ze dne 20. prosince 1985 o ochraně spotřebitele v případě smluv uzavřených mimo obchodní prostory.

[12] Směrnice Evropského parlamentu a Rady 97/7/ES ze dne 20. května 1997 o ochraně spotřebitele v případě smluv uzavřených na dálku, ve znění směrnice 2002/65/ES ze dne 23. září 2002, směrnice 2005/29/ES ze dne 11. května 2005 a směrnice 2007/64/ES ze dne 13. listopadu 2007; zrušena od 14. 6. 2014.

technologií zvyšuje počet způsobů, jakými mohou spotřebitelé získávat informace o nabídkách kdekoli ve Společenství a zadávat objednávky" (bod odůvodnění 4), byť automatizovaný internetový prodej tehdy ještě prakticky neexistoval. Příloha směrnice proto vůbec nezmiňuje webové aplikace, zato však uvádí videotext, teleshopping nebo telefon s lidskou účastí. Směrnice však tehdy již znala elektronickou poštu, která se již rozšiřovala právě z internetu. Dodavatel je kupř. povinen před uzavřením smlouvy poskytnout spotřebiteli četné předběžné informace o sobě i o zboží (článek 4), náležitosti písemného potvrzení (článek 5), spotřebitel má právo do 7 dnů odstoupit od smlouvy (článek 6). Směrnice prošla několika novelizacemi a byla platná až do 13. 6. 2014.

Dle čl. 4 (předběžné informace) odst. 1 písm. a) směrnice 97/7/ES před uzavřením jakékoli smlouvy na dálku musí být spotřebiteli předem sdělena: *„totožnost dodavatele a v případě smluv vyžadujících platbu předem rovněž jeho adresa"*. Již zde je tedy vyžadována pouze *totožnost dodavatele*, a nikoli sdělení o tom, jaká fyzická osoba dodavatele v případě právnické osoby zastupuje!

Dalšími aspekty ochrany spotřebitele se zabývá směrnice 1999/44/ES[13] ze dne 25. května 1999 o některých aspektech prodeje spotřebního zboží a záruk na toto zboží. Tuto směrnici je možné dodnes považovat za základ ochrany spotřebitelů při koupi spotřebního zboží v EU. V čl. 5 odst. 1 je kupříkladu stanovena známá dvouletá „záruční doba" vůči spotřebitelům, neboť prodávající odpovídá, pokud se *„rozpor se smlouvou projeví ve lhůtě dvou let po dodání zboží"*, a v článku 6 je upřesněn rozsah poskytování záruky. Tato směrnice se však nezabývá určením subjektu.

V ochraně spotřebitelů spočívá jisté dilema unijního práva. Na jedné straně by EU zřejmě ráda vytvořila velký vnitřní trh i pro spotřebitelské statky, což znamená umožnit snadný přeshraniční prodej zboží a služeb dodavatelům,[14] lhostejno kde na území EU jsou usazeni a mají provozovny. Na druhé straně žádná země nechce vystavit své občany potenciálním nájezdům neseriózních přeshraničních dodavatelů, pokud by tito mohli splňovat jen nízký standard stanovený některým jiným členským státem.

[13] Směrnice Evropského parlamentu a Rady 1999/44/ES ze dne 25. května 1999 o některých aspektech prodeje spotřebního zboží a záruk na toto zboží, ve znění směrnice 2011/83/EU ze dne 25. října 2011 o právech spotřebitelů.

[14] Srov. např. bod odůvodnění 3 níže probírané směrnice 1999/44/ES.

Novou je směrnice 2011/83/EU, o právech spotřebitelů,[15] (dále jen „DirPS“) která zrušila a nahradila výše zmiňovanou směrnici 97/7/ES. Členským státům byla stanovena lhůta na transpozici tak, že vnitrostátní předpisy musí být používány od 13. 6. 2014. Úprava týkající se určení totožnosti subjektu je v čl. 6 odst. 1. Předpis ocitujeme včetně přidaného zvýraznění:

> Článek 6
> **Požadavky na informace v případě smluv uzavřených na dálku a smluv uzavřených mimo obchodní prostory**
>
> 1. Před tím, než je spotřebitel vázán smlouvou uzavřenou na dálku nebo smlouvou uzavřenou mimo obchodní prostory či odpovídající smluvní nabídkou, poskytne obchodník spotřebiteli jasným a srozumitelným způsobem tyto informace:
>
> ...
>
> b) **totožnost obchodníka**, například jeho **obchodní jméno**;
>
> c) **zeměpisnou adresu**, na níž je obchodník usazen, a jeho telefonní číslo, číslo faxu a e-mailovou adresu, pokud existují, které spotřebiteli umožňují urychleně obchodníka kontaktovat a efektivně s ním komunikovat, a případně adresu a totožnost obchodníka, v jehož zastoupení jedná;
>
> d) zeměpisnou adresu **místa podnikání** obchodníka, pokud se liší od adresy poskytnuté v souladu s písmenem c), a případně zeměpisnou adresu obchodníka, v jehož zastoupení jedná, na kterou může spotřebitel zaslat případné stížnosti;
>
> ...

Směrnice tedy vyžaduje jako povinné pouze *totožnost obchodníka,* například ve formě *obchodního jména*, *zeměpisnou adresu* usazení, ev. místa podnikání, pokud se liší. Telefonní číslo, fax a e-mailová adresa jsou podle DirPS pouze fakultativní.[16]

V čl. 6 odst. 5 DirPS se stanoví povinné zahrnutí do smlouvy: *„Informace uvedené v odstavci 1 tvoří nedílnou součást smlouvy uzavřené na dálku nebo smlouvy uzavřené mimo obchodní prostory a bez výslovného souhlasu smluvních stran je nelze měnit."* Čl. 6 odst. 8 DirPS stanoví, že informační požadavky doplňují ty, které jsou obsaženy ve směrnici 2000/31/ES (E-Commerce) a ve směrnici 2006/123/ES (o službách). Členské státy mohou zavést dodatečné informační požadavky. Současně však stanoví pravidlo pro případ rozporu. Pokud je některé ustanovení uvedených směrnic *„týkající se obsahu informací a způsobu jejich poskytování v rozporu s ustanoveními této směrnice, má přednost ustanovení této směrnice"*. To pochopitelně platí pouze tehdy, jedná-li se o smlouvy v oblasti působnosti směrnice DirPS.

[15] Směrnice Evropského parlamentu a Rady 2011/83/EU ze dne 25. října 2011 o právech spotřebitelů, kterou se mění směrnice Rady 93/13/EHS a směrnice Evropského parlamentu a Rady 1999/44/ES a zrušuje směrnice Rady 85/577/EHS a směrnice Evropského parlamentu a Rady 97/7/ES.

[16] Markou in LODDER, A. R., MURRAY, A. D. (eds), cit. dílo, s. 211.

V čl. 8 DirPS se stanoví formální požadavky na smlouvy uzavřené na dálku. Podle čl. 8 odst. 1 DirPS obchodník spotřebiteli poskytne *„**informace** stanovené v čl. 6 odst. 1 nebo mu je zpřístupní **způsobem odpovídajícím** použitému prostředku komunikace na dálku, a to jasným a srozumitelným jazykem …"* (zvýraznil autor). Po uzavření smlouvy musí dle čl. 8 odst. 1 DirPS obchodník spotřebiteli poskytnout *„potvrzení o uzavřené smlouvě na trvalém nosiči v přiměřené lhůtě po uzavření smlouvy uzavírané na dálku"*, přičemž toto potvrzení musí zahrnovat *„veškeré informace uvedené v čl. 6 odst. 1"*. Podmínku *trvalého nosiče (durable medium)* podle judikatury SDEU nesplňuje[17] webová stránka, neboť ta může být kdykoli jednostranně změněna. Mělo by však dostačovat jakékoli „médium dovolující uložení, přístup a nezměněnou reprodukci, včetně uživatelského účtu spotřebitele na obchodníkově webovém místě, do kterého obchodník může informaci nahrát."[18]

V tomto textu nepopisujeme požadavky DirPS vůbec úplně. Pro zajímavost však zmiňme, že právě v čl. 8 odst. 2 alinea 2 DirPS se stanoví požadavek, v německé nauce nazývaný *Button-Lösung* (srov. 5.2.1.1), že v případě úplatných spotřebitelských smluv má být přítomno tlačítko s textem *„objednávka zavazující k platbě"* nebo s *„jinou odpovídající a jednoznačnou formulací, která upozorní na skutečnost, že podáním objednávky vzniká povinnost zaplatit obchodníkovi"*. Není-li uvedené dodrženo, spotřebitel není smlouvou a objednávkou vázán. Směrnice DirPS si je též vědoma omezených komunikačních možností například na smartphonech. Jsou-li dle čl. 8 odst. 4 DirPS použity prostředky komunikace, které umožňují pouze omezený prostor nebo čas na zobrazení informací, pak dostačují omezenější informace dle čl. 6 odst. 1 DirPS. Například dostačuje uvádět svou totožnost a není nutné uvádět zeměpisnou adresu.

Druhou stěžejní unijní úpravou je směrnice 2000/31/ES o elektronickém obchodu[19] (dále jen „ECDir"). Tato směrnice se sice prvořadě dotýká *poskytovatelů*, a to sice poskytovatelů služeb informačních společnosti, nicméně i provozovatel elektronického obchodu (elektronického agenta) je takovým poskytovatelem a zájemce, resp. později kupující má vedle svého soukromoprávního postavení předsmluvní, resp. smluvní strany i postavení a práva *příjemce služeb* ve smyslu směrnice ECDir.

---

[17] Markou in LODDER, A. R., MURRAY, A. D. (eds), cit. dílo, s. 211.
[18] Markou in LODDER, A. R., MURRAY, A. D. (eds), cit. dílo, s. 211.
[19] Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu („směrnice o elektronickém obchodu").

Článek 5
Obecná informační povinnost

1. Vedle ostatních informačních požadavků podle práva Společenství dbají členské státy, aby poskytovatel služeb umožnil příjemcům služby a příslušným orgánům snadný, přímý a trvalý přístup přinejmenším k těmto informacím:
   a) **jméno poskytovatele služeb**;
   b) **zeměpisná adresa**, na níž je poskytovatel služeb usazen;
   c) údaje, které umožňují **rychlé navázání kontaktu** s poskytovatelem služeb a přímou a účinnou komunikaci s ním, včetně **adresy jeho elektronické pošty**;
   d) je-li poskytovatel služeb zapsán v obchodním rejstříku nebo v obdobném veřejném rejstříku, **obchodní rejstřík**, v němž je zapsán, a jeho **identifikační číslo**, nebo obdobné identifikační prostředky uvedené v rejstříku;
   e) podléhá-li jeho činnost povolovacímu režimu, údaje o příslušném kontrolním orgánu;
   f) pokud jde o regulovaná povolání:
      - profesní sdružení nebo obdobný subjekt, u něhož je poskytovatel zapsán,
      - profesní označení a členský stát, v němž bylo uděleno,
      - odkaz na profesní pravidla uplatňovaná v členském státu, v němž je poskytovatel usazen, a na prostředky přístupu k nim;
   g) vykonává-li poskytovatel služby činnost podléhající dani z přidané hodnoty, **identifikační číslo** podle čl. 22 odst. 1 šesté směrnice Rady 77/388/EHS ze dne 17. května 1977 o harmonizaci právních a správních předpisů členských států týkajících se daní z obratu — Společný systém daně z přidané hodnoty: jednotný základ daně [29].

   ...

Ve výše uvedeném čl. 5 ECDir se uvádějí obecné informační povinnosti a stanoví se, jaké informace poskytovatel musí uvádět. Kromě svého jména a zeměpisné adresy usazení musí být povinně uváděna adresa elektronické pošty, kterou tehdy ECDir považovala za údaj, jenž umožňuje rychlé navázání kontaktu. Dále musí být uveden název rejstříku, v němž je subjekt veden, a své identifikační číslo v něm. Případně musí být uvedeno daňové identifikační číslo pro účel daně z přidané hodnoty.

Dále musí být případně uvedeny informace relevantní pro regulovaná povolání, ev. o kontrolním orgánu, pokud vykonává činnost podléhající povolovacímu režimu z jiného právního předpisu. Samotná ECDir v čl. 4 stanoví, aby pro poskytovatele dle ECDir, tj. jen z důvodů poskytování služeb informační společnosti, se žádné předchozí povolení členskými státy nevyžadovala.

ECDir je důležitá z hlediska uznávání uzavírání elektronických smluv. Dle čl. 9 odst. 1 členské státy zajistí, aby jejich právní řády *„umožňovaly uzavírání smluv elektronickou cestou"(contracts to be concluded by electronic means)*[20] a že nebudou

[20] Znění § 561 obč. zák. je tedy inspirováno nejen § 40 odst. 3 zák. č. 40/1964 Sb., ale i zněním ECDir. České znění či překlad ECDir o „elektronické cestě" je zde nepřesný.

„z důvodu uzavření elektronickou cestou, zbaveny právních účinků a platnosti". Dle čl. 9 odst. 2 ECDir lze z toho vyjmout smlouvy týkající se práv k nemovitostem, smlouvy v oblasti rodinného nebo dědického práva a některé další.

Směrnice uvádí v čl. 10 odst. 1 ECDir informační povinnosti, tj. výčet informací, které musí být poskytnuty předem: *„a) jednotlivé technické kroky vedoucí k uzavření smlouvy; b) zda a jak je smlouva po svém uzavření poskytovatelem archivována a zda je přístupná; c) technické prostředky pro zjištění a opravu omylů vzniklých při zadávání dat před podáním objednávky; d) jazyky nabízené pro uzavření smlouvy"*.

Uvedené informace musí být *„jasné, srozumitelné a jednoznačné"*. Směrnice sice nestanoví vlastní jádrový krok uzavření smlouvy elektronickou cestou, ale, jak výše uvedeno, stanoví, že adresát informací bude informován o tom, jaké technické kroky k uzavření smlouvy vedou. Uzavření smlouvy může pochopitelně vyžadovat více než jen učinění podání objednávky. Umožnění toho, aby způsob a kroky byly popsány, činí směrnici technologicky nezávislou vůči budoucímu vývoji. Směrnice tak pro samotný akt uzavření smlouvy ustavuje meta-model, v němž dostačuje, je-li tento akt předem dostatečně popsán. Jsou však stanovena určitá další omezení.

Uvedené informační povinnosti z čl. 10 odst. 1 se dle čl. 10 odst. 4 ECDir netýkají smluv uzavíraných výhradně výměnou elektronické pošty apod. individuální komunikací. Dle čl. 10 odst. 3 ECDir *„Smluvní ustanovení a obecné obchodní podmínky musí být příjemci poskytnuty v takové formě, aby je mohl uchovávat a reprodukovat."* Uvedené znamená, že poskytovatel nemusí sám uchovávat smlouvu, musí však v uvedené formě poskytovat smluvní ustanovení a obecné obchodní podmínky.[21] Srov. výše požadavky na trvalý nosič *(durable medium)*. Pokud smlouvu neuchovává, musí na to podle 10 odst. 1 písm. b) ECDir předem upozornit.

V čl. 11 ECDir jsou ustanovení o podání objednávky *(placing of the order)*. Podotkněme, že krok, který ECDir popisuje jako podání objednávky, velmi často bude teprve považován za návrh na uzavření smlouvy. Dle čl. 11 odst. 2 poskytovatel musí příjemci poskytnout *„dostupné technické prostředky, jejichž prostřednictvím bude moci rozeznat a opravit chybná vstupní data před podáním objednávky"*. Dle čl. 11 odst. 1 ECDir je poskytovatel povinen *„neprodleně elektronickou cestou potvrdit příjem objednávky"*. Zde často platí, že poskytovatel zvlášť potvrzuje přijetí podání ve smyslu technického dojití a zvlášť přijetí ve smyslu přijetí objednávky (akceptace). Pro

[21] Lodder in LODDER, A. R., MURRAY, A. D. (eds), cit. dílo, s. 45.

dojití se stanoví zásada přístupu: *„objednávka a potvrzení o přijetí ... považovány za přijaté, pokud strany, kterým jsou určeny, k nim mají přístup"*. Odlišně lze stanovit ujednáním stran, kterými nejsou spotřebitelé. Odlišně opět platí pro smlouvy uzavírané výhradně výměnou elektronické pošty nebo obdobnou individuální komunikací.

Z hlediska našich potřeb provedený přehled obsahu uvedených směrnic dostačuje, byť upravují i další záležitosti. Pro úplnost uveďme, že výše uvedené směrnice se vztahují i na jiné smlouvy než ty, které jsou na straně podnikatele (obchodníka) uzavírány pomocí elektronického agenta. Rovněž tak se týkají případů podnikatelů (obchodníků), kteří nejsou právnickou osobou.

V jiných právních oblastech, například při poskytování finančních služeb, mohou být stanoveny dodatečné požadavky, nad rámec zde uvedených.

10.3.1.1 Souhrn

Z pohledu našeho zájmu se vyjevují tři důležité okruhy otázek. První z nich je, zda má být určena fyzická osoba zastupující právnickou osobou na straně elektronického agenta. Odpovědí je, že nikoli, že dostačuje uvést pouze: totožnost (typicky obchodní jméno, firmu), zeměpisnou adresu (usazení a místo podnikání), adresu elektronické pošty, veřejný rejstřík a číslo v něm a daňové číslo k DPH.

Druhou otázkou je, zda se upravují záležitosti uzavírání smluv elektronickými prostředky. Tyto náležitosti upravuje obecně směrnice ECDir v čl. 9 až 11. K uzavření takové smlouvy se nevyžaduje žádná zvláštní technologie provedení, zřejmě dostačuje uzavření smlouvy technikou *click-wrap*. Směrnice je ale technologicky otevřená vůči budoucím úpravám. Směrnice DirPS tyto záležitosti podle svého bodu odůvodnění 14 neupravuje a nedotýká se jich. Vnitrostátní právo může stanovit podrobnosti.

Konečně třetí otázkou je, zda a jak se má uchovávat smlouva. Ze směrnice ECDir plyne, že tu poskytovatel povinen uchovávat není. Ze směrnice DirPS plyne povinnost obchodníka poskytnout následně ale potvrzení o uzavřené smlouvě, které obsahuje všechny podstatné informace, určené v DirPS, a to na *trvalém nosiči (durable medium)*, kterým sice nemůže být webová stránka, ale „médium dovolující uložení, přístup a nezměněnou reprodukci", v praxi např. obyčejný soubor ve formátu PDF. Stejná forma je předepsána pro některé jiné povinně poskytované informace.

10.3.2 Transpozice v právu ČR

Výše uvedené směrnice unijního práva musí být do právního řádu členských států transponovány. Směrnice ECDir je transponována v českém právním řádu částečně v zákonu č. 480/2004 Sb., o některých službách informační společnosti, ve znění pozdějších předpisů a částečně v obč. zák. v § 1820 an. Směrnice DirPS je transponována v obč. zák. v § 1811 an. Transpozice obou směrnic jsou v rámci uvedených ustanovení v občanském zákoníku do určité míry promíseny.

Pro ty informace, pro které unijní směrnice vyžadují formu *trvalého nosiče (durable medium)*, vyžaduje občanský zákoník *textovou podobu*. V této formě se spotřebiteli poskytují například smlouva a znění všeobecných obchodních podmínek podle § 1827 odst. 2 obč. zák. Náležitosti textové podoby jsou definovány v § 1819 obč. zák. Textová podoba je zachována, *„jsou-li údaje poskytnuty takovým způsobem, že je lze uchovat a opakovaně zobrazovat"*. Takové vlastnosti splňují četné formáty počítačových souborů. V § 1819 obč. zák. dokonce není ani stanoven požadavek stejného zobrazení nebo možnost zachování přístupu. Druhé lze snad odvodit od opakovanosti zobrazení. Uvedené vlastnosti jsou zřejmě implikovatelné, aby záznam v textové podobě měl elementární smysl. Měly by být tedy vyloučeny takové formáty nebo konkrétní obsahy, které se v průběhu času mění, například kvůli tomu, že obsah odkazuje na vnější informace, zohledňuje čas nebo používá dynamický obsah jinak.

Pojem *textová podoba* byl do občanského zákoníku zřejmě přejat či použit právě s ohledem na použití v kontextu spotřebitelských smluv v § 1811 an. obč. zák., jejichž úprava do značné míry pochází z unijního práva. Vzhledem k původu pojmu pak vzniká otázka, zda je termín vůbec vhodné právně využívat v jiných právních souvislostech. Textová podoba nevyžaduje podpis (srov. § 561 obč. zák.) ani jiný způsob zajištění své pravosti nebo nezměněnosti (srov. § 562 obč. zák.). Právně teoreticky se rozhodně blíží pojmu písemnost, na což upozorňuje například Polčák.[22] K pojmu písemnost srov. část 5.1.3 výše.

10.3.3 Využití elektronické pečeti/podpisu pro elektronický obchod?

V této části zkusíme zjistit, zda je možné využít (zaručenou, kvalifikovanou) elektronickou pečeť nebo elektronický podpis pro provoz elektronického obchodu, který provozuje právnická osoba.

[22] POLČÁK, R. Elektronické právní jednání – změny, problémy a nové možnosti v zákoně č. 89/2012 Sb. *Bulletin advokacie*. 2013, č. 10, s. 35.

Jak je uvedeno výše, pro v této kapitole zkoumaný případ provozování elektronického obchodu, např. ve scénáři B2C,[23] není pro tento způsob jednání elektronickým agentem předepsán žádný zvláštní způsob zajištění. Výjimkou je povinnost poskytnout některé informace v textové podobě.

Běžně dostačuje, že se požadované informace zobrazují na internetových stránkách, které jsou tvrzeně pod kontrolou dané právnické osoby, a že ta v rámci kontraktačního procesu uvádí požadované informace o své totožnosti a další výše uvedené požadované informace. Dále potvrzení o objednávce či obsah smlouvy, jakož i všeobecné obchodní podmínky musí být k dispozici ke stažení uživatelem v textové podobě, tj. v určitém formátu souboru elektronického dokumentu. I uvnitř těchto elektronických dokumentů musí případně být uvedeny požadované informace o totožnosti a související požadované informace o této právnické osobě. Mezi požadované informace běžně nenáleží určení fyzické osoby jako zástupce při právním jednání. Nejedná se zde o pouze o právní výklad. Situace je doložena více než sedmnáctiletým stavem praxe a provozem pravděpodobně mnoha tisíc takových elektronických obchodů jen v ČR.

V rámci uvádění totožnosti je však potřeba tuto uvádět přesně, a to včetně právní formy uváděné v přístavku (např. „s. r. o.“ nebo „a. s.“). V případě vynechání označení právní formy je přinejmenším německá nauka[24] názoru, že to může přivodit ručení zástupců (jednatelů, prokuristů, členů představenstva...) za společnost. Beurskens spatřuje důvod v tom, že v rámci uvažování o uzavření smlouvy protistrana vyhodnocuje i riziko insolvence. Nedostačuje proto mít uvedené správné daňové identifikační číslo pro DPH nebo identifikaci v rámci veřejného rejstříku, ale je nutné mít správně uvedenu i formu právnické osoby, kterou přístavek vyjadřuje.

Kučera uvádí, že k uzavření spotřebitelské smlouvy dostačuje metoda *click-wrap (clickthrough)*, avšak upozorňuje[25] na potřebu pečlivého včlenění všeobecných obchodních podmínek i jejich dostupnosti v textové podobě, jakož i na podrobnosti určení toho, kdy dochází k uzavření smlouvy. Obdobně např. Härting v rámci německého práva nabádá,[26] že dle § 305 odst. 1 a 2 BGB musí být smluvní protistrana nejen na existenci všeobecných obchodních podmínek důrazně upozorněna, musí mít

[23] Business to consumer (podnikatel vůči spotřebiteli).
[24] BEURSKENS, M. Nomen est omen? – Falschfirmierung im elektronischen Geschäftsverkehr. *Neue Juristische Wochenschrift*. 2017, č. 18, s. 1265–1270.
[25] KUČERA, Z. Uzavírání spotřebitelských smluv na internetu, *Rekodifikace a praxe.* 2015, č. 5, s. 4.
[26] HÄRTING, N., cit. dílo, s. 151.

možnost se s nimi seznámit a ponechat si je, jakož je i odsouhlasit. Doporučuje proto mít v rámci objednacího formuláře jasné upozornění na všeobecné obchodní podmínky, pro přechod na něž dostačuje přeskok jediným hyperlinkem, a současně by se v objednacím formuláři mělo nacházet i zaškrtávací políčko o souhlasu s všeobecnými obchodními podmínkami. Zlozvykem podle Härtinga je *copy & paste* přístup k tvorbě jejich obsahu, popř. jejich inkrementální skládání z různých zdrojů, čímž se internetem šíří často právně nesmyslná nebo nesrozumitelná znění.

Ačkoli právo nestanoví způsob zajištění, v technické praxi dnes běžně bývají webové stránky elektronických obchodů zajišťovány tzv. „serverovým certifikátem“,[27] který bývá běžně spojen s jednou nebo několika málo webovými adresami.[28] Současně je v něm uveden subjekt, který má být považován za provozovatele těchto webových míst. V závislosti na poskytovateli certifikátu a úrovni zajištění postupu ověření existuje i několik úrovní míry jistoty, že uvedené údaje jsou pravé.

Použití serverového certifikátu by mělo umožnit nezávislé ověření toho, že webové stránky pochází od toho subjektu, který je uveden v serverovém certifikátu,[29] a ten by měl být shodný se subjektem, například právnickou osobou, která je uvedena jako tvrzený provozovatel daného webového místa. Následné použití protokolu **`https`** namísto **`http`** v prohlížeči při sezení pak běžně zajišťuje z hlediska kryptologie jednak to, že obsah komunikace nemůže být odposlechnut, jednak to, že spojení od webového serveru až k počítači uživatele je odolné vůči útoku muže uprostřed, tj. že uživateli je prezentován skutečně ten obsah, který webový server vytváří. Serverový certifikát však nezajišťuje odolnost vůči útoku na samotný webový server. Jedná se však o opatření praktické bezpečnosti, které se v současnosti zdá být vyhovující pro značnou část elektronických transakcí. Z právního hlediska je použito dobrovolně, pro zvýšení důvěry uživatele.

V systematice eIDAS jsou serverové certifikáty nazvány jako *„certifikáty pro autentizaci internetových stránek“*. Česká terminologie je zde mírně zavádějící, neboť termín v anglickém znění je *„certificate for website authentication“*, tj. *certifikát pro autentizaci webového místa*. Tento překlad by byl vhodnější, neboť certifikát skutečně

[27] Pojem technické praxe.

[28] Technicky existují služby jako Cloudflare aj. služby doručování obsahu, které využívají serverové certifikáty i jinak.

[29] Nejnižší úrovně míry ověření skutečné ověření pravosti subjektu neposkytují. Např. certifikáty služby *Let's encrypt* ověřují běžně pouze to, že tvrzený subjekt kontroluje daný server. To se ověřuje pouze technicky, aniž by se ověřovala tvrzená totožnost subjektu.

autentizuje celé webové místo, nikoli však jednotlivé internetové stránky. Jejich autenticita (pravost) je z hlediska uživatele prohlížeče až odvozená právě od toho, že je server daného webového místa nabízí v rámci daného sezení. Pro všechny takto zajištěné stránky jednoho webového místa existuje běžně pouze jeden serverový certifikát. Jakmile se daná stránka uloží na disk nebo např. vytiskne, svůj průkaz autenticity vůči třetí osobě, která není fyzicky přítomna s uživatelem, se do značné míry ztrácí. To uživateli nemusí nutně vadit, pokud to ovšem neočekává například právě na základě definice v čl. 3 bod 38 eIDAS, že tímto certifikátem se rozumí *„potvrzení, které umožňuje autentizovat internetové stránky a spojuje je s fyzickou nebo právnickou osobou, jíž je certifikát vydán“*. Uvedené vlastnosti platí jen během vlastního sezení a autenticita stránek je odvozená od webového místa. Nařízení pak obsahuje ještě úpravu *kvalifikovaného certifikátu pro autentizaci internetových stránek* (čl. 3 bod 39 eIDAS), který musí navíc splňovat požadavky přílohy IV eIDAS. Dle čl. 45 odst. 2 eIDAS Komise může vyhlásit čísla technických norem, které by byly základem pro domněnku vyhovění, že některý serverový certifikát splňuje požadavky přílohy IV. Na principu použití a autentizačních účinků však ani kvalifikovanost verze nic nemění. V případě kvalifikované verze bude jistěji ověřena totožnost subjektu v certifikátu, neboť kvalifikovaný poskytovatel bude muset podle čl. 24 odst. 1 eIDAS ověřovat totožnost (fyzické, právnické) osoby, které je kvalifikovaný certifikát vydáván, a bude v režimu dohledu kvalifikovaného poskytovatele, jakož i odpovědnosti za škodu. Právnická osoba si tedy může nechat pro provoz svého internetového obchodu vystavit *(kvalifikovaný) certifikát pro autentizaci internetových stránek*.

