UNIVERZITA KARLOVA

Právnická fakulta

Mgr. Jiří Švejda

Elektronická právní jednání se zaměřením na prostý elektronický podpis

Rigorózní práce

Pověřený akademický pracovník: prof. JUDr. PhDr. David Elischer, Ph.D.

Tematický okruh: Občanské právo

Datum vypracování práce (uzavření rukopisu): 27.03.2024

Prohlašuji, že jsem předkládanou rigorózní 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 260 581 znaků včetně mezer.

Mgr. Jiří Švejda

V Praze dne 27.03.2024

Obsah

1. Úvod ... 1
2. Obecná úprava podpisu a jeho význam ... 4
2.1. Význam podpisu ... 4
2.2. Funkce podpisu ... 5
2.3. Historická úprava ... 7
3. Současná právní úprava a jednotlivé druhy elektronických podpisů ... 10
3.1. Kvalifikovaný elektronický podpis ... 10
3.2. Zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronické podpisy ... 11
3.3. Zaručený elektronický podpis ... 12
3.4. Prostý elektronický podpis ... 14
3.5. Biometrický podpis ... 21
4. Písemná forma právního jednání a elektronické prostředky ... 25
4.1. Písemná forma právního jednání ... 25
4.1.1. Zachycení obsahu ... 27
4.1.2. Určení jednající osoby ... 28
4.1.3. Elektronický nebo jiný technický prostředek ... 30
4.1.4. Písemná forma, listina a písemnost v elektronické podobě ... 30
4.1.5. Písemnost *versus* dokument ... 32
4.1.6. Vzájemný vztah ustanovení § 561 a § 562 občanského zákoníku ... 34
4.1.7. Dílčí závěr ... 37
4.2. Digitální kontinuita a související praktické aspekty ... 38
4.2.1. Aktuální digitální kontinuita ... 39
4.2.2. Potenciální digitální kontinuita ... 40
4.2.3. Autenticita dokumentu *versus* pravost dokumentu ... 41
4.2.4. Platnost elektronických podpisů a pečetí ... 42
4.2.5. Ověřování pravosti elektronického podpisu ... 44
4.2.6. Vyvratitelná domněnka pravosti dokumentu ... 46
4.2.7. Uchovávání *versus* archivace ... 49
4.2.8. Elektronická časová razítka ... 51
4.2.9. Kontejnery ... 53
4.2.10. Stárnutí elektronických dokumentů ... 53
4.2.10.1. Vznik elektronického podpisu a hashování dokumentů ... 54
4.2.10.2. Certifikáty ... 56
4.2.10.3. Důkaz o existenci elektronického podpisu v čase ... 59
4.2.11. Jaké dokumenty lze elektronicky podepsat a jakými formáty podpisů ... 61
4.2.12. Dílčí závěr ... 64
4.3. Elektronické smlouvy ... 66

4.3.1. *Click-wrap* smlouvy 66
4.3.2. *Click-through* smlouvy 67
4.3.3. *Browse-wrap* smlouvy 68
4.3.4. *Shrink-wrap* smlouvy 68
4.3.5. *Blockchain* a *smart contracts* 69
4.4. Důkazní účinky elektronických podpisů *versus* (ne)platnost písemného právního jednání 71
5. Rozbor současné judikatury 73
5.1. Analýza jednotlivých rozhodnutí a souvisejících rozporů 73
5.1.1. Email bez elektronického podpisu a požadavek písemné formy 74
5.1.2. Předžalobní výzva doručená emailem 77
5.1.3. Možnost následné změny písemné formy 77
5.1.5. Naskenovaný vlastnoruční podpis 78
5.1.6. Unikátní ID a *click-through* smlouvy 78
5.1.7. Dvoufaktorové ověření v podobě SMS zprávy 79
5.1.8. Podpis myší do prázdného pole na internetové stránce 81
5.1.9. Prostý elektronický podpis je (ne)dostačující ke splnění písemné formy 82
5.1.10. Neplatné elektronické podpisy a platně uzavřená smlouva 86
5.1.11. Záměna požadavku písemné formy a identifikace 86
5.2. Návrh sjednocení přístupu českých soudů 87
6. Perspektiva elektronických podpisů v budoucím vývoji 89
6.1. Možné dopady eIDAS 2.0 89
6.2. eDoklady 91
7. Závěr 92

1. Úvod

Digitalizace a s ním spojené elektronické právní jednání je každodenní součástí našich životů již desítky let. I přes to, že první úprava právního jednání elektronickými prostředky, resp. elektronických podpisů, byla na úrovni Evropské unie schválena v minulém tisíciletí[1] a soukromé právo s právním jednáním prostřednictvím informačních technologií počítalo od 90. let minulého století,[2] určité otázky zůstávají sporné dodnes.

Vzhledem k rozvoji nových technologií, včetně technologií informačních, a jejich exponenciálnímu růstu je zcela jasné, že bude docházet i nadále ke stále vyšší míře digitalizace v oblasti právního jednání a s tím spojeného nárůstu uzavírání smluv na dálku.[3] Otázkou tedy je, jakou vhodnou formou nahradit tradiční instituty, jako jsou písemná právní jednání, listiny a vlastnoruční podpisy, aby byla zajištěna právní jistota všech jednajících stran.

Trend poslední doby, který lze pozorovat ve společnosti, je opouštění složitých postupů a snaha o dosažení co největší míry zjednodušení běžného života. Toto je ve většině případů i základní myšlenka nových technologií.

Předmětem této práce jsou tak právní jednání elektronickými prostředky se zaměřením na prostý elektronický podpis, tedy nejnižší formu elektronického podpisu. Ten je upraven jak na úrovni Evropské unie v nařízení eIDAS, tak v českém právním řádu, konkrétně v zákoně o službách vytvářejících důvěru. Právní jednání elektronickými prostředky jsou pak reflektována i občanským zákoníkem, nicméně vyvstávají v této souvislosti sporné otázky týkající se zachování písemné formy právního jednání, a to jak v akademické obci, tak v judikatuře soudů. Zejména nekonzistentní či nejasné rozhodování soudů pak vytváří právní nejistotu, která je v praxi spojena také s vynakládáním nadbytečných nákladů, což je bezesporu nechtěný stav.

V této souvislosti je věnována pozornost i vyšším formám elektronických podpisů, a to za účelem komparace jejich jednotlivých aspektů a celkového srovnání právě s prostým elektronickým podpisem. Dle názoru autora totiž v mnohých případech není při jejich ověření dostatečně kladen důraz na jednotlivé aspekty, které mají přinést vyšší míru spolehlivosti. Subjekty či orgány veřejné moci se tak mnohdy spokojí s pouhým konstatováním, že je tato

[1] Směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy.
[2] § 40 občanského zákoníku a § 24a hospodářského zákoníku.
[3] Nejčastěji prostřednictvím e-shopů, aplikací či platforem.

vyšší míra podpisu připojena, a to i v případech, kdy je jejich digitální kontinuita narušena, případně se nejedná o vyšší úroveň elektronického podpisu, a důkazní funkce může teoreticky spadnout na úroveň elektronického podpisu prostého. Ve světle připravovaných změn lze navíc očekávat praktické zjednodušení vytváření vyšších forem elektronických podpisů, a proto bude těmto aspektům zapotřebí věnovat větší pozornost.

Cílem této práce je tak odpovědět na následující výzkumné otázky:

1) Je prostý elektronický podpis dostatečný k dodržení písemné formy právního jednání?

2) Může být písemná forma právního jednání splněna i bez připojení podpisu?

3) Jaké jsou výhody vyšších úrovní elektronických podpisů oproti prostému elektronickému podpisu a jsou vždy brány v potaz?

4) Je současná právní úprava správně aplikována soudy?

Práce je členěna do šesti kapitol. První kapitola je tvořena úvodem. Ve druhé kapitole je představena obecná úprava a význam podpisu se stručným historickým exkurzem potřebným pro posouzení možné aplikovatelnosti dřívějších závěrů na aktuální právní úpravu.

Třetí kapitola je věnována současné úpravě a jednotlivým druhům elektronických podpisů, tedy dělení na kvalifikovaný elektronický podpis, zaručený elektronický podpis a prostý elektronický podpis a české specifikum v podobě zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu pro elektronické podpisy, lidově známý jako uznávaný elektronický podpis.[4] Na závěr kapitoly je také rozebrán v praxi čím dál tím více užívaný biometrický podpis.

Čtvrtá kapitola se věnuje písemné formě právního jednání, tedy podrobnému rozboru ustanovení § 561 a § 562 občanského zákoníku, a to včetně jejich vzájemného vztahu. Dále jsou rozebrány aspekty digitální kontinuity u vyšších forem elektronických podpisů a jejich komparace s prostým elektronickým podpisem. V poslední části kapitoly je věnována pozornost různým typům elektronických smluv a rozdílům mezi důkazními účinky jednotlivých typů elektronických podpisů a (ne)platnosti písemného právního jednání.

[4] Ačkoli toto označení obsahuje i kvalifikovaný elektronický podpis, jak bude rozebráno níže.

V páté kapitole se autor této práce věnuje rozboru současné judikatury, respektive jejím rozporům zejména v otázkách emailu bez elektronického podpisu a (ne)splnění požadavku písemné formy, vztahu ustanovení § 561 a § 562 občanského zákoníku, povaze naskenovaného vlastnoručního podpisu, unikátního ID a click-through smluv, dvoufaktorového ověření v podobě SMS zprávy, podpisu myší do prázdného pole na internetové stránce, požadavku na vyšší formy elektronických podpisů ke splnění písemné formy a záměny požadavku písemné formy a identifikace. V poslední části kapitoly je rozebráno možné řešení pro sjednocení soudní praxe.

V šesté kapitole je nastíněna perspektiva elektronických podpisů v budoucím vývoji, zejména s ohledem na plánovanou novelu nařízení eIDAS, známou pod označením eIDAS 2.0. a nedávno spuštěnou aplikaci eDoklady.

Druhá a třetí kapitola jsou zpracovány prostřednictvím deskriptivní metody, kapitoly čtyři a pět pak prostřednictvím metody deskriptivní a analytické.

Ačkoli se z pohledu autora jedná o téma velmi aktuální, na akademické úrovni je řešeno převážně časopiseckou literaturou uvedenou v této práci. Z akademických prací lze zmínit disertační práci Kmenta,[5] která se ovšem věnuje spíše nařízení eIDAS jako celku včetně komparace s úpravou německou, a problematika prostých elektronických podpisů a rozporné judikatury, řešená v této práci, je zmíněna spíše okrajově. Blíže se tématice rozebírané v této zabývá disertační práce Jareše,[6] která byla publikována v průběhu přípravy této rigorózní práce. Autor této práce tak z disertační práce při přípravě nevycházel, ale použil ji pouze ke srovnání svých závěrů. To samé platí o diplomové práci Běhounkové.[7] Oproti posledně dvěma zmíněným je v této práci detailněji rozebrána judikatura jednotlivých soudů, komparace jednotlivých aspektů vyšších forem elektronických podpisů s podpisem prostým a náležitosti udržování digitální kontinuity. Nejedná se tak o komparaci s již existující literaturou.

[5] KMENT, Vojtěch. *Elektronické právní jednání: Srovnávací analýza s důrazem na využití elektronického podpisu podle práva EU, České republiky a Německa*. Praha, 2018. Disertační práce. Právnická fakulta Univerzity Karlovy.
[6] JAREŠ, Adam. *SMLOUVA PODEPSANÁ ELEKTRONICKÝM PODPISEM*. Plzeň, 2022. Disertační práce. Západočeská univerzita v Plzni Fakulta právnická.
[7] BĚHOUNKOVÁ, Tereza. *Písemná forma právního jednání v elektronickém obchodu*. Diplomová práce. Praha: Právnická fakulta Univerzity Karlovy, 2023.

2. Obecná úprava podpisu a jeho význam

Pro pochopení dané problematiky je nejprve nutné rozebrat, jaký má podpis význam a jaké jsou jeho funkce. Dále je třeba věnovat pozornost historické genezi právní úpravy, a to z důvodu posouzení možné aplikovatelnosti předešlých závěrů a soudních rozhodnutí na právní úpravu současnou.

2.1. Význam podpisu

I přes dlouhý historický vývoj a význam podpisu jako právního institutu občanský zákoník neobsahuje jeho pozitivní definici.[8] Jeho funkci historicky plnil zejména podpis vlastnoruční, který je různými autory označován odlišně. Dle Podaného se jedná o specifickou křivku vytvořenou psacím nástrojem a psacím médiem na hmotný substrát (obvykle na papír), který zachycuje dané právní jednání. Mělo by se jednat o jedinečné, snadno opakovatelné vyjádření dané osoby, avšak těžko napodobitelné osobou jinou. Jednání je pak spojeno s danou osobou vpitím či vtlačením do hmotného substrátu.[9] Dle Kmenta se jedná o aktivní činnost ruky podepisující osoby, při které dochází k trvalému vtělení tahu písma do psacího materiálu, kdy schopnost provést ustálený podpis spočívá v biomotorické paměti dané osoby. Jelikož tah pera na papír má více aspektů, jako je sklon, rychlost a tlak pera, jeho napodobení či padělání je obtížnější ve srovnání s pouhým obrazovým vyhotovením.[10] Korbel a Melzer[11] podpis chápou jako vlastnoruční písemný projev prostřednictvím znaků, které mají význam písma. Tím pak může být jméno a příjmení, samotné jméno či příjmení nebo pseudonym, přezdívka či zkratka. Dle Smejkala[12] jde spíše o společenský zvyk, resp. dohodu, jímž se vyjadřuje souhlas s obsahem podepisovaného dokumentu. Nemusí se ovšem jednat nutně o podpis vlastnoruční, ale dle autora by se mohlo stejně jednat o podpis vlastnonožní či jakýkoli jiný.

Rozdílem od jiných biometrických parametrů je pak dle Kmenta volní uvážení podepisující osoby, kdy podepsání určité písemnosti vyjadřuje projev její vůle.[13] S tím souhlasí i Podaný,

[8] Dle Polčáka není vlastnoruční podpis definován v žádném jemu známém právním řádu a jedná se o právní obyčej, vizte POLČÁK, R. Praxe elektronických dokumentů, *Bulletin advokacie*. 2011, č. 7–8, s. 53–61, s. 55.
[9] PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra. *Advokátní deník* [online]. 2020 [cit. 2023-04-11]. Dostupné z: https://advokatnidenik.cz/2020/05/04/podepisovani-soukromych-listin-vcera-dnes-a-zitra/.
[10] KMENT, Vojtěch. *Elektronické právní jednání: Srovnávací analýza s důrazem na využití elektronického podpisu podle práva EU, České republiky a Německa*. op. cit. 5, s. 60.
[11] KORBEL, František a MELZER, Filip. Písemnost, elektronický a biometrický podpis v elektronickém právním jednání. *Bulletin advokacie*. 2014, roč. 2014, č. 12, s. 32.
[12] SMEJKAL, Vladimír. Kryptografický a dynamický biometrický podpis podle platné právní úpravy. Právní rozhledy [online]. roč. 2019, č. 10 [cit. 23.09.2023]. Dostupné z: beck-online.cz.
[13] KMENT, Vojtěch. *Elektronické právní jednání: Srovnávací analýza s důrazem na využití elektronického podpisu podle práva EU, České republiky a Německa*. op. cit. 5, s. 60-61

dle kterého dochází k vytvoření podpisu až v souvislosti s právním jednáním, tj. nikoli předem.[14]

Tradičně je podpis tvořen kombinací jména a příjmení či jejich různých zkratek. Dle Zuklínové[15] je ovšem možné pro účely podpisu i použití pseudonymu.[16] Podle Nejvyššího soudu neuvedení jména a příjmení osoby, nebo jejich nečitelnost, nemá z hlediska požadavku dodržení písemné formy význam.[17] Vrchní soud v Olomouci dokonce připustil, že osoba může mít více podpisů a tyto střídat, podle toho, zda jedná sama za sebe, nebo v zastoupení za právnickou osobu.[18]

2.2. Funkce podpisu

V odborné literatuře je věnována pozornost i funkcím podpisu. Kment s přihlédnutím k německé nauce dovozuje sedm funkcí podpisu.[19] Jsou jimi funkce:

- ověřovací – srovnáním se vzorem se zjistí pravost podpisu;
- identifikační – podpis se váže k osobě určité totožnosti;
- pravostní – podpis pod písemností dokládá, že podepsaná osoba písemnost podepsala a je pravá;
- uzavírací – podpis indikuje konečnost vůle a chrání ji na listině před doplňováním;
- varovací – podepisující osoba je vytvořením podpisu varována o právní závaznosti;
- zachovávací – podpis a písemnost umožňují trvalé zachycení právního jednání;
- důkazní – podepsanou písemnost je možné použít jako důkaz.

Čermák[20] dovozuje funkce:

- označovací – slouží k identifikaci osoby, která učinila právní úkon;
- deklarační – osoba jednat chtěla a projevila svou vlastní vůli; a
- důkazní – ověření totožnosti jednajícího.

[14] PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra, op. cit. 9.
[15] ZUKLÍNOVÁ, Michaela. Právní jednání podle občanského zákoníku č. 89/2012 Sb. Komentář, srovnání se zahraničím a vybraná platná judikatura. 1. vyd. Praha: Linde, 2013. [online] dostupné z právního informačního systému CODEXIS [cit. 2023-04-12]. Komentář k § 561.
[16] § 79 občanského zákoníku.
[17] Rozhodnutí Nejvyššího soudu ze dne 29. 11. 2007, sp. zn. 29 Odo 965/2006.
[18] Rozhodnutí Vrchního soudu v Olomouci ze dne 13. 10. 2022, č.j. 5 Cmo 111/2022-378.
[19] KMENT, Vojtěch. *Elektronické právní jednání: Srovnávací analýza s důrazem na využití elektronického podpisu podle práva EU, České republiky a Německa*. op. cit. 5, s. 65.
[20] ČERMÁK, Karel. Elektronický podpis – pohled soukromoprávní. *Bulletin advokacie*. 2002, roč. 2002, č. 11 - 12, s. 67 - 68

Melzer a Korbel[21] pak za funkce podpisu považují:

- stvrzení konečnosti a vážnosti projevu vůle;
- identifikaci jednajícího;
- záruku autentičnosti (ochrana před falšováním).

Polčák[22] shledává funkce podpisu tyto:

- identifikace osoby;
- deklarace vůle; a
- fixace obsahu.

Dle současné komentářové literatury[23] plní podpis funkce následující:

- identifikace osoby;
- vyjádření vůle; a
- konečnost právního jednání.

Z výše uvedeného vyplývá, že jednou z nejdůležitějších a zároveň základní funkcí podpisu je funkce identifikační. Tu však nelze zaměňovat s prostředkem identifikace, který je v nařízení eIDAS upraven zvlášť.[24] Dle rozhodnutí Nejvyššího soudu[25] navíc platí, že podpis nemá sloužit primárně k identifikaci osoby. S tím souhlasí i Donát, Tomíšek a Fencl, kteří v této souvislosti uvádějí, že hlavní funkcí podpisu je vyjádření konečnosti vůle, nikoli identifikace podepisující osoby.[26] Zatímco existence jedinečného subjektu vycházející z identity je tedy samozřejmostí, otázkou zůstává, s jakou pravděpodobností je zapotřebí tuto identitu prokázat. Tato míra pravděpodobnosti je v případě soukromoprávních jednání závislá na vůli jednajících stran, neboť na rozdíl od veřejného práva[27] soukromoprávní předpisy žádnou konkrétní úpravu neobsahují. Bude tedy vždy záviset na konkrétních okolnostech.[28] Odlišné budou pak případy

[21] KORBEL, František a MELZER, Filip. Písemnost, elektronický a biometrický podpis v elektronickém právním jednání, op. cit. 11, s. 32.
[22] POLČÁK, R. Praxe elektronických dokumentů, op. cit. 8, s. 55.
[23] JANOUŠEK, Michal. § 561 [Písemná forma právního jednání]. In: LAVICKÝ, Petr a kol. Občanský zákoník I. Obecná část (§ 1−654). 2. vydání. Praha: C. H. Beck, 2022, s. 1792, marg. č. 15.
[24] Srov. článek 3 odst. 1 a kapitolu II nařízení eIDAS.
[25] Rozhodnutí Nejvyššího správního soudu ze dne 27. 7. 2017, sp. zn. 2 As 80/2017.
[26] DONÁT, Josef, Jan TOMÍŠEK a Ivan FENCL. *Je publikovaná judikatura k elektronickým podpisům skutečně relevantní?* [online]. [cit. 2023-06-18]. Dostupné z: https://www.epravo.cz/top/clanky/je-publikovana-judikatura-k-elektronickym-podpisum-skutecne-relevantni-116077.html.
[27] Srov. např. zákon č. 250/2017 Sb., o elektronické identifikaci.
[28] K tomu srov. rozhodnutí Nejvyššího správní soudu ze dne 28. 6. 2013, sp. zn. 5 As 1/2011: „*Přímo může být identifikována osoba zpravidla jménem, nepřímo např. podle telefonního čísla, registračního čísla automobilu,*

opakujících se transakcí, které jsou navíc potvrzeny následným jednáním stran (např. poskytování služeb či proplacení faktur), kdy nadměrné požadavky na identifikace vytvářejí zbytečné transakční náklady, a situací, kdy se bude jednat o právně či fakticky významné jednání. Rozhodujícím faktorem pro platné právní jednání v tomto ohledu však vždy zůstává, zda lze zjistit, kdo je podepisující osobou a zda tuto nelze snadno zaměnit s osobou jinou. V této souvislosti je však vhodné upozornit na ustanovení § 565 OZ a (podle některých autorů) domněnku uznání pravosti a správnosti, a to i v případě, kdy se strany dohodnou na nižší míře spolehlivosti identifikace.[29] Dle jiných názorů se však nejedná o domněnku pravosti a správnosti listiny. Jedná se pouze o zakotvení pravidla, že důkazní břemeno ohledně pravosti a správnosti listiny nese ten, kdo se jí dovolává.[30] Pravost a správnost listiny tak není třeba vyvracet, postačí jejich zpochybnění.[31]

Podpis se zpravidla umisťuje za text zachycující projev vůle. Tím se potvrzuje veškeré předchozí znění textu, tedy vyjádření vůle a potvrzení její konečnosti. Podpis je však možné umístit i na místo jiné, pokud je zřejmé, v jakém rozsahu podpis text stvrzuje.[32, 33] Dle judikatury Nejvyššího soudu ČR není zapotřebí stvrzovat každý list zvlášť.[34]

Poslední důležitou funkcí, na které se většina autorů shodne, je funkce důkazní. Ta bude blíže rozebrána v kapitole 4.4.

2.3. Historická úprava

Jak již bylo zmíněno v této práci výše, úprava elektronických podpisů sahá až do minulého tisíciletí. Na Evropské úrovni byla obsažena ve Směrnici EU pro elektronické podpisy ze dne

---

čísla sociálního pojištění, čísla cestovního pasu, apod. Nepřímou identifikaci lze provést rovněž pomocí kombinace významných kritérií, která ji umožňují rozeznat zúžením skupiny, do které patří (věk, povolání, bydliště atd.). Z uvedeného vyplývá, že míra dostatečnosti určitých identifikátorů z hlediska provedení identifikace závisí na souvislostech konkrétní situace. Např. běžné příjmení nepostačí k identifikaci - tj. jednoznačnému určení - osoby v celé populaci země nebo ve velkém městě, ale pravděpodobně bude stačit např. k identifikaci studenta ve třídě nebo ubytovaného hosta v hotelu nebo účastníka konkrétního semináře konaného v daném čase v daném místě.“.

[29] KORBEL, František; KOVÁŘ, Dalibor a AMLER, Pavel. *Interpretace elektronického podpisu a související identifikace v soukromém právu*. Online. Dostupné z: https://www.pravniprostor.cz/clanky/obcanske-pravo/interpretace-elektronickeho-podpisu-souvisejici-identifikace-v-soukromem-pravu. [cit. 2023-06-18].

[30] Opačný názor zastává Nejvyšší soud ve svém rozhodnutí ze dne 29. 11. 2018, sp. zn. 33 Cdo 2181/2018.

[31] BERAN, Vladimír. § 565 [Pravost a správnost soukromé listiny]. In: PETROV, Jan, VÝTISK, Michal, BERAN, Vladimír a kol. Občanský zákoník. 2. vydání (2. aktualizace). Praha: C. H. Beck, 2023, marg. č. 18.)

[32] BERAN, Vladimír. § 561 [Písemná forma]. In: PETROV, Jan, VÝTISK, Michal, BERAN, Vladimír a kol. Občanský zákoník. 2. vydání (1. aktualizace). Praha: C. H. Beck, 2022, marg. č. 1.

[33] JANOUŠEK, Michal. § 561 [Písemná forma právního jednání]. In: LAVICKÝ, Petr a kol. Občanský zákoník I. Obecná část (§ 1−654). 2. vydání. Praha: C. H. Beck, 2022, s. 1792, marg. č. 11.

[34] Rozhodnutí Nejvyššího soudu ze dne 30. 11. 2016, sp. zn. 22 Cdo 2526/2016.

13. prosince 1999.[35] Zajímavé je, že po téměř 25 letech se definice elektronického podpisu výrazněji nezměnila,[36] a nedošlo ani k zásadní změně u jeho vyšší formy, a to zaručeného elektronického podpisu.[37] Právní účinky elektronických podpisů byly taktéž upraveny podobně jako v současnosti, konkrétně jim nesměly být odepírány právní účinky nebo nesměly být odmítány jako důkazy v soudním řízení.[38] Lze tedy konstatovat, že tehdejší úprava byla zdařilá, neboť nebylo zapotřebí zásadnějších změn.

V českém právním řádu byla úprava písemné formy právního jednání obsažena v ustanovení § 40 občanského zákoníku 1964,[39] konkrétně od tzv. velké demokratizační novely provedené zákonem č. 509/1990 Sb., kterým se mění, doplňuje a upravuje občanský zákoník 1964.

Dle § 40 odst. 3 občanského zákoníku 1964 platilo, že: „*Písemný právní úkon je platný, je-li podepsán jednající osobou; činí-li právní úkon více osob, nemusí být jejich podpisy na téže listině, ledaže právní předpis stanoví jinak. Podpis může být nahrazen mechanickými prostředky v případech, kdy je to obvyklé*“. § 40 odst. 4 občanského zákoníku 1964 pak stanovoval, že: „*Písemná forma je zachována, je-li právní úkon učiněn telegraficky, dálnopisem nebo elektronickými prostředky, jež umožňují zachycení obsahu právního úkonu a určení osoby, která právní úkon učinila*“.

Úprava v jednom paragrafu mohla svádět k nesprávnému výkladu jako nedělitelného celku. V praxi však takový výklad nebyl zaujímán a ani o platnosti prostého faxu bez podpisu jako písemného jednání nevznikaly větší pochybnosti. [40]

Po implementaci výše uvedené směrnice EU pro elektronické podpisy a přijetí českého zákona o elektronickém podpisu byla na konec znění § 40 odst. 3 občanského zákoníku 1964 doplněna věta: „*Je-li právní úkon učiněn elektronickými prostředky, může být podepsán elektronicky*

[35] Směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy.
[36] Srov. čl. 2 odst. 1 směrnice, dle kterého se elektronickým podpisem rozumí údaj v elektronické podobě, který je připojen či logicky spojen s jinými elektronickými daty a který slouží jako metoda ověření pravosti.
[37] Srov. čl. 2. odst. 2 směrnice, dle kterého se zaručeným elektronickým podpisem rozumí elektronický podpis, který splňuje tyto požadavky: a) je jednoznačně spojen s podepisující osobou, b) umožňuje zjistit totožnost podepisující osoby, c) je vytvořen s využitím prostředků, které podepisující osoba může mít plně pod svou kontrolou, a d) je spojen s daty, ke kterým se vztahuje tak, aby bylo možno zjistit jakoukoli následnou změnu těchto dat.
[38] Srov. článek 5 směrnice EU pro elektronické podpisy a článek 9 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).
[39] Obdobná úprava byla obsažena i v § 24 a hospodářského zákoníku.
[40] KORBEL, František; KOVÁŘ, Dalibor a AMLER, Pavel. *Interpretace elektronického podpisu a související identifikace v soukromém právu*, op. cit. 29.

podle zvláštních předpisů.“ Dle Matejky se jednalo o právo elektronické právní jednání podepsat, nikoli povinnost.[41]

Elektronický podpis byl v zákoně o elektronickém podpisu definován jako „*údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě*“.[42] Definice tedy navíc oproti současné úpravě obsahovala požadavek ověření identity podepsané osoby.

Mimo tuto skutečnost však v současné právní úpravě nedošlo v porovnání s předchozí právní úpravu k žádné výrazné obsahové změně. Došlo však k systematické změně, kdy ustanovení § 40 občanského zákoníku 1964 je upraveno v § 561 občanského zákoníku, zatímco čtvrtý odstavec § 40 občanského zákoníku 1964 byl vyčleněn do samostatného ustanovení § 562 odst. 1 občanského zákoníku.[43]

Obecně lze tedy konstatovat, že právní úprava před účinností současných právních předpisů obsahovala velmi podobnou úpravu, a proto tehdejší právní polemika nad problematikou písemné formy a vybraná soudní rozhodnutí a závěry odborné literatury mají relevanci i dnes.[44]

[41] MATEJKA, Ján. Úprava elektronického podpisu v právním řádu ČR. *Právník*. roč. 2001, č. 6. s. 557–586 [online] dostupné z právního informačního systému CODEXIS [cit. 2023-09-18].
[42] § 2 písm. a) zákona o elektronickém podpisu.
[43] BEZOUŠKA, P., HAVEL, B. Občanský zákoník: Srovnávací komentář. [Systém ASPI]. Wolters Kluwer [cit. 2023-6-3]. ASPI_ID KO89_p12012CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X, § 562.
[44] Což reflektují i vybraná soudní rozhodnutí uvedená v kapitole **Error! Reference source not found.**.

3. Současná právní úprava a jednotlivé druhy elektronických podpisů

Elektronické podpisy jsou v současné době v českém právním řádu upraveny jednak na úrovni národní legislativy prostřednictvím ZSVD a dále na úrovni práva Evropské unie nařízením eIDAS.

Nařízení eIDAS a ZSVD upravují nejenom elektronické podpisy, ale i elektronické pečetě a elektronická časová razítka. Zatímco elektronické podpisy mohou užívat pouze fyzické osoby,[45] elektronické pečetě mohou užívat pouze právnické osoby.[46] V případě elektronických podpisů jde o projev právního jednání, zatímco v případě elektronických pečetí jde o zaručení původu a integrity.[47] Tato práce se specificky elektronickým pečetím blíže nevěnuje, pouze je bere v potaz tam, kde se závěry práce pro elektronické podpisy dají použít obdobně. Elektronická časová razítka jsou z důvodu udržení aktuální digitální kontinuity blíže rozebrána v kapitole 4.2.8.

ZSVD rozlišuje kvalifikovaný elektronický podpis,[48] zaručený elektronický podpis založený na kvalifikovaném certifikátu (uznávaný elektronický podpis),[49] zaručený elektronický podpis[50] a jiný typ elektronického podpisu.[51] Nařízení eIDAS pak upravuje kvalifikovaný elektronický podpis,[52] zaručený elektronický podpis[53] a prostý elektronický podpis.[54] Podpisy jsou řazeny od nejvyšší úrovně po úroveň nejnižší.

3.1. Kvalifikovaný elektronický podpis

Kvalifikovaný elektronický podpis je definován jako *zaručený elektronický podpis, který je vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů a který je založen na kvalifikovaném certifikátu pro elektronické podpisy*.[55]

Tento podpis má z elektronických podpisů nejvyšší míru důvěryhodnosti. Pouze této nejvyšší úrovni explicitně přiznává nařízení eIDAS účinky vlastnoručního podpisu[56] a jako u jediného

[45] Článek 3 odst. 9 nařízení eIDAS.
[46] Článek 3 odst. 24 nařízení eIDAS.
[47] Článek 3 odst. 25 nařízení eIDAS.
[48] § 5 ZSVD.
[49] § 6 ZSVD.
[50] § 7 ZSVD.
[51] § 7 ZSVD.
[52] Článek 25 nařízení eIDAS.
[53] Článek 26 nařízení eIDAS.
[54] Článek 3 odst. 10 nařízení eIDAS.
[55] Článek 3 odst. 12 nařízení eIDAS.
[56] Článek 25 odst. 2 nařízení eIDAS.

podpisu explicitně upravuje požadavky na ověřování jejich platnosti.[57] To však dle některých autorů nemusí samo o sobě nic vypovídat, neboť tuto formulaci eIDAS opakuje u všech služeb vytvářejících důvěru a u ostatních úrovní elektronických podpisů neříká, že by tento účinek mít neměly.[58]

Kvalifikovaný elektronický podpis zajišťuje funkci integrity podepsaných dat a identifikaci podepisující osoby.[59] Dle Podaného se identita podepsané osoby u kvalifikovaného elektronického podpisu odvíjí od kvalifikovaného certifikátu a od použití kvalifikovaného prostředku pro vytvoření podpisu.[60] Kvalifikovaným prostředkem pro vytváření elektronických podpisů se rozumí prostředek pro vytváření elektronických podpisů, který splňuje požadavky stanovené v příloze II nařízení eIDAS.[61] Tím je v praxi nejčastěji certifikovaná čipová karta (jejíž funkci může plnit i eObčanka) nebo USB token. To je rozdíl oproti zaručenému elektronickému podpisu, který tyto náležitosti nevyžaduje. Kvalifikovaným certifikátem pro elektronický podpis je certifikát pro elektronický podpis, který je vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a splňuje požadavky stanovené v příloze I nařízení eIDAS.[62] Identita však nemusí být ani v případě tohoto podpisu jednoznačná,[63] jak bude rozvedeno v kapitole 4.4.

3.2. Zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronické podpisy

Nařízení eIDAS neobsahuje specifické náležitosti zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu. Vyplývá z něj toliko, že podpis musí splňovat požadavky uvedené v článku 26 eIDAS a být založen na kvalifikovaném certifikátu pro elektronický podpis.

Dle českého zákona *se uznávaným elektronickým podpisem rozumí zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis nebo kvalifikovaný elektronický podpis*.[64] V praxi pak právě zaručený elektronický podpis založený na

[57] Článek 32 nařízení eIDAS.
[58] DONÁT, Josef, Jan TOMÍŠEK a Ivan FENCL. *Je publikovaná judikatura k elektronickým podpisům skutečně relevantní?*, op. cit 26.
[59] PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra, op. cit. 9.
[60] *Ibid*.
[61] Článek 3 odst. 23 eIDAS.
[62] Článek 3 odst. 15 eIDAS.
[63] K tomu srov. např. KORBEL, František, KOVÁŘ, Dalibor, POTOČŇÁK, Štefan: Elektronická identita při elektronickém (hmotně)právním jednání, *Právní rozhledy*. roč. 2019, č. 18, s. 630 nebo DONÁT, Josef, Jan TOMÍŠEK a Ivan FENCL. *Je publikovaná judikatura k elektronickým podpisům skutečně relevantní?*, op. cit 26..
[64] § 6 odst. 2 ZSVD.

kvalifikovaném certifikátu pro elektronické podpisy bývá chybně jedna ku jedné zaměňován s pojmem uznávaný elektronický podpis. Uznávaným podpisem přitom dle ZSVD je jak tento typ elektronického podpisu, tak elektronický podpis kvalifikovaný.[65]

V případě zaručeného elektronického podpisu je podpis založený na kvalifikovaném certifikátu (tj. software podle přílohy I nařízení eIDAS), ale nevyžaduje již použití kvalifikovaného prostředku pro vytvoření podpisu (tj. hardware podle přílohy II eIDAS). Je tedy splněna pouze jedna ze dvou dodatečných podmínek pro kvalifikovaný elektronický podpis. Ve vztahu k tomuto podpisu se jedná o národní výjimku, která není v rámci Evropské unie uznávána.[66]

Dle ZSVD se uznávaný elektronický podpis užije v případě, kdy se podepisuje elektronický dokument, kterým se právně jedná vůči veřejnoprávnímu podepisujícímu nebo jiné osobě v souvislosti s výkonem jejich působnosti.[67] Jedná se tedy o úlevu přiznanou soukromoprávním osobám při jednání vůči veřejnoprávním osobám bez nutnosti investice prostředků do pořízení kvalifikovaného podpisu. Příkladem užití uznávaného elektronického podpisu jsou jednání vůči finanční správě či určitá jednání v rámci zadávání veřejných zakázek. Úroveň důvěryhodnosti uznávaného elektronického podpisu je tímto na druhou stranu snížena, v uvedených případech je však toto snížení akceptovatelné.

Uznávaný elektronický podpis také zajišťuje funkci integrity podepsaných dat a identifikaci podepisující osoby.[68] Kvalifikovaný certifikát je vydáván kvalifikovanými poskytovateli služeb vytvářejících důvěru na žádost konkrétní osoby po ověření její totožnosti. Podpis vytváří jen tato osoba a nelze jej přenést jinam. Jak bude blíže rozvedeno v kapitole 5.1, kvalifikovaný certifikát bývá někdy chybně vnímán soudy jako podstatná náležitost písemné formy právního jednání.

3.3. Zaručený elektronický podpis

Zaručený elektronický podpis je upraven především v článku 26 eIDAS a je jím podpis, který není založen na certifikátu pro elektronický podpis vydaným kvalifikovaným poskytovatelem služeb. Zaručený elektronický podpis musí splňovat tyto požadavky:

a) je jednoznačně spojen s podepisující osobou;

[65] § 6 odst. 2 ZSVD.
[66] PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra, op. cit. 9.
[67] § 6 odst. 1 ZSVD.
[68] PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra, op. cit. 9.

b) umožňuje identifikaci podepisující osoby;

c) je vytvořen pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou; a

d) je k datům, která jsou tímto podpisem podepsána, připojen takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat.

U tohoto typu podpisu je vyžadováno technické zabezpečení důvěryhodnosti, avšak stále ještě není požadována důvěryhodnost údajů uvedených v připojeném certifikátu. Dle Polčáka[69] plní základní funkce listinného podpisu prakticky jen zaručený elektronický podpis, a to z důvodu identifikace podepisující osoby, jejího seznámení s obsahem dokumentu a ověření integrity dokumentu, tedy fixace jeho obsahu. Tyto aspekty pak vedou k vyšší míře důkazní spolehlivosti.[70]

Problémem (nejenom) zaručených elektronických podpisů je však dle Polčáka na rozdíl od procesu podpisu nedostatečná úprava ověřování pravosti podepsaných dokumentů, což v praxi vede k často nadbytečnému expertnímu posouzení. Druhým problémem je pak časová stabilita zaručeného elektronického podpisu. Ověření je dvousložkové, za prvé se ověřuje integrita podepsaného dokumentu a za druhé pravost certifikátu vydaného poskytovatelem certifikačních služeb. Při ověření pravosti certifikátu je zapotřebí ověření provedené poskytovatelem na základě stejného systémového certifikátu. Z dlouhodobého hlediska pak tyto faktory představují zvýšené riziko, neboť může dojít k zániku daného poskytovatele či zničení potřebných certifikátů, nemluvě o v čase jednodušším zfalšování původního certifikátů způsobené nárůstem výpočetní kapacity. Řešením dle Polčáka pak není ani takzvané přepodepisování, neboť *de iure* dochází k vzniku nového dokumentu a přepodepsání je závislé na více faktorech, ani připojení časového razítka, které pouze prokazuje existenci dokumentu v určitém čase a jeho ověřitelnost je taktéž limitována příslušným certifikátem jako v případě podpisu. Za nejvhodnější řešení pak Polčák považuje důvěryhodné systémy ukládání.[71] Této tématice je věnována kapitola 4.2.

Ohledně funkcí zaručeného elektronického podpisu nepanuje shoda. Dle Čermáka měl zaručený podpis označovací funkci vždy, omezenou funkci deklarační však až po novele

[69] POLČÁK, R. Praxe elektronických dokumentů, op. cit. 8, s. 56
[70] *Ibid.*
[71] POLČÁK, R. Praxe elektronických dokumentů, op. cit. 8, s. 58-59.

občanského zákoníku 1964.[72] Dle Podaného však ani zaručený elektronický podpis identitu podepsané osoby nezaručuje.[73] Autor této práce je názoru, že identifikace je nejasná již ze samotného nařízení eIDAS. Jedná se sice o jeden z požadavků samotného zaručeného podpisu, nicméně není stanoveno, jaká míra důvěryhodnosti identifikace má být spojena. Certifikát pro zaručený elektronický podpis totiž může vytvořit kdokoli, dokonce i podepisující osoba sama.[74] Hlavní výhodou této úrovně podpisu oproti prostému elektronickému podpisu je však zajištění integrity podepsaného dokumentu.

Z praktického hlediska lze podotknout, že zaručený elektronický podpis lze mimo jiné vytvořit prostřednictvím služby SIGN[75] společnosti Bankovní identita, a.s.[76]

3.4. Prostý elektronický podpis

Definice prostého elektronického podpisu vyplývá z článku 3 odst. 10 nařízení eIDAS, a to „*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*“. Jedná se tedy o zbytkovou množinu všech elektronických podpisů, které nenaplňují znaky vyšší úrovně elektronických podpisů uvedených výše.

ZSVD pak v § 7 uvádí, že „*k podepisování elektronickým podpisem lze použít zaručený elektronický podpis, uznávaný elektronický podpis, případně jiný typ elektronického podpisu*“. Jak již bylo zmíněno výše, uznávaný elektronický podpis je v případě ZSVD legislativní zkratkou, která zahrnuje jak zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis, tak kvalifikovaný elektronický podpis.[77] V případě jiného typu elektronického podpisu se tak musí jednat právě o prostý elektronický podpis.

Dle některých autorů může být prostým elektronickým podpisem například jméno a příjmení napsané na konci e-mailu, (dynamický) biometrický podpis, či připojení podpisových dat na

[72] ČERMÁK, Karel. Elektronický podpis – pohled soukromoprávní. *Bulletin advokacie*. 2002, roč. 2002, č. 11 - 12, s. 68.
[73] PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra, op. cit. 9.
[74] KORBEL, František, KOVÁŘ, Dalibor, POTOČŇÁK, Štefan: Elektronická identita při elektronickém (hmotně)právním jednání, op. cit. 63, s. 629.
[75] https://www.bankid.cz/pro-firmy.
[76] Na základě zákona č. 49/2020 Sb., kterým se mění zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, a zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, a některé další zákony.
[77] § 6 odst. 2 ZSVD.

základě jiného úkonu, jako je kliknutí na tlačítko potvrzující projev vůle nebo potvrzení jménem, heslem či kódem.[78]

Dle Polčáka má prostý elektronický podpis právní účinky, a to i přes to, že plní identifikační funkci pouze slabě. Podpisem tak je patička v emailu, ale i naskenovaný vlastnoruční podpis vložený do příslušného dokumentu. Dodržení písemné formy právního jednání je ovšem zapotřebí odlišit od důkazní funkce podpisu, respektive od praktického aspektu, kdy k vyvrácení domněnky pravosti podpisu stačí pouhé opačné tvrzení podepisujícího. Soud by se však pokaždé měl tímto důkazem zabývat, a ne jej pouze bez dalšího odmítnout.[79] V této souvislosti je vhodné podotknout, že např. prostým elektronickým podpisem v podobě naskenovaného vlastnoručního podpisu již bylo možné požádat o kompenzační bonus dle § 7 odst. 5 zákona o kompenzačním bonusu.[80]

Oproti tomu Podaný uvádí, že by nikdo nepovažoval dokument v listinné podobě za podepsaný, pokud by bylo jméno a příjmení jednající osoby uvedeno v textovém editoru. Taktéž shledává jako nedostatečné připojení vizitky sponkou, vytištění nebo nakopírování obrazu vlastnoručního podpisu, či nalepení kancelářského papírku s vlastnoručním podpisem. Tyto formy jsou dle Podaného analogií prostého elektronického podpisu a proti těmto formám se vyhrazuje, respektive v případě společenské poptávky požaduje stejný přístup. Prostý elektronický podpis dle Podaného na rozdíl od zaručeného a kvalifikovaného elektronického podpisu nevyužívá tzv. asymetrickou kryptografii, tedy možnost zjištění změny dat, tj. zajištění jejich integrity. Prostý elektronický podpis nezaručuje ani identitu podepisující osoby.[81]

Dle článku 25 odst. 1 eIDAS „*elektronickému podpisu 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 že nesplňuje požadavky na kvalifikované elektronické podpisy*“. Dle Podaného však toto ustanovení neříká nic o tom, jaké mají právní účinky být. Komparativním výkladem ustanovení článku 25 odst. 2 eIDAS dospívá k názoru, že to nemůže být účinek vlastnoručního podpisu. Z toho důvodu lze prostý elektronický podpis použít pouze

[78] DONÁT, Josef, Jan TOMÍŠEK a Ivan FENCL. *Je publikovaná judikatura k elektronickým podpisům skutečně relevantní?*, op. cit 26.
[79] POLČÁK, R. Praxe elektronických dokumentů, op. cit. 8**,** s. 56 – 57.
[80] Zákon č. 159/2020 Sb., o kompenzačním bonusu v souvislosti s krizovými opatřeními v souvislosti s výskytem koronaviru SARS CoV-2.
[81] PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra, op. cit. 9.

tam, kde by v případě dokumentů v listinné podobě postačily k podpisu mechanické prostředky. Totéž pak platí o ustanovení § 7 ZSVD. [82]

S tímto závěrem ovšem nesouhlasí např. Korbel, Kolář a Amler[83] ani autor této práce. Dle logiky článku 3 odst. 10 eIDAS platí výše zmíněné ustanovení pro všechny elektronické podpisy. Určitá míra důkazní pravděpodobnosti o jednání konkrétní osobou tak musí být i v případě prostého elektronického podpisu zachována vždy a nelze jej považovat za nedůvěryhodný, nepoužitelný či dokonce neplatný.