Tak jako provozovatelé elektronických obchodů dobrovolně používají serverové certifikáty, dokonce je používali před přijetím nařízení eIDAS jen na základě čl. 2 odst. 3 Listiny, stejně dobře mohou tito provozovatelé, jsou-li právnickými osobami, používat *zaručené elektronické pečeti*, popř. *zaručené elektronické pečeti založené na kvalifikovaném certifikátu*, pro automatizované potvrzování vydávaných nebo zasílaných potvrzení nebo obsahů smluv, které byly uzavřeny, popř. jiných informací, které se musí poskytovat v textové podobě. Nemůže jim přitom být na újmu, že v kvalifikovaném certifikátu není vyjádřena žádná fyzická osoba. Povinnost provádět zvláštní vyšší zajištění není dána, povinnost uvádět fyzickou osobou jako zástupce právnické osoby není dána.

Pro obecnou kontraktaci elektronickými agenty není v právu ČR stanoven požadavek písemné formy právního jednání a tím ani podpisu. Z toho pak plyne dovolení použití zaručené nebo kvalifikované elektronické pečeti i na základě čl. 10 ZSVD.

Fyzické osoby tím diskriminovány nijak nejsou. Jsou-li provozovatelem elektronického agenta ve formě elektronického obchodu, mohou vydávané elektronické dokumenty automatizovaně podepisovat pomocí AdES nebo $AdES_{QC}$. K této možnosti mohou využít i pseudonym na místě svého jména. Jelikož to žádný zákon nezakazuje, mohou i právnické osoby sebou vydávané dokumenty s textovou podobou při provozu elektronického obchodu jen automatizovaně podepisovat, například pomocí AdES nebo $AdES_{QC}$ některého svého vhodně zvoleného zaměstnance. K takovému účelu by pravděpodobně bylo vhodnější použití jeho pseudonymu.

Stejně dobře mohou právnické osoby postupovat tak, jak činily dosud, totiž že sebou vydáváné elektronické dokumenty, související s elektronickým obchodem, jako jsou potrvzení o objednávce, obsah smlouvy, obecné obchodní podmínky, smluvní ustanovení apod., ani elektronicky nepodepisují, ani elektronicky nepečetí.

10.3.4 Jednání právnické osoby jiným elektronickým agentem

Bude-li se jednat o soukromé právní jednání právnické osoby elektronickým agentem, které bude jiného druhu, než jsou výše rozebraná právní jednání (distanční a spotřebitelské smlouvy, elektronický obchod...), jejichž úprava vychází z unijního práva, pak je dle autora v takovém případě rozhodné, zda je předepsána písemná forma (nebo vyšší), anebo dostačuje jednání bez určení formy.

V druhém případě není náležitostí jednání podpis. Pro soukromé právní jednání je pak na základě legální licence v čl. 2 odst. 3 Listiny a neodporování § 8 až § 10 ZSVD následně dovoleno použití zaručené, kvalifikované nebo prosté elektronické pečeti dle eIDAS.

Autor však nevylučuje, že v těchto jiných případech použití elektronického agenta bude nutné v rámci obsahu elektronického právního jednání určit fyzickou osobu zástupce právnické osoby, která skutečně jednala, aby se vyhovělo požadavkům českého práva na jednání právnické osoby, že jednal oprávněný zástupce právnické osoby, projev jehož vůle je elektronickým agentem realizován.

V těchto případech může poněkud zanikat autentizační význam zaručených nebo kvalifikovaných elektronických pečetí. Praktický smysl zřejmě dává zejména automatizované vytváření pečetí v rámci systémů B2B, jejichž náležitosti jsou předem předjednány smluvně.

10.4 Jednání právnické osoby v písemné formě

Předepisuje-li právní řád pro právní jednání písemnou formu nebo se na ní dohodnou strany, je v občanském zákoníku třeba se věnovat jeho ustanovením § 561 a § 562. Čtyři možnosti jejich výkladu jsou provedeny již výše (srov. 5.1.5). Výklad kombinace občanského zákoníku s § 7 ZSVD je již též proveden výše (srov. 9.4) a nezbylo by zde než námitky a potíže opakovat.

V rámci praxe právnických osob je patrné, že použít druhy techniky podpisů bez autentizačních vlastností může být v řadě scénářů naprosto paradoxní, neboť podepisující osoba prakticky nikdy nepodepisuje jen za sebe sama, ale za právnickou osobu. Takové podpisy by ani dobře nezakládaly odpovědnost členů statutárních orgánů vůči jiným orgánům právnické osoby, ev. vůči její vlastníkům. Jejich použití je však vhodné, pokud jsou důkazní potřeby zajištěny nějak spolehlivě jinak.

Chce-li si být podepisující právnická osoba naopak co nejvíce jistá dodržením formy, splnit ji s rezervou, použije její zástupce kvalifikovaný elektronický podpis (srov. 6.5.3) a pro podepisovanou písemnost (srov. 5.1.3) použije střídmý datový formát a konzervativní výklad toho, co je písemností. V rámci obsahu písemnosti musí být pro určitost i uvedeno, která fyzická osoba ji bude elektronicky podepisovat a že ji podepisuje jako zástupce určené právnické osoby.

Plynou-li požadavky na formu pouze ze vzájemného ujednání stran, chtějí-li strany použít nižší úroveň podpisu, než je QES, a přesto mít plnou právní jistotu, pak se pochopitelně mohou dohodnout například na „textové formě“, jejíž náležitosti si sami určí, a potvrzování uvažovaným druhem elektronického podpisu, například $AdES_{QC}$.

10.4.1 Topologie připojených elektronických podpisů a pečetí

Může-li právnická osoba na základě svého zakladatelského právního jednání v určitém případě právně jednat v písemné formě pouze současným jednáním více členů svého statutárního orgánu, v tradiční listinné podobě by na listinu tito členové připojili své vlastnoruční podpisy vedle sebe či těsně nad sebou.

Technika digitálních podpisů, které jsou podkladem podpisů QES (ev. AdES) i pečetí QESeal (ev. AdESeal), umožňuje uvedená potvrzení vůči podepsané písemnosti v elektronickém dokumentu libovolně přiřazovat. Budeme-li podepisovaná data považovat za kořen stromu, tak nad tímto kořenem lze vytvořit v podstatě jakoukoli stromovou strukturu z výše uvedených digitálních objektů. Nejběžnější asi budou dva případy. Prvním je souřadné přiřazování digitálních objektů na stejnou úroveň. Druhou hlavní možností je posloupnost. V rámci posloupnosti platí, že následující digitální objekt potvrzuje (zpravidla) celý obsah, včetně předchozích digitálních objektů. V druhém případě lze kdykoli i zpětně určit, v jakém časovém pořadí jednotlivé potvrzující digitální objekty vznikaly.

Čistě technicky lze vytvořit výše uvedená spojení i heterogenně, tj. použít jak elektronický podpis, tak elektronickou pečeť. Z čistě právního hlediska autor nespatřuje důvod pro takové jednání, neboť by měl dostačovat elektronický podpis zástupce. Důvodem snad mohou být vyšší důkazní účinky pro spoléhající se osobu, popř. zvláštní vnitřní postupy právnické osoby.

Připojuje-li jedna stvrzující strana dvě potvrzení složené z pečeti a podpisu, je technicky možné mít například pořadí kontrasignací 1. QES a 2. QESeal anebo pořadí kontrasignací 1. QESeal a 2. QES, ale i bez sekvence, tj. zcela souřadně QES a QESeal.

Může vzniknout otázka, zda je výše uvedené pořadí právně rozhodné. Autor je obecně názoru, že pokud je v elektronickém dokumentu jasně uvedeno, že jedná fyzická osoba určitého jména jako zástupce určité právnické osoby, jejíž název aj. dostatečná identifikace jsou též uvedeny, pak na pořadí nezáleží. V takovém případě je totiž uvedení QESeal zřejmě navíc, dostačoval by podpis fyzické osoby QES jako zástupce právnické osoby pro platnost právního jednání právnické osoby. Důvody připojení QESeal však mohou být důkazní.

Pokud identifikace právnické osoby v dokumentu není zcela jasná,[30] pak se autor domnívá, že je vhodná kontrasignace, a to v pořadí 1. QESeal (AdESeal) a 2. QES (AdES). Důvodem je, že QESeal (AdESeal) obsahuje identifikační název společnosti. Fyzická osoba, která připojuje svůj QES (AdES), tedy již by měla mít spolehlivou

[30] Nejasnost určení právnické osoby uvnitř písemnosti je z hlediska dobře vedené právnické osoby a přípravy dokumentů nonsens. Uvedení názvu právnické osoby např. v QES nebo v QESeal ale může mít příznivý důsledek na automatizaci zjištění toho, o čí právní jednání se jedná. Zatímco formátu uvnitř obecného dokumentu software rozumět nemusí, formátům elektronického podpisu rozumět může.

možnost seznámit se s tím, že dokument je již zapečetěn jménem právnické osoby a že její podpis navazuje za pečetí chronologicky a bude (měl by) být považován za jednání v zastoupení právnické osoby, a nikoli za její vlastní jednání coby fyzické osoby. Je to však otázka spíše dobré praxe, která vylučuje zpochybnění podepsané fyzické osoby, že jednala svým vlastním jménem, než že by porušení tohoto pravidla mělo vést k neplatnosti právního jednání.

V praxi si lze představit různé obchodní procesy přípravy dokumentů, které mají charakter vnitřního postupu uvnitř právnické osoby. Pokud se příprava realizuje automaticky, je možné si představit, že informační systém připraví návrh elektronického dokumentu zapečetěný automaticky pomocí AdESeal a následně se výsledek posune k fyzické osobě. Ta si díky ověření AdESeal může být jista, že dokument prošel požadovaným vnitřním procesem, a po zvážení může připojit svůj QES.

Celkově je praxe uvedených stromů digitálních objektů sice lákavá intelektuálně, autor však upozorňuje, že digitální objekt jako QES nebo QESeal by měl být ideálně doplněn o časové razítko. To uvedené stromy zesložiťuje a ověřujícím softwarům může působit potíže. Je vhodné proto navržené konstrukce si přinejmenším otestovat proti běžnému ověřujícímu softwaru.

11. Souhrn a závěr

Počítačový specialista a vizionář Lanier na přelomu milénia vyjádřil zásadní skepsi vůči výpočetní technice. Software, který svou vnitřní složitostí tvoří převažující část dnešního IT, je dle něj křehký. Jeho slovy: „Software se zlomí dříve, než se ohne. Vyžaduje perfektnost v universu, které dává přednost statistice.“[1] Chce tím vyjádřit, že počítačové chyby přichází náhle, bez jakéhokoli předchozího varování. Systémy fungují buď (zcela), anebo (vůbec).

Naprostá počítačová rigidnost na druhou stranu slouží lidem velmi dobře, neboť výpočetní technika provádí běžně naprosto přesně to, co jí je zadáno. Podpisové algoritmy asymetrické kryptografie pak dokáží poskytnout binární výsledek o tom, zda je podpis platný, nebo nikoli. Spojení IT a uvedených algoritmů poskytuje praktickou jistotu o tom, že výsledný elektronický podpis byl vytvořen za pomoci zcela určitého soukromého klíče, nebo-li dat pro vytváření elektronického podpisu, v právní terminologii. Zda podepisující osoba dokázala udržet „křehké“ IT i data pro vytváření elektronického podpisu pod svou výhradní kontrolou, je otázkou toho, jaké technologie využívá a jak s nimi zachází.

Právní rámec, například i zde v textu rozebírané nařízení eIDAS, se pak v zásadě snaží zajistit více nebo méně důkladně to, aby používané prvky systému podléhaly kontrole jak uživatele, tak ještě jiných nezávislých odborně kontrolujících očí. Tak se zařízení QSCD musí certifikovat a kvalifikovaní poskytovatelé certifikačních služeb podléhají nezávislému auditu a kontrole vnitrostátním orgánem dohledu.

Níže v souhrnu je přesto konstatováno, že právní rámec nařízení eIDAS je spíše neúplný. Vzhledem k dlouhé periodě novel unijní legislativy lze situaci napravit nejspíš jen podrobnější vnitrostátní implementací.

Přesto při jakékoli úrovni opatření zůstává, a asi vždy bude zůstávat, určité *zbytkové riziko*, že elektronický podpis bude úspěšně napaden.

Autor je přesvědčen, že zbytkové riziko lze podstatně zmírnit, pokud podepisující osoba dobrovolně (chybí-li k tomu nutící legislativa) nakládá se svou technologií pečlivě a chrání ji jak fyzicky, tak z pohledu počítačové bezpečnosti. Je si

[1] LANIER, J. One-Half of a Manifesto, Wired, roč. 2000, č. 12. Dostupné z: <https://www.wired.com/2000/12/lanier-2/>.

však vědom, že taková péče může být na úkor snadné použitelnosti, někdy je mimo dosah i u počítačových odborníků.

Lze však souhlasit s Čermákem jr., že k „popírání a dokazování pravosti [vlastnoručního] podpisu dochází v praxi velmi zřídka“.[2] Čermák predikoval, že tomu bude stejně i v případě podpisů elektronických. Skutečně ani po 15 letech od jeho článku se soudní judikatura nezaplnila případy zfalšovaných elektronických podpisů, a to ani v ČR, ale ani v Německu. Důvodů může být několik.

Na základě veřejně přístupných údajů poskytovatelů služeb autor zjistil, že v ČR bylo za rok 2013 vydáno do 250 tisíc kvalifikovaných certifikátů, tj. disponovaly jím nejvýše *3,6 % populace* aktivního věku. Po více než dekádě rozvoje se jedná o malou penetraci, a to zřejmě zejména do rukou těch technicky zdatnějších i vybavenějších jednotlivců. Jiným důvodem je, že provést ekonomicky lukrativní útok je zřejmě obtížné. Většina právních jednání sestává z více kroků. Falešné vytvoření dokumentu závazku by bylo problematicky vymahatelné, neboť dle § 1791 odst. 1 obč. zák. věřitel je v případě sporu povinen prokázat jeho kauzu. Obdobně tomu bylo v § 495 zák. č. 40/1964 Sb. Falšování též běžně bude nejen civilní, ale i trestní delikt. Kauzu není nutné prokazovat v případě směnek. Ty v tradiční praxi jsou asi nejčastějším případem sporů o pravost vlastnoručního podpisu, směnky však nelze vystavit v elektronické verzi. Obdobně tomu je s jinými cennými papíry.

Jinou otázkou je, proč pouze 3,6 % populace si pořídilo kvalifikovaný certifikát pro elektronický podpis. Je možné, že valná část populace nemá případy užití (*use case*), které by ospravedlnily náklady na něj. Je ale také možné, že populace považuje zaručené a kvalifikované elektronické podpisy za obtížně použitelné anebo též za ohrožující. Složitost přinejmenším právní úpravy, která je koneckonců dokumentována i tímto textem, naznačuje, že možných míst selhání je mnoho.

Poskytovatelé služeb se budou snažit těžit z nového nařízení eIDAS a tyto nerozhodnuté zájemce získat pro vzdáleně vytvářené elektronické podpisy, proveditelné ze smartphonů běžných osob. Tím se bezesporu usnadní použitelnost a nasaditelnost. Některá rizika z použití však mohou naopak narůst, a to i tím, když se používání masověji rozšíří mezi populaci vysloveně laickou.

[2] ČERMÁK K. jr., cit. dílo, s. 73.

Autor se v tomto souhrnu proto snaží vypořádat s výše zmíněným zbytkovým rizikem i trochu jiným způsobem než pouze šroubováním požadavků na technickou, fyzickou, organizační aj. bezpečnost, která u průměrného uživatele nemusí být realisticky dosažitelná. Snaží se upozornit na právní a potažmo technická řešení, která by rizika podepisujících či spoléhajících osob snížila jiným způsobem.

Dilematem k řešení je, k čí tíži připsat elektronické právní jednání potvrzené kvalifikovaným elektronickým podpisem, jehož (technická) platnost je úspěšně ověřena, ale jehož provedení údajná podepisující osoba následně přesto popírá.[3]

Touto otázkou se v mnoha dílčích aspektech zabývá celý tento text. Zde se proto nezabýváme již znovu jednotlivostmi, ale výsledky, ke kterým lze dojít na základě celého textu, ve vyšší rovině abstrakce a reflexe podrobně rozebraných problémů.

11.1 Veřejné právo

Autor se domnívá, že v rámci vertikálních vztahů by zbytková rizika z používání kvalifikovaných nebo zaručených elektronických podpisů na sebe měl zásadně vzít stát, nebo by mu měly být soudy přisuzovány k jeho tíži.

Je to totiž právě stát, který stanoví případnou povinnost používání kvalifikovaných a zaručených elektronických podpisů ve vertikálních vztazích, a současně je to stát, kdo právně stanoví veškeré náležitosti související s poskytováním kvalifikovaných služeb vytvářejících důvěru vydávání kvalifikovaných certifikátů pro elektronické podpisy,[4] jakož i s vytvářením a používáním daných elektronických podpisů. Jestliže navzdory těmto pravomocím státu vznikají faktické okolnosti nebo právní nejistoty, jaké jsou například popisovány v tomto textu výše, pak zejména laický uživatel informačních technologií není jakkoli v pozici, aby daným situacím čelil.

Výše uvedené neznamená, že by stát nebo soudy měly akceptovat jednání, které by dané situace zneužívalo. Jestliže však nejsou patrné žádné příznaky zneužití ani jiného souvisejícího porušení právní povinnosti, autor se kloní ke shora uvedené zásadě.

Uvedená koncepce je i realistická. Vertikální jednání, zejména ta, která se konají v písemné podobě, mají pravidelně charakter procesního řízení. Jeho charakterem je, že rozhodující právní akt, nejčastěji individuální správní akt, provádí strana úřadu nebo

[3] Podobné základní dilema platí i v případě právního nebo jiného jednání právnické osoby, potvrzené kvalifikovanou elektronickou pečetí. Právní hodnocení situace zde však může být odlišné, neboť právo může vyžadovat určení konkrétní fyzické osoby jako zástupce právnické osoby.

[4] Ev. kvalifikovaných certifikátů pro elektronické pečeti.

jiného orgánu veřejné moci. Podání aj. úkony jednotlivců zpravidla nemívají takový význam, aby se někomu třetímu běžně vyplatilo[5] takové úkony falšovat nebo jinak napadat, zejména však případy takového falšování vyjdou najevo v řádu nejvýše týdnů. Subjekty jednotlivců, které přesto pracují s vyšším rizikem, by měly být přiměřeně schopnější se postarat o bezpečnost svého vybavení IT. V praxi činný informační systém datových schránek pracuje s takovým asymetrickým modelem, který si na straně protějšků orgánů veřejné moci právně, tj. u běžných fyzických osob a právnických osob soukromého práva, vystačí i jen se slabou autentizací přihlášení se jménem a heslem. V případě zájmu však fyzické osoby i právnické osoby mohou stupeň svého zabezpečení pro autentizaci dobrovolně zvýšit. Prozatím se jeví jako uspokojivý.

Na straně úřadů aj. orgánů veřejné moci pak ani nařízení eIDAS nebrání tomu, aby stát pro ně stanovil doplňkové požadavky na systémové prostředí i na aplikace vytvářející podpis, jakož i na další využívané systémy, zejména síťové, ale i systémy pro správu dokumentů, tj. zejména systémy spisové služby a archivace. K těmto krokům by stát měl být nucen i s ohledem na to, že úřady a jiné orgány veřejné moci vydáváná rozhodnutí aj. akty mají charakter *veřejné listiny*.[6] Ty se těší presumpci správnosti, která by ale nebyla opodstatněná, pokud by zázemí úřadů aj. orgánů veřejné moci nebylo dostatečně zabezpečené.

11.2 Soukromé právo

Rozhodnout o řešení dilematu v horizontálních vztazích soukromého práva je podstatně obtížnější, neboť jakékoli obecné normativní řešení příklonu na stranu podepisující osoby, anebo na druhou stranu spoléhající osoby, může být v konkrétním případě nespravedlivé. Nestanovení řešení ale působí právní nejistotu, je tedy rovněž protichůdné vůči finálním hodnotám práva. Toto dilema autor řeší výše navrženým systémem skutkových domněnek (srov. 9.4.1). Jejich síla může být případně korelována podle stavu platného práva, pokud v něm časem dojde ke změnám.

Jedna z existujících ochran v soukromém právu ČR je, že u právního jednání se předpokládá kauza. Ta sice nemusí být v právním jednání vyjádření, v případě sporu však je věřitel povinen ji prokázat (srov. výše počátek této kapitoly). Jinou prevencí

[5] Z uvedeného mohou existovat výjimky např. v případě dispozičních procesních úkonů u soudních sporů, popř. významných správních řízení apod. Soukromý subjekt pak učiní dobře, pokud si svá rizika autentizace a přístupu do datové schránky ošetří vyšší úrovní zabezpečení.

[6] Srov. 9.2 výše.

soukromého práva je, že k provádění právního jednání v elektronické podobě by nikdo neměl být nucen. Volba formy je otázkou smluvní svobody.

Určitým vzorem podobného dilematu je otázka omylu, kdy objektivně seznatelný projev vůle neodpovídá původní vnitřní vůli jednající osoby, ale protějšek na něj spoléhá. Německá nauka zde téměř století váhala, zda za takové situace dát přednost jednající osobě, anebo jejímu protějšku. Situaci nakonec vyřešila právní úpravou rozporovatelnosti, což představuje aposteriorní institut zpětného zpochybnění svého jednání s charakterem jeho zpětvzetí. V případě sporu však rozporovatelnost nemusí být soudem uznána. Soudy případy neřeší tak, aby vždy vznikala co nejmenší škoda, ale podle práva a pravidel judikatury, které se pro institut rozporovatelnosti vytvořily.

V německém právu upravený institut rozporovatelnosti *(Anfechtung)* je obecně vhodný i pro rozporování těch elektronických právních jednání, jejichž vytvoření nebo obsah údajně jednající osoba popírá. V rámci německé úpravy je důležité, že rozporovatelnost je institut již fáze realizace práva a pokrývá nejen situace omylů, ale i případy, kdy právní jednání bylo vylákáno lstivým klamem *(arglistige Täuschung)*.

Oproti tomu česká úprava stejné situace budí dojem, že namítání neplatnosti[7] se uplatní až v případném soudním řízení.

Bezpochyby je proto třeba zdůraznit, že i když český občanský zákoník institut rozporovatelnosti neobsahuje, přesto je vhodné či nutné, aby údajně jednající osoba jednoznačně informovala dotčené osoby, že dané právní jednání popírá, a to co nejdříve poté, co se o této situaci dozví. Z hlediska soukromého práva to může být nutné i tehdy, pokud se domnívá, že dotčená osoba sama lest způsobila, o lsti věděla nebo je původcem lsti nepřímo. Takové oznámení ruší nejpozději k okamžiku informování dobrou víru dotčených osob, je podstatné z hlediska prevence dalších škod[8] i pro možnost odmítat alespoň odpovědnost za škody, které by vznikly následně v důsledku ponechání dobré víry.

V praxi může být situace složitější, neboť takový skutkový stav může mít znaky trestného činu podvodu[9] nebo jiného trestného činu.[10] V rámci vyšetřování orgány

[7] Ustanovení § 586 odst. 1 obč. zák.
[8] Ustanovení § 2900 an. obč. zák.
[9] Ustanovení § 209 trest. zák.
[10] Například trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 trest. zák., nebo opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat dle § 231 trest. zák.

činnými v trestném řízení nebo i svépomocného obstarování důkazů[11] může být někdy výhodnější znalost dočasně pozdržet.

Současně je ale třeba upozornit, že zfalšovanému elektronickému právnímu jednání zpravidla zcela chybí atribut vůle jednajícího, o právní jednání se nejedná[12] a půjde o zdánlivé právní jednání. Toto právní hodnocení nicméně nic nemění na výše uvedené vhodnosti takové jednání přesto popřít. Často teprve v pozdějších fázích se projeví, co z tvrzení stran bude vzato za prokazatelné.

11.2.1 Soukromé x veřejné právo

Jak je uvedeno výše, zbytková rizika lze na straně jednotlivců uřídit v případě jak ryze veřejného, tak ryze soukromého právního jednání jednotlivců. Averze k rizikům v oblasti soukromého práva nejvýše způsobí, že si osoby nebudou chtít prostředky a certifikáty pro vytváření kvalifikovaných či zaručených elektronických podpisů pořizovat.

Potíž vyvstává tehdy, pokud je jednotlivec nucen k jejich pořízení z důvodů splnění požadavků veřejného práva, ale rizika mu vznikají v jeho osobní sféře, z potenciálních vztahů soukromého práva. Některými novými možnostmi řešení této potíže se zabývají další části níže.

11.3 Model omezení použitelnosti nebo finančního limitu

Dokonalejší právní úpravou by bylo možné mnohé výše probírané potíže zmenšit, mnohé i odstranit. Přesto se asi nikdy nepodaří odstranit úplně všechny možné potíže. Zejména je třeba reflektovat, že praxe ani po dvaceti letech využívání digitálních podpisů, tj. základu kvalifikovaného elektronického podpisu, nevede na využívání jednoúčelových podpisových zařízení, které jediné by mohly mít dostatečně zajištěnou bezpečnost z hlediska jistoty kontroly nad vytvářením elektronického podpisu ve vztahu k podepisovanému obsahu tak, jako tomu je v případě klasických (papírových) listin.

V případě univerzálních, a proto nutně velmi složitých výpočetních prostředků, jakými jsou osobní počítače nebo smartphony, je dosažení stejné úrovně bezpečnosti kontroly vždy částečně jen iluzorní.[13]

---

[11] Míněno v rámci vlastních prostředků výpočetní, komunikační a síťové techniky jednající osoby nebo vyžádáním třetích neutrálních osob o zajištění jejich záznamů.

[12] Ustanovení § 551 obč. zák.

[13] Podobně zdůrazňuje Mason in MASON, S. *Electronic Signatures in Law,* cit. dílo, 2016, s. 152–156.

Autor je proto názoru, že mnohem pragmatičtějším přístupem k užití kvalifikovaných elektronických podpisů nebo pečetí by byl model obsahující apriorní omezení jejich použitelnosti, které by vedlo k zásadnímu omezení rizik podepisujících nebo pečetících osob. Možné druhy omezení použitelnosti by například mohly být:

- pouze k úkonům pro veřejné právo,
- pouze v rámci profesního nebo zaměstnaneckého působení,
- pouze v rámci finančního limitu za časovou periodu.

Takové možnosti jsou i rozebírány výše v textu.[14] Autor nevylučuje, že mohou existovat i další vhodná omezení podle druhu činnosti. Z hlediska finančního omezení je z hlediska podepisující osoby zajímavější kumulativní omezení než jen finanční omezení na jedinou transakci. Realizace takových funkcí by asi ještě před 10 lety byla jen obtížně představitelná. Při stavu současné konektivity jsou však možné i doplňkové služby vytvářející důvěru, u kterých by se v rámci každého podpisu registrovala určitá hodnota dané elektronické transakce. Popřípadě lze zavést služby vytvářející důvěru charakteru smíšeného elektronického podpisu, podepisující osobou a poskytovatelem služby. Bez obou složek by elektronický podpis nebyl platný. Podepisující osoba by pak běžně poskytla svoji vůli ve vztahu k podepsaným datům, poskytovatel přídavnou kontrolu, že transakce nepřekračuje stanovený kumulativní finanční limit. Implementaci lze provést tak, aniž by částku kontrolující poskytovatel musel být seznámen s obsahem elektronické transakce. Implementace by pochopitelně vyžadovala, aby součástí obsahu právní elektronické transakce byla explicitně i určitá finanční částka, která reprezentuje její hodnotu. To je technicky možné, představuje však i právní otázku, která může vyžadovat důkladnou právní analýzu, jaké hodnoty je třeba jakým konáním nebo právním jednáním přiřazovat, aby ochrana byla účinná a současně nebránila elektronickým transakcím. Rozvoj tímto směrem by bezpochybně znamenal nejen rozvoj v oblasti techniky a služeb, ale i související rozvoj a změny práva.

Podobný model omezení finančních částek existuje v případě platebních karet, kreditních i debetních. Je zcela funkční a tyto karty se masivně využívají v široké populaci. Udává se, že v současnosti má platební kartu 95 % osob v ČR.[15] Bezpochyby případ užití pro platby v obchodech nebo výběry hotovosti z bankomatů je mnohem častější než podepisování se, přesto tato situace svědčí i o tom, že platební karty mají

[14] Srov. 6.16.10.

[15] Dostupné z: <https://www.novinky.cz/finance/406790-petina-cechu-plati-v-obchodech-jen-kartami.html>.

zvládnuta rizika, přičemž zřejmě velmi důležitým, ne-li nejdůležitějším opatřením je finanční omezení rizik na určitý, předem stanovený limit.

11.4 Převod elektronického jednání na (rozporovatelný) proces

Jinou možností modifikace provádění elektronického právního jednání by bylo převést jednorázovost právního jednání na určitý proces, nebo alespoň spolehlivé vytváření záznamů o jednotlivých právních jednáních.

Kupříkladu podstatná část bezpečnosti informačního systému datových schránek běžných fyzických osob netkví v tom, že přihlášení osoby podléhá autentizaci, ale je dána spíše tím, že odeslaná zpráva je v systému uložena po dobu 90 dnů. To je dostatečně dlouhá doba na to, aby si osoba, z jejíž schránky k odeslání případně podvržené zprávy došlo, neoprávněného úkonu všimla.

Zasílání různých potvrzení o průběhu kroků nákupu v elektronickém obchodě má vedle informativního významu rovněž smysl v poskytnutí určité bezpečnosti.

Podobnou povahu procesu mají kupříkladu i správní aj. řízení. Vlastností všech těchto řízení mimo jiné je, že nesrovnalosti jsou běžně brzy odhaleny.

Obdobně rigidní je i mechanismus bankovních výpisů. Ty tvoří nepřetržitou posloupnost. Jednou z výsledných vlastností je brzké zachycení jakékoli nesrovnalosti.

Provoz elektronických obchodů vůči spotřebitelům má v současnosti též charakter procesu, neboť spotřebitel má právo na odstoupení od smlouvy.

Převedení jednání na rozporovatelný proces by pochopitelně měnilo charakter právního jednání, které by se stalo méně definitivním. To může být často nežádoucí z hlediska efektivity jednání. Podpoření právního jednání procesem, jehož výsledkem je nevyhnutelně záznam pro jednající osobu, však může posílit její důvěru aspoň v to, že se o jakémkoli případném zneužití brzy dozví.

11.5 Charakteristika nařízení eIDAS

Podstatná část tohoto textu se zabývá výkladem evropského nařízení eIDAS. Nařízení není v oblasti služeb vytvářejících důvěru úplné a v případě digitálních objektů odvozených od elektronického podpisu má charakter jen tzv. rámcového nařízení. V případě digitálních objektů je výše v textu zdokumentována dokonce jeho jen pilířovitá pojmová struktura, mezi níž se nacházejí neupravené mezery. V jejich rámci

se právní úprava propadá zřejmě zpět do vnitrostátního práva. V navazující části níže je proto uvedena souhrnně právní argumentace pro možnost podrobnější implementace nařízení eIDAS, umožňující případné zaplnění mezer.

11.5.1 Důvěryhodné seznamy

Důvěryhodný seznam je institut či koncept z nařízení eIDAS, který autor považuje jednak za podařený, jednak za hodný pozornosti, a to i na úrovni tohoto závěrečného souhrnu.

Pozoruhodnost spočívá v tom, že nařízení předepisuje vydávat důvěryhodný seznam ve *„formě vhodné pro automatické zpracování"*. Tato forma v rámci nařízení eIDAS plní roli jakéhosi esperanta EU, z něhož je obsah strojově přeložitelný do kteréhokoli úředního jazyka EU.

Autor tento institut v rámci eIDAS vykládá tak, že u důvěryhodných seznamů je třeba presumovat jejich správnost i jejich přeshraniční uznání v rámci jiných členských států,[16] ačkoli tyto vlastnosti nejsou v nařízení explicitně vyjádřeny. Vzhledem k tomu, že u jiných veřejných listin k přeshraničnímu uznávání v rámci EU bez dalšího nedochází, je otázkou, zda by tento institut a způsob jeho provedení mohl poskytnout inspiraci pro řešení přeshraničního uznávání jiných listin a/nebo dokumentů.

Důvěryhodný seznam má ovšem charakter rejstříku se záznamy rigidního obsahu, navíc rejstříku nepříliš rozsáhlého.

11.6 Důvody pro/proti podrobnější vnitrostátní implementaci

Jak je uvedeno průběžně v tomto textu, jakož i v souhrnu bezprostředně výše, nařízení eIDAS je neúplné. Vzniká proto otázka, zda by nebyla vhodnější podrobnější implementace nařízení v ČR, než byla zvolená „minimalistická" varianta v ZSVD.

Zde ve shrnutí jsou pouze velmi stručně uvedeny seznamy určitých argumentů, které jsou uplatnitelné při diskursu o způsobu implementace. Jejich odůvodnění plyne z pravidel evropského práva pro implementaci legislativního aktu druhu nařízení.

11.6.1 Co je dovoleno/vhodné při implementaci nařízení

Při implementaci je dovoleno, ev. je vhodné:

- přijmout konkretizační úpravu,

[16] Srov. 6.9.3.

- přijmout doplňovací úpravu,[17]
- derogovat rozpornou nebo efektivitu ohrožující úpravu,
- přijmout institucionální a kompetenční úpravu pro prosazování práva EU,
- přijmout úpravu procesně kontrolní,
- přijmout úpravu sankcí, ev. procesu jejich ukládání,
- využití institutů nařízení jinde v právním řádu,
- odstranění ev. rozporů mezinárodně právního charakteru.

Z uvedených implementačních úprav by pozitivně ovlivnily neúplnost nařízení eIDAS zejména první dva druhy úpravy, tj. konkretizační a doplňovací.

11.6.2 Co je zakázáno při implementaci nařízení

Při implementaci je zakázáno, resp. je neloajální:

- zakrýt unijní povahu práva,
- přijímat nebo ponechat v platnosti úpravu v rozporu s nařízením,
- přijímat jinak protichůdnou úpravu vůči nařízení.

Vzácně je pouze možné přijmout či ponechat v platnosti vnitrostátní úpravu stejného smyslu nebo znění, pokud úprava unijní je značně roztříštěná, a byla by z tohoto důvodu pro adresáty práva EU nepochopitelná. Roztříštěnost úpravy však v případě nařízení eIDAS nenastává.

11.6.3 Důvody protiprávnosti nedoplnění

Některé důvody pro podrobnější implementaci mohou mít až intenzitu právní povinnosti přijmout podrobnější implementaci. Ke zvážení jsou důvody:

- rozpor s obecnými právními zásadami práva EU, zejména právní jistotou,
- právní jistota jako obecná hodnota jakéhokoli právního řádu,
- rozpor se základními právy EU; zejména ohrožení práva vlastnictví,
- dosažení cíle nařízení z důvodu loajality státu k EU; finálním účelem nařízení eIDAS je podpořit provádění elektronických transakcí na vnitřním trhu, k tomu je zapotřebí adresátům vytvořit skutečnou právní jistotu.

[17] Při doplnění je zřejmě kritické zjistit, zda mezera v unijní úpravě se vyskytuje záměrně v tom smyslu, že nezaplněnou mezerou zůstat má. Doplnit je zřejmě pak možné všechny ostatní mezery.

11.6.4 Věcné právní důvody pro doplnění

Kromě výsledků analýzy (pilířovitost) nařízení samo v řadě míst indikuje svoji vlastní neúplnost. Důvody pro doplnění souhrnně jsou zejména:

- rámcovost nařízení, zejména pro digitální objekty [čl. 1 písm. c) eIDAS];
- vyloučení požadavků na uzavírání a platnost smluv (čl. 2 odst. 3 eIDAS);
  - zahrnuje i požadavky na vůli, projev vůle, jejich vztah atd.;
- vyloučení požadavků na formu (čl. 2 odst. 3 eIDAS);
- neupravení aplikací vytvářejících podpis a systémového prostředí (bod od. 56 eIDAS);
  - nařízení neupravuje předložení obsahu k podpisu podepisující osobě;
- nediskriminace vůči Francii aj. státům, resp. jednotný účinek práva EU v členských státech; nedoplněné nařízení eIDAS má v právním řádu ČR významně horší právní vlastnosti a funkci, než má stejné nedoplněné nařízení v právním řádu Francie a států s podobnou civilní úpravou; k dosažení aspoň rovnocennosti je třeba nařízení doplnit;
- příklad německé implementace ve VDG; VDG není „maximální" implementací, přesto se Německo v řadě ohledů (např. atributy) nezdráhalo nařízení poměrně razantně doplnit, jindy i konkretizovat.

Rámcovost (pilířovitost), vyloučené požadavky z působnosti nebo neupravené oblasti problematiky ponechávají členskému státu prostor pro vnitrostátní implementaci. Srovnání s právními řády Francie, resp. Německa vyjevuje, že taková doplnění jsou nutná, resp. možná.

11.6.5 Důvody pro doplnění pro subjekty veřejného sektoru

Některou nařízením neupravenou problematiku může být vhodné zvlášť upravit pro případ úřadů aj. orgánů veřejné moci. Důvody jsou zejména:

- vydávají často dokumenty charakteru veřejné listiny s presumpcí správnosti;
- není v rozporu s čl. 27 aj. eIDAS;
- vyloučení uzavřených systémů (čl. 2 odst. 2 eIDAS).

K faktickým důvodům možnosti stanovení vyšší úrovně požadavků náleží, že tyto subjekty mívají stacionární povahu buď zcela, nebo aspoň svého zázemí. V jejím rámci je spíše možné plnit i náročnější požadavky na bezpečnost.

11.6.6 Věcné právní důvody proti doplnění

Kromě důvodů pro doplnění existují i důvody proti doplnění, které mohly být důvodem přijetí „minimální" implementace v ČR. Autor tyto důvody připouští, v závorce však uvádí i protiargumenty:

- v nařízení zpravidla chybí výslovné zmocnění nebo aspoň nenormativní upozornění o možnosti doplňovací implementace (sepisovatelé nařízení si zřejmě nemuseli být vědomi potřeby doplnění; přinejmenším z hlediska právních řádů zemí střední Evropy);
- formulace doplnění je obtížná z hlediska dilematu práv podepisující vs. spoléhající osoby (pro řešení tohoto dilematu je třeba formulovat opatrně);
- výsledek doplnění nebude přehledný (chybějící úprava vyvolává zmatky též);
- nekompatibilita technická (německá úprava atributů ve VDG se nezdráhá);
- nekompatibilita právní (německá úprava atributů ve VDG se nezdráhá).

Autor připouští, že zde uvedené důvody představují určité protidůvody, kvůli kterým je nutné při formulaci doplnění nebo konkretizací při implementaci postupovat opatrně.

11.7 Závěr

Soustředíme-li se na právní jednání dle nauky soukromého práva Německa nebo ČR, pak původem právního jednání je lidská vůle, která se chce vnějškově manifestovat projevem, jenž na sebe naváže vůlí chtěné a právem dovolené právní následky. K právnímu jednání pak dojde, je-li tato vůle skutečně vnějškově projevena, a to účinným způsobem.

Ačkoli je právní nauka přesvědčena, že přitom pravidelně dochází k souladu mezi vůlí a projevem, současně připouští, že tomu tak nemusí být vždy. Nikomu nelze doporučit, aby v prostoru běžící dražby zdravil svého známého pozdvižením ruky.

Rozšíření možnosti komunikace prostřednictvím elektronických prostředků umožňuje „pouze" projev vůle formovat a šířit zcela novými a dříve nebývalými způsoby k adresátům. Takové užití má své mnohé výhody, ale může mít i svá úskalí.

Lidská praxe si zpravidla sama najde způsoby, jakými v určitém prostředí mezi sebou mohou osoby navzájem interagovat, aby k omylům pokud možno nedocházelo,

ať již jsou povahy nahodilé, nebo záměrně vyvolané někým s nečestnými úmysly, ale i pro ten případ, že by někdo sebou provedené právní jednání hodlal zpětně popřít.

V praxi 19. a 20. století, se vzrůstem obecné gramotnosti, se ujala zvyklost důležitější právní jednání provádět v písemné formě, stvrzené vlastnoručním podpisem. Pro akty podobné důležitosti v rámci elektronického prostředí či přenosu byla kryptografií navržena technika takzvaných digitálních podpisů, které jsou na území EU po roce 1999 známy spíš pod svým právním názvem, jako takzvané (kvalifikované) elektronické podpisy. Tento text se zabývá právním stavem po nabytí účinnosti nové unijní úpravy v nařízení eIDAS. Byl dokončen asi půlrok po implementaci nařízení eIDAS v Německu. V ČR se časově nacházíme po půlce přechodného období, které uplyne v září 2018.

Institut byl v tomto textu zkoumán nejen z pohledu co nejkvalitnějšího výkladu platného práva EU, ČR a Německa, ale i v úrovni teorie právního jednání obecně a ve srovnání s funkcemi vlastnoručního podpisu konkrétně. Teoretické základy pomáhají vést výklady či návrhy na změny systematicky koherentním způsobem. Zda a jak se bude kvalifikovaný elektronický podpis šířit nebo jak se bude rozvíjet jeho podoba, je stále otevřené téma. Tento text se snaží vysvětlit právní stránku panující situace.

11.7.1 Závěry komparace

Použití metody srovnání právních řádů Německa a ČR v předmětu této práce je rozhodně přínosné již v oblasti teorie právního jednání. Německá teorie se jeví jak propracovanější, tak podstatně bohatší. Též úprava elektronické formy v BGB je přesnější než písemné formy právního jednání učiněném elektronickými prostředky v občanském zákoníku. Současně je též restriktivnější. Německo používá podrobnou úpravu důkazních účinků ve svém civilním procesním soudním řádu ZPO, která v ČR vůbec nemá odpovídající protějšek. Úprava důkazních účinků digitálních objektů jako kvalifikovaný elektronický podpis byla v ZPO vytvořena ovšem spíše pro předchozí platnou právní úpravu v *Signatursgesetz* než pro tu stávající z eIDAS. Němečtí komentátoři i autor vesměs soudí, že z hlediska Německa je nařízení eIDAS v řadě právních aspektů krokem zpět. Německým komentátorům, podobně jako autorovi, též vadí neúplnost úpravy v nařízení eIDAS.

Dovolení elektronického podpisu prostého v ZSVD pro splnění písemné formy právního jednání v občanském zákoníku je zřejmě nevhodné.

Nelze však tvrdit, že by německá úprava implementace nařízení eIDAS byla provedena řádově kvalitněji než implementace česká. Především je velmi zarážející, že Německo přijalo implementační zákon *eIDAS-Durchführungsgesetz* až rok po účinnosti nařízení eIDAS.[18] Český ZSVD, na rozdíl od německého VDG, recipuje digitální objekty z eIDAS pro celý právní řád, zatímco VDG je formulován tak, jako by se aplikace nařízení eIDAS přes všechny oblasti práva rozuměla „samo sebou". Český ZSVD ovšem není zcela důsledný. Recipuje sice použití elektronických podpisů a elektronických pečetí, využívá kvalifikovaná elektronická časová razítka, avšak nerecipuje ve stejné úrovni obecnosti například ty důkazní účinky, které jsou v eIDAS stanoveny.

Německá implementace ve VDG též rozhodně není „maximální implementací", protože řadu mezer nařízení odtažitě pomíjí. Prostřednictvím uložené poučovací povinnosti se ve VDG však dosahuje odpovědnosti za případnou nedbalost zejména podepisující se osoby. Ustanovení zřejmě nahrazuje stanovení povinností pro podepisující nebo spoléhající se osobu. Stejná legislativní technika byla v Německu užita již dříve v *Signatursgesetz*. Český ZSVD je v téže otázce nedostatečný. V právním řádu ČR by však jen poučení ani nemuselo dostačovat. Německý VDG též obsahuje konkretizační ustanovení o zneplatňování (odvolávání) certifikátu. Tato ustanovení dosahují zhruba té úrovně přesnosti úpravy, kterou se vyznačoval v ČR dříve platný ZEP a která v eIDAS chybí. Tuto či podobnou úpravu by bylo vhodné převzít či navrhnout a v ČR doimplementovat.

Z hlediska implementačního zásahu je asi nejvýraznější úpravou stanovení pravidel pro přídavné atributy. Autor je názoru, že určit přídavné atributy může i jen poskytovatel služeb. Atributy stanovené v § 12 VDG však mají právní charakter. Jejich určení ve vnitrostátní implementaci pak napomáhá jednotnému výkladu jejich významu, byť jen v rámci jednoho právního řádu, v případě VDG německého.

Použití komparace pomáhá k pochopení v podstatě všech tří úprav (EU, ČR, Německo). Zcela zvláštní potaz je přitom třeba vzít na odchylnosti práva EU z důvodů jeho zvláštního charakteru práva společenství (Unie).

[18] V části služeb vytvářejících důvěru.

11.7.2 Závěr o předporozumění právního jednání

Právní jednání jako vyjádření vůle je projevem dospělé a poučené lidské vůle, která vznikla dlouhodobou reflexí reality. Vyjadřující osoba ví, jak jejímu projevu bude rozuměno, resp. jak by mu mělo být rozuměno v daném prostředí nebo danými adresáty, jakož i to, jak jednání bude rozuměno prizmatem právního řádu.

Toto (před)porozumění je výsledkem učení se a nápodoby již od dětského věku, předávané z generace na generaci, jakož i školami aj. komunikací ve společnosti. Je symptomatické, že právo plnou svéprávnost přiznává až dosažením plnoletosti, tedy v době dostatečné pohlavní i rozumové vyspělosti. Teprve tehdy má smysl plně započít sebeurčování i právním jednáním.[19] Typicky se člověk snaží *„brát se o vlastní štěstí"*, jak zmiňuje § 3 obč. zák., pojem *sebeurčování* nám pak naznačuje, že složitost lidského štěstí má mnoho různých faset.

Při právním jednání elektronickými prostředky se mnoho osob ocitá v prostředí, které pro ně může být nové a kdy si nejsou jisty, jaké následky jejich počínání vyvolá, jak mu budou jiní rozumět, jaké má právní následky. Lze to snad přirovnat k situaci rozpaků, když si máte zcela sami v cizině obstarat některou základní potřebu jako jídlo nebo dopravu, přičemž neznáte místní řeč ani zvyky, v horším případě ani znaky písma.

Tvůrci systémů pro elektronické právní jednání proto učiní dobře, když se přidrží takových forem, které jsou v elektronickém světě již zaběhlé. Systémy pro elektronické právní jednání by ale zřejmě mohly využít i formy zcela nové. Podmínkou pro využívání však je, aby budoucí uživatelé měli možnost připravit se „nanečisto", a to nejlépe interaktivním způsobem. Pochopitelně, že jim nová forma musí poskytnout i nějaké výhody, které dřívější formy neposkytují.

Autor přitom nepochybuje, že se pro právní jednání i v elektronickém prostředí udrží i forma obdobná současné písemné formě, neboť je to jazyk, resp. právní jazyk, který umožňuje zachycení podrobností právního jednání, jež jsou v řadě případů potřebné. Pro jeho potvrzování pak stále bude zapotřebí určitá forma „podpisu". I pro tyto formy právního jednání je a bude zapotřebí určité předem získané jistoty, jak se takové jednání provádí a jaké má následky. Povinnost poučení[20] dle německého práva je z toho pohledu nejen požadavkem právním, ale i určitého uvádění do praxe. Určité poučení zájemcům o „elektronické podepisování" snad přináší i tento text.

[19] O sebeurčení u právního jednání hovoří Flume. Srov. 3.3.2.
[20] Srov. 7.3.3.

11.7.3 Neúplnost eIDAS, vhodnost a možnosti podrobnější implementace

Jedním ze závěrů tohoto textu nutně je upozornění na neúplnost nařízení eIDAS a z toho plynoucí právní nejistoty. V kontextu samotného práva EU byly již samostatně shrnuty v závěru kapitoly o nařízení.[21]

Jednou z možných hypotéz toho, proč bylo nařízení eIDAS koncipováno představeným způsobem, je, že sepisovatelé návrhu pocházeli ze zemí ovlivněných francouzským *Code civil*.[22] V těchto státech bude řada právních povinností odvoditelná jen z technických norem, které jsou prováděcími akty nařízení eIDAS vyhlašovány.

V rámci výše předcházejícího shrnutí (srov. 11.6) je vyložena právní argumentace odůvodňující, že v případě nařízení eIDAS je právně možná mnohem podrobnější implementace, než která byla v ČR provedena, aniž by se členský stát dostal do rozporu s pravidly evropského práva.

Obtížnost podrobnější implementační úpravy dnes spíše spočívá v tom, že je obecně nelehké řešit rozdělení odpovědnosti mezi podepisující osobu a spoléhající se osobu. To však neznamená, že by se na úsilí o přesnější úpravu mělo rezignovat.

Níže jsou nalezeny ty oblasti práva, které zejména je vhodné implementovat v právním řádu. Výklad je přitom soustředěn na implementaci v kontextu právního řádu ČR, neboť stav a potřeby jsou zde pro autora nejpřehlednější. Koncentrovaně jsou zde probrány ty oblasti, v nichž buďto implementace chybí, nebo ji autor považuje za sice provedenou, ale chybně nebo ne dostatečně. Neprovede-li implementaci zákonodárce, měly by uvedeným oblastem věnovat pozornost aspoň smluvní úpravy. Níže provedené dělení není dle jednotného hlediska, ale věcně na tři oblasti a na dvě oblasti odvětví práva.

11.7.3.1 Hlavní doplnění a konkretizace implementace v ČR

Do českého práva by se rozhodně měl doimplementovat způsob stanovení kryptografických schémat a stanovení působnosti některého úřadu.[23] Uvedené je důležité nejenom z hlediska bezpečnosti a důvěryhodnosti vyšších verzí elektronického podpisu, z hlediska právní jistoty každého, ale i s ohledem na společnou technickou normalizaci. Je pochopitelně vhodné, aby taková metodika byla otevřená budoucím

[21] Srov. 6.16.
[22] Srov. 6.17.
[23] Srov. 8.8.1.

kryptografickým schématům. Měl by se řešit i vztah k podpisovým schématům, užívaným v jiných členských státech.

Autorovi by se kvůli lepší právní jistotě spoléhající osoby zamlouvalo, kdyby způsob ověřování totožnosti[24] žadatele o kvalifikovaný certifikát byl stanoven podle dříve používané úpravy, tj. aby se vyžadovala aspoň jedna úvodní osobní návštěva certifikované fyzické osoby a její prokázání se aspoň dvěma osobními doklady, z čehož jeden by typicky měl být občanský průkaz nebo cestovní pas.

Autor též doporučuje, aby existovala vhodná právní úprava pro vkládání jiných znaků certifikované osoby do kvalifikovaného certifikátu. Částečnou inspirací může být německá úprava[25] v § 12 VDG. Výhodou je získání jednotnosti právního významu položek certifikátu na státní úrovni, nebo aspoň jednotné úrovně ověření údajů a lepší právní jistota pro spoléhající se osobu. Nevýhodou je omezení pružnosti kvalifikovaného poskytovatele upravit své postupy na míru potřeb svých zákazníků, což mu umožňuje se i marketingově profilovat. Vkládat do kvalifikovaného certifikátu jakékoli znaky má smysl především tehdy, pokud jsou znaky aspoň nějak ověřovány. V některých případech (např. adresa elektronické internetové pošty) však může mít smysl do certifikátu vložit i jen tvrzený údaj. Kvalifikovaný certifikát pak je aspoň dokladem o tom, že stejný údaj tvrdila certifikovaná osoba i vůči někomu jinému dříve, totiž vůči kvalifikovanému poskytovateli při žádosti o kvalifikovaný certifikát. Nalézt vhodnou rovnováhu mezi výše uvedenými zájmy a potřebami může vyžadovat analýzu stávající praxe i konzultace s kvalifikovanými poskytovateli. Za ideální by autor považoval, pokud by zákonodárce zavedl možnosti omezení použitelnosti kvalifikovaného certifikátu pro elektronický podpis (srov. 11.3 výše), byť jen v rámci právních vztahů upravených právním řádem ČR.

Je velmi vhodné, aby česká implementace byla doplněna o výslovné oprávnění žádat o zneplatnění[26] kvalifikovaného certifikátu, zejména samotnou certifikovanou osobou (žadatelem o certifikát apod.). Zvážit lze i obdobné oprávnění i pro ty osoby, které potvrzovaly některé znaky, jež jsou v kvalifikovaném certifikátu uvedeny. Inspirací zde může být jak německá úprava[27] v § 14 VDG, tak dřívější úprava v ZEP a v něm existující institut držitele certifikátu.

[24] Srov. 8.8.2.
[25] Srov. 7.3.2.
[26] Srov. 8.8.3.
[27] Srov. 7.3.5.

České právo by mělo stanovit působnost subjektu,[28] který za členský stát oznamuje vůči Komisi provedení nebo zánik certifikace QSCD/QSealCD, i způsob jeho činnosti. Autor nepovažuje situaci, když český právní řád tuto působnost a činnosti opomíjí, za situaci s existencí nařízení slučitelnou. Jakýkoli český subjekt vyrábějící či unikátně nasazující QSCD/QSealCD pak bude zřejmě odkázán nejen na zahraniční či přeshraniční určené subjekty certifikující bezpečnost produktů informačních technologií (určené zkušebny[29]), ale i na přeshraniční úřad, který Komisi oznamuje provedení nebo zánik certifikace QSCD/QSealCD. Takový přeshraniční úřad se zjevně bude řídit právním řádem toho členského státu, který jeho působnost zřizuje a jemuž se bude muset podřídit i případný český subjekt uvádějící na trh QSCD/QSealCD. Činnost „určených zkušeben" obecně může být přeshraniční. Není nutné, aby se v ČR zřizovaly subjekty určených zkušeben. ČR by však měla disponovat úřadem, který bude schopen služeb i přeshraničně určených zkušeben využívat a případně provádět oznamování a zánik certifikací QSCD/QSealCD.

Dle autora by měl být proveden rozbor, zda jsou vyšší verze elektronického podpisu nebo pečeti využitelné ve veřejné správě pro stvrzování nikoli pouze dokumentů, ale rovněž obecných elektronických dat. Je-li tomu tak, pak by implementace měla být doplněna i o příslušnou recepci nejen ve vztahu k dokumentům, ale i k těmto datům.[30]

Autor považuje za právně nutné, aby česká implementace zahrnula aspoň velmi obecné stanovení povinností podepisující osoby.[31] Inspiraci je možné hledat v dřívější úpravě v ZEP, ale i v německé úpravě[32] poučovacích povinností[33] podle § 13 odst. 1 VDG, nebo dle dříve účinného německého Signatursgesetz nebo § 6 Signatursverordnung. Úprava by měla být spíše obecná. Neměla by restriktivně ovlivňovat poskytování služeb vytvářejících důvěru, jejichž technická implementace se teprve připravuje. Případné konkrétnější povinnosti by buď měly být uložitelné až prováděcí vyhláškou, nebo být stanoveny určité zásady jejich odvození z technických parametrů služeb vytvářejících důvěru. Taková stanovení povinností by v zásadě měla nahrazovat právní deficit povinností, který v jiných právních řádech bude plynout čistě

[28] Srov. 8.8.4.
[29] Srov. 6.1.6.2.
[30] Srov. 8.8.5.
[31] Srov. 8.9.4.
[32] Německá úprava vždy dbala především na to, aby si držitel QSCD byl vědom, že vytvoření QES má stejné právní účinky jako vlastnoruční podpis.
[33] Srov. 7.3.3.

z existence a používání technických norem.[34] Úprava by též měla brát ohled na možné varianty automatizace vytváření elektronických podpisů (srov 11.7.3.3 níže).

Ačkoli určité povinnosti spoléhajících osob a stran lze z nařízení implikovat,[35] z hlediska právní jistoty podepisujících nebo pečetících osob by bylo vhodné stanovit aspoň ty nejobecnější povinnosti i pro spoléhající se osoby. I v jejich případě by se mělo jednat aspoň o takové povinnosti, které v jiných právních řádech budou plynout čistě z existence a používání technických norem.Chyba: zdroj odkazu nenalezen

Zvláštní povinnosti při vytváření i při ověřování platnosti vyšších verzí elektronického podpisu lze klást na veřejnoprávní subjekty (srov. 11.7.3.5 níže).