Bylo by možné namítat, že ze samotného znění definice elektronického podpisu vyplývá, že nemůže jít o data, která jsou součástí elektronické písemnosti (typicky dopsané jméno na konci textu). S tím ovšem autor této práce nesouhlasí, neboť nařízení eIDAS o jiné formě dat v případě podpisu nehovoří. I v případě jména dopsaného na konec textu jde totiž o připojení dat, která jsou s dokumentem logicky spojena. Naopak požadavek článku 3 odst. 10 nařízení eIDAS bude splňovat i připojení značky charakterizující podpis, připojení kódu uživatele a další běžné způsoby. Na tomto místě lze pak zmínit i nedávné rozhodnutí kanadského soudu, který shledal emotikon zdviženého palce jako souhlas s návrhem na uzavření smlouvy.[84]

Neuplatní se ani argument článkem 3 odst. 13 nařízení eIDAS, který definuje data pro vytváření elektronických podpisů jako „*jedinečná data, která podepisující osoba používá k vytváření elektronických podpisů*," tedy fakt, že musí jít o jedinečná data, která jsou spojena s podepisující osobou a nikdo jiný je používat nemůže. Tato náležitost opět z nařízení eIDAS nevyplývá. Analogicky lze argument připodobnit k paralele s vlastnoručním podpisem, na který se uplatní stejné nároky, a v praxi lze narazit na více lidí podepisujících se např. třemi křížky. V této souvislosti lze také upozornit na zmíněnou judikaturu umožňující, aby se jedna osoba podepisovala více podpisy. [85] Jinými slovy, neplatí, že každá osoba musí mít pouze jeden unikátní podpis.

Dle recitálu 49 eIDAS by elektronickému podpisu „*neměly být upírány právní účinky na základě skutečnosti, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikovaný elektronický podpis. Právní účinky elektronických podpisů v členských státech by však měly*

[82] *Ibid.*
[83] KORBEL, František; KOVÁŘ, Dalibor a AMLER, Pavel. *Interpretace elektronického podpisu a související identifikace v soukromém právu*, op. cit. 29.
[84] Rozhodnutí Court of King's Bench v kanadské provincii Saskatchewan v případu South West Terminal Ltd v Achter Land and Cattle Ltd [2023 SKKB 116].
[85] Rozhodnutí Vrchního soudu v Olomouci ze dne 13. 10. 2022, č.j. 5 Cmo 111/2022-378.

být vymezeny vnitrostátním právem, s výjimkou požadavků stanovených v tomto nařízení, podle něhož by měl mít kvalifikovaný elektronický podpis rovnocenný právní účinek jako podpis vlastnoruční.“ Podaný z tohoto recitálu dovozuje, že by elektronické podpisy nižší úrovně těžko mohly mít účinek stejný, popř. i vyšší, než podpis vlastnoruční.[86] S tím autor této práce nesouhlasí, neboť pouhým gramatickým výkladem i s přihlédnutím k první části recitálů tento závěr dovodit nelze.

Podaný pak uvádí, že v případě prostého elektronického podpisu není jasné, že podpis vytvořila podepisující osoba, že byl podpis vytvořen za účelem podepisování ani že jej k písemnosti tato osoba připojila.[87] Z toho důvodu by dle Podaného měl mít prostý elektronický podpis v soukromém právu velice omezené použití. S tím autor této práce nesouhlasí. V praxi by to vedlo k používání pouze kvalifikovaných elektronických podpisů či zaručených podpisů založených na kvalifikovaném certifikátu, což je proti smyslu úpravy nařízení eIDAS a ZSVD. Navíc by v praxi takový požadavek byl neproveditelný a neudržitelný.

Dle důvodové zprávy v případě právních jednání jiných než dle § 5 ZSVD je možné použít všechny typy elektronických podpisů, které nařízení eIDAS zná, mimo jiné i (prostý) elektronický podpis, a dochází tak k rozšíření parity s vlastnoručním podpisem i na tyto typy elektronických podpisů.[88] Dle Korbela, Koláře a Amlera lze i pohyb prstem po dotykovém zařízení postavit naroveň podpisu na papír. Dle autorů totiž žádný elektronický podpis neplní funkci jednoznačné identifikace podepisujícího. Tu totiž neplní ani vlastnoruční podpis, který sám o sobě v případě předložení listiny třetí straně není důkazem o tom, že listinu její autor podepsal a je zapotřebí spoléhat na tvrzení předkládající strany o pravosti podpisu a obecné občanskoprávní zásady. Na druhou stranu, v případě prostého elektronického podpisu použitím např. vícefaktorového ověření je důkazní síla a možnost zjištění identifikace podepisující osoby vyšší. Při srovnání vlastnoručního podpisu na papír a prostého elektronického podpisu tak autoři dospívají k závěru, že je zapotřebí podpis posuzovat v širších okolnostech, které v případě vhodných technických řešení mohou i v případě prostého elektronického podpisu vést k větší důkazní síle.[89]

[86] PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra, op. cit. 9.
[87] *Ibid.*
[88] Důvodová zpráva ZSVD k § 7.
[89] KORBEL, František; KOVÁŘ, Dalibor a AMLER, Pavel. *Interpretace elektronického podpisu a související identifikace v soukromém právu*, op. cit. 29.

Dle Korbela, Koláře a Amlera zákonodárce umožňuje subjektům soukromého práva svobodně rozhodovat o tom, zda preferují jednat elektronickými prostředky a zda v daném kontextu považují prostý elektronický podpis za důvěryhodný a dostatečný pro účely potvrzení obsahu písemného právního jednání, stvrzení vážnosti vůle a identifikaci jednající osoby. [90] Předností prostých elektronických podpisů je fakt, že se snadno vytváří. Z toho důvodu dochází i ke snaze posílit jejich postavení a použití. Peterka pak na druhou stranu jako odstrašující příklad uvádí příklad dlužního úpisu nebo udělení plné moci a jejich podepsání v textovém editoru.[91] Obdobné přirovnání pak používá i Podaný.[92] Tyto příklady jsou však dle autora této práce hraniční situací. I v případě prostého elektronického podpisu totiž závisí na širších okolnostech, které mohou v některých případech, jak bylo rozebráno výše, vést dokonce i k vyšší míře důvěry a důkazní síly ve srovnání i např. s vlastnoručním podpisem. Nelze tedy kategoricky dospět k závěru, že forma prostého elektronického podpisu je *a priori* slabá a neměla by se bez dalšího používat, ale vždy posuzovat jednotlivé případy v závislosti na konkrétních okolnostech.

Svůj význam má prostý elektronický podpis také dle § 6 odst. 1 písm. a) zákona o právu na digitální služby,[93] kde ovšem neplní funkci projevu vůle. Ten zachycuje osoba oprávněná provádět ověřování pravosti podpisu. To samé platí v případě projevu vůle prostřednictvím informačního systému veřejné správy (splňující podmínky zákona o informačních systémech veřejné správy)[94] dle § 6 odst. 1 písm. b) zákona o právu na digitální služby.[95] Takovým systémem může být například prostředí s úrovní záruky splňující požadavky zákona o elektronické identifikaci.[96, 97]

Dle Peterky nelze umožnit použití prostých elektronických podpisů zcela obecně v případech, kde je vyžadována písemná forma, a stavět je na roveň vlastnoručním podpisům. V případě univerzální akceptace prostého elektronického podpisu by totiž dle Peterky mohlo dojít ke dvoukolejnosti mezi požadavky na písemnou formu v listinné a elektronické podobě. To

[90] *Ibid.*
[91] PETERKA, Jiří. *Zatímco technické obory přitvrzují, právo naopak měkne*. Online. Dostupné z: https://www.pravniprostor.cz/clanky/spravni-pravo/zatimco-technicke-obory-pritvrzuji-pravo-naopak-mekne. [cit. 2023-07-14].
[92] PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra, op. cit. 9.
[93] Zákon č. 12/2020 Sb. o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů.
[94] § 2 písm. b) zákona č. 365/2000 Sb. o informačních systémech veřejné správy.
[95] MATEJKA, J., MATES, P. Zákon o právu na digitální služby. Komentář. [Systém ASPI]. Nakladatelství Leges [cit. 2023-4-21]. ASPI_ID KO12l2020CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X, § 6.
[96] Zákon č. 250/2017 Sb. o elektronické identifikaci, ve znění pozdějších předpisů.
[97] PETERKA, Jiří. *Zatímco technické obory přitvrzují, právo naopak měkne*, op. cit 91.

vše v situaci, kdy technická řešení své požadavky zpřísňují, a právo by je naopak rozvolňovalo.[98] S tímto závěrem se autor této práce částečně ztotožňuje. Je však zapotřebí vnímat prostý elektronický podpis jako samostatnou kategorii v rámci nové technologie, kdy srovnání s vlastnoručním podpisem není vždy možné ani na místě. V některých případech použití prostého elektronického podpisu namísto podpisu vlastnoručního je méně vhodné než v jiných, a to právě v závislosti na konkrétních okolnostech (např. dvoufaktorové ověření či dynamický biometrický podpis). Pokud totiž technické řešení odpovídá vyšším standardům, lze dle názoru autora právě v tomto případě právní požadavky snížit. To však nemění nic na faktu, že definice podpisu bude naplněna v jakémkoli případě (tedy kdy není zákonem vyžadován podpis vlastnoruční). Dle Berana pak prosté napsání jména v emailu není jako elektronický podpis dostatečné, neboť autentizační funkce je velice limitována. Písemná forma však v takovém případě může být zachována podle ustanovení § 562 odst. 1 OZ.[99]

Oproti Peterkovi jsou pak členové platformy Rozumné právo. Ti mají za to, že prostý elektronický podpis je přímo dle nařízení eIDAS postaven na roveň podpisu vlastnoručnímu, pokud je jednání spojeno s vůlí podepsat, tj. stvrzení konečnosti a závaznosti jednání. Automaticky přednastavený podpis tak tento účinek mít nemusí.[100] S tím se autor této práce neztotožňuje, neboť jak bylo rozebráno výše, nařízení eIDAS dává rovnocenné účinky vlastnoručního podpisu pouze podpisu kvalifikovanému.[101] Tento fakt je ovšem nutné odlišovat od situací, kdy je používán vlastnoruční podpis, aniž by byl zákonem takový požadavek stanoven.

Čermák uvádí, že lze souhlasit se závěry, dle kterých připojení pouhého podpisu k emailu je podpisem, avšak spíše s účinky určení osoby autora než ověření její totožnosti. Funkci označovací tedy prostý elektronický podpis plnil vždy. Deklarační funkce (srov. kapitolu 2.2) je však již problematičtější. Důvodem je, že prostý elektronický podpis může za elektronickou zprávu umístit kdokoli bez ohledu na to, kdo zprávu vytvořil, kdo ji odesílá a kdo má v úmyslu právně jednat. Deklarační funkce byla dle názoru Čermáka ovšem záměrně zákonodárcem novelou občanského zákoníku 1964[102] oslabena a na jejím základě dovodil, že za elektronický

[98] *Ibid.*
[99] BERAN, Vladimír. § 561 [Písemná forma]. In: PETROV, Jan, VÝTISK, Michal, BERAN, Vladimír a kol. Občanský zákoník. 2. vydání (1. aktualizace). Praha: C. H. Beck, 2022, marg. č. 9.
[100] ROZUMNÉ PRÁVO. *Platforma Rozumné právo: Je třeba zjednodušit elektronické právní jednání*. Online. Dostupné z: https://www.pravniprostor.cz/clanky/ostatni-pravo/platforma-rozumne-pravo-je-treba-zjednodusit-elektronicke-pravni-jednani. [cit. 2023-08-14].
[101] Článek 25 odst. 2 nařízení eIDAS.
[102] Novela občanského zákoníku č. 509/1990 Sb., blíže v kapitole 2.3.

podpis lze považovat i prosté připojení jména a příjmení či jiného označení osoby k běžnému e-mailu.[103] Důkazní funkce je pak také splněna, avšak s určitými specifiky oproti podpisu vlastnoručnímu (blíže v kapitole 4.4). Hulmák obecně nezpochybňuje platnost právních jednání učiněných kliknutím myši, odesláním vyplněného formuláře e-mailem nebo zadáním PIN kódu. Pokud je ovšem vyžadována písemná forma, dochází v případě prosté e-mailové zprávy s připojeným jménem a příjmením k nejednoznačné identifikaci. Z toho důvodu pak dle Hulmáka běžný e-mail povahu písemného právního jednání v zásadě nemá.[104] Dle Korbela a Melzera lze souhlasit s tím, že připojení textu jména a příjmení autora do datové zprávy představuje prostý elektronický podpis, pokud je identifikace odesílatele zprávy jednoznačná. To však musí být posouzeno ve vztahu ke konkrétním okolnostem.[105] Matejka a Chum jsou názoru, že podpis ve formě jména připojeného k běžnému emailu je prostým elektronickým podpisem, stejně jako faksimile vlastnoručního podpisu zaslané např. formou přílohy, PIN kód apod.[106] Dle názorů Matejky a Güttlera[107] či Smejkala, Kodla a Uřičara[108] je možné mimo jiné za prostý elektronický podpis považovat i audio(vizuální) stopu. Prostý elektronický podpis je pak pro splnění požadavku splnění písemné formy právního jednání dostatečný i podle názoru České národní banky[109] či Úřadu pro ochranu hospodářské soutěže.[110]

Autor této práce se pak ztotožňuje s názory autorů, dle kterých je jméno a příjmení připojené v textové podobě na konec emailu prostým elektronickým podpisem a je splněna písemná forma právního jednání. Je totiž zapotřebí rozlišovat mezi funkcemi podpisu pro účely dokazování a zákonnými náležitostmi pro platnost právního jednání. Pro účely splnění projevu vůle, tedy stanovení, kdo právně jedná, je pak zapotřebí přihlížet i k ostatním okolnostem, a nepřenášet tuto vlastnost na podpis samotný. Tato problematika bude blíže rozebrána v kapitole 4.4. S tím souhlasí i Donát, Tomíšek a Fencl, dle kterých nelze z nařízení eIDAS

[103] POLČÁK, R. Praxe elektronických dokumentů, op. cit. 8**,** s. 68.
[104] HULMÁK, Milan. Elektronický právní styk. Právní rozhledy, 2005, č. 7, s. 229-234.
[105] KORBEL, František a MELZER, Filip. Písemnost, elektronický a biometrický podpis v elektronickém právním jednání, op. cit. 11, s. 34.
[106] MATEJKA, Ján a CHUM, Václav. K PRÁVNÍ ÚPRAVĚ ELEKTRONICKÉHO PODPISU. *Bulletin advokacie*. 2002, roč. 2002, č. 3, s 3.
[107] MATEJKA, Ján a Vojen GÜTTLER. *Electronic Written Documents and Biometric Options of Their Signing – Problem of Evidentiary Reliability and Personal Data Protection*, Vol. 8, No 1 (2018), s. 44.
[108] SMEJKAL, Vladimír, Jindřich KODL a Miroslav UŘIČAŘ. Elektronický podpis podle nařízení eIDAS, *Revue pro právo a* technologie, roč. 6, č. 11, roč. 2015, s. 228.
[109] ČESKÁ NÁRODNÍ BANKA. *K některým ustanovením zákona č. 257/2016 Sb., o spotřebitelském úvěru*. Online. Dostupné z: https://www.cnb.cz/cs/dohled-financni-trh/legislativni-zakladna/stanoviska-k-regulaci-financniho-trhu/RS2017-02/. [cit. 2023-12-18], otázka č. 11.
[110] Výkladové stanovisko ÚOHS k novele zákona o významné tržní síle, § 3b, s. 20 – 21, dostupné zde: https://www.uohs.cz/cs/vyznamna-trzni-sila/metodicka-cinnost/vykladova-stanoviska-a-doporuceni.html.

dovozovat, že prostý elektronický podpis není elektronickým podpisem, a dokonce ani že nemůže mít právní účinky vlastnoručního podpisu.[111]

3.5. Biometrický podpis

Dalším (pod)typem elektronického podpisu je biometrický podpis. Z pohledu ZSVD a nařízení eIDAS se jedná o prostý elektronický podpis,[112] který je ale oproti ostatním druhům, jako je například prostý text napsaný v textovém editoru nebo v emailu, technologicky více komplexní. Jak již název napovídá, do písemnosti v elektronické podobě jsou vložena jedinečná biometrická data podepisující osoby. Může se jednat o data statická (např. otisk prstu, speciální snímek obličeje, oka, křivku vlastnoručního podpisu, digitalizovaný vzorek DNA ze slin či krve) nebo dynamická (např. vzorek hlasu, chůze, specifické atributy vlastnoručního podpisu jako je rychlost, přítlak a další).[113] V praxi se lze nejčastěji setkat s dynamickým vlastnoručním podpisem, tedy podpisem, který podepisující osoba nenapíše na papír, ale na podpisovou plochu (tablet, signpad). Zařízení podpis zaznamená, následně jej zpracuje podle předem stanovených kritérií a vloží do písemnosti.[114, 115]

Oproti vlastnoručnímu podpisu však dochází k oddělení okamžiku vytvoření podpisu a připojení podpisu k podepisovanému dokumentu. S tím dle Podaného souvisí riziko snazšího zneužití, neboť dochází k odevzdání jedinečných biometrických dat a s nimi spojené identity podepisující osoby do unikátního vzorku. Riziko pak nespočívá v jeho napodobení, ale v možnosti zneužití odebraného vzorku jako takového. Poskytovatel služby totiž může bez omezení podpis připojit i k jiným dokumentům, a to bez vědomí či souhlasu podepisující se osoby, nebo naopak podpis na dokument, který osoba chtěla podepsat, nepřipojit.[116] Tato data navíc zůstávají po dobu života člověka neměnná. Při jejich úniku tak nelze oproti heslům apod. uniklá data zablokovat a změnit. Data také nelze zpřísňovat co do jejich náležitostí a tím je činit složitějšími a bezpečnějšími proti padělání.[117] Nemusí se nutně jednat o neoprávněný přístup či zveřejnění dat z uzavřeného systému. Biometrická data se totiž vkládají do

[111] DONÁT, Josef, Jan TOMÍŠEK a Ivan FENCL. *Je publikovaná judikatura k elektronickým podpisům skutečně relevantní?*, op. cit 26.
[112] V rozhodnutí Krajského soudu v Ostravě ze dne 28. 3. 2022, sp. zn. 11 Co 338/2020 byl dokonce soudem (chybně) označen za zaručený elektronický podpis.
[113] PETERKA, Jiří. *Elektronický podpis na rozcestí*. Online. Dostupné z: https://www.lupa.cz/clanky/elektronicky-podpis-na-rozcesti/. [cit. 2023-10-11].
[114] PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra, op. cit. 9.
[115] PETERKA, Jiří. *Jak rozumět dynamickým biometrickým podpisům?* Online. Dostupné z: https://www.lupa.cz/clanky/jak-rozumet-dynamickym-biometrickym-podpisum/. [cit. 2023-09-11].
[116] PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra, op. cit. 9.
[117] TOMÁNEK, Jaroslav. *Biometrický podpis - mýty a fakta*. Online. Dostupné z: https://www.ica.cz/Userfiles/files/zpravy/Biometricky_podpis.pdf. [cit. 2023-09-14], s 33.

podepisovaného dokumentu, samozřejmě v zašifrované podobě. S postupným vývojem technologií však bude čím dál tím snazší tato data rozšifrovat a zneužít. Samozřejmě je zapotřebí zvážit i regulaci vztahující se ke zpracování osobních údajů, kde biometrické údaje spadají do zvláštních kategorií osobních údajů.[118] Je otázkou, zda zpracování těchto osobních údajů je zapotřebí, obzvlášť v situaci, kdy ke zpracování dochází z iniciativy zpracovatele.[119]

Dle Podaného se navíc nejedná o služby vytvářející důvěru podle nařízení eIDAS či ZSVD, neboť zde neexistují žádné zákonné požadavky nebo licence upravující požadavky na použité zařízení či jejich poskytovatele. Navíc je otázkou, kdy dochází k podpisu písemnosti. Zda vytvořením biometrického podpisu, jeho připojením k podepisovanému dokumentu, nebo oběma procesy zároveň.[120]

Dle některých dřívějších názorů biometrický podpis mohl splňovat náležitosti podpisu zaručeného.[121] Jednalo se však o názory ojedinělé a většina autorů je názoru opačného.[122] Biometrický elektronický podpis totiž nesplňuje náležitosti článku 26 eIDAS, jelikož není spojen s podepisující osobou jednoznačně, ale pouze s vysokou pravděpodobností. Nejedná se totiž o možnosti ano či ne, ale o porovnání podpisu s jeho vzorem za pomoci jednotlivých atributů, jako je rychlost, tlak, tvar apod. Tyto mohou být teoreticky napodobeny jinou osobou. Dále není vytvořen pomocí dat pro vytváření elektronických podpisů, neboť v terminologii nařízení eIDAS nejde o biometrická data jako součást integrity člověka, ale stejně jako u vyšších úrovní podpisu o výpočetní data (tzv. soukromý klíč). Tato data jsou pak využívána i při ověřování jejich platnosti, kdy výpočetním procesem dochází k výsledku ano, ne či nelze ověřit. Konečně také biometrický podpis není připojen takovým způsobem, kdy je možné zjistit jakoukoliv následnou změnu dat. Naopak, na datech je nezávislý, a to i v době samotného

[118] Článek 9 odst. 1. Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), vývoj postoje ÚOOÚ popsán např. zde: KORBEL, František; KOVÁŘ, Dalibor; NEŠPŮREK, Robert a OTEVŘEL, Richard. *Dynamický biometrický podpis nově vždy jako zvláštní kategorie osobních údajů*. Online. Dostupné z: https://www.pravniprostor.cz/clanky/pravo-it/dynamicky-biometricky-podpis-nove-vzdy-jako-zvlastni-kategorie-osobnich-udaju. [cit. 2023-08-24], dále např. JAREŠ, Adam. *SMLOUVA PODEPSANÁ ELEKTRONICKÝM PODPISEM*, op. cit. 6, str. 117 a násl.
[119] PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra, op. cit. 9.
[120] *Ibid.*
[121] TOMÁNEK, Jaroslav. *Biometrický podpis - mýty a fakta*, op. cit. 117, SMEJKAL, Vladimír. Kryptografický a dynamický biometrický podpis podle platné právní úpravy, *Právní rozhledy* č. 10/19, s. 343.
[122] PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra, op. cit. 9., KORBEL, František; KOVÁŘ, Dalibor a AMLER, Pavel. *Interpretace elektronického podpisu a související identifikace v soukromém právu*, op. cit. 29, KORBEL, František a MELZER, Filip. Písemnost, elektronický a biometrický podpis v elektronickém právním jednání, op. cit. 11, TOMÁNEK, Jaroslav. *Biometrický podpis - mýty a fakta*, op. cit. 117.

vytvoření podpisu, jak již bylo popsáno výše.[123] Data navíc nejsou pod výhradní kontrolou podepisující osoby, pokud jsou vytvořena prostředkem příjemce podpisu (např. banky, dopravní společnosti atd.). Biometrický podpis je totiž většinou vytvořen na zařízení (tablet, smartpen) ve vlastnictví osoby odlišné od osoby podepisující.[124] K vytvoření biometrického dynamického podpisu je navíc zapotřebí součinnost třetí ověřující osoby.[125]

Mezi výhody biometrického podpisu oproti vyšším formám podpisu patří neomezená doba platnosti, jelikož není využíván certifikát s omezenou dobou platnosti, snadná přenosnost (tj. není nutné instalovat certifikát a související klíče na každý počítač), může jej využít téměř kdokoli, bez nutnosti předem zřízeného certifikátu, a potřebná infrastruktura může být poskytnuta třetí stranou. Na druhé straně s tímto typem podpisu vystává řada nevýhod. Jak již bylo zmíněno výše, mezi ně patří způsob svázání podpisu s dokumentem, obtížné ověření pravosti, snadné zneužití, nemožnost revokace podpisu a nedostatečná kontrola nad technickými prostředky sloužícími k jeho vytvoření. K jeho ověření je navíc na rozdíl od elektronických podpisů založených na certifikátech nutná součinnost podepisující osoby. Certifikát jako takový totiž může ověřit kdokoli, neboť certifikát je k podpisu přiložen a veden ve veřejném registru. Řešením tohoto problému by tak mohlo být vytvoření registru elektronických dynamických podpisů, do kterého by se osoba musela předem podepsat. Tato varianta by však v praxi znamenala nemalé náklady spojené s pořízením a údržbou takového registru, a odebrala jednu z hlavních výhod, tedy potřeby jednání před podpisem samotným (v podstatě stejné jako při zřízení certifikátu),[126] zároveň by vyvolávala otázky také z hlediska právní úpravy zpracování osobních údajů. V případě druhém, tedy ověřením ex post, může osoba součinnost odmítnout, případně změnit dynamický aspekt podpisu (jiný tlak, rychlost apod.). Stejný problém však vyvstává u ověření podpisu vlastnoručního.

S tzv. digitalizovaným podpisem, který je obdobou dynamického biometrického podpisu, navíc již počítá ustanovení § 18 zákona o občanských průkazech a rozumí se jím „*vlastní rukou*

[123] PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra, op. cit. 9.
[124] TOMÁNEK, Jaroslav. *Biometrický podpis - mýty a fakta*, op. cit. 117, s 31.
[125] PETERKA, Jiří. *Jak rozumět dynamickým biometrickým podpisům?* Online. Dostupné z: https://www.lupa.cz/clanky/jak-rozumet-dynamickym-biometrickym-podpisum/. [cit. 2023-09-11].
[126] VALÁŠEK, Michal. *Nahradí dynamické biometrické podpisy ty současné elektronické?* Online. Dostupné z: https://www.lupa.cz/clanky/nahradi-dynamicke-biometricke-podpisy-ty-soucasne-elektronicke/. [cit. 2023-08-26].

provedené písemné vyjádření vlastního jména, popřípadě jmen, a příjmení, popřípadě pouze příjmení, na podpisové zařízení“.[127]

Biometrický (dynamický) podpis je tak dle názoru autora logické technologické řešení, s jehož použitím se setkáváme stále častěji. Je však vždy vhodné zvážit, vhledem k výše nastíněným rizikům, zda je jeho použití vhodné ve všech situacích a nepostačil by prostý elektronický podpis v jiné podobě.

[127] Zákon č. 269/2021 Sb. o občanských průkazech, ve znění pozdějších předpisů.

4. Písemná forma právního jednání a elektronické prostředky

Jednou ze základních zásad občanského práva je zásada bezformálnosti, dle které je na osobách, jakou formu jednání si zvolí. Také právní jednání elektronickými prostředky tak může být ve formě písemné nebo ve formě jiné. V některých případech tak podpis není vůbec vyžadován, a jako platné právní jednání postačí ústní dohoda, v případě elektronických prostředků například jednání učiněné videohovorem či po telefonu, a to jak se záznamem, tak bez něj. V případě záznamu je zapotřebí rozlišovat, zda je záznam zachycením již proběhlého jednání (např. záznam kamery o předání zboží, který předání dokumentuje), kdy se nejedná o právní jednání učiněné elektronickými prostředky, ale jeho důkaz, či provedení jednání (projev vůle), např. hlasová zpráva obsahující objednávku zboží.[128] Požadavek písemné formy pak může uložit přímo zákon, či si jej mohou sjednat smluvní strany.[129] V této souvislosti je navíc zapotřebí rozlišovat, zda stačí prostá písemná forma, či je zapotřebí úředně ověřený podpis či veřejná listina.

4.1. Písemná forma právního jednání

Náležitosti písemné formy jsou specifikovány ve větě první ustanovení § 561 odst. 1 občanského zákoníku, dle kterého se „*k platnosti právního jednání učiněného v písemné formě vyžaduje podpis jednajícího*“. Tato věta směřuje na klasické právní jednání s vlastnoručním podpisem, na které jsme byli před příchodem technologií zvyklí. Podpis nemusí být čitelný a není-li zákonem stanoveno jinak, může jím být příjmení, jméno a příjmení, pseudonym či pouhá parafa. V některých případech se ovšem může jednat i o pojmenování člena příbuzenského nebo obdobného vztahu (např. Tvá matka).[130, 131] Podpis slouží k ověření platnosti listiny, není však součástí projevu vůle. Pokud tedy podpis chybí v případě, kdy písemná forma vyžadována není, je právní jednání stále platné. Pokud je však vyžadována písemná forma a podpis připojen není, jde o právní jednání relativně neplatné.[132] V některých případech, kdy například zákonná ustanovení nedovolují, aby jednání bez splnění požadované

[128] KMENT, Vojtěch. *Elektronické právní jednání: Srovnávací analýza s důrazem na využití elektronického podpisu podle práva EU, České republiky a Německa*. op. cit. 5, s. 97 – 98.
[129] K tomu srov. § 559 občanského zákoníku a např. rozhodnutí Okresního soudu v Kladně ze dne 27. 2. 2024, sp. zn. 208 C 179/2023.
[130] BERAN, Vladimír. § 561 [Písemná forma]. In: PETROV, Jan, VÝTISK, Michal, BERAN, Vladimír a kol. Občanský zákoník. 2. vydání (1. aktualizace). Praha: C. H. Beck, 2022, marg. č. 1.
[131] JANOUŠEK, Michal. § 561 [Písemná forma právního jednání]. In: LAVICKÝ, Petr a kol. Občanský zákoník I. Obecná část (§ 1−654). 2. vydání. Praha: C. H. Beck, 2022, s. 1792, marg. č. 11.
[132] Zuklínová v DAVID, O., DEVEROVÁ, L., DOLANSKÁ BÁNYAIOVÁ, L., DVOŘÁK, J., DVOŘÁK, T., FIALA, J., FRINTA, O., HOLČAPEK, T., HURDÍK, J., KINDL, T., MACKOVÁ, A., PAULY, J., PAVLÍK, P., PELIKÁN, R. a kol. Občanský zákoník: Komentář, Svazek I, (§ 1-654). [Systém ASPI]. Wolters Kluwer [cit. 2023-6-3]. ASPI_ID KO89_a2012CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X, § 561.

formy vyvolávalo právní následky, nebo jsou smluvní strany formou vázány, se však může jednat dokonce o neplatnost absolutní.[133] Pro úplnost lze pak podotknout, že textace zákona, podle které by se mohlo zdát, že úprava směřuje pouze na jednostranná jednání, je lichá. Naopak, podpis je vyžadován od všech podepisujících osob.[134]

Dle věty druhé ustanovení § 561 odst. 1 občanského zákoníku pak „*podpis může být nahrazen mechanickými prostředky tam, kde je to obvyklé.“* Tato věta již připouští použití i jiných (mechanických) prostředků, kterými mohou být například podpisová razítka, vytištěné podpisy apod., tedy prostředky v praxi využívané k autentizaci osoby s nízkou mírou důvěry zejména při mnohonásobném opakování podpisu (typicky hromadná korespondence).[135] Dle judikatury Nejvyššího soudu ČR však nahrazení vlastnoručního podpisu zaměstnavatele mechanickými prostředky není přípustné např. na výpovědi z pracovního poměru.[136]

Podaný mechanické prostředky přirovnává k prostému mechanickému podpisu a jako příklad uvádí podpisové razítko, vytištěný podpis anebo faksimile podpisu. Tím je samozřejmě snížena i důvěra autentizace jednající osoby. Dle Podaného lze pak k této kategorii prostých mechanických podpisů přirovnat prosté elektronické podpisy.[137] S tím se autor této práce neztotožňuje, neboť prosté elektronické podpisy s sebou nesou zpravidla daleko více dat a jejich důkazní síla je vyšší (k tomu více v kapitole 3.4).

Dle věty třetí ustanovení § 561 odst. 1 občanského zákoníku „*jiný právní předpis stanoví, jak lze při právním jednání učiněném elektronickými prostředky písemnost elektronicky podepsat*“. Jiným právním předpisem je v tomto případě ZSVD a nařízení eIDAS.

Dle ustanovení § 562 odst. 1 OZ je písemná forma „*zachována i při právním jednání učiněném elektronickými nebo jinými technickými prostředky umožňujícími zachycení jeho obsahu a určení jednající osoby*“, aniž by zde byl stanoven jakýkoli požadavek na existenci podpisu.

[133] JANOUŠEK, Michal. § 561 [Písemná forma právního jednání]. In: LAVICKÝ, Petr a kol. Občanský zákoník I. Obecná část (§ 1−654). 2. vydání. Praha: C. H. Beck, 2022, s. 1792, marg. č. 11. a HANDLAR, Jiří. § 582 [Nedostatek formy]. In: LAVICKÝ, Petr a kol. Občanský zákoník I. Obecná část (§ 1−654). 2. vydání. Praha: C. H. Beck, 2022, s. 1865, marg. č. 6.
[134] JANOUŠEK, Michal. § 561 [Písemná forma právního jednání]. In: LAVICKÝ, Petr a kol. Občanský zákoník I. Obecná část (§ 1−654). 2. vydání. Praha: C. H. Beck, 2022, s. 1791, marg. č. 3.
[135] *Ibid*, s. 1795, marg. č. 34.
[136] Rozhodnutí Nejvyššího soudu ČR, sp. zn. 21 Cdo 682/2018, ze dne 18. 12. 2018.
[137] PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra, op. cit. 9.

Musí však být zachovány zmíněné podmínky, tedy (i) zachycení obsahu a (ii) určení jednající osoby.[138]

Za zmínku na tomto místě stojí, že občanský zákoník nepoužívá jednotnou terminologii. Na mnoha místech je totiž použita terminologie *elektronická podoba* či *elektronické forma*. V této souvislosti autor považuje tato za synonyma, která v rámci zákona mají stejný smysl. Blíže k tomuto tématu vizte kapitolu 4.1.4.

4.1.1. Zachycení obsahu

Podmínkou zachycení obsahu se rozumí možnost obsah právního jednání uchovat a opakovaně zobrazovat. Podle Polčáka písemnost není projevem vůle, ale pouze jeho vnější jevovou formou.[139] Dle Donáta a Tomíška není podstatné, zda je text na hmotném nosiči, jako je papír či jiný pevný podklad, případně elektronický dokument vytvořený a zobrazený v textovém editoru.[140] Dle Korbela, Kováře a Amlera je podmínka splněna, pokud se jedná o grafické znázornění souboru znaků, které jsou písmem, včetně textu v e-mailu, který je možné uchovat například na datových nosičích či uložit v cloudu.[141] Dle Berana je nutné uchování obsahu na listině nebo na jiném médiu umožňující opakované zobrazení.[142] Dle Janouška je zapotřebí způsobilost uchovat informační hodnotu dat a možnost se s nimi opakovaně seznamovat, aniž by byla ovlivněna jejich kvalita.[143]

Z výše uvedených názorů vyplývá, že lze analogicky aplikovat náležitosti trvalého nosiče dat. Ten je v českém právním řádu definován v řadě předpisů jako „*jakýkoli nástroj, který umožňuje uchování informací, aby mohly být využívány po dobu přiměřenou účelu těchto informací, a který umožňuje reprodukci těchto informací v nezměněné podobě*“.[144]

---

[138] MELZER, F., TÉGL, P. a kol. Občanský zákoník. Velký komentář. Sv. III. § 419-654. Praha: Leges, 2014, komentář k § 561 odst. 1; KORBEL, František a MELZER, Filip. Písemnost, elektronický a biometrický podpis v elektronickém právním jednání, op. cit. 11; KORBEL, František, KOVÁŘ, Dalibor, POTOČŇÁK, Štefan: Elektronická identita při elektronickém (hmotně)právním jednání, op. cit. 63.

[139] POLČÁK, Radim. Elektronické právní jednání – změny, problémy a nové možnosti v zákoně č. 89/2012 Sb. *Bulletin advokacie*, 2013, č. 10, s. 34.

[140] DONÁT, Josef a TOMÍŠEK, Jan. Právo v síti: průvodce právem na internetu. V Praze: C.H. Beck, 2016. ISBN 978-80-7400-610-4, s. 159.

[141] KORBEL, František; KOVÁŘ, Dalibor a AMLER, Pavel. *Interpretace elektronického podpisu a související identifikace v soukromém právu*, op. cit. 29.

[142] BERAN, Vladimír. § 562 [Elektronické a jiné technické prostředky]. In: PETROV, Jan, VÝTISK, Michal, BERAN, Vladimír a kol. Občanský zákoník. 2. vydání (1. aktualizace). Praha: C. H. Beck, 2022, marg. č. 2.

[143] JANOUŠEK, Michal. § 562 [Písemná forma právního jednání učiněného elektronickými prostředky]. In: LAVICKÝ, Petr a kol. Občanský zákoník I. Obecná část (§ 1−654). 2. vydání. Praha: C. H. Beck, 2022, s. 1801, marg. č. 12.

[144] Srov např. § 90/2 zákona č. 170/2018 Sb., o distribuci pojištění a zajištění (IDD), § 2 odst. 3 písm. h) zákona č. 370/2017 Sb., o platebním styku, § 3 odst. 2 písm. k) zákona č. 257/2016 Sb., o spotřebitelském úvěru, § 2 odst.

Danou problematikou se rovněž zabýval SDEU, např. ve svém rozhodnutí *Inconsult Anstalt v. Finanzmarktaufsicht Liechenstein*,[145] dle kterého internetová stránka, aby mohla být označena za „trvanlivé médium“, musí (i) umožnit zákazníkovi ukládat informace způsobem vhodným pro jejich pozdější využití po dobu odpovídající účelu těchto informací (ochrana zájmů zákazníka); to může znamenat dobu, během které probíhala smluvní jednání, i kdyby nedošlo k uzavření smlouvy, dobu, po kterou je smlouva v účinnosti, a nezbytně dlouhou dobu po tom, co se smlouva stala bezpředmětnou, a (ii) umožnit reprodukci uložených informací v nezměněném stavu.

V jiném rozhodnutí ve věci BAWAG Bank Österreich v. Verein für Konsumenteninfo[146] SDEU dovodil, že informace předané do schránky elektronické pošty začleněné do internetových stránek online bankovnictví lze považovat za poskytnuté na trvanlivém médiu, pokud poskytovatel aktivně oznámí uživateli existenci a dostupnost uvedených informací na uvedené internetové stránce.

Jednotná definice či názor, co se zachycením obsahu rozumí, tak neexistuje. Z výše uvedeného však vyplývá, že by měla být umožněna možnost uložení a opakovaného využití informací v nezměněné podobě.

4.1.2. Určení jednající osoby

Podmínka určení jednající osoby, respektive jeho míra, je o něco komplikovanější. Občanský zákoník totiž na rozdíl od jiných předpisů (např. zákona o elektronické identifikaci)[147] nevyžaduje prokázání totožnosti jednajícího, ale pouhou určitelnost. Dle Korbela, Kováře a Amlera[148] v případě existence požadavku písemné formy dostačuje k určení jednající osoby podle ustanovení § 562 odst. 1 občanského zákoníku i potenciální určitelnost, tedy situace, kdy použitý elektronický nebo jiný technický prostředek důkazně umožňuje určení podepisující osoby. Stejný názor zastává i Janoušek.[149] Dle něj ke splnění požadavku stačí prostá autentizace (například přihlášení se heslem), autentizace předmětem (například použitím

1 písm. q) zákona č. 256/2004 Sb., o podnikání na kapitálovém trhu, § 3 písm. cc) zákona č. 37/2004 Sb., o pojistné smlouvě, § 14/2 zákona č. 634/1992 Sb., o ochraně spotřebitele atd.

[145] Rozsudek Soudního dvora EU ze dne 27. ledna 2010, ve věci E-4/09.

[146] Rozsudek Soudního dvora EU ze dne 25. ledna 2017, ve věci C-375/15.

[147] § 2 zákona č. 250/2017 Sb., o elektronické identifikaci, ve znění pozdějších předpisů.

[148] KORBEL, František; KOVÁŘ, Dalibor a AMLER, Pavel. *Interpretace elektronického podpisu a související identifikace v soukromém právu*, op. cit. 29.

[149] JANOUŠEK, Michal. § 562 [Písemná forma právního jednání učiněného elektronickými prostředky]. In: LAVICKÝ, Petr a kol. Občanský zákoník I. Obecná část (§ 1−654). 2. vydání. Praha: C. H. Beck, 2022, s. 1801, marg. č. 12.

tokenu), biometrická autentizace (například otisk prstu, dynamikou podpisu, naskenováním tváře či oční duhovky, vzorkem hlasu atd.) anebo autentizace s prvky autorizace (SMS zpráva s univerzálním heslem, potvrzení požadavku otiskem prstu apod.). Všechny způsoby umožňují osobu určit, způsoby však mají rozdílnou míru pravděpodobnosti autentizace a reálné identifikace jednajícího. Dle Janouška však dle ustanovení § 562 odst. 1 občanského zákoníku nejsou zapotřebí zvláštní kvalifikované prostředky jako podmínka k zachování písemné formy právního jednání a prosté určení jednající osoby je tak dostačující. Dle Korbela, Kováře a Amlera[150] a Melzera a Tégla[151] je možná i identifikace přihlášením osobními identifikačními údaji v rámci sítě prostřednictvím IP adresy a fyzické adresy počítače tzv. „MAC" adresy (Media Access Control).[152] Dle Berana však zjišťování identity osoby prostřednictvím těchto identifikačních dat nelze po adresátovi požadovat.[153]

Dle Korbela, Kováře a Amlera[154] tak nelze bezdůvodně zpřísňovat požadavky na zjišťování identity v soukromoprávním jednání za účelem vyšší právní jistoty (což je navíc otázkou důkazní, nikoli platnosti jednání). Vyšší požadavky navíc vedou automaticky k širšímu zpracování osobních údajů, což je v rozporu se zásadou minimalizace zpracování osobních údajů.[155] Z toho důvodu tak nelze podmínku určení jednající osoby vykládat jako požadavek nezpochybnitelného prokázání, ale pouze jako potenciální určitelnost, která bude nejčastěji odvozena z tvrzení podepisující osoby.[156] Ke stejnému závěru pak dospívají i Korbel a Melzer.[157]

Pokud tedy zákon nestanoví výslovně jinak, včetně vyšších požadavků na ověření osoby, například při identifikaci osoby dle zákona proti legalizaci výnosů z trestné činnosti a

[150] *Ibid.*
[151] Melzer, F., Tégl, P. a kol. Občanský zákoník. Velký komentář. Sv. III. § 419-654. Praha: Leges, 2014, komentář k § 561 odst. 1.
[152] KORBEL, František; KOVÁŘ, Dalibor a AMLER, Pavel. *Interpretace elektronického podpisu a související identifikace v soukromém právu*, op. cit. 29.
[153] BERAN, Vladimír. § 562 [Elektronické a jiné technické prostředky]. In: PETROV, Jan, VÝTISK, Michal, BERAN, Vladimír a kol. Občanský zákoník. 2. vydání (1. aktualizace). Praha: C. H. Beck, 2022, marg. č. 2.
[154] KORBEL, František; KOVÁŘ, Dalibor a AMLER, Pavel. *Interpretace elektronického podpisu a související identifikace v soukromém právu*, op. cit. 29.
[155] Článek 5 odst. 1 písm. c) GDPR a recitál 11 eIDAS.
[156] KORBEL, František; KOVÁŘ, Dalibor a AMLER, Pavel. *Interpretace elektronického podpisu a související identifikace v soukromém právu*, op. cit. 29.
[157] KORBEL, František a MELZER, Filip. Písemnost, elektronický a biometrický podpis v elektronickém právním jednání, op. cit. 11, s. 34.

financování terorismu,[158] identifikaci osoby dle zákona o hazardních hrách,[159] nebo při ověření podpisu, je na smluvních stranách, jakou míru určitelnosti budou vyžadovat.[160]