11.7.3.2 Doplnění a konkretizace implementace v ČR – popiratelnost

Otázky popiratelnosti vyšších verzí elektronických podpisů, jako jsou QES nebo $AdES_{QC}$, druhů a rozsahu použitelných námitek, jsou a budou dle autora kontroverzní. Nařízení eIDAS i s vhodnou právní implementací (např. výše dle 11.7.3.1 nebo níže dle 11.7.3.3) dokáží vhodně snížit rizika podepisující osoby a spoléhající osoby, ale nedokáží je zřejmě nikdy odstranit úplně beze zbytku. Před pouhým rokem by nikdo nedokázal předpovědět ani odhadnout, že vůbec může vzniknout zranitelnost ROCA,[36] tím méně apriorně navrhnout vhodnou právní úpravu důkazních pravidel, která by tehdy neznámou zranitelnost dokázala vzít v potaz.

Na druhé straně je nutné reflektovat, že vyšší verze elektronických podpisů, jako jsou QES nebo $AdES_{QC}$, představují nezanedbatelný výsledek úsilí o technické bezpečí i o právní jistotu. Autor se proto domnívá, že v rámci soukromého práva je vhodné elektronickým podpisům, jako jsou QES nebo $AdES_{QC}$, u nichž byla ověřena technická platnost, přiznávat pravost, a to na úrovni již zmiňované skutkové domněnky[37] pravosti. Do úvahy přichází, zda pro tyto účely do českého práva formálně nezavést i důkazy *prima facie*. V obou případech je výhodou to, že uvedené digitální objekty získávají i určitý právně důkazní význam, aniž by se pro ně zaváděla úroveň právní domněnky. Ta je zde v elektronické praxi příliš vysoká pro vyvrácení. Rozdíl mezi QES a $AdES_{QC}$ (ev. AdES) pak bude spočívat v tom, jaké druhy prokazatelných námitek budou dostačovat

[34] Srov. 6.17.
[35] Srov. 8.9.5.
[36] Srov. 6.15.7.
[37] Srov. 9.4.1.

k otřesení zmíněnou skutkovou domněnkou. Stejné důkazní pravidlo si tedy poradí s několika různými provedeními vyšších verzí elektronického podpisu.

Na základě první skutkové domněnky o pravosti podpisu pak dle autora lze použít další jednotlivé skutkové domněnky, že původcem podepsaných dat (elektronického dokumentu) je podepsaná osoba,[38] že podepsaná data jsou úplná a neporušená, že obsah podepsaných dat (elektronického dokumentu) buď vyjadřuje vůli podepsané osoby a je právním jednáním, nebo že jimi podepsaná osoba ověřila pravdivost podepsaného obsahu v datech (elektronickém dokumentu). Uvedené skutkové domněnky nahrazují dříve platnou úpravu,[39] která spíše nebyla kongruentní se skutečně obsaženými požadavky v ZEP. Vzhledem k neúplnosti úpravy v nařízení eIDAS autor nepovažuje za bez dalšího použitelnou právní domněnku z druhé věty § 565 obč. zák.[40] Vzhledem ke stejné neúplnosti lze různě napadat i výše uvedené skutkové domněnky.

Vznášení námitek proti nim lze nicméně omezit doplněním implementace o vhodné obecné povinnosti podepisující osoby (srov. 11.7.3.1). Jejich stanovení tak není pouze otázkou spadání pod hlavní chybějící implementační doplnění a konkretizace, ale i pod zde probíranou otázku popiratelnosti a jejího omezení vhodnou implementací.

Další nezávislou implementačně doplňkovou problematikou mohou být vlastnosti aplikace vytvářející elektronický podpis (tzv. SCA[41]) a širšího systémového prostředí, ve kterém se aplikace využívá. Jejich náležitosti jsou z působnosti regulace nařízením eIDAS záměrně vynechány.[42] Dle názoru autora by vnitrostátní implementace tuto mezeru zaplnit mohla. Podle míry automatizace vytváření podpisu (individuální, dávkový, elektronickým agentem) se ovšem požadavky mohou i značně lišit. Autor se v současné fázi vývoje domnívá, že příliš podrobné určení vlastností SCA a systémového prostředí může být provedeno i nevhodně a potenciálně podvázat rozvoj takových aplikací i jejich nasazování. Může být ale vhodné určit vlastnosti SCA a systémového prostředí velmi obecně. Požadavky by měly být i realistické. Vyšší úroveň požadavků je

[38] Tj. osoba uvedená v kvalifikovaném certifikátu, na němž je QES nebo $AdES_{QC}$ založen.
[39] Srov. 8.9.1 (seznámení se s obsahem), 8.9.2 (projev vůle v obsahu datové zprávy) a 8.9.3 (integrita, soulad s originálem).
[40] Srov. 9.4.1.
[41] Signature Creation Application.
[42] Bod odůvodnění 56 nařízení eIDAS.

zde ale právně i technicky možná a žádoucí pro stranu veřejnoprávních podepisujících (srov. 11.7.3.5).

11.7.3.3 Doplnění a konkretizace implementace v ČR – automatizace

Je žádoucí, aby právní řád (ČR) reflektoval, že v elektronické praxi je příležitostně potřeba využívat automaticky vytvářená elektronická stvrzení technologií digitálních podpisů, a to zhruba v té úrovni technologie, kterou je běžně implementován $AdES_{QC}$. Tyto potřeby mají v současnosti zřejmě nejčastěji subjekty veřejné správy v rámci různých druhů správních řízení, mohou je ale potřebovat i soukromé právnické osoby, vzácněji i fyzické osoby.

Tyto případy užití byly v ČR dříve řešeny technicky a právně pomocí elektronické značky.[43] Nařízení eIDAS takový zvláštní právní institut nezná, ani znak automatizace výslovně nestanoví pro žádný druh elektronického podpisu.[44] Autor zastává v ČR zřejmě nový právní názor, že automatizované stvrzení je běžně shodně možné provést elektronickým podpisem AdES nebo elektronickou pečetí AdESeal,[45] což je ostatně přístup, který používá i samotné nařízení eIDAS.Chyba: zdroj odkazu nenalezen V zásadě shodně je možné pro automatické stvrzování použít i elektronický podpis $AdES_{QC}$ nebo elektronickou pečeť $AdESeal_{QC}$, které se budou navíc těšit z lepší průkaznosti o jednajícím subjektu, jehož totožnost bude zachycena v příslušném podkladovém kvalifikovaném certifikátu. Tento přístup vychází zejména z jinak pojatého významu zaručené elektronické pečeti.Chyba: zdroj odkazu nenalezen Dobře odpovídá obecné právní zásadě rovnosti subjektů, tj. i právnických osob a fyzických osob vůči sobě. Širší odborná technická i právní veřejnost by měla tento výklad prozkoumat. Orgán dohledu jej může konzultovat s Komisí. Bude-li výklad shledán za přijatelný, bylo by vhodné právní řád ČR doplnit v tom smyslu, aby výše uvedená ekvivalence stvrzování byla využívána pravidelně. Implementace zde spíše než přijetí doplňujících či konkretizačních implementačních ustanovení znamená metodický výklad a konzistentní využívání výše zmíněné ekvivalence pro automatizovaná stvrzení v jiných právních předpisech právního řádu.

Pro soukromé právo může být navíc vhodné výslovně upravit právní jednání elektronickým agentem. Výslovná úprava právního jednání elektronickým agentem je

[43] Srov. 8.9.7.
[44] Srov. 6.16.15.
[45] Srov. 6.6.4.

v českém právním řádu zřejmě nutná v případě právnické osoby, v jejímž případě platné právo zásadně počítá s jednáním jejího zástupce, typicky některé osoby fyzické. Výjimkou je právní jednání pomocí elektronického obchodu, kde úprava vznikla transpozicí unijních směrnic a uvádění zástupce nutné není (srov. 11.7.5 níže). Z hlediska skutečného charakteru provozu i skutečných potřeb právnických osob je totiž nepřirozené, aby provoz automatizovaného systému, často v nepřetržitém provozu, musel být vázán na jakoukoli fyzickou osobu, zástupce. Úprava by proto měla spočívat v připuštění bezprostředního právního jednání přímo právnickou osobou. V technické i právní praxi je následně též nezbytné zajistit, aby pro protější strany bylo rozeznatelné, že se jedná o právní jednání a které konkrétní právnické osoby. Použití zaručené elektronické pečeti $AdESeal_{QC}$ je jedním z prostředků, s jehož pomocí uvedené rozeznání lze zajistit v obou rovinách, technické i právní. Uvedené neznamená, že by použití zaručené elektronické pečeti $AdESeal_{QC}$ znamenalo podpis a potažmo splnění písemné formy právního jednání. Taková možnost je zvážitelná zcela samostatně. Bez provedení dalších analýz se autor nedomnívá, že by takové rozšíření až na písemnou formu bylo nyní vhodné. Uvedené neznamená ani to, že by právnické osobě bezprostředně přičitatelné právní jednání mělo být umožněno vždy. Uvedené je vhodné pro elektronického agenta jako zástupce právnické osoby sui generis (kvazi zástupce), který bývá v činnosti nepřetržitě, který ale nemá samostatnou lidskou vůli a jeho nasazení podléhá řízení ze strany vedení společnosti. Použití zaručené elektronické pečeti $AdESeal_{QC}$ by ani nemělo být výlučným způsobem, jak jednání právnické osoby elektronickým agentem dovolit. Jen z nařízení eIDAS lze dále například využít (kvalifikované) certifikáty pro autentizaci internetových stránek (webového místa).

Ohledně otázky možnosti použití QES nebo QESeal pro automaticky vytvářená stvrzení je autor zdrženlivý. Aspoň zatím nepovažuje otázku za kladně zodpověditelnou.[46]

Pokud by se autorův výše zmíněný přístup k výkladu použitelnosti elektronických podpisů nebo elektronických pečetí pro automatizovaně vytvářená právní jednání (jednání elektronickými agenty) a jiná automatizovaná stvrzování neujal, nezbývalo by českému zákonodárci pravděpodobně nic jiného než v právním řádu obnovit institut elektronické značky a nechat jej působit souběžně s právními pojmy z nařízení eIDAS. Proti tomuto způsobu lze především namítnout to, že může snižovat

[46] Srov. 6.6.5.

efektivnost jednotné unijní úpravy a jako takový být předmětem kritiky, včetně námitky neloajality členského státu. Autor však nepovažuje za uspokojivou ani možnost, že by automatické stvrzování bylo dostupné pouze právnickým osobám pomocí zaručené (či dokonce kvalifikované) elektronické pečeti, nikoli však osobám fyzickým, pro které jsou tyto druhy elektronické pečeti nepoužitelné. Stejně nepraktické a až právně diskriminující je pak naopak zase vyžadování vazby na fyzickou osobu, zastupující právnickou osobu při právním jednání elektronickým agentem. Zde představený výklad a doporučení naopak uvedené potřeby řeší.

11.7.3.4 Doporučení revize v soukromém právu ČR

V soukromém právu si dle autora zaslouží revizi zákonodárce či normotvůrce dvě oblasti, a to sice jednak ověřování podpisů soukromých listin podle katastrálního zákona, jednak připuštění elektronického podpisu prostého pro splňování písemné formy právního jednání. Obě tyto zmíněné platné úpravy vzešly z adaptačního zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, a ze změnového zákona č. 298/2016 Sb.

Dle § 64 odst. 1 písm. a) katastrální vyhlášky č. 357/2013 Sb. je pravý[47] (pravost je považována za prokázanou) takový uznávaný elektronický podpis, jehož podkladový kvalifikovaný certifikát obsahuje jméno (jména) a příjmení a údaj umožňující jednoznačnou identifikaci podepisující osoby (identifikátor MPSV). Tato koncepce je v rozporu s tím, jak bývá *pravost* běžně chápána, tedy v tom smyslu, že podpis je pravým vyjádřením vůle podepisující osoby, která bývá následně vztahována i na celou podepsanou písemnost. Citované ustanovení dokáže zajistit pouze to, že k osobě, jejíž uznávaný elektronický podpis je uveden, je možné z údajů vedených v informačních systémech MPSV zjistit nebo ověřit, na základě jednoznačného identifikátoru MPSV, další údaje[48] o podepisující osobě. Výstižnou formulací zde je, že z takového elektronického podpisu lze provést ověření pravosti jiných údajů o (údajně) podepsané osobě. Nikoli však to, že se jedná o podpis pravý. Nikoli to, že podepsaná písemnost představuje pravý projev vůle podepsané osoby. Nikoli ani to, že by existovala jakákoli „úřední" osoba, která by daný konkrétní podpis jakkoli ověřila.

Uvedený koncept je v materiálním rozporu i s alternativním způsobem zjištění pravosti elektronického podpisu postupem podle § 64 odst. 1 písm. b) katastrální

[47] Srov. 5.1.5.2 a 8.9.11.
[48] Například adresu bydliště, datum narození apod.

vyhlášky č. 357/2013 Sb., dle nějž podepsaná osoba uznává před katastrálním úřadem, tedy při osobní přítomnosti, že obsah písemnosti v elektronické podobě je projevem její vůle, jakož že je i držitelem příslušného kvalifikovaného certifikátu. Je pak v rozporu i s dalšími běžnými možnostmi zajišťování pravosti vlastnoručního podpisu. Ten je buď úředně ověřený (§ 7 odst. 2 katastr. zák. č. 256/2013 Sb.), nebo alespoň dle § 63 odst. 1 písm. a) a c) katastrální vyhlášky č. 357/2013 Sb. ověřen prohlášením advokáta o pravosti, nebo opět uznáním před katastrálním úřadem. Všechny jiné způsoby ověření pravosti, včetně úředně ověřeného podpisu, tedy předpokládají osobní přítomnost podepsané osoby u příslušné podpis ověřující osoby. Jedná se o „úředního svědka" vytvoření podpisu či jeho uznání za vlastní (pravý), ve vztahu ke konkrétní písemnosti.

Pouze shora citovaný případ § 64 odst. 1 písm. a) katastr. vyhl. č. 357/2013 Sb. představuje výjimku z jinak zavedených pravidel ověřování podpisu. Toto ustanovení proto představuje neodůvodněnou výjimku a dle autora by mělo být v právním předpisu zrušeno, neboť neodpovídá ani označením (pravost), ani zajišťovacím postupem (chybí „úřední svědek" podpisu). Perspektivně může být nahrazeno novou úpravou, která bude obsahovat elektronické notářství nebo úřední ověřování elektronických podpisů.[49] Současná právní úprava trpí přesně tím nedostatkem, který by legislativa elektronických podpisů mít neměla, totiž že z důvodů plnění veřejnoprávních požadavků se vytváří riziko v soukromoprávních vztazích (srov. výše 11.2.1), zde v majetkové sféře elektronicky podepisující osoby. Za pozornost stojí i legislativní styl. Bylo by vhodnější, aby se v platném právu používal důsledně například obrat „ověřený podpis", zatímco pojem pravost byl rezervován jen pro popis skutkového stavu, nebo pro případná důkazní pravidla soudního řízení, jako jsou skutkové nebo právní domněnky apod. Nelze totiž vyloučit, že pravost i úředně ověřeného vlastnoručního podpisu může být popřena. Dobrý normotvůrce nebude mást adresáty práva formulacemi, které u některých mohou vyvolávat nerealistická očekávání.

Připuštění elektronického podpisu prostého pro splňování písemné formy právního jednání, které plyne z § 7 ZSVD, autor nepovažuje za vhodné, jelikož do značné míry ruší varovací funkci formy a tím i právní ochranu podepisující osoby.[50] Definici vyhoví prakticky všechny druhy techniky[51] elektronických podpisů, z nichž ale

[49] Vytvoření takové služby a její právní úpravy je možné, byť přináší některé netriviální potíže, které nejsou při ověřování vlastnoručního podpisu běžné.
[50] Podrobně srov. 9.4, 5.1.5, 5.1.3 a 6.4.
[51] Srov. 4.5.

pouze digitální podpis a biodynamický podpis mají určitou autentizační funkci, ostatní druhy techniky jsou bez dalšího navíc i důkazně bezcenné.

Dle německého právního řádu je pro písemnou formu právního jednání prostřednictvím elektronické formy dovoleno použití pouze kvalifikovaného elektronického podpisu (QES) a judikatura vyloučila i použití biodynamického podpisu.[52]

Není-li provedena analýza rizik, kterou autor již dříve doporučil,[53] autor navrhuje pro splnění písemné formy právního jednání i v právním řádu ČR ponechat pouze QES. Pokud si ale formu právního jednání volí ze zákona strany, musí jim zůstat i svoboda způsobu stvrzení právního jednání, tedy při právním jednání učiněném elektronickými prostředky i použití jakéhokoli druhu techniky elektronického podpisu.

11.7.3.5 Doporučení implementace pro veřejné právo ČR

Listiny vyhovující podmínce v § 134 o. s. ř. se označují jako veřejné listiny a těší se takzvané presumpci správnosti.[54] Tyto listiny lze již v současnosti často vydat i v elektronické podobě, a i tyto veřejné listiny v elektronické podobě se těší presumpci správnosti. Presumpce správnosti veřejných listin je pro český právní řád natolik charakteristická vlastnost, že ji nelze z právních předpisů veřejného práva třeba i vědomě vypustit, aniž by to přineslo zborcení zavedených správních postupů v jiných oblastech. Zřejmě právě presumpce správnosti je důvodem, proč adaptační zákon předepsal, že podle jeho § 5 ZSVD musí veřejnoprávní podepisující podepisovat výlučně pomocí QES a podle § 11 ZSVD musí být podepsaný elektronický dokument opatřený QTS. Přikázené digitální prvky plní ochrannou funkci daných veřejných listin.

Jestliže však výše autor doporučuje výklad, že v případě soukromých listin se u písemností opatřených QES má uplatňovat nejvýše skutková domněnka pravosti podpisu a následně též skutková domněnka správnosti podepsaného obsahu (srov. 11.7.3.2), jsou tyto důkazní účinky mnohem slabší než v případě veřejné listiny, opatřené stejným QES. Presumpce správnosti se vztahuje přímo na obsah veřejné listiny. V případě elektronického provedení bývá QES často jediný ochranný prvek, který je přítomen, neboť QTS lze opatřit libovolně. V případě tradiční papírové podoby

[52] Srov. 5.2.5.2.

[53] KMENT, V. Nahradí ..., cit. dílo, s. 35.

[54] Alternativní určení podmínky je v § 567 obč. zák. Konkurence mírně různých definičních podmínek veřejné listiny ve dvou různých právních předpisech je někdy i předmětem kritiky, zde se nám však jedná pouze o vystižení jejich podstatné právní vlastnosti, presumpce správnosti.

veřejné listiny však ochranné prvky rovněž nebyly příliš vyšší. Kromě podpisu oprávněné úřední osoby se navíc vyskytoval pouze otisk úředního razítka, jehož napodobení v současnosti již nepředstavuje technickou potíž.

Mnohem vyšší úroveň spolehlivosti obsahu veřejných listin musí tedy spočívat v něčem jiném, než jsou ochranné prvky použité na vyhotovení listiny, ať se jedná o její elektronickou, anebo listinnou (papírovou) podobu. Tím něčím jiným je prostředí, v němž jsou veřejné listiny produkovány a v němž se i vede trvalá evidence vytvořených veřejných listin, a to včetně jejich původního obsahu. V rámci obecných agend jsou listiny součástí spisů, jednotlivé spisy i spisy navzájem pak jsou upraveny pravidly spisové služby, částečně obecně závaznými právními předpisy a částečně vnitřními předpisy, přizpůsobujícími spisovou službu na míru konkrétního správního úřadu, soudu apod.

Záležitosti „prostředí", v němž veřejné listiny jsou produkovány a uchovávány, mají více aspektů. Jednou z již zmíněných náležitostí jsou elektronické spisy a elektronická spisová služba. V textu jsme se věnovali pozadí[55] zpracovávání listin u veřejnoprávních původců. Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby, není téměř dva roky od účinnosti nařízení eIDAS vůbec přizpůsobena terminologii nařízení, ale zůstává ve znění poplatném ZEP. I z provedené letmé rešerše jen například přípustných formátů elektronických dokumentů plyne, že oblast není upravena pro adresáty práva přehledně. Jedná se o důsledek resortismu a segmentace veřejného práva.[56] Systémy spisové služby by však měly tvořit horizontálně jednotnou úpravu napříč všemi resorty a vhodně i pro státní správu soudů. Měly by být co nejsnadněji použitelné. Autor je názoru, že taková změna vyžaduje organizačně institucionální změnu. Problematika spisové služby si vyžaduje vysokou pozornost a měla by být vyčleněna přímo pod vedení e-governmentu.[57] Spisová služba musí představovat pevný a pravý dokumentární základ o řízeních, a to i v případě komunikace dokumenty v elektronické podobě, s elektronickými podpisy. Navíc by

[55] Srov. 9.2.

[56] Německé veřejné právo trpí stejnou segmentací jako české, neboť vychází z obdobných ústavně právních premis.

[57] Historicky byla spisová služba přičleněna k tematice archivování. Archivace je další fáze záchovy vybraných významných dokumentů. Její těžiště však spočívá spíše v kulturním významu archiválií. Oproti tomu spisy a dokumenty mají ve fázi před archivací význam především právní. Nové elektronické provedení vyžaduje významně odlišnou praxi, než která byla užívána dříve, a klade nové, jiné a technicky náročnější požadavky.

měla být snadno použitelná, a to napříč resorty, neboť veřejné právo příležitostně může vyžadovat komunikaci či spolupráci zcela různorodě zaměřených úřadů.[58]

Dalšími aspekty „prostředí" v němž vznikají veřejné listiny jsou okruhy požadavků bezpečnosti, tj. organizační, fyzické, technické a personální požadavky. Popisovat je zde přesahuje účel textu. Z hlediska problematiky elektronických podpisů je však třeba upozornit, že nařízení eIDAS tyto okruhy požadavků v případě subjektů veřejné správy (v ČR veřejnoprávní podepisující) ponechává mimo svou působnost, a to záměrně, neboť činnost veřejné správy na své vnitřní provozní straně je zásadně mimo pravomoce, které byly na EU přeneseny zakládajícími smlouvami. Českému zákonodárci by proto nemělo nic bránit v tom, aby pro uvedené okruhy předepsal, v souvislosti s nařízením eIDAS, další přídavné požadavky. Na rozdíl od stanovení povinností obecným uživatelům se zde vůbec nemusí obávat, že by se dostal do střetu s unijní úpravou. Může tak činit i formou obecně závazných předpisů, jakož i formou vnitřních předpisů v rámci veřejné správy, nebo jejich vhodnou kombinací. Takové přídavné požadavky mohou významně zvýšit bezpečnost vytvářených elektronických podpisů, jakož především i produkci a evidenci celých veřejných listin. Lze předepsat konkrétní požadavky na aplikace vytvářející podpis, na systémové prostředí, na zabezpečení kybernetické bezpečnosti atd.

11.7.4 Nízká používanost a možnost jiných koncepcí

Po 17 letech od zavedení evropskou směrnicí DirES používají kvalifikovaný elektronický podpis stále jen jednotky procent populace. Snazší používání považuje autor pouze za jeden přístup k tomuto jevu. Vhodným až nutným se mu jeví přehodnotit dosavadní přístupy a pokusit se navrhnout takový model používání, který by právně omezil rizika nebo finanční hodnotu rizik. V rámci souhrnu je výše uvedeno několik návrhů řešení jdoucích takovými směry.[59]

Téměř zcela jistě lze očekávat rozvoj vytváření kvalifikovaného podpisu na dálku, poskytovaného formou kvalifikované služby vytvářející důvěru. Dosud sice

[58] Kupříkladu služba vzdáleného nahlížení do spisů napříč resorty vyžaduje mimo jiné mít funkční systém elektronické identifikace, zajištěný státem. V ČR však vůbec nevznikl zdola, ani jako reflexe této potřeby e-governmentu, ale až jako druhá část implementace nařízení eIDAS v oblasti elektronické identifikace, zákonem č. 250/2017 Sb. o elektronické identifikaci, který bude účinný od 1. 7. 2018.

[59] Srov. 11.3 a 11.4

nebyla přijata a Komisí vyhlášena odpovídající technická norma, služba však již je v EU poskytována,[60] zřejmě po alternativním certifikačním postupu používaného QSCD.

11.7.5 Elektronické právní jednání právnické osoby a elektronická pečeť

Nařízení eIDAS zavedlo institut elektronické pečeti. Zaručená nebo kvalifikovaná elektronická pečeť umožňuje, aby původ pečetí opatřených dat byl přičten přímo určité právnické osobě, aniž by se nutně vyjadřovalo, která fyzická osoba z právnické osoby danou elektronickou pečeť vytvořila. Pečeť ale není podpisem.

Analýza právní úpravy EU a potažmo ČR ukazuje, že v případě elektronického obchodu, jako zvláštního druhu elektronického agenta, provozovaného právnickou osobou, není obsažen požadavek na určování fyzického zástupce právnické osoby. Tato právní úprava je v praxi masově a dlouhodobě využívána, takto uzavírané smlouvy jsou přičítány přímo právnické osobě. Zdroj úpravy pochází z unijního práva. Pro uzavření těchto smluv není běžně vyžadována písemná forma právního jednání. Pro povinně poskytované informace, které se dle zkoumaných úprav poskytovat musí, se dle práva ČR používá takzvaná textová podoba. Pro její potvrzení je možné přídavně využít i zaručenou elektronickou pečeť, takové potvrzení je však ryze dobrovolné, právně není nutné a technicky se zatím nepoužívalo. Bude záležitostí praxe, zda vedle dnes již běžné autentizace internetových stránek se technicky ujme i další dobrovolný bezpečnostní a právní mechanismus.

V případě jiných elektronických právních jednání, pro něž český právní řád nestanoví písemnou formu jako povinnou, není využití zaručených elektronických pečetí sice vyloučeno, ale nemusí dostačovat, neboť taková pečeť nebude bez dalšího považována za projev vůle a jednání zástupce, kterým je typicky fyzická osoba.

Za zváženíhodné proto autor považuje, zda neuvolnit požadavky českého právního řádu tak, aby při soukromém právním jednáním elektronickým agentem, nevyžadujícím dle práva písemnou formu, dostačovalo i stvrzení zaručenou elektronickou pečetí. Při takovém scénáři vynechání fyzického zástupce dobře odpovídá praktickým potřebám právnických osob i realitě funkce technických systémů.

[60] Jmenovitě Itálie.

11.7.6 Kvalifikovaný elektronický podpis vs. vlastnoruční podpis

Kvalifikovaný elektronický podpis (QES) byl navržen tak, aby nahradil vlastnoruční podpis. Dle čl. 25 odst. 2 eIDAS má kvalifikovaný elektronický podpis právní účinek rovnocenný vlastnoručnímu podpisu.

Celý tento text se nicméně musel věnovat zjišťování mnoha podrobností, které v souvislosti s QES vyvstávají. Z hlediska účinků splňování formy je QES přijatelný všude tam, kde rozhodné právo připustí elektronickou podobu pro písemné právní jednání. Přijatelnost se tedy řídí dovolením písemnosti v elektronické podobě.

Z hlediska důkazního práva se však ekvivalence dle čl. 25 odst. 2 eIDAS neuplatňuje. Jak autor v textu,[61] tak německý zákonodárce[62] jsou názoru, že reality vytváření vlastnoručního podpisu a kvalifikovaného elektronického podpisu jsou natolik odlišné, že vyžadují odlišné posuzování. V rámci soukromého práva považuje autor i německý zákonodárce za vhodné z technické platnosti podpisu QES usuzovat na pravost podpisu v úrovni důkazu *prima facie*, tj. skutkové domněnky. Z pravosti podpisu QES se konsekventně odvozuje pravost obsahu, opět v úrovni *prima facie*.

V oblasti veřejných listin se v českém i německému právu oproti tomu uplatňuje presumpce správnosti. Presumpcí správnosti je zde třeba rozumět vyvratitelnou právní domněnku o pravosti (správnosti) obsahu veřejné listiny na základě technické platnosti podpisu QES a přítomnosti obsahových náležitostí dané veřejné listiny. Ochranným prvkem typicky bude pouze QES (a QTS).

Zatímco u soukromých listin bude listinu popírající straně stačit prokázat vážné pochybnosti o pravosti buď podpisu QES, nebo podepsaného obsahu, u veřejných listin bude nutné provést důkaz opaku. Důkazem opaku zde bude především, že buď podpis QES není pravý, nebo že listina jako celek není pravá.[63]

Tato rozdílná důkazní úroveň je možná pouze díky tomu, že u veřejnoprávních podepisujících musí stát zajistit prostředí vytváření a evidence veřejných listin tak, aby buď nemohlo k jejich falešnému vytvoření dojít, nebo byla evidence aspoň natolik průkazná, že zfalšování napadené veřejné listiny vyvstane s evidencí ve spisové službě.

---

[61] Srov. 9.4.1.
[62] Srov. 7.4.
[63] Další možný důkaz opaku, že veřejnou listinou prokazované skutečnosti nejsou správné, v zásadě nezávisí na podobě veřejné listiny.

Bez zajištění těchto podmínek by důkazní mechanismus vyvratitelné právní domněnky nemohl úspěšně fungovat a právě tyto jej odlišují od posuzování soukromých listin.

V kontextu nařízení eIDAS stojí za pozornost, že dle čl. 35 odst. 2 eIDAS u kvalifikované elektronické pečeti (QESeal) platí domněnka integrity dat a správnosti původu dat, s nimiž je kvalifikovaná elektronická pečeť spojena. Z technické platnosti QESeal tedy na důkazní úrovni (právní) domněnky platí pravost původu dat, což se velmi přibližuje výše uvedené presumpci správnosti veřejných listin, zde ovšem u listin (dat) obecných, tedy i u listin soukromých. U soukromých listin je proto opatření pečetí QESeal důkazně významně silnější než opatření podpisem QES. Tato důkazní systematika nařízení eIDAS není srozumitelná, neposkytuje dobrou logiku a je předmětem právní kritiky.[64] Důkazní nesoulad je pravděpodobně důsledkem vypuštění příliš silných právních domněnek podpisu QES u elektronického dokumentu, které byly přítomny v návrhu nařízení eIDAS od Komise,[65] ale během zákonodárného procesu byly z výsledného znění vypuštěny, zatímco obdobné ustanovení o důkazní síle QESeal zůstalo ponecháno, snad s důvěrou v to, že právnické osoby se dokáží o sebe postarat lépe než průměrná fyzická osoba.

[64] Srov. 6.15.12.
[65] Srov. 6.15.11 a pozn. pod čarou Chyba: zdroj odkazu nenalezen.

Slovníčky

Autor používá v tomto textu pro české vyjádření pojmů unijního práva tučně zvýrazněné obraty v následující tabulce. Obraty v závorkách jsou alternativní.

Česky (zásada)	**Německy** (Grundsatz)	**Anglicky** (principle of...)	**Francouzsky** (le principe...)
přímá použitelnost (platnost)	unmittelbare Geltung	direct applicability	d'applicabilité directe
přednost	Vorrang	primacy (supremacy)	de primauté
přímý účinek	unmittelbare Anwendbarkeit	direct effect	de l'effet direct
užitečný účinek (plná účinnost; plný účinek; užitečnost; účinnost; plný užitek; efektivita)	(nützliche, praktische, volle) Wirksamkeit	effectiveness	de l'effet utile

Tab A. – Přehled překladů některých pojmů nauky práva EU

Autor používá pro český překlad pojmů německého práva v BGB a německé civilní nauky v tomto textu, pro konzistentní udržení kontextu, tato slova či obraty.

Česky (pro kontext BGB a německé civilní nauky)	**Německy** (BGB, nauka civilního německého práva)
vyjádření vůle	die Willenserklärung
právní transakce	das Rechtsgeschäft
právní chování	rechtliches Verhalten
právní konání	die Rechtshandlungen
jednání podobná právním transakcím	geschäftsähnliche Handlungen
reálné akty	die Realakte
(faktická jednání)	(Tathandlungen, tatsächliche Handlung)
nicotnost	die Nichtigkeit
rozporovatelnost	die Anfechtbarkeit
lidské jednání	menschlichen Handlungen
činnosti vůle	Willensbetätigungen
vůle k jednání	der Handlungswille
vůle k vyjádření (vědomí k vyjádření)	der Erklärungswille (die Erklärungsbewußtsein)
vůle k transakci	der Geschäftswille
horizont objektivního příjemce	objektiver Empfängerhorizont
obvod moci	der Herrschaftsbereich
teorie vůle	die Willenstheorie
teorie vyjádření	die Erklärungstheorie
teorie platnosti	die Geltungstheorie
vyjádření platnosti (prohlášení platnosti)	die Geltungserklärung
regulace	die Regelung
styk, provoz	der Verkehr

Tab. B – Přehled překladů některých pojmů německého civilního práva

Seznam zkratek

Zkratky názvů právních předpisů aj. pramenů práva

ABGB	Allgemeines bürgerliches Gesetzbuch; Obecný zákoník občanský (právní předpis Rakouska a později Československé republiky); srov. též o. z. o.
AO	Abgabenordnung (právní předpis Německa)
BGB	Bürgerliches Gesetzbuch; německý občanský zákoník (právní předpis Německa)
De-Mail-G	De-Mail-Gesetz (právní předpis Německa)
DirES	Directive 1999/93/EC, on a Community framework for electronic signatures; Směrnice 1999/93/ES o rámci společenství pro elektronické podpisy
DirPS	Směrnice 2011/83/EU o právech spotřebitelů
ECDir	E-Commerce Directive; Směrnice o elektronickém obchodu (směr. 2000/31/ES)
EGBGB	Einführungsgesetz zum Bürgerlichen Gesetzbuche (právní předpis Německa)
eIDAS	Nařízení (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
E-SIGN	Electronic Signatures in Global and National Commerce Act (právní předpis USA)
FGO	Finanzgerichtsordnung (právní předpis Německa)
GG	Grundgesetz; Základní zákon (ústava Německa)
Listina	usnesení Předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky
obč. zák.	Zákon č. 89/2012 Sb., občanský zákoník
o. s. ř.	Zákon č. 99/1963 Sb., občanský soudní řád,
o. z. o.	Obecný zákoník občanský císařství rakouského; v ČR zrušen; srov. též ABGB
SEU	Smlouva o Evropské unii
SFEU	Smlouva o fungování Evropské unie
SigG	Signaturgesetz vom 16. Mai 2001 (německý zákon platný 2001–2017)
SigG97	Gesetz zur digitalen Signatur (německý zákon platný 1997–2001)
SigV	Signaturverordnung (německá vyhláška platná 2001–2017)
SigV97	Verordnung zur digitalen Signatur (německá vyhláška platná 1997–2001)
spr. řád	zákon č. 500/2004 Sb., správní řád
UETA	Uniform Electronic Transactions Act (právní předpis v USA)
VDG	Vertrauensdienstegesetz (právní předpis Německa)
VwVfG	Verwaltungsverfahrensgesetz (právní předpis Německa)
zák. č. 40/1964 Sb.	Zákon č. 40/1964 Sb., občanský zákoník; zrušen
zák. o archivnictví	Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů
ZEP	Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)

ZEÚ	Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů
ZPO	Zivilprozessordnung; Civilní procesní řád (právní předpis Německa)
ZSVD	Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce

Ostatní zkratky

Pozn.: Byly voleny zkratky obvyklé v oblasti svého užívání. Zkratky používané právně i technicky jsou v tomto textu vždy použity jako právní pojmy, neplyne-li výslovně jinak.

AdES	Advanced Electronic Signature; Zaručený elektronický podpis (právní pojem nařízení eIDAS, dříve též směrnice DirES a zákona ZEP)
AdESeal	Advanced Electronic Seal; Zaručená elektronická pečeť (právní pojem nařízení eIDAS)
$AdES_{QC}$	Advanced Electronic Signature based on a Qualified Certificate; Zaručený elektronický podpis založený na kvalifikovaném certifikátu [pro elektronický podpis] (právní pojem nařízení eIDAS a dříve též zákona ZEP)
$AdESeal_{QC}$	Advanced Electronic Seal based on a Qualified Certificate; Zaručená elektronická pečeť založená na kvalifikovaném certifikátu [pro elektronickou pečeť] (právní pojem nařízení eIDAS)
AIFO	Agendový identifikátor fyzické osoby (právní pojem z oblasti základních registrů)
B2B	Business To Business; Podnikatel vůči podnikateli (technický pojem)
B2C	Business To Consumer; Podnikatel vůči spotřebiteli (technický pojem)
BFH	Bundesfinanzhof
BGBl.	Bundesgesetzblatt; Spolková sbírka zákonů; náhledy na <http://www.bgbl.de/>
BGH	Bundesgerichtshof
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
BNotK	Bundesnotarkammer
BSI	Bundesamt für Sicherheit in der Informationstechnik
BMWE	Bundesministeriums für Wirtschaft und Energie
CA	Certification Authority; Certifikační autorita (pojem technické praxe PKI)
CAdES	Formát(y) pro zaručené elektronické podpisy využívající podpis v CMS (technický pojem)
CEN	Comité Européen de Normalisation; Evropský výbor pro normalizaci (evropská normalizační organizace)
CENELEC	Comité Européen de Normalisation Electrotechnique; Evropská komise pro standardizaci v elektrotechnice (evropská normalizační organizace)
CMS	Cryptographic Message Syntax (technický pojem; syntaxe formátu kryptograficky chráněných zpráv, původem z PKCS#7)
CommonPKI	Profily PKI pro nasazení v oblasti elektronického podpisu, původem z Německa
CRL	Certificate Revocation List; Seznam zneplatněných certifikátů (pojem praxe PKI)
CWA	CEN Workshop Agreement [druh dokumentu (specifikace) organizace CEN]
ČR	Česká republika

ČSFR	Česká a Slovenská Federativní Republika, ev. Československá federativní republika.
DTBS/R	Data To Be Signed/or Representation; Data určená k podepsání nebo jejich reprezentace (technický pojem z technických specifikací mandátu M/460)
EAL	Evaluated Assurance Level; Úroveň míry záruky hodnocení (technické úrovně míry zajištění bezpečnosti produktů informačních technologií)
EDI	Electronic Data Interchange; Elektronická výměna dat (technický pojem)
EGVP	Elektronisches Gerichts- und Verwaltungspostfach; Elektronická správní a soudní poštovní schránka (technická specifikace anebo technické provedení)
EN	European Norm; Evropská norma (evropská technická norma od ESOs)
ENISA	European Union Agency for Network and Information Security; Evropská agentura pro bezpečnost sítí a informací (agentura EU)
EESSI	European Electronic Signature Standardization Initiative (pracovní skupina existující v letech 1999–2004; vytvořená ad hoc v rámci ICTSB na žádosti a za podpory Evropské komise)
ES	Evropská společenství
ESI	Electronic Signature Infrastructure (pracovní skupina pro technické specifikace a normy elektronického podpisu v rámci ETSI)
ESOs	European Standard Organisations; Evropské normalizační organizace – zahrnuje CEN, CENELEC a ETSI
ESVO	Evropské sdružení volného obchodu
ETSI	European Telecommunications Standards Institute (evropská normal. organizace)
ETUI	European Trade Union Institute
EU	Evropská unie
FG	Finanzgericht; Finanční soud (v Německu)
HI	Human Interface; Lidské rozhraní (technický pojem z technických specifikací mandátu M/460)
HID	Human Interface Device; Zařízení lidského rozhraní (technický pojem z technických specifikací mandátu M/460)
ICT	Information and Communication Technologies; Informační a komunikační technologie (technický a marketingový pojem)
ICTSB	Information and Communication Technology Standards Board (malá pracovní skupina složená z účasti CEN, CENELEC a ETSI pro kooperaci při řešení otázek normalizace při překryvu činností organizací v oblasti informačních a komunikačních technologií)
IDABC	Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens (projekt EU)
IEC	International Electrotechnical Commission (mezinárodní normalizační organizace)
IETF	Internet Engineering Task Force (normalizační organizace internetu)
ISDS	Informační systém datových schránek
ISO	International Organization for Standardization (mezinárodní normalizační organizace)
IT	Information Technologies; Informační technologie (technický pojem)

ITSEC	Information Technology Security Evaluation Criteria (technická kritéria pro hodnocení [úrovně] zajištění bezpečnosti v informačních technologiích)
ITU	International Telecommunication Union (též normalizační organizace)
KosIT	Koordinierungsstelle fur IT-Standards (německá zájmová organizace)
LOTL	List of the Lists; Seznam [důvěrohodných] seznamů (právní pojem rámce eIDAS)
M/460	Standardisation Mandate to the European Standardisation Organisations CEN, CENELEC and ETSI in the field of Information and Communication Technologies Applied to Electronic Signatures; mandát od Evropské komise z 22. 12. 2009
MPSV	Ministerstvo práce a sociálních věcí
NGSCB	Next Generation Secure Computing Base (technologie společnosti Microsoft)
NS	Nejvyšší soud
OASIS	Organization for the Advancement of Structured Information Standards (normalizační organizace charakteru komerčního konsorcia)
OLG	Oberlandesgericht
OTP	One Time Password; Jednorázové heslo (technický pojem)
p7s	Formát souboru pro odloučený digitální [elektronický] podpis (technický pojem)
PAdES	Formát(y) pro zaručené elektronické podpisy využívající podpis v PDF (technický pojem)
PC	Personal Computer; Osobní počítač (technický pojem)
PCS	Poskytovatel certifikačních služeb (právní pojem směrnice DirES a zákona ZEP)
PDF	Portable Document Format (technický pojem; specifikace fy Adobe; též norma ISO)
PDF/A	Portable Document Format – Archiving (technický pojem; verze PDF pro dlouhodobou archivaci)
PEPPOL	Pan-European Public Procurement Online (projekt EU)
PIN	Personal Identification Number (technický pojem; autentizace druhu „něco vím“)
PINPad	PIN Pad (technický pojem, periferní jednotka pro nezávislé zadávání PIN)
PKC	Publik Key Cryptography; Kryptografie veřejného klíče (technický pojem)
PKCS	Public Key Cryptography Standards (technický pojem; specifikace fy. RSA Labs)
PKI	Public Key Infrastructure; Infrastruktura veřejného klíče (technický pojem)
QC	Qualified Certificate; Kvalifikovaný certifikát (podle kontextu právní pojem rámce eIDAS, dříve též směrnice DirES a ZEP, anebo navazujících technických norem)
QES	Qualified Electronic Signature; Qualifizierte elektronische Signatur; Kvalifikovaný elektronický podpis (právní pojem nařízení eIDAS; dříve též SigG)
QESeal	Qualified Electronic Seal; Kvalifikovaná elektronická pečeť (právní pojem nařízení eIDAS)
QSCD	Qualified electronic Signature Creation Device; Kvalifikovaný prostředek pro vytváření elektronických podpisů (právní pojem nařízení eIDAS)
QSealCD	Qualified electronic Seal Creation Device; kvalifikovaný prostředek pro vytváření elektronických pečetí (právní pojem nařízení eIDAS)
QTS	Qualified electronic Time Stamp; Kvalifikované elektronické časové razítko (právní pojem nařízení eIDAS)

QTSP	Qualified Trust Service Provider; Kvalifikovaný poskytovatel služeb vytvářejících důvěru (právní pojem nařízení eIDAS; viz též TSP)
RegTP	Regulierungsbehörde für Telekommunikation und Post (předchůdce BNetzA)
SAK	Signaturanwendungskomponent; Podpisová aplikační komponenta (právní pojem ze SigG a SigV)
SCA	Signature Creation Application; Aplikace vytvářející podpis (technický pojem z technických specifikací mandátu M/460)
SCD	Signature-Creation Data; Data pro vytváření podpisu (technický pojem z technických specifikací mandátu M/460)
SCDev	Signature-Creation Device; Prostředek pro vytváření podpisu (technický pojem z technických specifikací mandátu M/460)
SDEU	Soudní dvůr Evropské unie
SSCD	Secure-Signature-Creation Device; Prostředek pro bezpečné vytváření podpisu (právní pojem směrnice DirES a ZEP, popř. technických norem ETSI ESI)
SSEE	Sichere Signaturerstellungseinheit; Bezpečná jednotka pro vyhotovení podpisu (právní pojem zákona SigG, odpovídá pojmu SSCD)
STORK	Secure idenTity acrOss boRders linKed (projekt EU pro elektronickou identifikaci)
SVA	Signature Verification Application; Aplikace ověřující podpis (technický pojem z technických specifikací mandátu M/460)
SVD	Signature-Verification Data; Data pro ověřování podpisu (technický pojem z technických specifikací mandátu M/460)
sw/hw	Software or Hardware (technická komponenta nebo systém realizovatelný tak i tak)
TOE	Target of Evaluation; Předmět hodnocení (technický pojem označující předmět, u něhož se zjišťuje míra bezpečnosti produktu IT)
TL	Trusted List; Důvěryhodný seznam (právní pojem nařízení eIDAS)
TR	Technical Report [druh dokumentu (zpráva) organizace ETSI]
TS	Technical Specification [druh dokumentu (specifikace) organizace ETSI]
TS	Trust Service; Služba vytvářející důvěru (právní pojem nařízení eIDAS)
TSP	Trust Service Provider; Poskytovatel služeb vytvářejících důvěru (právní pojem nařízení eIDAS; viz též QTSP)
TSL	Trust-service Status List; Seznam stavu důvěryhodných služeb (technický pojem)
USB	Universal Serial Bus (technický pojem; sběrnice a rozhraní)
VAD	Verification Authentication Data; Ověřovací autentizační údaje (technický pojem z technických specifikací mandátu M/460; např. PIN nebo výsledek biometrické operace ověření osobní totožnosti)
W3C	World Wide Web Consortium (normalizační konsorcium)
WIPIWIS	What Is Presented Is What Is Signed; Co je předloženo, to je podepsáno (technická zásada; vyžaduje spolehlivé předložení dat určených k podpisu podepisující osobě)
X.509	Technická norma ITU, jejíž profily se používají pro obsah [kvalifikovaného] certifikátu pro [elektronický podpis, elektronickou pečeť, autentizaci internetových stránek] (technický pojem)
XAdES	Formát(y) pro zaručené elektronické podpisy využívající XML Signature (technický pojem)

Použitá literatura

Odborné články z časopisů, monografie a studie

ABEL, S. Urkundenbeweis durch digitale Dokumente. *Multimedia und Recht* (MMR). 1 Jg. (1998), Heft 12, s. 644–650.

BETTENDORF, J. Elektronische Dokumente und Formqualität. *Rheinische Notar-Zeitschrift* (RNotZ). 5. Jg. (2005), Heft 6, s. 277–294.

BEURSKENS, M. Nomen est omen? – Falschfirmierung im elektronischen Geschäftsverkehr. *Neue Juristische Wochenschrift*. 2017, č. 18, s. 1265–1270.

BOGUSZAK, J. – ČAPEK, J. – GERLOCH, A. *Teorie práva*. 2., přeprac. vydání. Praha: ASPI Publishing, 2004.

BLIND, K. – JUNGMITTAG, A. The impact of patents and standards on macroeconomic growth: a panel approach covering four countries and 12 sectors. *Journal of Productivity Analysis.* Volume 29, Issue 1, February 2008.

BUCKLEY, J. S. – TANK, M. H. K. – WHITAKER, R. D. – KROMER, J. P. *The Law of Electronic Signatures and Records*. 2016 edition: Thomson Reuters, 2016. ISBN 978-0-314-63532-7.

CORNELIUS, K. Vertragsabschluss durch autonome elektronische Agenten. *Multimedia und Recht*. 2002, roč. 8, č. 6. s. 353–358.

DRENSKA, M. *Die rechtlichen Aspekte des elektronischen Handels in Bezug auf den Vertragsabschluss*. Dissertation. Augsburg: Juristischen Fakultät der Universität Augsburg, 2006.

ČERMÁK, K. ml. Elektronický podpis: pohled soukromoprávní. *Bulletin advokacie.* 2002, č. 11, s. 64–77.

DONÁT, J. – MAISNER, M. – PIFFL, R. *Nařízení eIDAS : komentář.* Praha: C. H. Beck, 2017.

DUMORTIER, J. – KELM, S. – NILSSON, H. – SKOUMA, G. – VAN EECKE, P. *The legal and market aspects of electronic singnatures – final report, Legal and market aspects of the application of Directive 1999/93/EC and practical applications of electronic signatures in the Member States, the EEA, the Candidate and the Accession countries*. Interdisciplinary centre for Law & Information Technology (ICRI) – Katholieke Universiteit Leuven, Leuven: October 2003. Dostupné z: <http://www.epractice.eu/files/media/media_581.pdf>; navštíveno 11/2013.

DVOŘÁK, J. – ŠVESTKA, J. – ZUKLÍNOVÁ, M. *Občanské právo hmotné. Svazek I. Díl první: Obecná část.* 1. vyd. Praha: Wolters Kluwer ČR, 2013. ISBN 978-80-7478-326-5.

ELISCHER, D. Protiprávnost – co je jejím zdrojem v soukromém právu? *Časopis pro právní vědu a praxi.* 2016, č. 4, s. 501–526.

EINSELE, D. *BGB § 126a Elektronische Form*. In: SÄCKER, J. (ed.) *Münchener Kommentar zum Bürgerlichen Gesetzbuch: BGB Band 1: Allgemeiner Teil §§ 1–240, ProstG, AGG*. 7. Auflage. München: C. H. Beck, 2015. Dostupné z: <https://beck-online.beck.de/>.

FISCHER-DIESKAU, S. – HORNUNG, G. Erste höchstrichterliche Entscheidung zur elektronischen Signatur. *Neue Juristische Wochenschrift.* 60. Jg. (2007), Heft 40, 2007, s. 2897–2899.

FLUME, W. *Allgemeiner Teil des Bürgerlichen Rechts. Band 2, Das Rechtsgeschäft*. Berlin: Springer, 1992.

FRIMMEL, M. *Elektronický obchod: právní úprava*. Praha: Prospektrum, 2002.

FUKUYAMA, F. *Velký rozvrat: lidská přirozenost a rekonstrukce společenského řádu*, Praha: Academia, 2006. 376 s. ISBN: 80-200-1438-1.

FULLER, L. L. Consideration and Form. *Columbia Law Review.* Vol. 41, No. 5 (May, 1941), s. 799–824.

GERLOCH, A. *Teorie práva.* 3. vydání. Plzeň: Aleš Čeněk, 2004.

GERLOCH, A. *Teorie práva.* 7. vydání. Plzeň: Aleš Čeněk, 2017.

HÄRTING, N. *Internetrecht*. Köln: Verlag Dr. Otto Schmidt KG, 2014.

HARVÁNEK, J. et al. *Právní teorie*. Plzeň: Aleš Čeněk, 2013.

HOEREN, T. *Internetrecht.* Skriptum, Münster: April, 2017.

HOEREN, T. – SIEBER, U. – HOLZNAGEL, B. (eds). *Handbuch Multimedia-Recht, Rechtsfragen des elektronischen Geschäftsverkehrs.* 35. Ergänzslieferung. München: C. H. Beck, 2013.

HORÁLKOVÁ, M. *Německo-český právnický slovník*. Voznice: LEDA, 2010.

HULMÁK, M. a kol. *Občanský zákoník VI. Závazkové právo. Zvláštní část (§ 2055–3014). Komentář.* 1. vydání. Praha: C. H. Beck, 2014. 2072 s.

JANDT, S. Beweissicherheit im elektronischen Rechtsverkehr — Folgen der europäischen Harmonisierung. *Neue Juristische Wochenschrift*. 2015, s. 1205–1211.

KMENT, V. Evropské nařízení eIDAS: Impuls pro sjednocení elektronického podpisu a identifikace v EU. *Jurisprudence,* č. 6, 2014, s. 25–35.

KMENT, V. Nahradí elektronický podpis prostý ten tradiční vlastnoruční? *Bulletin advokacie*. Roč. 2016, č. 12, s. 31–35.

KUNT, M. – LECHNER, T. *Spisová služba.* 2., aktualizované vydání. Praha: Leges, 2017.

KÖHLER, H. *BGB, Allgemeiner Teil : ein Studienbuch*. München: C. H. Beck, 1996.

KORBEL, F. – MELZER, F. Písemnost, elektronický a biometrický podpis v elektronickém právním jednání. *Bulletin advokacie.* 2014, č. 12, s. 31–36.

KOŠČÍK, M. Pojem a obsah právních úkonů na internetu. *Revue pro právo a technologie* [online]. 2011, roč. 2, č. 4, s. 30–75. [cit. 2017-12-07]. Dostupné z: <https://journals.muni.cz/revue/article/view/4089>.

KUČERA, Z. Uzavírání spotřebitelských smluv na internetu, *Rekodifikace a praxe.* Roč. 2015, č. 5, s. 4.

KUNT, M. – LECHNER, T. *Spisová služba*. 2., aktualizované vydání. Praha: Leges, 2017.

LANIER, J. One-Half of a Manifesto. *Wired*. Roč. 2000, č. 12. Dostupné z: <https://www.wired.com/2000/12/lanier-2/>.

LAVICKÝ, P. a kol. *Občanský zákoník I. Obecná část (§ 1–654). Komentář.* Praha: C. H. Beck, 2014. ISBN: 978-80-7400-529-9.

LECHNER, T. *Elektronické dokumenty v právní praxi*. Praha: Leges, 2013. 256 s.

LINDGREN, K. E. The Positive Corporate Seal Rule and Exceptions Thereto and the Rule in Turquand's Case. *Melbourne University Law Review*. Vol. 9, Sep 1973, s. 192–219. Dostupné z: HeinOnline.

LINDNER-FIGURA, J. *Kapitel 6. Form des Mietvertrages*. In: LINDNER-FIGURA, J. – OPRÉE, F. – STELLMANN, F. (Hrsgb.). *Geschäftsraummiete: Handbuch*. 4. Auflage. C. H. Beck, 2017. 1118 s.

LODDER, A. R. – MURRAY, A. D. (eds). *EU regulation of e-commerce : a commentary*. Cheltenham: Edward Elgar Publishing, 2017.

MACUR, J. Právní a skutkové domněnky při dokazování listinou v civilním soudním řízení. *Právní rozhledy*. 2001, č. 2, s. 60–64.

MASON, S. *Electronic Signatures in Law.* 3rd edition. New York: Cambridge University Press, 2012.

MASON, S. *Electronic Signatures in Law*. 4th edition, London: Institute of Advanced Legal Studies – University of London, 2016. Dostupné z: <http://humanities-digital-library.org/index.php/hdl/catalog/book/electronicsignatures>.

MASON, S. Electronic signatures: the essentials. In: *InsideOut Magazine* [online], 15th December 2015 [31. 8. 2016]. Dostupné z: <http://communities.lawsociety.org.uk/in-house/insideout-magazine/electronic-signatures-the-essentials/5052726.fullarticle>.

MASON S. Informal Debate on the Issues Relating to Terminology and Clarification of Concept in Respect of the EU e-Signature Legislation, In: *SCRIPTed* [online], 2012, 9:1, s. 82–103, s. 84 [31. 8. 2016]. Dostupné z: <http://script-ed.org/?p=327>.

MCCULLAGH, A. – LITTLE, P. – CAELLI, W. Electronic Signatures: Understand the Past to Develop the Future. (1998) 21(2). *University of New South Wales Law Journal* 452. [1. 11. 2016]. Dostupné z: <http://www.austlii.edu.au/au/journals/UNSWLawJl/1998/56.html>.

MENEZES, A. – VAN OORSCHOT, P. – VANSTONE, S. *Handbook of Applied Cryptography.* CRC Press, 1996, reprint London: 2001. Dostupné z: <http://cacr.uwaterloo.ca/hac/>.

MELZER, F. – TÉGL, P. a kolektiv. *Občanský zákoník – velký komentář. Svazek III. § 419–654.* 1. vyd. Komentátor. Praha: Leges, 2014. ISBN 978-80-7502-003-1.

MÜLLER-HENGSTENBERG, C. D. – KIRN, S. Intelligente (Software-)Agenten: Eine neue Herausforderung unseres Rechtssystems – Rechtliche Konsequenzen der „Verselbstständigung" technischer Systeme. *Multimedia und Recht*. 2014, č. 5, s. 307–313.

NEMEC, M. – SYS, M. – SVENDA, P. – KLINEC, D. – MATYAS, V. *The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli*, předpublikační verze, 2017. Dostupné z: <https://crocs.fi.muni.cz/_media/public/papers/nemec_roca_ccs17_preprint.pdf>; navštíveno 11/2017.

PALANDT, O. *Bürgerliches Gesetzbuch*. 69. neubearb. Aufl. München: C. H. Beck, 2010.

PETROV, J. – VÝTISK, M. – BERAN, V. a kol. *Občanský zákoník: komentář*. Praha: C. H. Beck, 2017. 3120 s.

POLČÁK, R. Okamžik doručení do datové schránky. *Revue pro právo a technologie*. 2010, roč. 1, č. 2, s. 22–24.

POLČÁK, R. Elektronické právní jednání – změny, problémy a nové možnosti v zákoně č. 89/2012 Sb. *Bulletin advokacie*. 2013, č. 10. s. 34–40.

POLČÁK, R. Praxe elektronických dokumentů. *Bulletin advokacie.* 2011, č. 7–8, s. 53–61.