4.1.3. Elektronický nebo jiný technický prostředek

Občanský zákoník pojmy elektronický nebo jiný technický prostředek blíže nespecifikuje. Dle Berana je elektronickým nebo jiným technickým prostředkem prostředek umožňující komunikaci na dálku, například počítač, telefon, telegraf či dálnopis.[161] Dle Janouška se jedná jak o hardwarové, tak softwarové aplikace. Tedy technický prostředek umožňující komunikaci na dálku, například počítač, telefon, fax, dálnopis, telefax nebo jiná elektronická komunikační zařízení, síť elektronických komunikací či elektronická pošta.[162]

Obdobnou definici lze najít v zákoně o některých službách informační společnosti,[163] podle kterého se elektronickými prostředky rozumí „*zejména síť elektronických komunikací, elektronická komunikační zařízení, automatické volací a komunikační systémy, telekomunikační koncová zařízení a elektronická pošta*“. Dle důvodové zprávy se pak elektronickými prostředky rozumí jak hardware, tak softwarové aplikace (včetně např. chatovacích aplikací). V definici elektronických prostředků je navíc obsažena i elektronická pošta, která je dále definována jako „*textová, hlasová, zvuková nebo obrazová zpráva poslaná prostřednictvím veřejné sítě elektronických komunikací, která může být uložena v síti nebo v koncovém zařízení uživatele, dokud ji uživatel nevyzvedne*“.[164]

4.1.4. Písemná forma, listina a písemnost v elektronické podobě

Písemná forma právního jednání není občanským zákoníkem detailněji definována. Definici je tak třeba odvodit z nauky, praktického užití či jiných právních předpisů. Ustanovení § 561 odst. 1 občanského zákoníku sice výslovně zmiňuje elektronický podpis písemnosti, nicméně ani to

[158] Například povinnost identifikace klienta podle § 7 a § 8 zákona č. 253/2008 Sb. o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů.
[159] § 77 zákona č. 186/2016 Sb. o hazardních hrách, ve znění pozdějších předpisů.
[160] KORBEL, František, KOVÁŘ, Dalibor, POTOČŇÁK, Štefan: Elektronická identita při elektronickém (hmotně)právním jednání, op. cit. 63; JANOUŠEK, Michal. § 562 [Písemná forma právního jednání učiněného elektronickými prostředky]. In: LAVICKÝ, Petr a kol. Občanský zákoník I. Obecná část (§ 1−654). 2. vydání. Praha: C. H. Beck, 2022, s. 1802, marg. č. 16.
[161] BERAN, Vladimír. § 562 [Elektronické a jiné technické prostředky]. In: PETROV, Jan, VÝTISK, Michal, BERAN, Vladimír a kol. Občanský zákoník. 2. vydání (1. aktualizace). Praha: C. H. Beck, 2022, marg. č. 2.
[162] JANOUŠEK, Michal. § 562 [Písemná forma právního jednání učiněného elektronickými prostředky]. In: LAVICKÝ, Petr a kol. Občanský zákoník I. Obecná část (§ 1−654). 2. vydání. Praha: C. H. Beck, 2022, s. 1801, marg. č. 10.
[163] § 2 písm. c) zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), ve znění pozdějších předpisů.
[164] § 2 písm. b) zákona o některých službách informační společnosti.

situaci neusnadňuje. Písemnost je totiž také použita na mnoha místech občanského zákoníku v různých souvislostech, avšak taktéž není blíže definována. Dle některých autorů jí je myšleno grafické zachycení lidské řeči posloupností znaků (písmen a čísel) a může jí být jak text psaný rukou, písemnost na hmotném substrátu, ale i písemnost v elektronické podobě.[165] Zde lze najít podobnost s požadavkem zachycení obsahu rozebíraný v kapitole 4.1.1. Dle Polčáka jsou základními náležitostmi písemnosti trvalost, písemná forma a autenticita.[166] S výjimkou spotřebitelských vztahů[167] pak není ani důležitý jazyk písemnosti, její struktura, ani lokalizační a temporální dovětek.[168] Ty však navíc u elektronických podpisů oproti podpisu vlastnoručním zpravidla najít můžeme. Dle Kmenta je na písemnost nutné přiměřeně použít ustanovení upravující písemné právní jednání.[169]

Dle ustanovení § 3026 odst. 1 občanského zákoníků platí, že „*nevylučuje-li to povaha písemnosti, platí ustanovení tohoto zákona o listině obdobně i pro jinou písemnost bez zřetele na její podobu*". Lze tak dovodit, že písemnosti mohou mít jak podobu listiny (tj. hmotného nosiče), tak mohou být v podobě jiné, a to právě například elektronické či jako text zachycený na nepřenositelném hmotném nosiči. Všechny tyto podoby mají pak stejné právní účinky jako písemnost, resp. písemností jsou. Pokud je však zákonem stanoven požadavek listiny, je vyloučeno použití písemnosti v elektronické či jiné podobě (např. při požadavku na vlastnoruční text, podpis apod.).[170]

Ani listina však není občanským zákoníkem definována. Teorie definuje listinu jako „*písemnost, která zachycuje děj, stav nebo událost, a to na obvyklém a přenositelném nosiči*".[171] Dle Polčáka jde o písemnost zachycenou na papíře nebo podobném podkladě. Z toho Polčák dovozuje, že každá listina je písemností, avšak ne každá písemnost musí být listinou. Následně však uvádí, že elektronický dokument může splňovat náležitosti písemnosti,

[165] PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra, op. cit. 9.
[166] POLČÁK, R. Praxe elektronických dokumentů, op. cit. 8, s. 55.
[167] § 1811 odst. 1 občanského zákoníku.
[168] JANOUŠEK, Michal. § 561 [Písemná forma právního jednání]. In: LAVICKÝ, Petr a kol. Občanský zákoník I. Obecná část (§ 1−654). 2. vydání. Praha: C. H. Beck, 2022, s. 1792, marg. č. 11.
[169] KMENT, Vojtěch. *Elektronické právní jednání: Srovnávací analýza s důrazem na využití elektronického podpisu podle práva EU, České republiky a Německa*. op. cit. 5, s. 98.
[170] BERAN, Vladimír. § 3026 [Písemnosti a veřejné listiny]. In: PETROV, Jan, VÝTISK, Michal, BERAN, Vladimír a kol. Občanský zákoník. 2. vydání (2. aktualizace). Praha: C. H. Beck, 2023, marg. č. 2.
[171] BAJURA, J., ČÁP, Z., ČERNÁ, S., DOLANSKÁ BÁNYAIOVÁ, L., DVOŘÁK, J., DVOŘÁK, T., ELIÁŠ, J., ELISCHER, D., FIALA, J., FIALA, V., FRINTA, O., HAAS, K., HAJN, P., HOLČAPEK, T. a kol. Občanský zákoník: Komentář, Svazek VI, (§ 2521-3081). [Systém ASPI]. Wolters Kluwer [cit. 2023-7-26]. ASPI_ID KO89_f2012CZ., ISSN 2336-517X, § 3026.

pokud jsou splněna její základní kritéria (trvalost, písemná forma a autenticita) a nejde o podklad, na kterém je zachycena.[172]

Obecně lze dovodit, že písemnost musí mít náležitosti viditelného a čitelného textu, v podobě písmen, bez ohledu na to, zda je text na papíře nebo jiném zařízení, které umožňuje zaznamenání či zachycení, tedy trvalejší existenci písemnosti.[173] Datum však obligatorní součástí není.[174] Dle Kmenta je dle jazykového výkladu možné dovodit, že se má jednat o uspořádaný souhrn písmen, myšlenkové mapy a jiné útvary. Písmena však nemusí být nutně součástí slov či vět, ale i jakéhokoli matematického či jiného systému užívaného pro komunikaci sdělení. Lze tak uvažovat i o použití znaků či číslic, které jsou běžně používány při vyjádření algebraických i geometrických systémů či v programovacích jazycích. Dle teleologického výkladu Kment odkazuje na ustanovení § 562 odst. 1 občanského zákoníku, jehož náležitosti byly již rozebrány výše. Z něj dovozuje, že písemnost má plnit hlavně funkci zachycení obsahu, ať už na hliněných deskách, papíru, či datových nosičích.[175]

Konzervativní výklad písemnosti tak je vyjádření v existujícím jazyce, jehož obsah je trvaleji zachycen prostřednictvím existujících symbolů (zpravidla abecedy a čísel) s možností využití tabulek, grafů, obrázků apod. Musí se však jednat o právní jednání dle občanského zákoníku. Novinový článek, zdrojový kód, umělecké literární dílo apod. definici písemnosti v tomto smyslu nenaplní.[176] Je vhodné podotknout, že písemnost v elektronické podobě může v určitých situacích obsahovat více informací než v podobě listinné. Jde například o 3D modely, technické plány apod. Je však vždy důležité zachycení jejich obsahu k určitému časovému okamžiku, aby nemohlo dojít k následným změnám mimo kontrolu jednajících stran. Tím by měla být splněna funkce zachycení obsahu s možností následné reprodukce v nezměněném stavu.[177]

4.1.5. Písemnost *versus* dokument

Na tomto místě je vhodně upozornit, že z pohledu zákona často zaměňované pojmy listina, písemnost a dokument nemusí mít stejný význam. Zatímco vztah listiny a písemnosti byl

[172] POLČÁK, R. Praxe elektronických dokumentů, op. cit. 8, s. 54.
[173] KMENT, Vojtěch. *Elektronické právní jednání: Srovnávací analýza s důrazem na využití elektronického podpisu podle práva EU, České republiky a Německa*. op. cit. 5, s. 99.
[174] Rozhodnutí Nejvyššího soud ČR – senát ze dne 15. 8. 2023, č.j. 23 ICdo 60/2022 – 76.
[175] KMENT, Vojtěch. *Elektronické právní jednání: Srovnávací analýza s důrazem na využití elektronického podpisu podle práva EU, České republiky a Německa*. op. cit. 5, s. 99 – 100.
[176] *Ibid*, s. 100.
[177] *Ibid*, s. 101.

rozebrán v kapitole 4.1.4 výše, přičemž ani jeden z těchto pojmů nemá zákonnou definici, dokument právem definován je. Definice je obsažena v nařízení eIDAS, podle kterého se elektronickým dokumentem rozumí „*jakýkoli obsah uchovávaný v elektronické podobě, zejména jako text nebo zvuková, vizuální nebo audiovizuální nahrávka*“,[178] a v českém národní legislativě v ustanovení § 2 písm. e) zákona o archivnictví a spisové službě,[179] dle kterého se dokumentem rozumí „*každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, ať již v podobě analogové či digitální, která byla vytvořena původcem nebo byla původci doručena*“.

Dle Tichého „*elektronická forma předpokládá elektronický dokument, tedy elektronická data, která jsou obsažena (uchovávána) v určité databázi a bez technických prostředků nejsou čitelná. Předpokládá se však, že data jsou čitelná v písemných znacích a lze je tak přechovávat*.“[180]

Dle Polčáka písemnost a elektronická písemnost nestojí na stejné úrovni, ale naopak pojem „písemnost“ zahrnuje všechny formy včetně elektronické či případně jiné v budoucnu vynalezené.[181] Dle Korbela s Melzerem je naopak listina s elektronickým dokumentem ekvivalentní.[182] Kment se s jejich názory však neztotožňuje. Jednak upozorňuje na povahu zákona o archivnictví jakožto předpisu veřejnoprávního, a také na účel definice, která má být pokud možno co nejširší za účelem dosažení archivace jakékoli informace v jakékoli formě, jak digitální, tak analogové. V případě analogové formy nejde o data ve smyslu nařízení eIDAS, a proto tyto informace nelze podepsat jinak než vlastnoručně. Definice dokumentu navíc obsahuje i obrazové či zvukové informace, které nemusí být právním jednáním.[183] Definice dokumentu dle výše uvedeného zákona o archivnictví je tedy širší než pojmy písemnost a právní jednání dle občanského zákoníku. Autor této práce z výše popsaných důvodů souhlasí s Kmentem a neztotožňuje se s názory Korbela a Melzera.

ZSVD ve svých ustanoveních § 5 až § 7 upravujících elektronické podpisy obsahuje podpis elektronického dokumentu. Dle Kmenta lze historickým i systematickým výkladem ZSVD

[178] Článek 3 odst. 35 nařízení eIDAS.
[179] Zákon č. 499/2004 Sb., o archivnictví a spisové službě, ve znění pozdějších předpisů.
[180] TICHÝ, Luboš. Komentář k § 562. In: ŠVESTKA, Jiří, Jan DVOŘÁK, Josef FIALA a kol. *Občanský zákoník. Komentář. Svazek I*. Praha: Wolters Kluwer ČR, 2014, s. 1391.
[181] POLČÁK, R. Praxe elektronických dokumentů, op. cit. 8, s. 55.
[182] KORBEL, František a MELZER, Filip. Písemnost, elektronický a biometrický podpis v elektronickém právním jednání, op. cit. 11, s. 31.
[183] KMENT, Vojtěch. *Elektronické právní jednání: Srovnávací analýza s důrazem na využití elektronického podpisu podle práva EU, České republiky a Německa*. op. cit. 5, s. 102.

dospět k závěru, že se jedná o elektronický dokument definovaný v eIDAS.[184] S tím však autor této práce nesouhlasí, neboť elektronický dokument je v nařízení eIDAS používán v jiném smyslu, zejména za účelem zákazu jeho diskriminace v soudním správním řízení.[185] Definice v eIDAS je navíc blíže definici dokumentu v zákonu o archivnictví, jak je rozebráno výše. V souvislosti s elektronickými podpisy nařízení eIDAS používá *data v elektronické podobě*, která nejsou blíže specifikována. Autor této práce však souhlasí s Kmentem, že se pro účely soukromého práva termín dokument obsažený v ZSVD má vykládat jako písemnost v elektronické podobě.

Autoři zabývající se oblastí spisové služby tak správně důsledně odlišují pojmy *písemnost* a *dokument*. Hlavním z důvodů je právě širší pojem dokument, dle kterého do správy spisové služby patří i audiovizuální záznamy (např. v soudním spisu), které nelze písmem zaznamenat, a přesto do působnosti zákona o archivnictví spadají. Autoři také zdůrazňují, že je důležité pojem písemnost chápat nezávisle na nosiči (ať už tradiční analogový, nebo digitální).[186]

4.1.6. Vzájemný vztah ustanovení § 561 a § 562 občanského zákoníku

Ke vztahu ustanovení § 561 odst. 1 a ustanovení § 562 odst. 1 občanského zákoníku vzniklo několik názorových proudů. Dle prvního je ustanovení § 562 odst. 1 zvláštní právní úpravou vůči obecné právní úpravě písemné formy s podpisem v § 561 odst. 1.[187] Dle jiných autorů pak na ustanovení § 562 odst. 1 navazuje úprava v ZSVD s úpravou identifikace podepisující se osoby. Dle tohoto názorového proudu je na rozdíl od prvního zapotřebí k jednání v písemné formě vždy připojit podpis.[188]

K prvnímu názorovému proudu se staví Beran, dle kterého je písemná forma zachována, i pokud nejsou splněny podmínky ustanovení § 561 odst. 1, tedy právní jednání není podepsáno. Beran argumentuje tím, že v opačném případě by byla úprava obsažená v ustanovení § 562 odst. 1 nadbytečná a postačovala by úprava obsažená v ustanoveních § 561 odst. 1 a § 3026 odst. 1 občanského zákoníku.[189] Dle Bezoušky[190] se taktéž jedná v případě ustanovení § 562

[184] *Ibid*, s. 103.
[185] Článek 46 eIDAS.
[186] KUNT, M. – LECHNER, T. *Spisová služba*. 2., aktualizované vydání. Praha: Leges, 2017, s. 76–77.
[187] BEZOUŠKA, P., HAVEL, B. Občanský zákoník: Srovnávací komentář. [Systém ASPI]. Wolters Kluwer [cit. 2023-6-3]. ASPI_ID KO89_p12012CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X, § 562.
[188] *Ibid*.
[189] BERAN, Vladimír. § 561 [Písemná forma]. In: PETROV, Jan, VÝTISK, Michal, BERAN, Vladimír a kol. Občanský zákoník. 2. vydání (1. aktualizace). Praha: C. H. Beck, 2022, marg. č. 1.
[190] BEZOUŠKA, P., HAVEL, B. Občanský zákoník: Srovnávací komentář. [Systém ASPI]. Wolters Kluwer [cit. 2023-6-3]. ASPI_ID KO89_p12012CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.

odst. 1 o zvláštní pravidlo. Svoji argumentaci podporuje stejně jako Beran, mimo jiné tím, že pokud by se jednalo o přístup druhý, tedy že právní jednání učiněné elektronickými prostředky vyžaduje k zachování písemné formy vždy, aby bylo elektronicky podepsáno, bylo by ustanovení § 562 odst. 1 nadbytečné, neboť v takovém případě nepřináší nic nového.

Dle platformy Rozumné právo je písemná forma zachována i při absenci podpisu. Pro zvýšení právní jistoty však členové navrhují novelu současného zákonného znění. Jako inspiraci uvádějí návrh novely slovenského občanského zákoníku, která zaváděla vyvratitelnou právní domněnku, podle které při použití elektronické adresy, kterou osoba již v právním styku někdy použila nebo tuto adresu předtím sama uvedla, se má se za to, že jedná právě tato osoba.[191] Toto řešení dle autora této práce reflektuje praxi, kdy uživatelé různých služeb používají stejné údaje, kterými nutně nemusí být pouze email, ale i údaje přihlašovací.

Korbel, Kovář a Amler[192] považují taktéž vzájemný vztah uvedených ustanovení za vztah speciality. Dle autorů oproti původní úpravě došlo k záměrnému oddělení ustanovení § 562 odst. 1 od ustanovení § 561 odst. 1, aby bylo zřejmé, že se zde podpis (v jakékoli formě) nevyžaduje, pokud jsou splněny podmínky zachycení jeho obsahu a určení jednající osoby. Pokud zákon výslovně nestanoví jinak, lze písemné smlouvy tedy uzavírat elektronicky i bez podpisu.[193] Stejně vnímají vztah těchto dvou ustanovení Donát, Tomíšek a Fencl.[194] Ti mimo jiné dovozují vztah speciality použitím gramatického výkladu a z důvodu použití spojky „*i*“ v ustanovení § 562 odst. 1, tedy souběhu více možných písemných forem. Ke stejnému závěru dospívají i Korbel a Melzer,[195] dle kterých se v případě prostého emailu použije věta druhá ustanovení § 561 odst. 1, a pokud by nebyla splněna ani podmínka podpisu ve smyslu tohoto ustanovení, pak ustanovení § 562 odst. 1. Jde tedy o zvláštní úpravu písemnosti bez podpisu. Stejný názor zastávají i Donát s Tomíškem[196] a Jareš.[197]

Autor této práce se s těmito tvrzení plně ztotožňuje. Jak bude rozebráno v kapitole 5.1.4, dospívají k němu i některé soudy.

---

[191] ROZUMNÉ PRÁVO. *Platforma Rozumné právo: Je třeba zjednodušit elektronické právní jednání*, op. cit. 100.
[192] *Ibid*.
[193] DONÁT, Josef a TOMÍŠEK, Jan. Právo v síti: průvodce právem na internetu, op. cit. 140, s. 160.
[194] DONÁT, Josef, Jan TOMÍŠEK a Ivan FENCL. *Je publikovaná judikatura k elektronickým podpisům skutečně relevantní?*, op. cit 26.
[195] KORBEL, František a MELZER, Filip. Písemnost, elektronický a biometrický podpis v elektronickém právním jednání, op. cit. 11, s. 34 – 35.
[196] DONÁT, Josef a TOMÍŠEK, Jan. Právo v síti: průvodce právem na internetu, op. cit. 140, s. 160.
[197] JAREŠ, Adam. *SMLOUVA PODEPSANÁ ELEKTRONICKÝM PODPISEM*, op. cit. 6, s. 71.

Druhý názorový proud zastávají například Podaný[198] či Peterka,[199] dle kterých výše zmíněné závěry nejsou správné. Jak již bylo rozebráno, jejich námitky směřují k dodržení písemné formy právního jednání bez podpisu, respektive s prostým elektronickým podpisem, proti kterému mají autoři několik výše diskutovaných výhrad. Tato otázka je však spíše spojena s důkazními účinky, které jsou rozebrány v kapitole 4.4 níže.

Hrdlička taktéž zastává názor, že ustanovení § 562 odst. 1 nelze považovat za *lex specialis* k ustanovení § 561 odst. 1. Z toho důvodu dle jeho názoru nesmí ani chybět elektronický podpis u datové zprávy.[200] Autor této práce považuje tento názor za již překonaný, o čemž svědčí i aktualizované vydání komentářové literatury.[201] Ohledně úkonu učiněného prostřednictvím datové schránky vůči orgánům veřejné moci se navíc uplatní zákonná fikce dle § 18 odst. 2 zákona o elektronických úkonech a autorizované konverzi dokumentů,[202] podle které „*úkon učiněný osobami uvedenými v zákoně, prostřednictvím datové schránky má stejné účinky jako úkon učiněný písemně a podepsaný, ledaže jiný právní předpis nebo vnitřní předpis požaduje společný úkon více z uvedených osob*“.

S alternativním výkladem přichází Kment, dle kterého požadavky ustanovení § 561 odst. 1 a § 562 odst. 1 občanského zákoníku platí současně a nemají vůči sobě vztah speciality. Kment ustanovení § 562 odst. 1 vykládá jako dovolení písemnosti v elektronické podobě a její náležitosti (zachycení obsahu a určení jednající osoby). V ustanovení § 561 odst. 1 pak shledává příkaz podpisu v elektronické podobě, tedy kumulativní náležitosti pro platné právní jednání v písemné (elektronické, pozn. autora) podobě.[203] Tento výklad je podobný názoru Hrdličky s tím rozdílem, že klade vyšší nároky na písemnou formu v elektronické podobě.

Kment ještě uvádí možnost opačného vztahu ustanovení. Dle tohoto pohledu určení jednající osoby nespočívá pouze v tvrzení o totožnosti, ale jako autentizace totožnosti jednající osoby dle míry spolehlivosti. Důsledkem by možnost použití prostého elektronického podpisu dle

[198] PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra, op. cit. 9.
[199] PETERKA, Jiří. *Zatímco technické obory přitvrzují, právo naopak měkne*, op. cit 91.
[200] HRDLIČKA, Miloslav. § 562 [Písemná forma právního jednání učiněného elektronickými prostředky]. In: LAVICKÝ, Petr a kol. Občanský zákoník I. Obecná část (§ 1−654). 1. vydání. Praha: C. H. Beck, 2014, s. 2025, marg. č. 1.
[201] JANOUŠEK, Michal. § 562 [Písemná forma právního jednání učiněného elektronickými prostředky]. In: LAVICKÝ, Petr a kol. Občanský zákoník I. Obecná část (§ 1−654). 2. vydání. Praha: C. H. Beck, 2022, s. 1801, marg. č. 9.
[202] Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů.
[203] KMENT, Vojtěch. *Elektronické právní jednání: Srovnávací analýza s důrazem na využití elektronického podpisu podle práva EU, České republiky a Německa*. op. cit. 5, s. 106.