POMAHAČ, R. – HANDRLICA, J. *Evropské správní právo*. Praha: C. H. Beck, 2012.

REED, CH. *How To Make Bad Law: Lessons from the computing and communications sector.* Queen Mary University of London, School of Law, Legal Studies Research Paper No. 40/2010. London, 2010.

REICH, D. O. – SCHMITZ, P. *Einführung in das Bürgerliche Recht : Grundlagen des BGB – Allgemeiner Teil – Allgemeines Schuldrecht – Besonderes Schuldrecht – Sachenrecht*. Wiesbaden: Gabler, 2000.

ROSSNAGEL, A. Rechtsetzung zu Sicherheitsdiensten : Europäisierung ja, Monopolisierung nein! *Multimedia und Recht*. 2012, s. 781–782.

ROSSNAGEL, A. (ed). Keine Wahrung der Schriftform bei Unterzeichnung auf einem elektronischen Schreibtablett. *Neue Juristische Wochenschrift* (NJW). 65. Jg. (2012), Heft 49, s. 3584–3586.

ROSSNAGEL, A. Neue Regeln für sichere elektronische Transaktionen. *Neue Juristische Wochenschrift.* 2014, s. 3686–3692.

ROSSNAGEL, A. Der Anwendungsvorrang der eIDAS-Verordnung – Welche Regelungen des deutschen Rechts sind weiterhin für elektronische Signaturen anwendbar? *Multimedia und Recht*. 2015, s. 359–364.

ROSSNAGEL, A. Beweiswirkungen elektronischer Vertrauensdienste Neue Regelungen durch die eIDAS-Verordnung der Europäischen Union. *Multimedia und Recht*. 2016, s. 647–652.

ROSSNAGEL, A. *Entwurf eines eIDAS-Durchführungsgesetzes – Verbändeanhörung.* Universität Kassel, Fachbereich Wirtschaftswissenschaften, Fachgebiet Öffentliches Recht, Umwelt- und Technikrecht, 31. Oktober 2016. Dostupné z: <https://www.uni-kassel.de/fb07/fileadmin/datas/fb07/5-Institute/IWR/Ro%C3%9Fnagel/Ro%C3%9Fnagel_Stellungnahme_zum_Referentenentwurf_VDG.pdf>; navštíveno 8. 8. 2017.

ROSSNAGEL, A. *Das Recht der Vertrauensdienste : Die eIDAS-Verordnung in der deutschen Rechtsordnung.* 1. Auflage. Baden-Baden: Nomos, 2016. ISBN 978-3-8487-3544-0.

SÄCKER, J. (ed.) *Münchener Kommentar zum Bürgerlichen Gesetzbuch: BGB Band 1: Allgemeiner Teil §§ 1–240, ProstG, AGG.* 7. Auflage. München: C. H. Beck, 2015.

SCHNEIER, B. *Applied cryptography: protocols, algorithms and source code in C.* 2nd edition, New York: John Wiley & Sons, 1996.

SEALED, TIME.LEX. SIEMENS: *CROBIES: Study on Cross-Border Interoperability of eSignatures – Head Document*, 2010. Dostupné z: <http://ec.europa.eu/digital-agenda/en/news/crobies-study-cross-border-interoperability-esignatures-2010>.

SKROBOTZ, J. FG Münster: Unzulässige Klageerhebung mit verwendungsbeschränkter Signatur. *Multimedia und Recht*. 2006, s. 636–639.

SMEJKAL, V. – KODL, J. – UŘIČAŘ, M. Elektronický podpis podle nařízení eIDAS. *Revue pro právo a technologie* [online]. 2015, roč. 6, č. 11.

SNEDDON, M. Legislating to Facilitate Electronic Signatures and Records: Exceptions, Standards and the Impact of the Statute Book. (1998) 21(2) *University of New South Wales Law Journal* 334. [1. 11. 2016] Dostupné z: <http://www.austlii.edu.au/au/journals/UNSWLawJl/1998/59.html>.

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

SPINDLER, G. *BGB § 126a Elektronische Form*. In: SPINDLER, G. – SCHUSTER, F. *Recht der elektronischen Medien.* 3. Auflage, C. H. Beck, 2015. Dostupné z: <https://beck-online.beck.de/>.

STOFFELS, M. *Gesetzlich nicht geregelte Schuldverträge : Rechtsfindung und Inhaltskontrolle*. Mohr Siebeck, 2001.

SVOBODA, P. *Úvod do evropského práva*. 5. vyd. Praha: C. H. Beck, 2013. Beckovy mezioborové učebnice. ISBN 978-80-7400-488-9.

ŠVESTKA, J. – DVOŘÁK, J. – FIALA, J. a kol. *Občanský zákoník – komentář. Svazek I. (§ 1 až 654)*. 1. vyd. Praha: Wolters Kluwer ČR, 2014. Komentáře Wolters Kluwer Kodex Rekodifikace. ISBN 978-80-7478-370-8.

THOMPSON, S. D. *Commentaries on the Law of Private Corporations (1908–1915)*, s. 997 – 1030. Dostupné z: HeinOnline.

VAN DAM, C. *European Tort Law.* 2nd edition. Oxford University Press, 2013.

VAN EECKE, P. (team supervisor). *Final Report of the Study on the specific policy needs for ICT standardisation*. European Union, 10. 5. 2007.

VINEY, G. – VAN GERVEN, W. – LEVER, J. – LAROUCHE, P. *Cases, Materials and Text on National, Supranational and International Tort Law.* Hart Publishing, 2000.

VON SAVIGNY, F. C. *System des heutigen Ramischen Rechts.* Band 3. Veit, Berlin, 1840.

WANG, F. F. *Law of Electronic Commercial Transactions : contemporary issues in the EU, US and China*. New York: Routledge, 2014.

WENDTLAND, H. *BGB § 126a Elektronische Form*. In: BAMBERGER, H. G. – ROTH, H. – HAU, W. – POSECK, R. (Hrsgb). *BeckOK BGB*. C. H. Beck. 44. Edition. Stand 01.11.2017. C. H. Beck. 2017. Dostupné pouze z: <https://beck-online.beck.de/>.

ZUKLÍNOVÁ, M. *Právní jednání podle občanského zákoníku č. 89/2012 Sb.* Praha: Linde, 2013.

Pozn.: Články časopisů *Multimedia und Recht* (MMR), *Neue Juristische Wochenschrift* (NJW) a *Rheinische Notar-Zeitschrift* (RNotZ) byly získány z on-line služby<http://beck-online.beck.de/>.

Jiné zdroje

British Institute of International and Comparative Law: *Introduction to English Tort Law*. s. 2. Dostupné z: <http://biicl.org/files/763_introduction_to_english_tort_law.pdf>; navštíveno 4/2016.

British Institute of International and Comparative Law: *Introduction to French Tort Law*. Dostupné z: <http://www.biicl.org/files/730_introduction_to_french_tort_law.pdf>; navštíveno 4/2016.

Bundesamt für Sicherheit in der Informationstechnik. *Digitale Gesellschaft – Glossar.* Dostupné z: <https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/ElektronischeSignatur/Glossar/esig glossar.html>; navštíveno 10/2017.

CEN, *Compass, European Standardisation in a nutshell*, September 2004. Dostupné z: <http://www.cost540.com/ppt/CEN/CEN-COMPASS.pdf>.

COMMISSION OF THE EUROPEAN COMMUNITIES, *Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures*, COM (2006) 120 final, Brussels, 2006. Dostupné z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0120:FIN:EN:PDF>.

COMMISSION OF THE EUROPEAN COMMUNITIES, *Action Plan on esignatures and e-identification to facilitate the provision of cross-border public services in the Single Market*, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, COM(2008)798, Brussels, November 2008. Dostupné z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0798:FIN:EN:PDF>.

CROCS Attack. Centre for Research on Cryptography and Security, Fakulta informatiky, Masarykova univerzita. Dostupné z: <https://www.fi.muni.cz/research/crocs/index.xhtml.cs>.

Česko vyváží stále více zboží do EU, nejvíce obchoduje se sousedními zeměmi. ČTK – aktualne.cz, 7. 9. 2016. Dostupné z: <https://zpravy.aktualne.cz/ekonomika/cesko-obchoduje-nejvice-se-sousednimi-zememi-vyznam-evropske/r~5f60bf74849511e68d00002590604f2e/>.

DEUTSCHES INSTITUT FÜR NORMUNG: *Fragen und Antworten: Sind Normen mit Gesetzen gleichzusetzen?*, www.din.de. Dostupné z: <http://www.din.de/cmd?cmsrubid=47513&menurubricid=47513&level=tpl-rubrik&menuid=47391&languageid=de&cmsareaid=47391 - Normen%20und%20Gesetze>; navštíveno 11/2013.

Drucksache 14/4662, *Entwurf eines Gesetzes über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften.* Deutscher Bundestag, 16. 11. 2000. Dostupné z: <http://dip21.bundestag.de/dip21/btd/14/046/1404662.pdf>.

Drucksache 14/4987, *Entwurf eines Gesetzes zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr.* Deutscher Bundestag, 14. 12. 2000. Dostupné z: <http://dip21.bundestag.de/dip21/btd/14/049/1404987.pdf>.

Drucksache 18/12494, *Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 ...* („eIDAS-Durchführungsgesetz“) Deutscher Bundestag, 24. 5. 2017. Dostupné z: <http://dip21.bundestag.de/dip21/btd/18/124/1812494.pdf>; navštíveno 8. 8. 2017. Basisinformationen über den Vorgang. Dostupné z: <http://dipbt.bundestag.de/extrakt/ba/WP18/808/80874.html>.

Důvodová zpráva ZSVD, Sněmovní tisk 763, Parlament ČR, PS 2013–2017. Dostupné z: <http://www.psp.cz/sqw/historie.sqw?o=7&T=763>; navštíveno 10/2017.

ENISA. *Security guidelines on the appropriate use of qualified electronic time stamps, Guidance for users.* Version 2.0, Final, December 2016, s. 19–20. Dostupné z: <https://www.enisa.europa.eu/publications/security-guidelines-on-the-appropriate-use-of-qualified-electronic-time-stamps>.

EN 419211-2 Protection profiles for secure creation device – Part 2: Device with key generation, s. 7.

ETSI TR 102 041 V1.1.1 (2002-02) Signature Policies Report.

ETSI TS 101 733 V2.2.1 (2013-04) Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES).

EUROPEAN COMMISSION, ENTERPRISE AND INDUSTRY DIRECTORATE-GENERAL: *M/460 EN Standardisation Mandate to the European Standardisation Organisations CEN, CENELEC and ETSI in the Field of Information and Communication Technologies applied to Electronic Signature*, Brussels, 22nd December 2009. Dostupné z: <http://www.etsi.org/images/files/ECMandates/m460.pdf>.

EUROPEAN COMMISSION: *Proposal for a Regulation of the European Parliament and of the Council on the electronic identification and trust services for electronic transactions in the internal market.* COM (2012) 238 final, 2012/0146 (COD), Brussels, 2012. Dostupné z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:EN:PDF>.

Koordinierungsstelle fur IT-Standards (KosIT): *Stellungnahme zum Referentenentwurf eines eIDAS-Durchführungsgesetzes.* Bremen, den 1. 11. 2016. Dostupné z: <http://www.bmwi.de/Redaktion/DE/Downloads/Stellungnahmen/Stellungnahmen-elDAS-VO/stellungnahme-bremen.pdf?__blob=publicationFile&v=4>.

Motive zu dem Entwurfe eines Bürgerlichen Gesetzbuches für das Deutsche Reich. 5 Bände, Verlag von J. Guttentag (D. Collin), Berlin/ Leipzig, 1888.

Motive zu dem Entwurfe eines Bürgerlichen Gesetzbuches für das Deutsche Reich. Band I, Verlag von J. Guttentag (D. Collin), Berlin/ Leipzig, 1888, 395 s. Digitalizováno na: <https://ia902605.us.archive.org/4/items/motivezudementw01germgoog/motivezudementw01germgoog.pdf>.

PDF Reference - Version 1.7, Adobe Portable Document Format. 6th edition, Adobe Systems Incorporated, November 2006.

Pětina Čechů platí v obchodech jen kartami. Novinky.cz, 24. 6. 2016. Dostupné z: <https://www.novinky.cz/finance/406790-petina-cechu-plati-v-obchodech-jen-kartami.html>.

PIFFL, R. – FELIX, O. *Nařízení eIDAS – Cíle, nástroje, důsledky.* Metodický seminář – Dopady nařízení eIDAS po 1. 7. 2016, Ministerstvo vnitra, Praha, 14. 6. 2016, s. 15/42. Dostupné z: <http://www.mvcr.cz/soubor/1-eidas-narizeni-eidas-cile-nastroje-dusledky.aspx>; navštíveno 22. 6. 2016.

Referentenentwurf des Bundesministeriums für Wirtschaft und Energie: Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) Nr. 910/2014. Dostupné z: <https://www.cr-online.de/referentenentwurf-eldas-vo.pdf>; navštíveno 8. 8. 2016.

Request for Comments: 5126 CMS Advanced Electronic Signatures (CAdES).

Odborné právní zdroje neodkazované (právo EU)

Pozn.: Právní zdroje týkající se práva EU zde uvedené byly použity během práce na textu, ale nejsou výslovně citovány, parafrázovány ani odkazovány, protože odpovídající zpracování nebylo do textu zařazeno z důvodu rozsahu.

HARTLEY, T. C. *The foundations of European union law: an introduction to the constitutional and administrative law of the European community*. 7th ed. Oxford: Oxford University Press, 2010. ISBN 978-0-19-956675-4.

HWANG, S.–P. Anwendungsvorrang statt Geltungsvorrang? Normlogische und institutionelle Überlegungen zum Vorrang des Unionsrechts. *Europarecht.* 2016, č. 4.

KACZOROWSKA, A. *European Union Law*. 3rd edition. New York: Routledge, 2013.

KRÁL, R. *Nařízení ES z pohledu jejich vnitrostátní aplikace a implementace*. Praha: C. H. Beck, 2006.

ONDŘEJKOVÁ, J. *Princip přednosti evropského práva v teorii a soudní praxi*. Praha: Leges, 2012.

PAUNIO, E. *Legal Certainty in Multilingual EU Law : Language, Discourse, and Reasoning at the European Court of Justice*. Surrey: Ashgate Publishing, 2013.

POTACSZ, M. – MAYER, C. *Effet utile as a Method of Interpretation*. In: TICHÝ, L. – POTACS, M. – DUMBROVSKÝ, T. (eds). *Effet utile*. Prague: Centre for Comparative Law of the Faculty of Law, Charles University, 2014.

PYM, A. *Transferre non semper necesse est*. Quaderns. Revista de traducció, 1998. Dostupné z: <http://usuaris.tinet.cat/apym/on-line/intercultures/1998_transferre.pdf>.

RUFFERT, M. *Art. 288 Rn. 20–22 (I. Verordnung)*. In: RUFFERT, M. – CALLIESS, C. (Hrsgb.) *EUV/AEUV*. München: C. H. Beck, 2016.

SCHROEDER, W. *IV . Prinzipien für die Anwendung der Rechtsquellen*. In: STREINZ, R. (Hrsgb.) *EUV/AEUV Vertrag über die Europäische Union und Vertrag über die Arbeitsweise der Europäischen Union*. C. H. Beck, 2012.

SCHÜTZE, R. *European Union law.* Cambridge: Cambridge University Press, 2015.

TICHÝ, L. – ARNOLD, R. – ZEMÁNEK, J. – KRÁL, R. – DUMBROVSKÝ, T. *Evropské právo*. 5,. přepracované vydání, Praha: C. H. Beck Praha, 2014. 758 s.

TOMÁŠEK, M. – TÝČ, V. – MALENOVSKÝ, J. et al. *Právo Evropské unie*. 2., aktualizované vydání. Praha: Leges, 2017. ISBN 978-80-7502-184-7.

TRIDIMAS, T. *The general principles of EC law*. Oxford: Oxford University Press, 1999. Oxford EC law library. ISBN 0-19-826012-1.

VON BOGDANY, A. – BAST, J. (eds). *Principles of European Constitutional Law*. Revised Second Edition. Oxford: HART Publishing, 2009. ISBN: 978-1-84113-822-0.

Odborné zdroje neodkazované – jiné

Pozn.: Právní aj. zdroje níže uvedené byly použity při práci na díle, ale nejsou v něm přímo odkazované z důvodů omezení zaměření díla. Týkají se zejména práva elektronického podpisu v Německu z let 2002 až 2017 a technické normalizace v EU.

BARTAK, G. F. 125 Jahre elektrotechnische Normung in Österreich. *Elektrotechnik & Informationstechnik*. 125. ročník, 2008, č. 5, s. 153–164.

BRAUCKMAN, J. – GRÖPER, R. Konzept und Nutzen von Certificate Policy und Certification Practice Statement. *Datenschutz und Datensicherheit (DuD)*. 2013, č. 8, s. 491–496.

DELOS, O. – LACROIX, S. – VAN EECKE, P. – CUSTERS, M. – JANIN, W. *Study on the standardisation aspects of eSignature, A study for the European Commission (DG Information Society and Media), Final Report.* Sealed, DLA Piper and Across communication, 2007. Dostupné z: <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=969>.

DLA Piper, Uninova, Technical University of Delft: *EU Study on the specific policy needs for ICT standardisation.* July 2007. 148 s. Dostupné z: <http://ec.europa.eu/enterprise/sectors/ict/files/full_report_en.pdf>.

ELLISON, C. – SCHNEIER, B. Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure. *Computer Security Journal.* 2000, Volume XVI, Number 1. Dostupné z: <https://www.schneier.com/paper-pki.pdf>.

FISCHER-DIESKAU, S. – HORNUNG, G. Die Beschränkung des qualifizierten Zertifikats – § 7 Abs. 1 Nr. 7 SigG als wichtiges Mittel der Risikokalkulation. *Multimedia und Recht*. 6. Jg. (2007), Heft 6, 2003, s. 384–389.

FISCHER-DIESKAU, S. – STEIDLE, R. Die Herstellererklärung für Signaturanwend-ungskomponenten – Eine Erleichterung zur Verbreitung elektronischer Signaturen? *Multimedia und Recht*. 9. Jg. (2006), Heft 2, s. 68–73.

GUTMAN, P. PKI: It's Not Dead, Just Resting. *Computer*. IEEE Computer Society, Volume 35, Issue 8, Aug 2002, s. 41–49.

GRAUX, H. – STAFFE, CH. *EFVS: Study on the European Federated Validation Services. Feasibility and Global Implementation Plan.* September 2009. Dostupné z: <http://ec.europa.eu/idabc/servlets/Doc31a6.pdf?id=32388>.

GRAUX, H. – STAFFE, CH. *EFVS: Study on the European Federated Validation Services. Analysis and Assessment.* September 2009. Dostupné z: <http://ec.europa.eu/idabc/servlets/Doce7b7.pdf?id=32389>.

GRAUX, H. – DELOS, O. – LACROIX, S. *EFVS: Study on the European Federated Validation Services. Completion of the framework for signature validation services.* March 2010. Dostupné z: <http://ec.europa.eu/idabc/servlets/Docf934.pdf?id=32633>.

GRAVESEN, G. – DUMORTIER, J. – VAN EECKE, P. Die europäische Signaturrichtlinie – Regulative Funktion und Bedeutung der Rechtswirkung. *Multimedia und Recht*. 2. Jg. (1999), Heft 10, s. 577–585.

HÄHNCHEN, S. Elektronische Akten bei Gericht – Chancen und Hindernisse. *Neue Juristische Wochenschrift (NJW)*. 58. Jg. (2005), Heft 32, s. 2257–2259.

KMENT, V. Elektronický podpis v praxi s komplikacemi. *ComputerWorld*. 2003, č. 4.

KRAWCZYK, P. When the EU Qualified Electronic Signature Becomes an Information Services Preventer. *Digital Evidence and Electronic Signature Law Review*. Vol. 7, 2010, s. 7–18.

KUTYŁOWSKI M. – BŁAŚKIEWICS, P. – KRZYWIECKI, Ł. – KUBIAK P. – PALUSZYŃSKI W. – TABOR M. *Technical and Legal Meaning of „Sole Control" – Towards Verifiability in Signing Systems.* In: ABRAMOWICZ, W. –MACIASZEK, L. – WĘCEL, K. (Eds.). *BIS 2011 Workshops.* LNBIP 97, Springer-Verlag Berlin Heidelberg, 2011, s. 270–281.

LAPP, T. Brauchen wir De-Mail und Bürgerportale? Überflüssige Anwendung mit Geburtsfehlern. *Datenschutz und Datensicherheit.* 2009, č. 11, s. 651–655.

MARTÍNEZ-NADAL, A. – FERRER-GOMILA, J. *Liability of Certification Authorities: A Juridical Point of View*. In DAVIDA G. I. – FRANKEL Y. (Eds). *Information Security (Proceedings).* 4th International Conference, ISC 2001 Malaga, Spain, 2001, s. 204–219.

MATES, P. – SMEJKAL, V. *E-government v České republice, Právní a technologické aspekty.* 2., podstatně přepracované a rozšířené vydání. Praha, Leges, 2012.

MIKOLETZKY, J. Vom Elektrotechnischen Verein in Wien zum Österreichischen Verband für Elektrotechnik – 125 Jahre OVE. *Elektrotechnik & Informationstechnik*. 125. ročník, 2008, č. 5, s. 147–152.

ROSSNAGEL, A. Das elektronische Verwaltungsverfahren – Das Dritte Verwaltungsverfahrensänderungsgesetz. *Neue Juristische Wochenschrift*. 56. Jg. (2003), Heft 7, s. 469–475.

ROSSNAGEL, A. Das neue Recht elektronischer Signaturen - Neufassung des Signaturgesetzes und Änderung des BGB und der ZPO. *Neue Juristische Wochenschrift.* 54. Jg. (2001), Heft 25, s. 1817–1826.

ROSSNAGEL, A. Die Ausgabe sicherer Signaturerstellungseinheiten. *Multimedia und Recht (MMR)*. 9. Jg. (2006), Heft 7, s. 441–446.

ROSSNAGEL, A. Die signaturrechtliche Herstellererklärung. *Multimedia und Recht*. 10. Jg. (2007), Heft 8, s. 487–493.

ROSSNAGEL, A. Europäische Signatur-Richtlinie und Optionen ihrer Umsetzung. *Multimedia und Recht.* 2. Jg. (1999), Heft 5, s. 261–266.

ROSSNAGEL, A. Die fortgeschrittene elektronische Signatur. *Multimedia und Recht*. 6. Jg. (2003), Heft 3, s. 164–170.

ROSSNAGEL, A. – ALTENHEIN, K. *Beck'scher Kommentar zum Recht der Telemediendienste: Telemediengesetz, Jugendmedienschutz-Staatsvertrag (Auszug), Signaturgesetz, Signaturverordnung, Vorschriften zum elektronischen Rechts- und Geschäftsverkehr*. München: C. H. Beck, 2013.

ROSSNAGEL, A. – FISCHER-DIESKAU, S. Elektronische Dokumente als Beweismittel – Neufassung der Beweisregelungen durch das Justizkommunikationsgesetz. *Neue Juristische Wochenschrift*. 59. Jg., Heft 12, s. 806–808.

ROSSNAGEL, H. *On Diffusion and Confusion – Why Electronic Signatures Have Failed.* In FISCHER-HÜBNER S., FURNELL S., LAMBRINOUDAKIS C. (Eds.). *Trust, Privacy, and Security in Digital Business (Proceedings)*. Third International Conference, TrustBus 2006, Kraków, Poland, September 2006. Berlin: Springer, 2006, s. 71–80.

SRIVASTAVA A., Resistance to change: six reasons why businesses don't use e-signatures. *Electronic Commerce Research*. Volume 11, Issue 4, November 2011, s. 357–382.

TETTENBORN, A. Die Evaluierung des IuKDG – Erfahrungen, Erkenntnisse und Schlußfolgerungen,. *Multimedia und Recht*. 2. Jg. (1999), Heft 9, 1999, s. 516–520.

Použité prameny práva Evropské unie

Pozn.: Prameny jsou uvedeny chronologicky; používány byly ve znění pozdějších předpisů, jak byly účinné k 1. 12. 2017, nebo k poslednímu dni své účinnosti; prameny byly získávany ze systému EUR-Lex na adrese <http://eur-lex.europa.eu>.

Směrnice 85/577/EHS ze dne 20. prosince 1985 o ochraně spotřebitele v případě smluv uzavřených mimo obchodní prostory.

Směrnice Evropského parlamentu a Rady 97/7/ES ze dne 20. května 1997 o ochraně spotřebitele v případě smluv uzavřených na dálku, ve znění směrnice 2002/65/ES ze dne 23. září 2002, směrnice 2005/29/ES ze dne 11. května 2005 a směrnice 2007/64/ES ze dne 13. listopadu 2007; zrušena od 14. 6. 2014.

Směrnice Evropského parlamentu a Rady 1999/44/ES ze dne 25. května 1999 o některých aspektech prodeje spotřebního zboží a záruk na toto zboží, ve znění směrnice 2011/83/EU ze dne 25. října 2011 o právech spotřebitelů.

Směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy, L 13/12 Úřední věstník Evropských společenství z 19. 1. 2000, 13/sv. 24 CS Úředník věstník Evropské unie, s. 239–248. **(„DirES")**. Dostupné z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:CS:PDF>.

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Official Journal of the European Communities, 19th Jan 2000, L 13/12-L 13/20. Dostupné z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:PDF>.

Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu („směrnice o elektronickém obchodu“) **(„ECDir“)**.

Rozhodnutí Komise 2000/709/ES ze dne 6. listopadu 2000 o minimálních kritériích, ke kterým by členské státy měly přihlížet při jmenování subjektů uvedených v čl. 3 odst. 4 směrnice 1999/93/ES.

Rozhodnutí Komise 2003/511/ES z 14. července 2003 o zveřejnění referenčních čísel obecně uznávaných technických norem pro produkty elektronického podpisu v souladu se směrnicí 1999/93/ES.

Směrnice Evropského parlamentu a Rady 2006/123/ES ze dne 12. prosince 2006 o službách na vnitřním trhu.

Nařízení Evropského parlamentu a Rady (ES) č. 765/2008 ze dne 9. července 2008 , kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93 (text s významem pro EHP).

Rozhodnutí Komise 2009/767/ES ze dne 16. října 2009, kterým se stanovují opatření pro usnadnění užití postupů s využitím elektronických prostředků prostřednictvím „jednotných kontaktních míst“ podle směrnice Evropského parlamentu a Rady 2006/123/ES o službách na vnitřním trhu, ve znění Rozhodnutí Komise 2010/425/EU ze dne 28. července 2010 a ve znění Prováděcího rozhodnutí Komise 2013/662/EU ze dne 14. října 2013.

Směrnice Evropského parlamentu a Rady 2011/83/EU ze dne 25. října 2011 o právech spotřebitelů, kterou se mění směrnice Rady 93/13/EHS a směrnice Evropského parlamentu a Rady 1999/44/ES a zrušuje směrnice Rady 85/577/EHS a směrnice Evropského parlamentu a Rady 97/7/ES. **(„DirPS“)**.

Směrnice Evropského parlamentu a Rady 2014/24/EU ze dne 26. února 2014 o zadávání veřejných zakázek a o zrušení směrnice 2004/18/ES, ve znění Nařízení Komise v přenesené pravomoci (EU) 2015/2170 ze dne 24. listopadu 2015.

Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES. **(„eIDAS“)**. Dostupné z: <http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32014R0910>.

Prováděcí rozhodnutí Komise (EU) 2015/296 ze dne 24. února 2015, kterým se stanoví procesní opatření pro spolupráci mezi členskými státy v oblasti elektronické identifikace podle čl. 12 odst. 7 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ...

Prováděcí nařízení Komise (EU) 2015/806 ze dne 22. května 2015, kterým se stanoví specifikace týkající se podoby značky důvěry EU pro kvalifikované služby vytvářející důvěru

Prováděcí nařízení Komise (EU) 2015/1501 ze dne 8. září 2015 o rámci interoperability podle čl. 12 odst. 8 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ...

Prováděcí nařízení Komise (EU) 2015/1502 ze dne 8. září 2015, kterým se stanoví minimální technické specifikace a postupy pro úrovně záruky prostředků pro elektronickou identifikaci podle čl. 8 odst. 3 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ...

Prováděcí rozhodnutí Komise (EU) 2015/1505 ze dne 8. září 2015, kterým se stanoví technické specifikace a formáty důvěryhodných seznamů podle čl. 22 odst. 5 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ...