ZSVD a ustanovení § 561 odst. 1 občanského zákoníku byla vyloučena požadavkem na určení jednající osoby dle ustanovení § 562 odst. 1., a tedy použití elektronického podpisu vyšší úrovně, který určení jednající osoby zajistí. Tento výklad (a popření výkladu prvního jako převládajícího) Kment podporuje argumentem, že předpokládané splnění požadavků písemné formy písemnosti v elektronické podobě není jisté. Srovnává písmena v písemnosti na listině, kde je jejich pořadí pevně dáno, zatímco v případě elektronické podoby mohou být změněna.[204]

Autor této práce s tímto přirovnáním nesouhlasí, neboť elektronické formáty, které uvádí Kment, nenaplní definici písemnosti. Je rozdíl mezi rozepsanou a neodeslanou emailovou zprávou, jejíž obsah může být jakkoli měněn, a nenaplní tak definici písemnosti, a odeslanou emailovou zprávou, jejíž editace není možná, a v tom případě k naplnění definice písemnosti dochází.

Další výklady nejsou vyloučeny. Například lze argumentovat, že i když ZSVD umožňuje použití prostého elektronického podpisu pro jiná jednání než ta, která jsou explicitně vyloučena, v kontextu soukromého práva není použití prostého elektronického podpisu dostačující k dosažení písemné formy právního jednání. Alternativně lze připustit, že ustanovení § 562 odst. 1 občanského zákoníku sice představuje speciální ustanovení ve vztahu k § 561 odst. 1 občanského zákoníku, avšak zároveň obsahuje i teleologickou definici právního jednání vyžadujícího písemnou formu, kterou nelze splnit pouhým prostým elektronickým podpisem. Tyto interpretace jsou však v rozporu s jazykovým výkladem.[205]

4.1.7. Dílčí závěr

Ačkoli je úprava obsažená v ustanoveních § 561 odst. 1 a § 562 odst. 1 občanského zákoníku v českém právním řádu ve svém principu již déle než 30 let,[206] výklad těchto ustanovení a jednotlivých částí je stále nejasný. Zatímco zachycení obsahu lze vykládat jako možnost uložení a opakovaného využití informací v nezměněné podobě, určení jednající osoby, resp. její míra je čistě v diskreci smluvních stran. Elektronický nebo jiný prostředek lze v současném vnímání chápat jako telefon, počítač či emailovou poštu nebo jinou komunikační platformu. Vztah písemnosti, elektronického dokumentu a listiny je takový, kde písemnost je nadřazeným pojmem. Písemnosti mohou mít jak podobu listiny (tj. hmotného nosiče), tak mohou být v podobě jiné, a to právě například elektronické. Od toho je však zapotřebí odlišovat

[204] *Ibid*, s. 106.
[205] *Ibid*, s. 108.
[206] Srov. kapitolu 2.3.

(elektronický) dokument, který je zejména veřejným právem, ale i nařízením eIDAS, používán v jiné souvislosti. Vzájemný vztah ustanovení § 561 odst. 1 a § 562 odst. 1 občanského zákoníku pak vyvolává největší diskuze. Ačkoli judikatura[207] i názory odborné veřejnosti jsou různé, nejčastější a podle autora této práce správný výklad je vztah speciality. K dodržení písemné formy právního jednání tak za splnění zákonných podmínek dle § 562 odst. 1 občanského zákoníku nemusí být k právnímu jednání připojena jakákoli forma elektronického podpisu.

4.2. Digitální kontinuita a související praktické aspekty

Klíčovou problematikou elektronických dokumentů, datových zpráv, podpisů a pečetí je jejich stárnutí. Jeho řešení je označováno jako udržování digitální kontinuity, kterou je „*soubor procesů, opatření a prostředků nutných k tomu, aby byl původce schopen zajistit dlouhodobou důvěryhodnost informací a dokumentů.*“[208] Dle Peterky digitální kontinuita spočívá v udržování elektronických dokumentů, datových zpráv, podpisů a pečetí ve stavu, který umožňuje s těmito nakládat způsobem jako při jejich vytvoření (aktuální digitální kontinuita), nebo ve stavu nižší míry, kdy je dostatečná pouhá potenciální možnost použití elektronických dokumentů, datových zpráv, podpisů a pečetí k zamýšlenému účelu (potenciální digitální kontinuita). Tato problematika však v praxi není dostatečně řešena.[209]

Důvodem zastarávání je ochrana vytvořených elektronických dokumentů před oslabováním kryptografických postupů a algoritmů. Bez omezení platnosti by nebylo možné z technické platnosti dovozovat právní pravost podpisů a dokumentů, neboť by z důvodu oslabení kryptografických algoritmů původně použitých při podpisu daného dokumentu bylo možné reálně najít (vypočítat) jiný kolizní dokument s jiným obsahem, ale stejným elektronickým podpisem. To by v praxi znamenalo možnost přenesení elektronického podpisu z původního dokumentu na dokument pozdější a v obou případech by byl podpis ověřen jako platný bez možnosti prokázání, který z dokumentů je pravý.[210] K tomu více v kapitole 4.2.10.

---

[207] Srov. kapitolu 5.1.4.
[208] NÁRODNÍ ARCHITEKTONICKÝ PLÁN - ARCHITEKTURA EGOVERNMENTU ČR. *Systémy správy dokumentů*. Online. Dostupné z: https://archi.gov.cz/nap:system_spravy_dokumentu?do=#digitalni_kontinuita. [cit. 2024-01-18].
[209] PETERKA, Jiří. *Jak na digitální kontinuitu (nejenom) v datových schránkách?* Online. Dostupné z: https://www.lupa.cz/clanky/jak-na-digitalni-kontinuitu-nejenom-v-datovych-schrankach/. [cit. 2023-11-18].
[210] NÁRODNÍ ARCHITEKTONICKÝ PLÁN - ARCHITEKTURA EGOVERNMENTU ČR. *Systémy správy dokumentů*, op. cit. 208.

Jednotlivé aspekty je navíc vhodné podrobněji rozebrat k pochopení rozdílu jednotlivých úrovní elektronických podpisů, pečetí a razítek a následného zjištění, zda je k jednotlivým aspektům v praxi přihlíženo. Často se lze totiž setkat s pouhou argumentací vyšší úrovní elektronických podpisů, pečetí či razítek, aniž by byly skutečnosti relevantní pro jejich vyšší úroveň dostatečně zkoumány.

4.2.1. Aktuální digitální kontinuita

V prvním případě, tedy aktuální digitální kontinuity, jde zejména o možnost autorizované konverze či předložení a práce s nimi. Tyto postupy bývají typicky podrobně upraveny technickými standardy a normami,[211] což vede k automatizaci vyhodnocení dokumentů prostřednictvím počítačových programů bez nutnosti přítomnosti lidského prvku.[212]

Problém s autorizovanou konverzí prostřednictvím Czech POINT nastává však v případě, kdy k pokusu o autorizovanou konverzi dochází po vypršení platnosti certifikátu, která není prodloužena např. přidáním dalšího časového razítka, a to před vypršením platnosti certifikátu. V praxi lze poukázat na nesprávné chování programu Adobe Reader, který v určitých situacích hlásí časové razítko jako platné, a to i když má časové razítko expirovaný certifikát. Jako rozhodný okamžik pro ověření platnosti podpisu používá totiž čas jeho připojení. To je způsobeno tím, že program Adobe Reader považuje za kořenový certifikát příslušné autority časového razítka vedený v seznamu Evropské Unie[213] přes jeho podmnožinu (seznamu EUTL vedený společností Adobe). Řešením je pouze odstranění prošlého certifikátu časového razítka ze seznamu důvěryhodných certifikátů v daném úložišti. Program pak bude důvěřovat vydavateli certifikátu (I.CA), ale certifikát autority časového razítka (na kterém je založeno časové razítko) již nebude považovat za kořenový, a bude zkoumat jeho platnost v čase (tedy k aktuálnímu času).[214] Ta samá situace pak nastává v případě konverze staršího dokumentu z datové zprávy v datové schránce.

Druhou problematickou částí je předložení dokumentu třetí osobě. Ta dokument může odmítnout ze stejného důvodu, tedy nemožnosti ověření platnosti podpisu. V případě orgánů veřejné moci tak zpravidla činí automaticky podatelna daného orgánu. V případě

[211] Srov např. články 32 a 40 nařízení eIDAS.
[212] PETERKA, Jiří. *Jak na digitální kontinuitu (2): Co když platnost elektronického podpisu už nejde ověřit?* Online. Dostupné z: https://www.lupa.cz/clanky/jak-na-digitalni-kontinuitu-2-co-kdyz-platnost-elektronickeho-podpisu-uz-nejde-overit/. [cit. 2023-11-22].
[213] European Union Trusted List, dostupný zde: https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home
[214] BÁJEČNÝ SVĚT. *Příklad ztráty digitální kontinuity*. Online. Dostupné z: https://www.bajecnysvet.cz/priklady/priklad010.php. [cit. 2023-11-25].

soukromoprávních osob však tyto systémy ve většině případů automatické nejsou, a k ověření tak musí dojít individuálně. Toto ověření probíhá zpravidla s využitím veřejně dostupných nástrojů a služeb, jakými jsou například Adobe Acrobat Reader, který však jak bylo zmíněno výše nemusí vždy poskytnout relevantní výsledek.[215] Na tomto místě je vhodné také podotknout, že záleží na exempláři daného dokumentu. U některých totiž jejich držitel může o digitální kontinuitu dbát, a jiný držitel totožného dokumentu v jiném vyhotovení kontinuitu nedodržovat. Může tak nastat situace, kdy bude totožný dokument, respektive konkrétní prvky, jako např. elektronický podpis, shledán stejnou ověřující osobou jako platný, a v případě druhého držitele neplatný.[216]

Již ze samotného názvu digitální kontinuita pak vyplývá, že jde o kontinuální proces, a nelze stárnutí dokumentů zabránit trvale. V praxi jde spíše o odkládání konce platnosti příslušných certifikátů, kdy je nutné kroky k jejich prodloužení činit vždy před jejich vypršením, a to do doby, dokud je digitální kontinuitu zapotřebí udržovat (typicky přidáváním časových razítek).[217, 218]

4.2.2. Potenciální digitální kontinuita

Druhý přístup potenciální digitální kontinuity klade na elektronické dokumenty, datové zprávy, podpisy a pečeti nižší požadavky. Potenciální možnost dosažení zamýšleného účelu je však na rozdíl od aktuální digitální kontinuity spojena zpravidla se zapojením dalšího prvku, neboť nelze provést čistě automatizované ověření. To je ve většině případů spojeno s časově a finančně náročným zkoumáním příslušného znalce, jejichž počet je navíc omezen. Tento postup tedy není vhodným a praktickým každodenním řešením, ale může posloužit jako záložní varianta v případě, kdy není aktuální digitální kontinuita dodržena, a to zpravidla před soudem. Je těžko představitelné, že bude jiný orgán veřejné moci, např. katastrální úřad či Czech POINT, potenciální digitální kontinuitu zkoumat či akceptovat v rámci běžného řízení posudek soudního znalce či jiného odborníka.[219]

[215] PETERKA, Jiří. *Jak na digitální kontinuitu (nejenom) v datových schránkách?*, op. cit. 209.
[216] *Ibid.*
[217] K tomu více např. zde BÁJEČNÝ SVĚT. *Kvalifikovaný el. podpis z roku 2012*. Online. Dostupné z: https://www.bajecnysvet.cz/priklady/priklad008.php. [cit. 2023-11-25].
[218] PETERKA, Jiří. *Jak na digitální kontinuitu (nejenom) v datových schránkách?*, op. cit. 209.
[219] PETERKA, Jiří. *Jak na digitální kontinuitu (2): Co když platnost elektronického podpisu už nejde ověřit?*, op. cit. 212.

4.2.3. Autenticita dokumentu *versus* pravost dokumentu

S problematikou aktuální a potenciální digitální kontinuity je dle Peterky spojen rozdíl mezi autenticitou a pravostí dokumentu, tedy to, co je zapotřebí z elektronického dokumentu dovodit.[220]

Autenticitou, označovanou též jako integritou dokumentu, se rozumí stav, kdy jde o původní dokument, tedy nedošlo k jeho změně. Ta je zpravidla zajištěna všemi druhy kryptografických elektronických podpisů, pečetí a časových razítek, tedy zaručeného elektronického podpisu, zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu, kvalifikovaného elektronického podpisu, zaručené a kvalifikované elektronické pečeti a elektronických časových razítek.[221] Výše uvedené elektronické prostředky (s výjimkou prostého elektronického podpisu, který integritu dokumentu nechrání) pak v tomto případě autenticitu zaručují lépe než podpis vlastnoruční, neboť v jeho případě nelze stoprocentně zaručit, že část textu nebyla vložena až po podpisu, případně nedošlo k záměně nepodepsaných stran vícestránkového dokumentu. Pokud je však elektronický dokument podepsán jednou z výše uvedených forem elektronického podpisu či opatřen elektronickou pečetí či razítkem a tyto jsou ověřeny jako platné, lze dovodit, že se elektronický dokument nezměnil, a je tedy autentický.[222]

Pravost spočívá v původu dokumentu od osoby, která jím projevuje svou vůli. Pravost se dovozuje zpravidla z autentizačních prvků obsažených v dokumentu či s dokumentem spojenými, tedy elektronickými podpisy, elektronickými pečetěmi a elektronickými časovými razítky.[223] Dle Peterky to platí pouze v případě kvalifikovaných a uznávaných prostředků, neboť pouze ty jsou založené na kvalifikovaných certifikátech, za jejichž správnost ručí jejich vydavatel. Podepsanou osobou je pak osoba uvedená v příslušeném certifikátu.[224] Avšak ani toto nemusí platit vždy.[225]

---

[220] *Ibid.*
[221] NÁRODNÍ ARCHITEKTONICKÝ PLÁN - ARCHITEKTURA EGOVERNMENTU ČR. *Systémy správy dokumentů*. Online. Dostupné z: https://archi.gov.cz/nap:system_spravy_dokumentu?do=#digitalni_kontinuita. [cit. 2024-01-18].
[222] PETERKA, Jiří. *Jak na digitální kontinuitu (2): Co když platnost elektronického podpisu už nejde ověřit?,* op. cit. 212.
[223] NÁRODNÍ ARCHITEKTONICKÝ PLÁN - ARCHITEKTURA EGOVERNMENTU ČR. *Systémy správy dokumentů*, op. cit. 221.
[224] PETERKA, Jiří. *Jak na digitální kontinuitu (2): Co když platnost elektronického podpisu už nejde ověřit?*, op. cit. 212.
[225] K tomu srov. např. KORBEL, František, KOVÁŘ, Dalibor, POTOČŇÁK, Štefan: Elektronická identita při elektronickém (hmotně)právním jednání, op. cit. 63, s. 630.

Rozdíl těchto funkcí lze analogicky najít pod různými označeními dle jednotlivých autorů v kapitole 2.2 výše. Pokud dokument podepíše osoba jiná než osoba určená dokumentem jako osoba jednající a nejde o případ zastoupení, jde o dokument, který není pravý, nicméně může být stále autentický. To samé platí, podepíše-li dokument osoba neexistující (fiktivní).[226] Dle Polčáka je pak prokazování autenticity v případě elektronických dokumentů snazší než v případě dokumentů listinných. Místo zkoumání papíru prostřednictvím znalce totiž stačí automatická výpočetní operace prostřednictvím příslušného software.[227] Kment ovšem tento závěr nepovažuje za správný. Dle jeho názoru by elektronický dokument neměl být bez dalšího rovnocenný listinné podobě a podpis vlastnoruční by neměl být rovnocenný kvalifikovanému elektronickému podpisu. Výklad Polčáka považuje Kment za přepjatý.[228]

4.2.4. Platnost elektronických podpisů a pečetí

V situaci, kdy je zapotřebí ověřit elektronický dokument, je vždy zapotřebí zkoumat platnost elektronických podpisů a pečetí a zda tyto patří jednající osobě. Pokud jsou platné, lze z nich následně dovodit, že je dokument jak autentický, tak pravý.

Pokud jsou podpisy uznávané, lze se dle Peterky spolehnout bez dalších důkazů na identitu podepsaného osoby. V takovém případě lze ověření zautomatizovat pomocí počítačového programu (ať už proprietárního nebo pomocí kvalifikované služby pro ověřování či jinak) a není zapotřebí cokoli dalšího (např. znalecký posudek, rozhodnutí soudu, osvědčení atd.). Pokud je udržována aktuální digitální kontinuita, jde o samonosný dokument, který obsahuje vše, co je potřeba pro zjištění a prokázání požadovaných vlastností. Není tomu tak ovšem u zaručených či prostých elektronických podpisů; například ve výše zmíněné situaci podpisu neexistující (fiktivní) osobou.[229]

Pokud již platnost podpisu nelze ověřit, nemusí to nutně znamenat, že podpis není pravý ani že dokument opatřený podpisem není pravý a autentický. Pravost se totiž v čase nemění, neboť je vztažena k okamžiku, kdy je podpis vytvořen, respektive kdy je elektronický dokument podepsán. Na čase je však závislá možnost ověření platnosti tohoto podpisu, kdy je v případě

[226] PETERKA, Jiří. *Jak na digitální kontinuitu (2): Co když platnost elektronického podpisu už nejde ověřit?,* op. cit. 212.
[227] POLČÁK, Radim. *Internet a proměny práva*. Téma (Auditorium). Praha: Auditorium, 2012. ISBN 978-80-87284-22-3, s. 255.
[228] KMENT, Vojtěch. *Elektronické právní jednání: Srovnávací analýza s důrazem na využití elektronického podpisu podle práva EU, České republiky a Německa*. op. cit. 5, s. 178.
[229] PETERKA, Jiří. *Jak na digitální kontinuitu (2): Co když platnost elektronického podpisu už nejde ověřit?*, op. cit. 212.

narušení aktuální digitální kontinuity zapotřebí doložit pravost a autenticitu dokumentu prostřednictvím dalších prostředků, neboť dokument již není samonosným. Takové doložení lze provést prostřednictvím potenciální digitální kontinuity.

V případě narušení aktuální digitální kontinuity nelze *a priori* bez dalšího dospět k závěru, že dokument je neautentický či nepravý. Možnost ověření se mimo jiné v čase ztrácí i u vlastnoručního podpisu vlivem vyblednutí listiny či podpisu, rozpadu papíru či změně křivky podepisující se osoby v důsledku fyziologického stárnutí či jiných změn.[230]

Jedním z možných řešení pro externí dosvědčení potenciální digitální kontinuity je dle Peterky služba elektronického notáře, resp. obdoba notářské úschovy, která v současnosti existuje pro listinné dokumenty. Ta by měla spočívat v předání elektronického dokumentu elektronickému notáři v době, kdy je zachována aktuální digitální kontinuita, aby měl notář možnost ověřit platnost podpisů, pečetí a časových razítek na daném dokumentu. Následně by notář uložil dokument u sebe způsobem zaručující autenticitu. V průběhu uložení by mohlo dojít ke ztrátě aktuální digitální kontinuity, například vypršením platnosti certifikátů. V případě potřeby by žadatel mohl požádat notáře o vydání dokumentu z elektronické úschovy, který by tak učinil v původní a nezměněné podobě. Připojil by však k dokumentu svou doložku s popisem vlastností dokumentu v době předání do notářské úschovy. Tato doložka by pak měla být dosvědčením původních vlastností dokumentu, tedy dovozením autenticity a pravosti dokumentu i po vypršení doby platnosti certifikátů elektronických podpisů či pečetí. Bylo by pak na znalci zhodnotit míru spolehlivosti vydané notářské doložky a s ní spojené doložení autenticity a pravosti dokumentu. Závěry znalce by však musely být akceptovány příslušným soudem či jiným správním orgánem v rámci zásady volného hodnocení důkazů.[231] S podobnou službou mimo jiné počítá i revize nařízení eIDAS.[232]

Alternativním přístupem by dle autora této práce mohla být zákonná úprava, která by stanovila fikci či právní domněnku pravosti a autenticity dokumentů uložených do elektronické notářské úschovy a požadavky na její technické provedení. To by samozřejmě bylo spojeno i s implementací zvoleného technického řešení pro přijímající osoby. Inspirací by pro toto řešení

[230] *Ibid.*
[231] PETERKA, Jiří. *Jak na digitální kontinuitu (3): Elektroničtí notáři, spisové služby, blockchain a vyvratitelné domněnky*. Online. Dostupné z: https://www.lupa.cz/clanky/jak-na-digitalni-kontinuitu-3-elektronicti-notari-spisove-sluzby-blockchain-a-vyvratitelne-domnenky/. [cit. 2023-11-25].
[232] Článek 45g návrhu revize nařízení eIDAS.

mohla být regulace spisových služeb.[233] Ta obsahuje detailní pravidla týkající se výběru, evidence, ochrany, zpracování, uložení a zpřístupnění archiválií. Ochrana před změnou dokumentů je v tomto případě zajištěna vedením tzv. transakčních protokolů, které jsou záznamem o veškeré činnosti v elektronickém systému spisové služby (např. změny parametrů protokolu, změny metadat, operace ve vztahu k dokumentům, jejich částem, spisům, přístupu uživatelů, informacích o smazání prázdných dílů, skartačních operacích, změn a smazání dokumentu, atd.).[234]

4.2.5. Ověřování pravosti elektronického podpisu

Elektronický podpis je možné ověřovat jak dle zákona o advokacii, tak dle notářského řádu. V prvním případě byla tato možnost vložena do ustanovení § 25a zákona o advokacii, a to novelou účinnou od 1. července 2022.[235] Ve druhém případě byla možnost vložena do ustanovení § 74a notářského řádu novelou s účinností od 1. září 2021.[236] V té souvislosti bylo vydáno i prováděcí nařízení vlády,[237] které upravuje formát a náležitosti dokumentu v elektronické podobě, u nějž lze provést legalizaci elektronického podpisu, a postup při provádění legalizace na dokumentu v elektronické podobě. S tím souvisí zákon o právu na digitální služby, konkrétně jeho ustanovení § 6, podle kterého lze mimo jiné požadavek úředního ověření vlastnoručního podpisu nebo uznávaného elektronického podpisu splnit využitím elektronického podpisu na dokumentu nedílně spojeném s kvalifikovaným elektronickým podpisem osoby oprávněné provádět ověřování pravosti podpisu, která postupem podle jiného právního předpisu[238] ověřila, že podepisující dokument před ní podepsal nebo uznal podpis za vlastní, a kvalifikovaným elektronickým časovým razítkem. Dalšími možnostmi jsou dle tohoto ustanovení ověření se záznamem informačního systému veřejné správy či využitím údajů základního registru obyvatel nebo portálu veřejné správy. [239] Pro úplnost lze uvést, že záznam v registru obyvatel je dle rozhodnutí Vrchního soudu v Praze jedinou správnou možností pro podání insolvenčních návrhů před 1. červencem 2022.[240]

---

[233] Zákon o archivnictví a spisové službě.
[234] NÁRODNÍ ARCHIV. *Spisová služba v otázkách a odpovědích*. Online. Dostupné z: https://www.nacr.cz/verejnost/2-predarchivni-pece/verejnopravni-puvodci/spisova-sluzba-otazky-odpovedi#transakce7. [cit. 2023-11-28].
[235] Zákonem č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci.
[236] Zákon č. 300/2021 Sb., kterým se mění zákon notářský řád.
[237] Nařízení vlády č. 317/2021 Sb., o postupu notáře při legalizaci elektronického podpisu.
[238] Zde je odkaz právě na zákon o advokacii a notářský řád.
[239] Ty nejsou v této práci dále rozebírány, neboť se nejedná primárně o problematiku prostého elektronického podpisu v soukromoprávního jednání.
[240] Rozhodnutí Vrchního soudu v Praze ze dne 28. 6. 2023, č. j. 3 VSPH 610/2023-A-122.

V praxi advokátní i notářské ověření pravosti elektronického podpisu fungují obdobně. Osoba, jejíž podpis má být ověřen, se dostaví k notáři či advokátovi spolu s elektronickým dokumentem, který je opatřen elektronickým podpisem. Není zde důležité, o jakou úroveň elektronického podpisu se jedná, je možné ověřit i prostý elektronický podpis. Notář či advokát následně ověří identitu osoby a připojí k dokumentu ověřovací doložku osvědčující pravost elektronického podpisu na dokumentu. Ověření identity osoby lze v případě notáře provést i vzdáleně s využitím prostředku pro elektronickou identifikaci[241] dle ustanovení § 64a odst. 2 notářského řádu. Buď v případě zajištění vysoké úrovně záruky[242] a pokud je prostředek vydáván a používán v rámci kvalifikovaného systému podle zákona o elektronické identifikaci, nebo za podmínky, za které lze použít prostředek pro elektronickou identifikaci pro účely prokázání totožnosti, kterou vyžaduje právní předpis nebo výkon působnosti, mimo rámec kvalifikovaného systému podle zákona upravujícího činnost bank.[243]

V případě notářského ověření osoba, jejíž podpis je legalizován, prohlásí, že dokument sama podepsala k němu připojeným elektronickým podpisem, který uznává za vlastní. Následně se ověřovací doložka opatří kvalifikovaným elektronickým podpisem ověřujícího a s elektronicky podepsaným dokumentem se spojí tak, aby nedošlo k porušení integrity dokumentu, na němž je elektronický podpis legalizován.[244] Obdobný postup platí v případě advokátního ověření.[245]

V obou případech dochází k ověření pravosti podpisu, nikoli jeho platnosti. Platností se advokát či notář nezabývají, což by u prostých elektronických podpisů ani nebylo technicky možné. Jak je zmíněno výše, rozhodující skutečností je prohlášení osoby o uznání podpisu za vlastní. Z pravosti podpisu se pak dá dovozovat pravost dokumentu, nelze však dovozovat autenticitu dokumentu od jeho podepsání do doby připojení ověřovací doložky. Z praktického hlediska je zajímavé podotknout, že notář připojí ověřovací doložku, kterou podepíše kvalifikovaným elektronickým podpisem notáře, a k elektronickému podpisu připojí kvalifikované elektronické časové razítko. Ověřovací doložku spojí s elektronicky podepsaným dokumentem prostřednictvím kontejneru ve formátu Associated Signature Containers – Extended (ASiC-E) tak, aby nedošlo k porušení integrity dokumentu, na němž je

[241] Např. prostřednictvím bankovní identity dle § 64a odst. 2 písm. b) notářského řádu.
[242] V souladu s prováděcím nařízením 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 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu.
[243] § 38ac zákona č. 21/1992 Sb., o bankách, ve znění zákona č. 49/2020 Sb. a pozdějších předpisů.
[244] § 74a odst. 1 a 2 notářského řádu.
[245] Srov §25a zákona o advokacii a aktuální stavovský předpis.

elektronický podpis legalizován.[246] Dle Peterky by pak notář měl navíc tento celek podepsat opět kvalifikovaným elektronickým podpisem, aby zafixoval obsah kontejneru a tím i vazbu mezi ověřovací doložkou a dokumentem s ověřovaným podpisem. Tím dochází ke vzniku nového dokumentu ve formátu ASiC kontejneru a jeho digitální kontinuita začíná běžet od začátku. To není zákonný požadavek (resp. požadavek stanovený prováděcím nařízením vlády), ale požadavek praktický. Pokud tak totiž notář neučiní, může ke ztrátě digitální kontinuity dojít v krátké době po jeho vytvoření. V takovém případě se kontejner rozpadne a nebude prokazatelná vazba mezi ověřovací doložkou a podepsaným dokumentem. Po rozpadnutí kontejneru pak připadá v úvahu pouze potenciální digitální kontinuita, která je posílena záznamem ve veřejně přístupné databázi Notářské komory. Z té však lze pouze prokázat, že daná osoba v daný den u konkrétního notáře podepsala nějaký dokument. Nelze však prokázat, o jaký dokument se jednalo. Pokud by však databáze obsahovala i otisk/hash dokumentu, byla by věrohodnost důkazu o obsahu dokumentu daleko větší (k tomu srov kapitolu 4.2.4).[247]

Aktuální digitální kontinuitu by si měl tedy příjemce ASiC kontejneru ohlídat a před propadnutím certifikátu přidat časové razítko, případně požádat notáře o zaslání nové verze kontejneru. Užití tohoto formátu je však v České republice velice omezené. Ačkoli s ním počítá nařízení eIDAS, většina veřejnoprávních orgánů neumí s tímto formátem pracovat. O tom svědčí mimo jiné i fakt, že tento formát nelze přenášet prostřednictvím datové schránky.[248]

Dokument s elektronicky ověřeným podpisem pak přináší řadu výhod. Jednak zaručuje autenticitu dokumentu, není jej potřeba autorizovaně konvertovat z listinné podoby a podepisující osoba není omezena počtem jeho vyhotovení.[249]

4.2.6. Vyvratitelná domněnka pravosti dokumentu

Do roku 2016 byla v ustanovení § 69a odst. 5 zákona o archivnictví a spisové službě upravena vyvratitelná domněnka pravosti dokumentu. Dle tohoto ustanovení platilo, že „*neprokáže-li se opak, dokument v digitální podobě se považuje za pravý, byl-li podepsán uznávaným elektronickým podpisem nebo označen uznávanou elektronickou značkou osoby, která k tomu*

[246] § 3 odst. 1 nařízení vlády č. 317/2021 Sb.
[247] PETERKA, Jiří. *Jak na digitální kontinuitu (3): Elektroničtí notáři, spisové služby, blockchain a vyvratitelné domněnky*, op. cit. 231.
[248] To by mělo být možné po novele vyhlášky ministerstva vnitra č. 194/2009 Sb., dostupné zde: https://odok.cz/portal/veklep/material/ALBSCNTFP8GB/.
[249] JAREŠ, Adam. *SMLOUVA PODEPSANÁ ELEKTRONICKÝM PODPISEM*, op. cit. 6, s. 104.

byla v okamžiku podepsání nebo označení oprávněna, a následně za doby platnosti uznávaného elektronického podpisu a kvalifikovaného certifikátu, na kterém je uznávaný elektronický podpis založen, nebo uznávané elektronické značky a kvalifikovaného systémového certifikátu, na kterém je uznávaná elektronická značka založena, opatřen kvalifikovaným časovým razítkem. To platí i pro dokumenty vzniklé z činnosti původců, kteří nejsou určenými původci“.[250]

V praxi to znamenalo, že zákonodárce problém stárnutí dokumentů žádným způsobem nepřipouštěl, což bylo samozřejmě v rozporu s realitou. Domněnka měla i dle stanoviska odboru archivní správy a spisové služby za účel „*právně eliminovat omezenou platnost kvalifikovaného certifikátu, respektive kvalifikovaného systémového certifikátu vydaného akreditovaným poskytovatelem certifikačních služeb, na kterém je založen zaručený elektronický podpis, respektive elektronická značka*“. [251] Domněnka pravosti pak ve skutečnosti mířila na změny dokumentu, tedy na jeho autenticitu. Neřešila však pravost ve smyslu této práce, tedy zda dokument pochází od podepisující osoby, ani zda byla dodržena digitální kontinuita. Pojmosloví zde bylo použito opačně. Domněnka byla zrušena zákonem č. 298/2016 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce, zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, s účinností od 1. ledna 2017. Tím odpadl hlavní argument k věčné platnosti kvalifikovaných certifikátů.

Vyvratitelná domněnka spolehlivosti záznamu

V českém právním řádu však i nadále existuje obdoba vyvratitelné domněnky pravosti, konkrétně v ustanovení § 562 odst. 2 občanského zákoníku. Dle tohoto ustanovení se má za to, že „*záznamy údajů o právních jednáních v elektronickém systému jsou spolehlivé, provádějí-li se systematicky a posloupně a jsou-li chráněny proti změnám. Byl-li záznam pořízen při provozu závodu a dovolá-li se jej druhá strana k svému prospěchu, má se za to, že záznam je spolehlivý*“.

[250] Znění zákona o archivnictví a spisové službě platné od 1. ledna 2015 do 18. září 2016.
[251] Stanovisko odboru archivní správy a spisové služby k užívání časového razítka v souvislosti s odesíláním a ukládáním dokumentů v digitální podobě, ze dne 6. dubna 2010 č. j. MV-36491-1/AS-2010, dostupné zde: https://www.mvcr.cz/soubor/uzivanicasrazstanas-pdf.aspx

Dle Zuklínové je první podmínka požadavkem provádění záznamů v časové posloupnosti právních jednání s vyloučením dodatečných změn (pozn. autora nic není vynecháno a není měněno pořadí). Druhá podmínka spočívá v ochraně provedených záznamů o právních jednáních před neoprávněnými zásahy s důsledkem změny záznamů, včetně změny v posloupnosti záznamu. V případě provozu závodu pak ani nemusí být tyto podmínky splněny.[252] Výraz spolehlivost v citovaném ustanovení zákona pak autor této práce chápe obdobně jako autenticitu dokumentu.

Dle Peterky se tomuto ustanovení dá rozumět jako zobecnění principu blockchainu či transakčních protokolů spisových služeb zmíněných výše, tedy že v záznamu není nic vynecháno, je ve správném pořadí a nedošlo k jeho změně. Nelze z něj však dovozovat správnost, přesnost či pravdivost, neboť tyto aspekty nejsou při zaznamenávání ověřovány. Systematické a posloupné vedení záznamů by pak v praxi bylo nejlepší prokazovat předem definovanou specifickou certifikací. Měl by být také kladen důraz na udržování digitální kontinuity, která je v případě transakčních protokolů spisových služeb a blockchainu řešena.[253] K tomu více v kapitole 4.3.5.

Dle Korbela využití domněnky spolehlivého záznamu, datové archivace a vhodného využívání cloudu s vhodnou transakční stopou může vést k přenesení důkazního břemene na osobu zpochybňující obsah takto uložených dokumentů.[254] Jak již bylo zmíněno, jde však pouze o autenticitu dokumentu, nikoli pravost.

Speciální vyvratitelná domněnka veřejné listiny s účinky vůči všem (*erga omnes*) je pak upravena v ustanovení § 568 občanského zákoníku. Oproti soukromým listinám zde nestačí zpochybnění skutečnosti obsažené v listině, ale je zapotřebí prokázat opak.[255] Ani v tomto případě však není řešena digitální kontinuita či autenticita původního elektronického dokumentu. Na tomto místě je vhodné podotknout, čeho se domněnka dle tohoto ustanovení

[252] ZUKLÍNOVÁ v DAVID, O., DEVEROVÁ, L., DOLANSKÁ BÁNYAIOVÁ, L., DVOŘÁK, J., DVOŘÁK, T., FIALA, J., FRINTA, O., HOLČAPEK, T., HURDÍK, J., KINDL, T., MACKOVÁ, A., PAULY, J., PAVLÍK, P., PELIKÁN, R. a kol. Občanský zákoník: Komentář, Svazek I, (§ 1-654). [Systém ASPI]. Wolters Kluwer [cit. 2023-10-4]. ASPI_ID KO89_a2012CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X, § 562.
[253] PETERKA, Jiří. *Jak na digitální kontinuitu (3): Elektroničtí notáři, spisové služby, blockchain a vyvratitelné domněnky*, op. cit. 231.
[254] KORBEL, František. *Aktuální novinky českého e-Governmentu a digitálních služeb*. Online. Dostupné z: https://www.pravniprostor.cz/clanky/spravni-pravo/aktualni-novinky-ceskeho-e-governmentu-digitalnich-sluzeb. [cit. 2023-11-29].
[255] BERAN, Vladimír. § 568 [Důkazní síla veřejné listiny]. In: PETROV, Jan, VÝTISK, Michal, BERAN, Vladimír a kol. Občanský zákoník. 2. vydání (2. aktualizace). Praha: C. H. Beck, 2023, marg. č. 3.

týká. Dle Mackové se totiž jedná o domněnku pravosti a správnosti obsahu,[256] zatímco dle Berana[257] a Lavického[258] se domněnka právě na pravost neuplatní a musí ji prokázat ten, kdo se jí dovolává. Ke zpochybnění pravosti tak není zapotřebí prokázání opaku, ale pouhé tvrzení.

4.2.7. Uchovávání *versus* archivace

V daném kontextu je zapotřebí rozlišovat mezi pojmy uchovávání a archivace dokumentů či informací. Dle preambule nařízení eIDAS by mělo nařízení „*zajistit dlouhodobé uchovávání informací, aby zajistilo dlouhodobou platnost elektronických podpisů a elektronických pečetí a zaručilo, že mohou být ověřeny bez ohledu na budoucí technologické změny*“.[259] Jinými slovy, cílem je zajistit digitální kontinuitu. Z toho důvodu pak články 34 a 40 nařízení eIDAS mluví o kvalifikované službě uchovávání kvalifikovaných elektronických podpisů a pečetí. Cílem těchto služeb pak není péče o dokument jako takový, ale pouze o jeho podpisy, časová razítka či pečetě.

Připravovaná revize nařízení eIDAS[260] v novém oddílu 10 počítá dokonce i se zřízením poskytování kvalifikovaných služeb v oblasti elektronické archivace. Ta obecně cílí primárně na péči o dokumenty jako takové. Dle navrhovaného znění revize nařízení eIDAS se elektronickou archivací rozumí „*služba zajišťující přijímání, uchovávání, výmaz a přenos elektronických údajů nebo dokumentů s cílem zaručit jejich integritu, přesnost jejich původu a právní znaky po celou dobu uchovávání*“. Jedná se o službu podobnou elektronické notářské úschově rozebrané v kapitole 4.2.4.

[256] MACKOVÁ, § 568 [Pravost a pravdivost veřejné listiny]. In: DAVID, O., DEVEROVÁ, L., DOLANSKÁ BÁNYAIOVÁ, L., DVOŘÁK, J., DVOŘÁK, T., FIALA, J., FRINTA, O., HOLČAPEK, T., HURDÍK, J., KINDL, T., MACKOVÁ, A., PAULY, J., PAVLÍK, P., PELIKÁN, R. a kol. Občanský zákoník: Komentář, Svazek I, (§ 1-654). [Systém ASPI]. Wolters Kluwer [cit. 2023-10-4]. ASPI_ID KO89_a2012CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.
[257] BERAN, Vladimír. § 568 [Důkazní síla veřejné listiny]. In: PETROV, Jan, VÝTISK, Michal, BERAN, Vladimír a kol. Občanský zákoník. 2. vydání (2. aktualizace). Praha: C. H. Beck, 2023, marg. č. 4.
[258] LAVICKÝ, Petr. § 568 [Pravost a správnost veřejné listiny]. In: LAVICKÝ, Petr a kol. Občanský zákoník I. Obecná část (§ 1−654). 2. vydání. Praha: C. H. Beck, 2022, s. 1822, marg. č. 3.
[259] Bod 61 preambule nařízení eIDAS.
[260] Návrh nařízení Evropského Parlament a Rady, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu, dostupný zde: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52021PC0281&from=EN.

Dle Peterky lze očekávat, že budoucí kvalifikované služby elektronické archivace budou v zásadě odpovídat již existujícím službám, a cílit tedy primárně na potenciální digitální kontinuitu, nikoli aktuální digitální kontinuitu.[261]

Uchovávání elektronických dokumentů

Jak již bylo zmíněno výše, zachování digitální kontinuity je hlavním cílem uchovávání elektronických dokumentů a připojených elektronických podpisů, pečetí a časových razítek. Péče spočívá v opakujícím se provádění určitých úkonů, které musí být uskutečněny vždy nejpozději před vypršením platnosti předchozích prostředků. Zpravidla jde o přidávání časových razítek a validačních informací (tj. informací pro pozdější ověření). Všechny tyto aspekty jsou upraveny příslušnými technickými normami a standardy, v tomto případě zejména standardy evropské agentury ETSI.[262]

Standardy upravují postup jak pro udržování aktuální digitální kontinuity, zejména aktivní péčí o podpisy a pečetě a v důsledku i elektronické dokumenty jako takové, tak pro důkazy o existenci těchto dokumentů, například v případě nepodepsaných elektronických dokumentů, tedy aspektů potenciální digitální kontinuity.

Standardy dále upravují tři různé modely uchovávání dokumentů podle toho, kde jsou uloženy. Prvním modelem je uchovávání s úložištěm, kdy jsou dokumenty, které mají být uchovány, uloženy přímo v úložišti poskytovatele dané služby, kde je zajištěna jejich digitální kontinuita, a klient je má k dispozici kdykoli ke stažení. Druhým modelem je uchovávání s dočasným úložištěm, kdy jsou dokumenty, které mají být uchovány, uloženy u klienta. Poskytovatel služby uchovává pouze údaje či otisk (hash) daného dokumentu dočasně, nejdéle do doby provedení dalšího úkonu, který poskytovatel provede sám od sebe (asynchronně). Důkazy jsou pak uchovávány poskytovatelem služby po omezenou dobu, kdy si je může klient stáhnout. Třetím modelem je uchovávání bez úložiště, kdy jsou dokumenty, které mají být ověřeny, uloženy u klienta, který je předává poskytovateli služby k provedení dalšího úkonu.

[261] PETERKA, Jiří. *Jak na digitální kontinuitu (4): Jak aktivně pečovat o starší dokumenty a datové zprávy*. Online. Dostupné z: https://www.lupa.cz/clanky/jak-na-digitalni-kontinuitu-4-jak-aktivne-pecovat-o-starsi-dokumenty-a-datove-zpravy/ [cit. 2023-11-30].

[262] ETSI TS 119 511 V1.1.1 (2019-06) dostupná zde: https://www.etsi.org/deliver/etsi_ts/119500_119599/119511/01.01.01_60/ts_119511v010101p.pdf a ETSI TS 119 512 V1.1.1 (2020-01) dostupná zde: https://www.etsi.org/deliver/etsi_ts/119500_119599/119512/01.01.01_60/ts_119512v010101p.pdf

Poskytovatel úkon provede spolu s požadavkem a výsledek ihned poskytne klientovi jako odpověď.[263]

V době vzniku této práce v České republice existovala pouze jedna služba splňující požadavky nařízení eIDAS na kvalifikovanou službu po uchovávání, a to od společnosti Software602 a.s.[264] Jedná se o třetí model, tedy řešení bez úložiště. Aby byla zachována aktuální digitální kontinuita, je tak vhodné nechat si řešení od společnosti Software602 a.s. zabudovat do úložiště dokumentů, které bude schopno rozpoznat, kdy je nutné učinit další kroky. Peterka jako příklad úložiště uvádí Portál občana. Nemuselo by se ani jednat o službu uchovávání s kvalifikovaným statusem, neboť v případě dodržení potřebných kroků je výsledek stejný. Status kvalifikované služby uchovávání v praxi pouze znamená dopředu provedené ověření o funkčnosti služby.[265]

4.2.8. Elektronická časová razítka

S uchováváním digitální kontinuity úzce souvisejí elektronická časová razítka. Ta jsou definována jako „*data v elektronické podobě, která spojují jiná data v elektronické podobě s určitým okamžikem a prokazují, že tato jiná data existovala v daném okamžiku*“.[266] Funkci zafixování obsahu sice splňují i elektronické podpisy a pečetě, nicméně je u nich obecně problém s určením data a času jejich vytvoření. Tato informace totiž pochází z nastavení počítače či jiného systému, kde je podpis si pečeť vytvořena, a lze ji tak velice jednoduše změnit právě změnou nastaveného času na daném počítači či v daném systému.

Elektronická časová razítka nařízení eIDAS rozlišuje na prostá a na kvalifikovaná.[267] V případě prostých elektronických časových razítek narážíme na stejný problém jako v případě elektronických podpisů a pečetí zmíněný v předchozím odstavci. V případě kvalifikovaných elektronických časových razítek je tomu však jinak. Jednou z jejich náležitostí je totiž požadavek (i) založení na zdroji přesného času, který je spojen s koordinovaným světovým časem. Dalšími (kumulativními) požadavky jsou pak (ii) spojení data a času s daty takovým způsobem, aby byla přiměřeně zamezena možnost nezjistitelné změny dat, a (iii) podepsání s použitím zaručeného elektronického podpisu opatřeného zaručenou elektronickou pečetí kvalifikovaného poskytovatele služeb vytvářejících důvěru nebo označeného jinou

[263] Strana 14 ETSI TS 119 511 V1.1.1 (2019-06) a strana 18-19 ETSI TS 119 512 V1.1.1 (2020-01).
[264] Seznam poskytovatelů služeb vytvářejících důvěru je dostupný zde.
[265] PETERKA, Jiří. *Jak na digitální kontinuitu (4): Jak aktivně pečovat o starší dokumenty a datové zprávy*, op. cit. 261.
[266] Článek 3 odst. 33 nařízení eIDAS.
[267] Srov. článek 41 a 42 nařízení eIDAS.

rovnocennou metodou.[268] Tato kombinace nám pak zaručuje opravdovou digitální stopu, ze které lze ověřit aktuální digitální kontinuitu.