Prováděcí rozhodnutí Komise (EU) 2015/1506 ze dne 8. září 2015, kterým se stanoví specifikace pro formáty zaručených elektronických podpisů a zaručených pečetí uznávaných subjekty veřejného sektoru podle čl. 27 odst. 5 a čl. 37 odst. 5 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ...

Prováděcí rozhodnutí Komise (EU) 2015/1984 ze dne 3. listopadu 2015, kterým se stanoví okolnosti, formáty a postupy pro oznamování podle čl. 9 odst. 5 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ...

Prováděcí rozhodnutí Komise (EU) 2016/650 ze dne 25. dubna 2016, kterým se stanoví normy pro posuzování bezpečnosti kvalifikovaných prostředků pro vytváření elektronických podpisů a pečetí podle čl. 30 odst. 3 a čl. 39 odst. 2 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ...

Informace týkající se údajů na důvěryhodných seznamech členských států oznámené podle rozhodnutí Komise 2009/767/ES, ve znění rozhodnutí 2010/425/EU a prováděcího rozhodnutí 2013/662/EU, a podle prováděcího rozhodnutí (EU) 2015/1505 (2016/C 233/01).

Použité právní předpisy Německa

Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), das zuletzt durch Artikel 1 des Gesetzes vom 20. Juli 2017 (BGBl. I S. 2787) geändert worden ist **(„BGB“)**.

BGB – anglický překlad od Langenscheidt Translation Service, aktualizován od Neil Mussetta a poté od Samson Übersetzungen GmbH a Dr. Carmen v. Schöning. Dostupné z: <https://www.gesetze-im-internet.de/englisch_bgb/>.

Einführungsgesetz zum Bürgerlichen Gesetzbuche in der Fassung der Bekanntmachung vom 21. September 1994 (BGBl. I S. 2494; 1997 I S. 1061), das zuletzt durch Artikel 2 Absatz 4 des Gesetzes vom 20. Juli 2017 (BGBl. I S. 2787) geändert worden ist **(„EGBGB“)**.

Zivilprozessordnung in der Fassung der Bekanntmachung vom 5. Dezember 2005 (BGBl. I S. 3202; 2006 I S. 431; 2007 I S. 1781), die zuletzt durch Artikel 11 Absatz 15 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist **(„ZPO“)**.

Abgabenordnung in der Fassung der Bekanntmachung vom 1. Oktober 2002 (BGBl. I S. 3866; 2003 I S. 61), die durch Artikel 6 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist **(„AO“)**.

Verwaltungsverfahrensgesetz in der Fassung der Bekanntmachung vom 23. Januar 2003 (BGBl. I S. 102), das zuletzt durch Artikel 11 Absatz 2 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist **(„VwVfG“)**.

Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste **(„IuKDG“)** v. 22. 7. 1997, BGBl. I S. 1870.

Gesetz zur digitalen Signatur (Signaturgesetz – **„SigG97“**), BGBl. I Jg. 1997, Nr. 52, S. 1872–1876.

Verordnung zur digitalen Signatur (Signaturverordnung – **„SigV97“**), BGBl. I Jg. 1997, Nr. 70, S. 2498–2502.

Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften Vom 16. Mai 2001, BGBl. Jg 2001 I Nr. 22, ausgegeben am 21. Mai 2001, s. 876–884.

Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), das durch Artikel 4 Absatz 111 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert worden ist. **(„SigG“)**.

Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr vom 13. Juli 2001, BGBl. Jg. 2001 I Nr. 35, ausgegeben am 18. Juli 2001, s. 1542–1549.

Signaturverordnung vom 16. November 2001 (BGBl. I S. 3074), die durch Artikel 4 Absatz 112 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert worden ist **(„SigV“)**.

Drittes Gesetz zur Änderung verwaltungsverfahrensrechtlicher Vorschriften Vom 21. August 2002, BGBl. Jg. 2002 Teil I Nr. 60, ausgegeben am 27. August 2002, s. 3322–3343.

Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz (Justizkommunikationsgesetz – **„JKomG“**) vom 22. März 2005, BGBl. Jg. 2005 I Nr. 18, ausgegeben am 29. März 2005, s. 837–858.

Gesetz über Personalausweise (Personalausweisgesetz – „PAuswG“) und den elektronischen Identitätsnachweis sowie zur Änderung weiterer Vorschriften vom 18. Juni 2009, BGBl. Jg. 2009 I Nr. 33, ausgegeben am 24. Juni 2009, s. 1346–1359.

De-Mail-Gesetz vom 28. April 2011 (BGBl. I S. 666), das durch Artikel 3 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist **(„De-Mail-G“)**.

Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften Vom 25. Juli 2013, BGBl. I Jg. 2013, Teil I, Nr. 43, ausgegeben am 31. Juli 2013, 2749–2760.

Gesetz zur Durchführung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG **(„eIDAS-Durchführungsgesetz“)**; Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 52, ausgegeben zu Bonn am 28. Juli 2017.

Vertrauensdienstegesetz vom 18. Juli 2017 (BGBl. I S. 2745), das durch Artikel 2 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist **(„VDG“)**.

Pozn. 1: Konsolidovaná znění právních předpisů Německa byla získána z: <http://www.gesetze-im-internet.de/>.

Pozn. 2: Právní předpisy Německa ve znění vydání ve Sbírce spolkových zákonů byly získány z: <http://www.bgbl.de/>.

Použité právní předpisy ČR vč. historických

Allgemeines bürgerliches Gesetzbuch für die gesammten Deutschen Erbländer der Österreichischen Monarchie, 946. Patent vom 1ten Junius 1811. Justizgesetzsammlung. Sken sbírky Justizgesetzsammlung z roku 1811 k dispozici na: <http://alex.onb.ac.at/cgi-content/alex?apm=0&aid=jgs&datum=10120003&zoom=2&seite=00000275>. Neúřední německý text ABGB dispozici na: <http://www.koeblergerhard.de/Fontes/ABGB1811.htm>.

Obecný zákonník občanský císařství rakouského, vytištěn v C. K. tiskárně dvorské a státní ve Vídni, 1862. Sken dostupný z: <http://lib.wikipravo.cz/libro/BookExplorer?akce=7&abbr=ozo&aktPage=1>.

Zákon č. 99/1963 Sb., občanský soudní řád („o. s. ř.“).

Listina základních práv a svobod, ústavní zákon č. 2/1993 Sb. ve znění ústavního zákona č. 162/1998 Sb. **(„Listina“)**.

Zákon č. 328/1999 Sb., o občanských průkazech.

Zákon č. 227/2000 Sb., o elektronickém podpisu **(„ZEP“)**.

Zákon č. 480/2004 Sb., o některých službách informační společnosti.

Nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb.

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

Zákon č. 499/2004 Sb., o archivnictví a spisové službě. **(„zák. o archivnictví “)**.

Zákon č. 500/2004 Sb., správní řád **(„spr. řád“)**.

Zákon č. 40/2009 Sb., trestní zákoník **(„trest. zák.“)**.

Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů **(„ZEÚ“)**.

Zákon č. 111/2009 Sb., o základních registrech.

Vyhláška č. 193/2009 Sb., o stanovení podrobností provádění autorizované konverze dokumentů.

Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek

Zákon č. 280/2009 Sb., daňový řád. Formát a struktura dat pro podání zveřejněné správcem daně na webové stránce: <https://adisepo.mfcr.cz/adistc/adis/idpr_pub/epo2_info/popis_struktury_seznam.faces>.

Zákon č. 89/2012 Sb., občanský zákoník (**„obč. zák.“** nebo **„OZ“**)

Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby.

Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce **(„ZSVD“)**.

Zákon č. 298/2016 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce.

Zákon č. 250/2017 Sb., o elektronické identifikaci.

Právní předpisy jiných jurisdikcí

Electronic Signatures in Global and National Commerce Act (E-SIGN), 15 USC § 7001–7003. S 106(5). **(„E-SIGN")**.

National conference of commissioners on uniform state laws: Uniform Electronic Transactions Act (1999), Denver, 1999. **(„UETA")**. Dostupné z: <http://uniformlaws.org/Act.aspx?title=Electronic%20Transactions%20Act>.

Judikáty (rozhodnutí a stanoviska)

Písemnost a písemná forma právního jednání:
Rozsudek Nejvyššího soudu ze dne 29. 1. 2009, sp. zn. 30 Cdo 1230/2007.
Rozsudek Nejvyššího soudu ze dne 10. 4. 2014, sp. zn. 23 Cdo 1593/2012.
Rozsudek Nejvyššího soudu ze dne 1. 6. 2017, sp. zn. 20 Cdo 1741/2017.

Podání, resp. doručování elektronických písemností vůči, resp. od soudů ČR:
Stanovisko pléna Nejvyššího soudu ze dne 5. 1. 2017 k podáním činěným v elektronické podobě a k doručování elektronicky vyhotovených písemností soudem, prováděnému prostřednictvím veřejné datové sítě, sp. zn. Plsn 1/2015.
Rozsudek Nejvyššího správního soudu ze dne 17. 2. 2012, čj. 8 As 89/2011 - 31.
Rozsudek Nejvyššího správního soudu ze dne 29. 3. 2016, čj. 8 Afs 179/2015 - 47.
Nález Ústavního soudu sp. zn. II.ÚS 3042/14 ze dne 19. 1. 2016 (N 7/80 SbNU 81).

Doporučující charakter norem DIN:
BGH, Urteil vom 14. Mai 1998, Az. VII ZR 184/97, Volltext = BGHZ 139, 16. Dostupné z: <http://www.schweizer.eu/bibliothek/urteile/index.html?id=11686>.

Náhrada škody 59.949 € za nesplněné předání věci z dražby na eBay při vydražené ceně 51 €:
OLG Köln Urteil vom 8. Dezember 2006 Az. 19 U 109/06. Dostupné z: <https://openjur.de/u/120462.html>.

Finanční omezení v kvalifikovaném certifikátu pro kvalifikovaný elektronický podpis:
BFH, 18.10.2006 – XI R 22/06. Dostupné z: <http://lexetius.com/2006,3265>, též jako dokument „BeckRS 2006, 24002769", dostupné z: <http://beck-online.beck.de/>.

FG Münster in SKROBOTZ J. (ed). *Unzulässige Klageerhebung mit verwendungsbeschränkter Signatur*, Multimedia und Recht (MMR), 9. Jg. (2006), Heft 9, 2006, s. 636–640.

> BFH in SKROBOTZ J. (ed). *Klageerhebung mit verwendungsbeschränkter Signatur*, Multimedia und Recht (MMR), 10. Jg. (2007), Heft 4, 2007, s. 234–236.

Nedodržení textové formy pro informace před uzavřením smlouvy:
OLG Köln Urteil vom 24. August 2007 Az. 6 U 60/07. Dostupné z: <https://openjur.de/u/127392.html>.

Nesplnění písemné formy ani elektronické formy biodynamickým podpisem:
OLG München Urteil vom 4. Juni 2012 Az. 19 U 771/12. Dostupné z: <http://openjur.de/u/498795.html>.

OLG München in ROSSNAGEL A. (ed). Keine Wahrung der Schriftform bei Unterzeichnung auf einem elektronischen Schreibtablett. *Neue Juristische Wochenschrift* (NJW), 65. Jg. (2012), Heft 49, 2012, s. 3584–3586.

Elektronické právní jednání: Srovnávací analýza s důrazem na využití elektronického podpisu podle práva EU, České republiky a Německa

Abstrakt (česky)

Cíle.

Cílem této práce je srovnávací analýza elektronického právního jednání podle práva EU, České republiky a Německa, s důrazem na využití vyšších verzí elektronického podpisu, zejména kvalifikovaného elektronického podpisu, který při právním jednání elektronickými prostředky má právní účinky vlastnoručního podpisu (kap. 6 až 10). Současně je věnována zvýšená pozornost i zcela novým institutům zaručené a kvalifikované elektronické pečeti, určeným výhradně pro využití právnickými osobami. Zkoumané právní úpravy zde vychází především z nedávno účinného evropského nařízení (EU) č. 910/2014 Sb., známého pod zkratkou eIDAS. Vyšší verze elektronického podpisu jsou využitelné pro právní jednání napříč celým právním řádem, v soukromém i veřejném právu.

Pro účel obecného poznání předchází srovnávací analýze teoretická část (kap. 2 až 4, částečně kap. 5), která se zabývá jednak pojmem právního jednání obecně, jednak se soustřeďuje na institut tradičních vlastnoručních podpisů a jejich funkcí, a to zejména na základě německé a české právní nauky, s dílčími exkurzy do common law, jakož i mezi požadavky vzniklé ze snah o elektronickou implementaci podpisu.

Vlastnoruční podpis je institut vzniklý z obyčejů. Jeho užívání se do značné míry ustálilo samo, pro vyhovění podepisující osobě i spoléhající se osobě, a to i v rámci autonomních vztahů soukromého práva. Ceremonie podpisu nabyla význam stvrzení právního jednání, přičemž výsledná listina s podpisem poté plní i důkazní funkci. Podpis se ujal pro právní jednání, které dle práva nebo dohody stran vyžaduje trvalejší zachycení obsahu a možnost dokladování či dokazování. Užitky (přínosy) by pak měly převažovat nad riziky a břemeny formálnosti.

Celá práce je proto vytvářena na ose dvou souvisejících otázek či výzev. První obecnou otázkou je, zda kvalifikovaný elektronický podpis splňuje požadavky na obdobně přijatelné rozdělení přínosů a rizik mezi podepisující a spoléhající se osobu. S tím souvisí i hlavní nosné dilema textu, k čí tíži případně připsat právní jednání,

pravost jehož podpisu údajně podepsaná osoba později popře. Druhou obecnou otázkou je, zda kvalifikovaný elektronický podpis představuje svými funkčními vlastnostmi ekvivalenci funkcí vlastnoručního podpisu. Kladná odpověď na druhou otázku by zřejmě měla implikovat i kladnou odpověď na otázku první. Obráceně implikace platit nemusí. Přijatelné rozdělení rizik a přínosů mezi obě osoby je tedy hlavní výzvou, funkční ekvivalence výzvou pomocnou. Nicméně právě teoretická analýza podpisu (kap. 4) vyjevuje, jaké vlastnosti zejména vlastnoruční podpis vlastně má. Obdobně teoretická analýza pojmu právního jednání odhaluje celkové požadavky na něj (kap. 2 a 3), jak se ustálily zejména v soukromém právu Německa a ČR, a je též užitečná pro představy a hodnocení provedení právního jednání pomocí elektronických prostředků, k čemuž slouží i rozbor platné právní úpravy v obou zmíněných státech (kap. 5).

Obsah.

V českém pojetí (kap. 2) se pojem právního jednání používá v širším obecném smyslu (2.1) v rámci teorie práva, jakož i v užším smyslu (2.2) v soukromém právu. Je provedena i historická retrospekce do obecného zákoníku občanského (2.3), která slouží k vysvětlení počátků dnešní české teoretické systematiky i pro časové ohlédnutí za vznikem pojmů (zde na počátek 19. století), které vznikaly především v němčině. Byly pak dále rozvíjeny pro použití v německém civilním kodexu BGB.

V německé nauce je pojem typicky užíván v rámci soukromého práva (kap. 3), ve kterém se pro něj používají hned dva výrazy, a to *das Rechtsgeschäft* a *die Willenserklärung*. Text vyjevuje, že německá nauka se od české liší i tím, že používá i jinak mírně odlišnou systematiku pojmů. Právní jednání (právní transakce) v německé nauce má vyhraněnější kvazi-normativní podstatu, obsahově se jedná o autonomní založení regulace vztahů mezi osobami. Dle probíraného teoretického pojetí Flumeho je charakteristický důraz na zákonné uznání (dovolenost obsahu), které dle něj lépe zajišťuje maximu zákonodárství *ius suum cuique tribuere* i v soukromých vztazích (3.3.2), jejichž tvorba by jinak byla příliš postižena „sebeláskou“ *(Selbstherrlichkeit)*. Flume požaduje, aby strany jednaly především pomocí *figur*, které platné právo předpřipravilo jako vzory právního jednání, například coby smluvní typy. Obdobnou formační *(channeling)* funkci práva nalézá v common law i Fuller (4.4), kterému se však spíše jedná o právní jistotu charakteru vztahu a rozhodnutelnost případného právního sporu. Flume se však jinak nachází na pozici ochrany soukromé autonomie i soukromého práva jako odvětví. Odmítá přímý účinek ústavních norem i jejich

nepřímý účinek *(die Drittwirkung)*, neboť se dle něj samy pro soukromé právo nehodí, ale mají se použít přímo předpisy a zásady bezprostředně ovládající soukromé právo, které jim odpovídají, zejména pak institut dobrých mravů.

Právě právní jednání jsou Flumemu důležitým prostředkem sebeurčení jedince, byť na pozadí existujícího právního řádu. V německé nauce trvalo ustálení teorie právního jednání nejméně století. Neuralgickým bodem je vztah vnitřní vůle a jejího vnějšího projevu. Zejména možnost omylu jednající osoby je pak právně teoreticky asi nejpodobnější otázkou dilematu tohoto textu, totiž toho, v čí neprospěch řešit případné popření pravosti údajně podepsanou osobou. Obdobně jako u omylu není jednoznačně morálně přiřaditelné selhání ani zavinění a zákonodárce nemá důvod stranit žádné ze stran soukromého právního jednání. Praxe se nyní kloní k výkladu právního jednání dle objektivního horizontu příjemce (3.2.1) a k teorii platnosti (*Geltungstheorie*, část 3.3.4) právního jednání. Dle Flumeho však žádná teorie není plně vyhovující, jedná se o *a priori* neřešitelný spor zásady sebeurčení a zásady sebeodpovědnosti jedince (3.3.5).

V kapitole 4 se provádí právně teoretický rozbor vlastnoručního podpisu a jeho alternativních elektronických forem. Řada náležitostí podpisu nebývá výslovně vyjádřena v právním řádu vůbec, jsou reflektovány pouze právní teorií. V kapitole jsou probírány právní teorie z ČR, Německa a z prostředí common law. Je proveden souhrn druhů technik elektronických podpisů, které jsou příležitostně uznávány. Dále je v kapitole obsažena reflexe pohledu kryptologie, která takzvaný digitální podpis považuje za důkaz původu dat či datové zprávy, popř. za autentizaci původce. Z technické praxe jsou reflektovány případné potřeby stanovení komitmentu nebo podpisových politik.

Kapitola 5 se již zabývá pojmem elektronického právního jednání, jeho vyjasněním, a to především s ohledem na nauku a platné soukromé právo užívané v ČR a v Německu. V obou právních řádech je standardem bezformální právní jednání. V německé nauce je k dispozici podrobnější teorie (5.2.1) právního jednání elektronickými prostředky, s členěním na elektronicky přenášená vyjádření vůle (5.2.1.1) a elektronicky vytvořená vyjádření vůle (5.2.1.2), která mohou být automatizovaná. V případě písemné formy právního jednání se systematika i pojmosloví mírně rozchází. V právu ČR je třeba věnovat pozornost pojmu „písemnost“ (5.1.3), zatímco v německém právu pojmu „elektronický dokument“ (*elektronische Dokument*, část 5.2.5.2). Platné právo obou států se značně rozchází v požadavcích náhrady

písemné formy právního jednání v elektronické podobě, kdy českému právu se zdá dostačovat elektronický podpis prostý (5.1.5), zatímco právo německé vyžaduje kvalifikovaný elektronický podpis (5.2.5.2). Česká úprava je proto předmětem kritiky v závěrech (5.3 a 11.7.3.4) textu.

Kapitola 6 se soustřeďuje na nové evropské nařízení eIDAS, na jeho část označovanou jako „služby vytvářející důvěru“, která pokrývá pojmy a instituty odvozené od elektronického podpisu. Výklad je veden v úrovni samotného nařízení eIDAS a práva Evropské unie. Množství termínů a podrobnost zpracování je dána komplexností rámce nařízení a množstvím otázek či nejasností, které ve zcela nové právní úpravě vznikají, a potřebou nevynechat žádnou právní otázku, která při používání vyšších verzí elektronického podpisu může vzniknout na straně podepisující (ev. pečetící) osoby nebo na straně spoléhající osoby (strany). Úvodní části (6.1 a 6.2) slouží především pro první hrubou orientaci čtenáře v nařízení. Je vyložen předmět a působnost nařízení (6.3), jejich dopady pro aplikaci. Podává se vysvětlení nové definice elektronického podpisu prostého (6.4) a jeho smysl. Návazně kontrastuje popis autentizačních elektronických podpisů (6.5), zejména zaručeného (6.5.1) a kvalifikovaného (6.5.3) elektronického podpisu, z čehož druhý uvedený má účinek rovnocenný vlastnoručnímu podpisu. Zcela nový je pojem elektronických pečetí (6.6). Práce podává i původní možnost výkladu účelu zavedení zaručené elektronické pečeti (6.6.4), kterým může být umožnit i elektronické potvrzování právního jednání přímo právnickou osobou, ovšem až v rámci vnitrostátní implementace. Doplňkovou službou je elektronické časové razítko (6.7). Vysvětluje se i pojem služeb vytvářejících důvěru a jejich poskytovatelů (6.8). Pro vnitrostátní, ale zejména přeshraniční právní styk jsou kritické důvěryhodné seznamy (6.9). Vyšší verze podpisu mohou vyžadovat kvalifikované prostředky pro vytváření elektronického podpisu (6.10). Nařízení obecně upravuje i problematiku ověřování (technické) platnosti kvalifikovaného elektronického podpisu (6.11). Jako součást rámce nařízení vzniká odpovědnost poskytovatele služeb vytvářejících důvěru (6.12) i členského státu (6.13). Samostatná je problematika povinnosti přijímání elektronických transakcí s elektronickým podpisem (6.14). Důkazní účinky vyšších verzí elektronických podpisů a pečetí plynou dobře ve srovnání s důkazními účinky i dalších upravených digitálních objektů (6.15). Kritika nedostatků nařízení je rozdělena na 15 dílčích problémů (6.16). Je představena možná hypotéza stavu (6.17), možnost ovlivnění předkladatele návrhu francouzským pojetím

z *Code civil*, ve kterém jsou četné právní povinnosti implikovány bez dalšího z technických norem a specifikací.

Kapitola 7 stručně popisuje implementaci v textu zkoumaných částí nařízení eIDAS v Německu, aby bylo možné následné srovnání s implementací českou. Implementace vždy nepřímo implikují i to, jak chápat a vykládat samotné nařízení eIDAS (kap. 6). Po popisu průběhu přijímání (7.1 a 7.2) pozdě přijatého zákona *eIDAS-Durchführungsgesetz* jsou hlavní podrobnosti věnovány v něm obsaženému zákonu *Vertrauensdienstegesetz* (7.3). Mírná novelizace postihla německý *Zivilprozessordnung* (7.4). V Německu dosud nebyla přijata prováděcí vyhláška.

Kapitola 8 obsahuje přehled obdobné implementace eIDAS ČR, jak byla provedena zejména adaptačním zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce. Nejčastěji bude pozornost věnována adaptivně-recepčním ustanovením (8.2). Je poskytnut i rozbor konkretizačních a doplňovacích ustanovení (8.3), institucionálně-kompetenčních (8.4) a sankčních (8.5). Recipované pojmy se využívají v desítkách novelizací (8.6) napříč právním řádem, nebyly však provedeny změny v důkazních pravidlech (8.7). Závěr kapitoly obsahuje přehled témat, která jsou považována za v implementaci opomenutá (8.8), a ustanovení, která byla derogována bez výslovné náhrady (8.9), takže dochází k menší či větší změně v právním řádu ČR.

Kapitola 9 pojednává o některých možnostech právního jednání s elektronickým podpisem dle právního řádu ČR, ve stavu po účinnosti adaptačního a změnového zákona k eIDAS. Uvádí se některé legislativní připomínky (9.1). Letmo je probíráno pozadí zpracování listin u veřejnoprávních původců (9.2) jakožto důležitého předpokladu zavedení a používání právní presumpce správnosti veřejných listin. Jsou zmíněny možnosti elektronického podání a splnění náležitostí podpisu při něm (9.3). Stručně je probrána možnost soukromého právního jednání (9.4), včetně vhodného konceptu důkazních účinků kvalifikovaného elektronického podpisu.

Kapitola 10 podává základní souhrn možností soukromého elektronického právního jednání právnickou osobou v právním řádu ČR. Právní úprava vychází z teorie fikce. Důsledkem je, že za právnickou osobu jednají její zástupci (10.1). Jsou zjištěny základní teoretické možnosti pojetí (10.2) elektronických agentů. Ukazuje se, že v případě právnických osob při automatickém provozu nebývá vazba na zastupující

osobu výhodná či praktická. Právní jednání elektronickým obchodem (10.3) vychází z práva EU, které určování fyzické osoby, jako za právnickou osobu jednajícího zástupce, nevyžaduje. Rozbor ukazuje, že pro technické zajištění povinně poskytovaných informací je možné fakultativně využít zaručené elektronické pečeti (10.3.3). V případě jiných elektronických agentů (10.3.4) je použití zaručených nebo kvalifikovaných elektronických pečetí možné, ale nemusí dostačovat. Na závěr se probírá splnění náležitostí písemné formy právního jednání při použití elektronických prostředků právnickou osobou (10.4).

Závěry (výsledky).

Implicitním závěrem je, že realizace kvalifikovaného elektronického podpisu je složitá (srov. kap. 6 a její rozsah). Tato skutečnost i potřeba pořizování potřebných elektronických prostředků působí jako zátěž podepisující osoby, která u vlastnoručních podpisů nemá obdobu, a zřejmě je hlavním důvodem jen nízké penetrace (začátek kap. 11 a 11.7.4) vyšších verzí elektronického podpisu.

Metodika rámce elektronických podpisů zajišťuje nezávislou odbornou kontrolu každé jeho určené součásti a poskytuje tak podepisující osobě možnost jednat právně autonomně a být si svou autonomií dostatečně jist. Nařízení eIDAS je však neúplné (11.5), neupravuje například bezpečnost aplikací vytvářejících podpis ani systémového prostředí. Z těchto důvodů by si podepisující osoba měla zajišťovat další potřeby své počítačové bezpečnosti dobrovolně. V oblasti veřejné správy by doplňkové potřeby bezpečnosti měly být zajištěny i právně (11.7.3.5), neboť si to vyžaduje presumpce správnosti veřejných listin.

Odpověď na obě výše zmíněné otázky textu, totiž zda kvalifikovaný elektronický podpis splňuje požadavky na obdobně přijatelné rozdělení přínosů a rizik mezi podepisující a spoléhající se osobu a zda představuje funkční ekvivalenci vlastnoručního podpisu, je tak odlišná normativně a věcně. Normativně kladnou odpověď stanoví samo nařízení (11.7.6), věcně však neúplnost úpravy způsobuje, že z hlediska věcného a potažmo důkazního lze vznášet různé námitky. Zmíněná neúplnost nařízení eIDAS neprospívá ani spoléhající se osobě, neboť se odráží i na její nižší právní jistotě.

V praxi existuje zatím jen nízká míra popírání pravosti (úvod kap. 11), a to i pro podpisy elektronické. V soukromém právu je dilema popírání podpisu oslabenou

povinností prokazování kauzy (11.2), ve veřejném právu existencí zázemí veřejnoprávního původce (11.1), jež ovšem musí být vytvářeno skutečně.

Neúplnost nařízení (11.5) závěr vícenásobně reflektuje. Zabývá se možnostmi jejího odstranění podrobnější vnitrostátní implementací, tj. doplňovacími a konkretizačními ustanoveními. Závěr proto obsahuje nejprve obecné přehledy právních argumentů pro podrobnější vnitrostátní implementaci v ČR i proti ní (11.6) a poté i konkrétní návrhy doplnění (11.7.3), včetně ohledu na popiratelnost (11.7.3.2) a automatizaci (11.7.3.3.), revize soukromého práva ČR (11.7.3.4) a doporučení pro veřejné právo (11.7.3.5). Pro jinou věcnou implementaci v právu ČR hovoří i srovnání s implementací německou (11.7.1).

I po doplněních asi vždy zůstanou určitá zbytková rizika, daná i křehkostí výpočetních systémů (úvod kap. 11). Namísto cesty upřesňování a konkretizace povinností jsou proto navrženy i zcela odlišné možnosti technického a právního rozvoje, které by umožnily se dilematu popiratelnosti vyhnout nebo jej vyřešit jinak. Navrženo je apriorní omezení použitelnosti (11.3) podle druhu jednání nebo výše finančního limitu. Jinou alternativou je převod jednání na rozporovatelný proces (11.4).

Možnost vytváření kvalifikovaného podpisu na dálku (11.7.4) může vést k vyššímu rozšíření používání, bez dalšího však neřeší právní ani technická dilemata.

Součástí závěru jsou i níže probírané předporozumění (11.7.2) a elektronické právní jednání právnické osoby a elektronická pečeť (11.7.5).

Dílčí souhrny jsou uváděny též průběžně v závěrech kapitol.

Původní poznatky.

V právně teoretické rovině je největším přínosem práce soustředěný popis vlastností a funkcí podpisu (kap. 4). Shrnují a propojují se zde poznatky právní doktríny české, německé a z common law. Navíc je prováděna i reflexe druhů techniky používaných pro implementaci elektronického podpisu, jakož i takzvaných komitmentů podpisu a podpisových politik, tedy požadavků vyplývajících spíše až z elektronických implementací podpisu než z praxe podpisů vlastnoručních. Kapitola 4 představuje právně teoretické porozumění podpisu, využitelné i pro případně nové druhy techniky, i pro právní úvahy rozmanitého druhu.

K dilematu popiratelnosti podpisu právní doktrína v nejobecnější rovině přispívá úvahou o střetu zásad sebeurčení a sebeodpovědnosti (3.3.5). Prvá zásada trvá na uplatnění pravé vnitřní vůle jedince, druhá akcentuje odpovědnost téhož jedince za skutečný projev vůle a vyzývá ke zdrženlivosti projevování se. Rozbor dále odhaluje, že k právnímu jednání je nutné předporozumění jedince (11.7.2) o tom, jak jej bude jeho adresát právně chápat. Elektronické právní jednání lze začít provádět i dosud neznámými způsoby, pokud právně jednající i právně spoléhající se osoba mají předem možnost seznámit se s tím, jaký projev bude mít jaký právní význam, nebo pokud je to dostatečně samozřejmé vzhledem k běžným zvykům. Platné právo tyto teoretické poznatky kazuisticky potvrzuje například povinností poučení (7.3.3) o právních účincích kvalifikovaného elektronického podpisu nebo stanovením informačních povinností o jednotlivých technických krocích vedoucích k uzavření smlouvy (dle směrnice ECDir, část 10.3.1). Obdobný smysl mají normativní poukazy na zvyklosti nebo i jen zavedenou praxi stran (např. § 545 a § 556 obč. zák.).

V tématu implementace legislativního aktu Evropské unie druhu nařízení tato práce překvapivě vyjevuje, že k dosažení jednotného účinku nařízení ve všech členských státech EU může být v České republice třeba nejen zdrženlivost vedoucí k nepřidávání žádných ustanovení v rámci předmětu úpravy, ale naopak přidání takových ustanovení, které doplní oprávnění a povinnosti, jež v jiných členských státech EU budou plynout ze zdrojů, které v ČR nejsou bez dalšího považovány za prameny práva. Takovými zdroji mohou být technické normy a specifikace, kterých je v souvislosti s nařízením eIDAS vyhlášeno několik desítek. Jejich vyhlašování představuje metodickou koncepci nařízení eIDAS. Práce zde proto vyslovuje i hypotézu, že předkladatelé návrhu nařízení v Komisi mohli být ovlivněni tímto pojetím, které pochází zejména z francouzského *Code civil* (6.17).

Práce popisuje v ČR málo známý takzvaný nový přístup *(New Approach)* k závaznosti technické normalizace, vyvinutý právem EU, a využívá ho v popisu výkladu čl. 29 eIDAS (6.10.2). Vyhovění technickým normám zakládá domněnku vyhovění, zvyšuje právní jistotu, ale neomezuje ostře vývoj produktů či služeb pouze na rámec technických norem. Z hlediska teorie práva je domněnka vyhovění zvláštní tím, že představuje alternativní splnění platnosti dispozice právní normy, a nikoli hypotézy, jako je tomu u právních domněnek.

Z nařízení eIDAS za pozornost jako novum stojí takzvané důvěryhodné seznamy (6.9) a jejich forma, neboť musí být zřízeny „ve formě vhodné pro automatické zpracování“ *(„a form suitable for automated processing“)*, která představuje i originární formu vedení důvěryhodného seznamu. Taková forma nevylučuje, že seznam je čitelný nebo kvazičitelný i lidsky, nicméně automatická zpracovatelnost má za následek nejen prvoplánové využití pro automatizaci (zejména vyhodnocování platnosti elektronických podpisů), ale druhotně implikuje i snadnou přeložitelnost obsahu do kteréhokoli jazyka, zejména do úředních jazyků jiných členských států EU. Obdobné právní úpravy a podkladové technologie by mohly být využity i pro vytváření výpisů z oficiálních úředních rejstříků členských států EU, odpadala by pak potřeba jejich úředně ověřených překladů při přeshraničním použití. Tato nová forma a zejména její originárnost a právní rozhodnost nahradila dřívější dichotomii strojově zpracovatelné podoby *(machine-processable)* a lidsky čitelné podoby důvěryhodných seznamů, z nichž právně rozhodná byla druhá uvedená.

K praktickému řešení dilematu popiratelnosti podpisu se v závěru navrhují jiné metody, než které jsou vyžity nařízením eIDAS. Jedná se v prvé řadě o návrh apriorní možnosti omezení použitelnosti elektronického podpisu zápisem takových omezení do kvalifikovaného certifikátu. Omezení by mohla mít povahu buď finančních limitů (6.16.10, 11.3), nebo omezení dle druhu činnosti (6.16.9, 11.3). Omezení dle druhu činnosti může mít značný význam například pro oddělení profesního a soukromého využití.

Další metodou, která může snižovat rizika elektronicky podepisujících osob, je návrh převádění jednorázového aktu podpisu na vícekrokový proces (11.4). Praktické i právní realizace mohou nabývat různých podob.

Práce vyjevuje jiný možný smysl a účel zavedení zaručené elektronické pečeti a kvalifikované elektronické pečeti, než byl dosud zastáván českou doktrínou (6.6.4). Navrhuje se, že smyslem uvedených pečetí je, aby i právně plnily stejný účel jako běžně plní podpis, až na to, že tento právní účinek není přímo proklamován nařízením, ale je ponecháno na vnitrostátní implementaci, zda takový účinek připustí. Z hlediska automatizace vytvoření jsou obecně rovnocenné zaručený elektronický podpis a zaručená elektronická pečeť, což je i přístup použitý samotným nařízením eIDAS v rámci jeho úpravy (6.6.4). Zde uvedené dva koncepty též odstraňují rozpory (rovnost,

nediskriminace) dosavadního výkladu, které vznikaly na úrovni základní práv EU i členských států.

Zaručená elektronická pečeť je kromě případů upravených samotným nařízením eIDAS použitelná i pro potvrzování povinně poskytovaných informací elektronickými obchody, které provozují právnické osoby (10.3.3), a to i v případě, že se jedná o právní jednání. Její použití je však právně fakultativní, jedná se o dobrovolně používaný bezpečnostní mechanismus, obdobně jako (kvalifikované) certifikáty pro autentizaci internetových stránek, jejichž vydávání nařízení eIDAS nově též pokrývá.

Při právním jednání elektronickým agentem právnické osoby text vyjevuje, že je spíše přirozené vynechat vazbu na konkrétní fyzickou osobu. Jedná-li se o právní jednání elektronickým obchodem, plyne vynechání zástupce z unijního práva (10.3.1). Závěr doporučuje doplnit (11.7.5) podobnou úpravu i pro jiné případy právního jednání právnické osoby elektronickým agentem do práva ČR.

Klíčová slova

Právní jednání, právní jednání právnické osoby, podpis, elektronický podpis, elektronická pečeť, teorie podpisu, eIDAS, elektronické právní jednání, elektronická transakce, písemnost, elektronický dokument, elektronické časové razítko, autentizace, identifikace, právní komparace, právo ČR, právo EU, právo Německa, kvalifikovaný elektronický podpis, kvalifikovaný certifikát, QES, AdES, QSCD, QESeal, AdESeal, QESealCD, QTS, důvěryhodné seznamy, služby vytvářející důvěru, TSP.

Electronic Legal Transaction: Comparative analysis with emphasis on the use of electronic signature under the EU law and laws of the Czech Republic and Germany

Abstract (English)

Objectives.

This thesis provides a comparative analysis of electronic legal transactions under the EU law and laws of the Czech Republic and Germany, while emphasising the utilisation of higher versions of electronic signature, especially of a qualified electronic signature, which has legal effects of a handwritten signature in legal transactions performed by electronic means (Chapters 6 to 10). At the same time, increased attention is also paid to entirely novel concepts of advanced and qualified electronic seal, which are intended exclusively for use by juristic persons. The laws under scrutiny are based especially on recently adopted Regulation (EU) No 910/2014, known as eIDAS.

To provide a general background, the comparative analysis is preceded by a theoretical part (Chapters 2 to 4, partially Chapter 5), dealing with the concept of legal transactions (also termed "legal acts" or "legal action") in general, while also focusing on the traditional handwritten signature and its functions, especially in view of the German and Czech legal doctrines and with occasional references to common law, as well as to requirements ensuing from various attempts at introducing an electronic form of signatures.

Handwritten signature is a concept originating in customary law. Its use has mostly established itself as a natural process, serving for the benefit of both the signing person (the "signatory") and the person relying on the signature (the "relying person"), also within autonomous relationships of private law. The signature ceremony has developed into a confirmation of a legal act made by the signatory, where the ensuing deed bearing the signature can also play an evidentiary role. Signature is also used for legal acts which – based on the law or mutual agreement of the parties – require that their contents be captured in a more permanent form, with the possibility of documenting or proving the acts. The benefits should then prevail over the risks and burdens associated with formality.

The entire thesis is therefore based on two interrelated questions, or challenges. The first general question is whether a qualified electronic signature meets the requirements for an analogously acceptable distribution of benefits and risks between the signatory and the relying person as in the case of a handwritten signature. This relates to the main dilemma discussed in the text – to whom should potentially be attributed a legal act if the authenticity of a signature attached is later repudiated by the person who allegedly signed the document? The second general question is whether a qualified electronic signature is equivalent to a handwritten signature in terms of its functions and properties. If the second question is answered in the affirmative, this should probably also imply a positive answer to the first question. This, however, will not be necessarily true *vice versa*. Consequently, an acceptable distribution of risks and benefits between the two persons is the main challenge, while functional equivalence only plays a subsidiary role. Nonetheless, a theoretical analysis of a signature (Chapter 4) is what determines the actual properties, in particular, of a handwritten signature. On a similar note, a theoretical analysis of the concept of legal act implies the overall requirements on such an act (Chapters 2 and 3) as they have been established especially in private laws of Germany and the Czech Republic, and it is also useful for getting the idea what a legal act performed through electronic means is as well as for evaluating such an act. This is also supported by an analysis of the applicable laws in the two mentioned countries (Chapter 5).

Contents.

In the Czech environment (Chapter 2), the notion of *legal act (legal transaction, legal action)* is used both in a broader general sense (2.1) in theory and in a narrower sense (2.2) in private law. A historical probe has also been made into the General Civil Code (2.3), with a view to explaining the foundations of the contemporary Czech theoretical system and also looking back at the inception of notions that were developed in early 19th century, especially in the German language. These notions were then developed for use in the German Civil Code, the BGB.

In German doctrine, the notion is typically used within private law (Chapter 3), where it is designated in two closely related ways, specifically as *das Rechtsgeschäft* and *die Willenserklärung*. The text shows how the German doctrine differs from the Czech one also by employing a slightly different structure of terminology. A legal act (a legal transaction) has a much more specific quasi-normative substance in the German

doctrine, where it typically refers to autonomous establishment of regulated relationships between persons. In his theoretical concept, *Flume* places a characteristic emphasis on legal acknowledgment, i.e. the permissibility of contents, which – according to *Flume* – better conforms to the legislative maxim of *ius suum cuique tribuere* also in private relationships (3.3.2), as their creation would otherwise be excessively affected by "self-aggrandisement" (*Selbstherrlichkeit*). *Flume* requires that the parties act mostly using various "*figures"*, which the applicable law pre-established as samples of legal action, for example as standard types of contracts. A similar channelling function of law is also found by *Fuller* in common law (4.4); however, he mostly focuses on the legal certainty associated with the nature of the relationship and the possibility of resolving a potential legal dispute. However, *Flume* otherwise deals with protection of private autonomy and private law as a sector. He rejects a direct effect of constitutional norms as well as their indirect effect (*die Drittwirkung*) because he believes that they, as such, do not fit into private law; what should rather be directly used are rules and principles immediately governing private law which correspond to the above norms, including especially the concept of good morals.

For *Flume*, legal acts play an important role in an individual's self-determination, albeit on the background of existing legislation. In the German doctrine, the process of establishing the theory of legal action took at least a century. The critical point lies in the relationship between inner will and its outer manifestations. In particular, the possibility of an error (also termed "mistake") on the part of the acting person is then likely to be, in theory, most similar to the dilemma discussed in this thesis, i.e. to whose detriment will be a potential repudiation of authenticity of a signature by the person who allegedly attached it. Similar to an error, it is not possible to unambiguously morally attribute a failure or fault, and the legislature has no reason to side with one of the parties to a private legal transaction. The practice now prefers to construe legal action based on the recepients's "objective horizon" (3.2.1) and the theory of validity (*Geltungstheorie,* section 3.3.4) of legal action. However, *Flume* does not find any of the theories entirely satisfactory as the matter in question entails an *a priori* unresolvable conflict between the principle of self-determination and the principle of self-responsibility of an individual (3.3.5).

Chapter 4 provides an analysis of a handwritten signature and alternative electronic forms in terms of theory of law. Many of the requisites of a signature are

often not explicitly laid down in the legislation and are only elaborated in the doctrine. The doctrines of the Czech Republic, Germany and common law are discussed in the thesis. A summary is provided of the types of techniques used to implement electronic signature which find various degrees of recognition. Electronic signature is also discussed from the viewpoint of cryptology, which considers a "digital signature" to be a proof of the origin of data or a data message, or authentication of the originator, as the case may be. In terms of electronic practice, this chapter reflects on the possible need for setting a commitment or signing policies.

Chapter 5 then proceeds to the notion of *electronic legal transaction ("act")* and its explication, especially in view of the jurisprudence and private law applicable in the Czech Republic and Germany. Both these jurisdictions refer to an informal legal act as a standard. The German doctrine provides a more detailed theory (5.2.1) of legal acts made by electronic means, with classification to electronically transmitted expressions of will (5.2.1.1) and electronically created expressions of will (5.2.1.2), which may be automated. In respect of the written form of a legal act, both the structure and terminology slightly differ. In Czech law, attention must be paid to the notion of *writing* (5.1.3), while German law is characteristic using the term *electronic document* (*elektronische Dokument,* section 5.2.5.2). The applicable laws of the two countries substantially differ in terms of the requirements for a written form of a legal transaction, where Czech law appears to satisfy itself with a simple electronic signature (5.1.5), while German law requires a qualified electronic signature (5.2.5.2). This is why the Czech legislation is criticised in the conclusions (5.3 and 11.7.3.4) of the thesis.

Chapter 6 focuses on the new EU Regulation (eIDAS), and specifically on its part denoted as *trust services*, which covers notions and concepts derived from electronic signature. Interpretation is provided in terms of the eIDAS Regulation itself and of the European Union law. The quantity of described terms and detail of elaboration ensue from the complexity of the framework established by the Regulation, and from the number of questions and issues that arise within this novel piece of legislation, the need to not omit any legal question that might arise in the use of higher versions of electronic signature on the part of the person attaching his/her signature (or seal) – the "signatory" or "creator of a seal" – and the relying person. The introductory sections (6.1 and 6.2) provide primarily the first basic insight into the Regulation. The subject and scope of the Regulation (6.3) are explained, along with its application.

Explication is provided for the new definition of simple electronic signature (6.4) and its sense. This is followed by description of authenticating electronic signatures (6.5), in particular an advanced (6.5.1) and qualified (6.5.3) electronic signature, where the latter has legal effects equivalent to a handwritten signature. The notion of electronic seals (6.6) is an absolute novelty. The thesis also provides a new opportunity for discussing the purpose of introducing an advanced electronic seal (6.6.4), which may also lie in enabling electronic confirmation of a legal act directly by the given juristic person, but rather only within subsequent national implementation. An electronic time stamp (6.7) is an additional service. Explanation is also given for trust services and their providers (6.8). Trusted lists (6.9) are crucial for national and, particularly, for cross-border legal transactions. Higher versions of signature may require qualified electronic signature creation devices (6.10). The Regulation also provides in general for the subject of (technical) validation of a qualified electronic signature (6.11). The Regulation establishes responsibilities of the trust services provider (6.12) and of the Member State (6.13). A separate issue is the duty to accept electronic transactions bearing an electronic signature (6.14). The evidentiary effects of the higher versions of electronic signatures and seals are made more clear in comparison with the evidentiary value of other regulated digital objects (6.15). The criticism of various shortcomings of the Regulation is divided into 15 individual issues (6.16). The author presents a possible status hypothesis (6.17) and suggests that the author of the draft might have been influenced by the French concept used in the *Code civil*, where numerous legal duties are implicated without further ado by technical standards and specifications.

Chapter 7 briefly describes implementation in the Germany of the parts of the eIDAS Regulation examined in the thesis, with a view to enabling subsequent comparison with Czech implementation. The manner of implementation always indirectly implies the way how the eIDAS Regulation is conceived and construed itself (Chapter 6). Following a description of the process of adopting (7.1 and 7.2) the belatedly enacted *eIDAS-Durchführungsgesetz*, the main attention is focused on the *Vertrauensdienstegesetz* (7.3), embodied in the former. A minor amendment was also made to the German *Zivilprozessordnung* (7.4). No implementing decree has yet been adopted in Germany.

Chapter 8 comprises an overview of similar implementation of the eIDAS in the Czech Republic, especially through transposition Act No. 297/2016 Coll., on trust

services for electronic transactions. Most attention will likely be paid to the adapting and recepting provisions (8.2). An analysis is also provided of the specifying and supplementing provisions (8.3), as well as the institutional and competence provisions (8.4) and provisions on sanctions (8.5). The transposed terms are used in dozens of amendments (8.6) throughout the legislation; but no changes were made to the rules of evidence (8.7). In the conclusion of this chapter, an overview is provided of topics which the author of the thesis believes to have been omitted during implementation (8.8) and provisions that were cancelled without explicit replacement (8.9), thus bringing smaller or bigger changes to the legislation of the Czech Republic.

Chapter 9 deals with certain options for legal acts executed with an electronic signature under the laws of the Czech Republic following the effective date of the transposing and amending law related to the eIDAS. Certain legislative comments are provided (9.1). A brief note is made on the background security of drafting documents by public-law creators (9.2), as an important prerequisite for the legal presumption of accuracy of public instruments. Certain options are mentioned in terms of electronic filing and fulfilment of the requisites within electronic filing (9.3). A concise discussion is dedicated to the possibilities of private legal transactions (9.4), including a suitable concept of evidentiary effects of a qualified electronic signature.

Chapter 10 provides a basic summary of the options for private electronic legal transactions made by a juristic person under the Czech legislation. The legislation is based on the fiction theory and requires that transactions be made for a juristic person by its representatives (10.1). The basic theoretical possibilities of the concept of electronic agent are debated (10.2). It becomes clear that a link to a specific representative is generally not suitable and practical in the case of automatic operation of juristic persons. Legal acts in electronic commerce (10.3) are based on the EU law, which does not require identification of a natural person acting for a juristic person as its representative. The analysis shows that an advanced electronic seal could be used optionally to technically secure the provision of mandatory information (10.3.3). In the case of other electronic agents (10.3.4), the use of advanced or qualified electronic seals is possible, but need not suffice. At the end of the chapter the thesis discusses the requirements for a written form to be met in the case of legal transactions made by a juristic person by electronic means (10.4).

Conclusions (results).

The thesis implicitly concludes that implementation of a qualified electronic signature is a complex issue (cf. Chapter 6 and its scope). This fact, together with the need for obtaining the necessary electronic devices, is a burden for the signatory which is unparalleled for handwritten signatures and is probably the main reason for the low penetration (beginning of Chapter 11 and section 11.7.4) of higher versions of electronic signature.

The methodology of electronic signatures ensures independent professional control of each of its component parts and thus provides the signatory with the possibility of making autonomous legal acts, together with an assurance of his/her autonomy. However, the eIDAS Regulation is incomplete (11.5) as it does not provide, for example, for the security of signature creation applications or of the system environment. This is why the signatory should arrange voluntarily for further needs of his/her computer security. In the public sector, additional security needs should also be arranged for by the law (11.7.3.5), as this is required by the legal presumption of accuracy of public instruments.

The answers to the two aforesaid questions dealt with in the thesis, i.e. whether a qualified electronic signature meets the requirements for a similarly acceptable distribution of benefits and risks between the signatory and the relying person, and whether it provides a functional equivalence to a handwritten signature, thus differ in terms of both the legal rules and substance. An affirmative answer in terms of the law is provided by the Regulation itself (11.7.6); however, given the gaps in its provisions, various objections can be raised in terms of substance and evidentiary value. The mentioned incompleteness of the eIDAS Regulation does not benefit the relying person either, as it reflects in the latter's lesser legal certainty.

Repudiation of authenticity is still rare in practice (introduction of Chapter 11), and this is also true of electronic signatures. In private law, the dilemma in repudation of authenticity is weakened by a duty to prove a cause (11.2), while in public law it relates to the background security of the public-law originator (11.1), which however must be real.

This conclusion corresponds to the multiple gaps in the Regulation (11.5). The thesis deals with the possibilities of overcoming the gaps by detailed national

implementation, i.e. by means of supplementing and specifying provisions. The conclusion therefore first provides a general overview of the legal arguments for and against a more detailed national implementation in the Czech Republic (11.6), followed by specific suggestions for supplementation (11.7.3), also as regards repudiation (11.7.3.2) and automation (11.7.3.3), revision of private law in the Czech Republic (11.7.3.4) and recommendations for public law (11.7.3.5). Different substantive implementation in Czech law is also advocated by comparison with German implementation (11.7.1).

However, even after supplementation, there will still likely be certain residual risks, also given the fragility of computer systems (introduction, Chapter 11). Instead of ever laying down further details and specifying more duties, the author therefore also suggests entirely different approaches for technical and legal development which would allow to avoid the dilemma of repudiation or deal with it otherwise. An *a priori* limitation of applicability (11.3) is proposed based on the type of the relevant act or the financial limit. An alternative could be to transform the relevant transaction into a contestable process (11.4).

The possibility of creating a qualified signature by distance means (11.7.4) could popularise the use of this type of signature; however, it does not, in itself, resolve the legal and technical issues.

The conclusion also comprises the notions of preconception (11.7.2.) and electronic legal acts by a juristic person and electronic seal (11.7.5) discussed below.

Partial summaries are also provided in the conclusions of the individual chapters.

Original findings.

In terms of theory of law, the greatest benefit of the thesis lies in a comprehensive description of the properties and functions of a signature (Chapter 4). It summarises and interlinks the findings of the Czech, German and common-law doctrines. Moreover, the thesis reflects on the types of techniques used to implement electronic signature, as well as signature "commitments" and "policies", i.e. requirements which more often follow from the various manners of implementing an electronic signature, rather than from the practice of handwritten signatures. Chapter 4 shows a concept of signature in terms of jurisprudence which could also perhaps be

used for new implementing techniques, and thus also for legal considerations of various types.

In respect of the dilemma of repudiation of signature, the legal doctrine contributes on the most general level by analysing the conflict of the principles of self-determination and self-responsibility (3.3.5). The former principle requires a superiority of the authentic inner will of an individual, while the latter accentuates the same individual's responsibility for the actual expression of will, and calls for restraint in such expression. The analysis further reveals that a legal transaction requires the individual's preconception (11.7.2) as to how the addressee will understand it in legal terms. Electronic legal transactions might take even currently unknown forms provided that the acting person and the relying person will be able to learn in advance what legal significance will be attached to the particular expression of will or that this will be sufficiently clear in view of the common usage. The applicable law confirms these theoretical findings in specific cases, e.g. in respect of the duty to provide advice (7.3.3) of the legal effects of a qualified electronic signature or setting the duties to provide information on the individual technical steps leading to execution of a contract (under the EU e-Commerce Directive, section 10.3.1). A similar role is played by the normative references to usages or even the established practice of the parties (e.g. Sections 545 and 556 of the Czech Civil Code).

In terms of implementing EU legislation adopted in the form of a regulation, the thesis surprisingly points out that in order to achieve uniform effects of such a regulation in all the EU Member States, it might be necessary in the Czech Republic not only to exercise self-restraint in terms of not adding any provisions to the subject of the legislation, but even – in contrast – adding such provisions that would supplement the rights and obligations which follow in other EU Member States from sources that are not automatically considered sources of law in the Czech Republic. Such sources could be technical standards and specifications, dozens of which have been published in connection with the eIDAS Regulation. Their publication corresponds to the methodical concept of the eIDAS Regulation. This is why the thesis also states a hypothesis that the proponents of the draft Regulation in the Commission might have been influenced by this concept, which follows especially from the French *Code civil* (6.17).

The thesis describes a so called "New Approach" developed in the EU law regarding the not strictly obligatory status of the technical standards, which is relatively

unknown in the Czech Republic, and uses that approach when describing interpretation of Art. 29 eIDAS (6.10.2). Compliance with the technical standards gives rise to a presumption of conformity and increases legal certainty, but does not strictly limit the development of products or services only within the technical standards. In terms of theory of law, the presumption of conformity is specific in that it represents alternative compliance with the disposition part of the legal rule, rather than with its hypothesis, as is true of legal presumptions.

A novelty introduced by the eIDAS that deserves attention are "trusted lists" (6.9) and their form, as they must be established "in a form suitable for automated processing", which is also an originary legal form of keeping a trusted list. This does not exclude that the list might also be human-readable or quasi-human-readable; nonetheless, automatic processability results not only in the intended use for automation (especially evaluation of validity of electronic signatures), but also secondarily implies the easy translatability of the contents into any language, especially into the official languages of other Member States. Similar legislative solutions and underlying technologies could also be used to create extracts (copies of entries) from official registers of the EU Member States; this would avoid the need for their certified translations in cross-border use. This new form and especially its originary and legally decisive nature replaced the previous dichotomy of machine-processable form and human-readable form of trusted lists, where the latter form was legally decisive.

In conclusion, different methods than those used in the eIDAS Regulation are suggested for a practical solution to the issue of repudiation of signatures. This is true, on the one hand, of the *a priori* option of restricting the applicability of an electronic signature by registering such limitations in the qualified certificate. The restrictions could take the form of financial limits (6.16.10, 11.3) or restrictions based on the type of activity (6.16.9, 11.3). A restriction based on the type of activity could have considerable significance, e.g., for distinguishing professional and private use.

Another method that could reduce the risks borne by persons using electronic signature, is the suggested transformation of a one-off act (signature) into a process consisting of several steps (11.4). Practical and legal implementation can take various forms.

The thesis indicates a different possible sense and purpose of introducing an advanced electronic seal and qualified electronic seal than that currently advocated by the Czech legal doctrine (6.6.4). It is suggested that the mentioned seals should also serve, in legal terms, the same purpose as that of a signature in general, save for the fact that this legal effect is not directly proclaimed by the Regulation, but it is rather left to national implementation whether it will admit such a consequence. In terms of automated creation, an advanced electronic signature and an advance electronic seal are generally equivalent, which is also the approach used by the eIDAS Regulation itself (6.6.4). The two concepts mentioned above also overcome the contradictions (equality, non-discrimination) of the current interpretation that have arisen at the level of fundamental rights, both in the EU and the Member States.

Other than in the use cases specified in the eIDAS Regulation itself, an advanced electronic seal is also applicable to confirm mandatory information provided by e-shops operated by juristic persons (10.3.3), even if a legal transaction is involved. However, its use is legally optional – it is a voluntary security mechanism, similar to (qualified) certificates for authentication of websites, which are now also covered by the eIDAS Regulation (in terms of their issuing).

In respect of legal transactions taken by an electronic agent of a juristic person, the thesis indicates that it would admittedly be a natural step to omit the link to a specific natural person. Where legal transactions are taken by an e-shop, the EU law itself does not require the involvement of a representative (10.3.1). In conclusion, it is suggested (11.7.5) to lay down in the Czech laws similar provisions also for other cases of legal acts taken by an electronic agent of a juristic person.

Keywords

Legal transaction, legal transaction of legal person, signature, electronic signature, electronic seal, legal theory of signature, eIDAS, electronic legal transaction, electronic transaction, writing, electronic document, electronic time stamp, authentication, identification, legal comparison, Czech law, the EU law, German law, qualified electronic signature, qualified certificate, QES, AdES, QSCD, QESeal, AdESeal, QESealCD, QTS, trusted lists, trust services, TSP.