Elektronické podpisy jsou na rozdíl od elektronických časových razítek spojeny s projevem vůle (v případě elektronických pečetí s vyjádřením původu). Z toho důvodu jsou v praxi pro udržování aktuální digitální kontinuity používána právě kvalifikovaná elektronická časová razítka.[269] Při každém připojení elektronického podpisu či elektronické pečeti je tak vhodné připojit i kvalifikované elektronické časové razítko. V případě orgánů veřejné moci tato povinnost vyplývá přímo ze zákona.[270]

Dokumenty s platným řetězcem elektronických časových razítek pak lze ověřit na Czech POINT i u poskytovatelů kvalifikovaných služeb. Problematické jsou však orgány veřejné moci, které nejsou schopny s řetězcem časových razítek pracovat. Ověřují totiž pouze dokument bez samostatných časových razítek, tj. těch, které byly použity k prodloužení aktuální digitální kontinuity.[271] Aktuální digitální kontinuitu pak správně neověřuje ani hojně užívaný program Adobe Acrobat Reader. Ten jednak při ověření podpisu s připojeným časovým razítkem, kterému vypršela platnost certifikátu, potvrdí, že podpis je platný, avšak z jiného důvodu. V jeho základním nastavení je totiž zaškrtnuta možnost „*Použít časová razítka ukončené písemnosti*“. To způsobuje, že program důvěřuje právě i časovým razítkům, kterým vypršela platnost jejich certifikátu. Pro ověření aktuální digitální kontinuity prostřednictvím tohoto programu je tak nutné tuto funkci vypnout. To však neznamená, že program bude správně ověřovat dokumenty s řetězcem časových razítek, kde je technicky aktuální digitální kontinuita zachována. K tomu totiž není program nastaven, a platnost podpisu označuje jako neznámou. To je způsobeno tím, že platnost každého časového razítka program posuzuje separátně, a nikoli v sousledném řetězci.[272] Tento fakt pak v praxi přináší značnou právní nejistotu o zachování aktuální digitální kontinuity a v teoretickém důsledku může vést k degradaci použitého elektronického podpisu, resp. jeho důkazních účinků.

[268] Článek 42 nařízení eIDAS.
[269] PETERKA, Jiří. *Jak na digitální kontinuitu (7): Co (ne)umí Czech POINTy, co elektronické podatelny a co Adobe Reader*. Online. Dostupné z: https://www.lupa.cz/clanky/jak-na-digitalni-kontinuitu-7-co-ne-umi-czechpointy-co-elektronicke-podatelny-a-co-adobe-reader/. [cit. 2023-12-05].
[270] § 11 ZSVD.
[271] PETERKA, Jiří. *Jak na digitální kontinuitu (7): Co (ne)umí Czech POINTy, co elektronické podatelny a co Adobe Reader*, op. cit. 269.
[272] *Ibid.*

4.2.9. Kontejnery

Jako dalším nástrojem k udržování aktuální digitální kontinuity mohou sloužit i tzv. kontejnery, do kterých je možné vložit dokument(y) či jiné objekty, kontejner uzavřít a opatřit elektronickým podpisem či elektronickým časovým razítkem. Standardizovaným druhem kontejnerů, se kterými nařízení eIDAS počítá, je kontejner formátu ASiC.[273] Tato forma je vhodná zejména pro datové formáty bez podpory přidávání elektronických časových razítek, podpisů či pečetí, kterými jsou například emailová zpráva, ke které nelze připojit časové razítko, čistě textové formáty (TXT), obrazové a zvukové záznamy apod.

Dalším příkladem mohou být datové zprávy zaslané prostřednictvím datových schránek. Datové zprávy jsou opařeny časovým razítkem (vstupním při odeslání zprávy a výstupním při jejím stažení), a jejich obsah tedy je fixován v čase. Kontejner, v tomto případě i datová zpráva, se tak chová jako časové razítko, tedy prokazuje, že v daném časovém okamžiku dokument i s tehdy platným elektronickým podpisem, pečetí či časovým razítkem existoval. K ověření je však zapotřebí použít nástroj či službu, jejichž prostřednictvím bude možné ověřit celý kontejner a z něj vybrat předmětný dokument. To je však problematické například u elektronických podatelen soudů, které neumí pracovat s datovými zprávami jako s kontejnery, tj. když jsou samotné datové zprávy přílohou, ale pouze s datovými zprávami jako takovými. Tuto funkci bohužel nenabízí ani jiné v současnosti dostupné služby, včetně Czech POINT či klientského portálu datových schránek.[274]

4.2.10. Stárnutí elektronických dokumentů

Dále je důležité rozebrat, co vlastně stárnutí elektronických dokumentů v praxi znamená a jaké má důsledky. Autenticita a pravost dokumentů je dovozována z elektronických podpisů a pečetí, případně ve spojení s časovými razítky. Je tedy potřeba mít jistotu, že se na elektronické podpisy, pečetě a razítka můžeme spoléhat, tedy že je bude možné ověřit. Právě ověření je však možné pouze po určitou dobu.

Jak již bylo zmíněno výše, zabezpečení vyšších úrovní elektronických podpisů, pečetí a časových razítek je zajištěno prostřednictvím takzvané asymetrické kryptografie, která pracuje se dvěma tajnými klíči (na rozdíl od symetrické, která je založena pouze na klíči jednom), a to na jednom klíči veřejném a na jednom soukromém. Oba klíče spolu souvisejí a jedná se o tzv.

[273] Srov. ETSI EN 319 162-1 V1.1.1 (2016-04) a ETSI EN 319 162-2 V1.1.1 (2016-04).
[274] PETERKA, Jiří. *Jak na digitální kontinuitu (7): Co (ne)umí Czech POINTy, co elektronické podatelny a co Adobe Reader*, op. cit. 269.

párová data. Zatímco soukromý klíč je plně pod kontrolou podepisující osoby, veřejný klíč je přikládán ke každému elektronickému podpisu a je volně dostupný. Je tak zapotřebí zajistit, aby při znalosti klíče veřejného nebylo možné jednoduše vypočítat klíč soukromý. I to je důvodem, proč je po čase nutné přejít na klíče nové, z pohledu počtu bitů větší, nebo jiný způsob spojování obou klíčů (podpisové algoritmy).[275] Pro úplnost je na místě zmínit, že prostý elektronický podpis založen na kryptografii vůbec není, jeho důvěra je tak ve srovnání s podpisy úrovní vyššího typu v tomto ohledu oslabena.

Kryptografická ochrana, stejně jako jakákoli jiná ochrana v oblasti informačních technologií, není však stoprocentní, neboť ji lze vždy prolomit s dostatečným vynaložením prostředků. Otázkou je, jaké množství času a výpočetní kapacity je k jejímu prolomení zapotřebí vynaložit. Pokud jsou tyto prostředky nereálné, např. pokud je množství času potřebné k prolomení v řádu milionů let, lze ochraně důvěřovat. Sama ochrana pak zůstává v čase neměnná, je však relativní vůči technickému vývoji, tedy nárůstu běžně dostupné výpočetní kapacity.[276] Z toho důvodu jsou certifikáty platné pouze po určitou dobu, po kterou si můžeme být jisti, že k prolomení s největší pravděpodobností nedojde. Pokud chceme udržovat aktuální digitální kontinuitu, je zapotřebí na konci doby platnosti certifikátu připojit nový prostředek, např. elektronické časové razítko, s novým certifikátem a s posílenou ochranou. V praxi tak dojde k novému, ještě silnějšímu zašifrování a tím související ochraně a důvěře v pravost a autenticitu dokumentu.

V případě elektronických podpisů, pečetí a časových razítek však nedochází k zašifrování dokumentu jako takového, ale k zašifrování vazby mezi těmito prostředky a daným dokumentem. Dojde tedy k zajištění nemožnosti změny obsahu dokumentu, ke kterému je prostředek připojen, a to včetně zkopírování a přenesení prostředku z jednoho elektronického dokumentu na druhý, či zamezení situaci, kdy bude vazba prostředku odpovídat dvěma a více dokumentům.[277]

4.2.10.1. Vznik elektronického podpisu a hashování dokumentů

Proces vzniku elektronického podpisu vyšší úrovně si lze představit jako spojení podepisovaného obsahu (dat v elektronické podobě – pro zjednodušení bude autor této práce

[275] PETERKA, Jiří. *Jak na digitální kontinuitu (9): Co jsou certifikáty a proč je musíme pravidelně obměňovat?* Online. Dostupné z: https://www.lupa.cz/clanky/jak-na-digitalni-kontinuitu-9-co-jsou-certifikaty-a-proc-je-musime-pravidelne-obmenovat/. [cit. 2023-12-10].
[276] PETERKA, Jiří. *Jak na digitální kontinuitu (8): Proč kryptografické algoritmy oslabují a elektronické dokumenty stárnou?* Online. Dostupné z: https://www.lupa.cz/clanky/jak-na-digitalni-kontinuitu-8-proc-kryptograficke-algoritmy-oslabuji-a-elektronicke-dokumenty-starnou/. [cit. 2023-12-09].
[277] *Ibid.*

hovořit o dokumentu, respektive jejich otisku, jak bude rozebráno v této kapitole níže), veřejného a soukromého klíče. Soukromý klíč, jak sám název napovídá, je specifický a unikátní pro konkrétní osobu vytvářející elektronický podpis. Ta jej má pod plnou kontrolou a rozhoduje o jeho použití, je tedy důkazem o existenci spojení osoby s konkrétním podpisem. Ne u všech dokumentů však bude výsledný elektronický podpis stejný. Dokument totiž musí v době připojení elektronického podpisu splňovat řadu požadavků, kdy jedním z nich je i jeho velikost. Z uživatelského hlediska je však toto omezení samozřejmě nepřívětivé, neboť uživatelé z pochopitelného důvodu chtějí mít možnost podepsat jakékoli dokumenty. Z toho důvodu je při elektronickém podepisování z podepisovaného elektronického dokumentu vytvořen jeho otisk, v angličtině *hash*. Ten vzniká při aplikaci tzv. hashovací (či počeštěle hašovací) funkce, kterou si lze představit jako konverzi datově velkého souboru do souboru menšího, s čímž je logicky spojena i ztráta určitých dat. Právě v tomto okamžiku nastává situace, kdy elektronický podpis může být ověřen jako platný i na dokumentu jiném, který je po procesu hashování výpočetně stejný. Proces hashování lze provést pouze jedním směrem, tedy vytvořením menšího dokumentu z dokumentu většího, nikoli naopak. S tím souvisí výše zmíněná důvěra v to, že nalezení vzájemně kolizních dokumentů musí být výpočetně velice náročné. Jinými slovy, pravděpodobnost nalezení kolizních dokumentů existuje, avšak je téměř zanedbatelná.[278]

I hashovací funkce, stejně jako elektronické podpisy, pečetě a časová razítka, však časem relativně oslabují, a proto se i tyto funkce v čase vyvíjí, respektive jejich řešení se více zabezpečuje. Existuje tak více hashovacích funkcí, které se liší velikostí jimi produkovaných hashů. K přechodu naposledy vyzval Národní bezpečnostní úřad v roce 2009, kdy doporučil nepoužívat hashovací funkce s výstupem menším než 160 bitů a doporučil neprodlený přechod od hashovací funkce SHA-1 na novou generaci SHA-2.[279] Tato nová generace obsahuje více funkcí založených na otiscích o velikostech 256 bitů, 384 bitů a 512 bitů. Důrazné doporučení vydalo ve stejné době i Ministerstvo vnitra. To však neznamená, že na funkci SHA-1 i v dnešní době nelze narazit. Většina služeb používaných v České republice pro ověřování elektronických dokumentů a podpisů tento formát plně podporují.[280] Z praktického hlediska

[278] *Ibid.*
[279] NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD. *Prohlášení NBÚ k využívání hashovacích funkcí*. Online. Dostupné z: https://web.archive.org/web/20090226093652/http:/www.nbu.cz/cs/ochrana-utajovanych-informaci/kryptograficka-ochrana/informace/. [cit. 2023-12-10].
[280] PETERKA, Jiří. *Jak na digitální kontinuitu (8): Proč kryptografické algoritmy oslabují a elektronické dokumenty stárnou?* Online. Dostupné z: https://www.lupa.cz/clanky/jak-na-digitalni-kontinuitu-8-proc-kryptograficke-algoritmy-oslabuji-a-elektronicke-dokumenty-starnou/. [cit. 2023-12-09].

však její použití doporučit nelze, a to právě z důvodu nižší míry důvěry či z důvodu nemožnosti ověření platnosti prostřednictvím služeb, které tento formát nepodporují. Naopak, americký Národní institut standardů a technologie již před pár lety určil jako nástupce funkci SHA-3.[281]

4.2.10.2. Certifikáty

Z certifikátu připojeného k elektronickému podpisu či pečeti zpravidla dovozujeme, kdo je jeho držitelem, jehož lze považovat za osobu, která příslušný prostředek k dokumentu připojila. To vyplývá i z definic nařízení eIDAS, dle kterých jde o spojení dat pro ověřování platnosti elektronických podpisů či pečetí s určitou osobou.[282]

Certifikáty jsou dvojího druhu, kvalifikované a nekvalifikované (komerční). Kvalifikované certifikáty pak v případě elektronických podpisů[283] i pečetí[284] musí splňovat jasné požadavky stanovené v přílohách nařízení eIDAS. V případě kvalifikovaných certifikátů za správnost jejich obsahu odpovídá jejich vydavatel, který v případě porušení svých povinností čelí vysokým sankcím. Na tomto základě je pak možné na certifikát spoléhat. To však nutně neplatí v případě certifikátů jiných než kvalifikovaných. Jejich obsah totiž může vytvořit kdokoli, a data v něm obsažená nemusí odpovídat skutečnosti,[285] tedy například u certifikátů zaručených elektronických podpisů.

Certifikáty neobsahují samotné soukromé klíče, na jejichž základě je identifikována podepisující osoba, jak bylo rozepsáno výše, neboť by tím byla narušena jejich důvěrnost. Naopak, certifikáty obsahují odpovídající veřejný klíč, který je s klíčem soukromým spojený (párová data). Z certifikátu lze tak vyčíst, že držitelem soukromého klíče, který je spárovaný s tímto veřejným klíčem, je osoba vytvářející elektronický podpis či pečeť. Je však z pohledu zabezpečení nutné, aby se z veřejného klíče nedal vypočítat klíč soukromý. Jejich spojení (párová data) by se tak nemělo používat po uplynutí příliš dlouhé doby, po které dojde k jejich relativnímu bezpečnostnímu oslabení.[286]

Doba platnosti certifikátu není legislativně upravena, určují ji certifikační autority na základě vývoje výpočetní techniky a účelu, ke kterému má certifikát sloužit. Certifikáty různých druhů

[281] Informace zveřejněna zde: https://csrc.nist.gov/projects/hash-functions/sha-3-project.
[282] Článek 3 odst. 14 a odst. 29 nařízení eIDAS.
[283] Článek 28 a násl. a příloha I nařízení eIDAS.
[284] Článek 38 a násl. a příloha III nařízení eIDAS.
[285] PETERKA, Jiří. *Jak na digitální kontinuitu (9): Co jsou certifikáty a proč je musíme pravidelně obměňovat?*, op. cit. 275.
[286] *Ibid.*

tak mohou mít rozdílnou dobu platnosti. Kvalifikované certifikáty pro elektronické podpisy mají dobu platnosti zpravidla 1 rok (v některých případech ale i 3 roky), v případě certifikátů časových razítek může být ale platnost i 5 let.[287] Po uplynutí doby platnosti certifikátu dochází k vydání tzv. následného certifikátu.[288] Tím dojde k vydání nového certifikátu a s tím spojenému vygenerováním nových párových dat, tedy nového soukromého a veřejného klíče. S tím je samozřejmě spojena změna velikosti klíčů, ale i případná změna algoritmu jejich generování a algoritmu podpisu.[289] Nejde tedy o obnovení certifikátu stávajícího, jak bývá občas chybně označováno.[290] Pro úplnost je vhodné dodat, že hashovací funkce je závislá na nastavení programu, nikoli na daném certifikátu.

Certifikát je možno předčasně revokovat, tj. ukončit jeho dobu platnosti dříve, než bylo původně nastaveno. Lze tak učinit například v případě kompromitace či ztráty soukromého klíče, kdy není technicky možné zneplatnit samotný soukromý klíč, ale právě jeho certifikát, jak bylo popsáno výše. V praxi jsou tak elektronické podpisy, pečetě či časová razítka vytvořená po revokaci certifikátu, na kterém jsou založena, ověřovány jako neplatné.[291] Revokace certifikátu však nemá vliv na elektronické podpisy vytvořené během platnosti certifikátu. Jiné nastavení by ani logicky nedávalo smysl. U elektronických dokumentů, které jsou navíc kromě elektronického podpisu opatřeny i kvalifikovaným časovým razítkem, je situace jednodušší. Jak bylo popsáno výše v kapitole 4.2.8, kvalifikované elektronické časové razítko je důkazem o tom, že elektronický podpis vznikl v konkrétním jasně určeném čase. Pokud tedy elektronický podpis vznikl před vypršením platnosti certifikátu, měl by být ověřen jako platný. Naopak, pokud je jasné, že elektronický podpis vznikl až po revokaci certifikátu, musí být ověřen jako neplatný. V ostatních případech, kdy nelze spolehlivě prokázat, zda elektronický podpis vznikl před revokací daného certifikátu, musí být platnost podpisu označena jako neznámá.[292]

[287] ČESKÁ POŠTA. *Časová razítka*. Online. Dostupné z: https://www.ceskaposta.cz/sluzby/certifikacni-autorita-postsignum/casova-razitka. [cit. 2023-12-13].
[288] I. CERTIFIKAČNÍ AUTORITA. *Následný certifikát*. Online. Dostupné z: https://www.ica.cz/Nasledny-certifikat. [cit. 2023-12-13].
[289] PETERKA, Jiří. *Jak na digitální kontinuitu (9): Co jsou certifikáty a proč je musíme pravidelně obměňovat?*, op. cit. 275.
[290] POSTSIGNUM. *Obnova certifikátů PostSignum*. Online. Dostupné z: https://www.postsignum.cz/obnova_certifikatu.html. [cit. 2023-12-13].
[291] PETERKA, Jiří. *Jak na digitální kontinuitu (10): Co je revokace certifikátu a jak komplikuje digitální kontinuitu*. Online. Dostupné z: https://www.lupa.cz/clanky/jak-na-digitalni-kontinuitu-10-co-je-revokace-certifikatu-a-jak-komplikuje-digitalni-kontinuitu/. [cit. 2023-12-14].
[292] *Ibid.*

Platnost certifikátů, resp. jejich revokaci, je tak zapotřebí vždy aktivně ověřit. To platí i pro všechny certifikáty danému certifikátu nadřazené. Poté, co je ověřeno, že nedošlo u elektronického podpisu, pečeti či časového razítka k žádné změně, a nebyla tedy narušena autenticita dokumentu, je zapotřebí ověřit řádnou dobu platnosti certifikátů a aktivně přezkoumat jejich revokaci. Při ověření platnosti podpisu pak musí být provedeny všechny zmíněné kroky. Pokud se tak nestane, nelze elektronický podpis prohlásit za platný. Zejména při získávání informací o platnosti revokace certifikátu, resp. jeho revokaci, pak v praxi nastávají nejčastější komplikace. Ty mohou spočívat buď v zastaralosti informací nebo v jejich nedostatečné aktualitě, tj. informace pochází z doby až po vzniku elektronického podpisu.[293] Informace o revokaci certifikátů vytvářejí vydavatelé certifikátu (certifikační autority) a ti mají ze zákona povinnost tyto informace uchovávat po dobu 10 let.[294] Dalším a aktuálnějším problémem je však samotný přístup k informacím. Automatizované nástroje jsou totiž naprogramovány tak, aby v samotném certifikátu našly, kde mají informaci o revokaci hledat. Nicméně informace o revokaci je zpravidla tímto způsobem dostupná pouze po dobu platnosti certifikátu, neboť po skončení jeho platnosti se nelze spoléhat na informace v něm obsažené, včetně té, kde informace o revokaci najít. Vydavatel certifikátu totiž může informaci umístit na jiné místo. Tuto skutečnost automatizovaný systém nedokáže rozpoznat, pokud není nové místo uvedeno přímo v certifikátu. Ověření by však v důležitých případech nemělo být problematické pro příslušného znalce, který informaci o revokaci může dohledat i na tomto jiném místě. Z praktického hlediska však tento postup není vhodným řešením pro každodenní využití. Tyto aspekty jsou z praktického pohledu digitální kontinuity relativně velký problém. Jeho částečným řešením je v současné době buď shromažďování informací o revokaci certifikátů buď osobami vytvářejícími elektronický podpis, pečeť či razítko, nebo osobami, které elektronické dokumenty přijímají. Typicky takto postupuje služba Czech POINT či podatelny soudů.[295] Nejedná se však o systémové řešení, na které se lze spolehnout bez dalšího. Problém by se však podle autora této práce dal vyřešit například stanovením standardizovaných pravidel pro danou problematiku, která by následně bylo možné zahrnout do automatizovaných řešení. Je však otázkou, jaké by vydavatelům certifikátů v souvislosti s tímto řešením vznikly náklady a zda by praktický přínos právě ve vztahu k nákladům byl efektivní.

[293] *Ibid.*
[294] §3 ZSVD
[295] PETERKA, Jiří. *Jak na digitální kontinuitu (10): Co je revokace certifikátu a jak komplikuje digitální kontinuitu*. Online, op. cit. 291.

4.2.10.3. Důkaz o existenci elektronického podpisu v čase

Oproti vlastnoručním podpisům, u kterých je jejich posuzování nezávislé na čase, je čas u elektronických podpisů, pečetí a časových razítek z výše uvedených důvodů zásadní. Při ověření času je zapotřebí jak jeho přesnost, tak spolehlivost této informace, tedy fakt, že se na daný údaj můžeme spolehnout. Dle Peterky[296] je pro volbu rozhodného okamžiku logické vycházet z údaje o čase, který se nevztahuje k vytvoření elektronického podpisu, pečetě či razítka, ale z údaje o čase získaného z něčeho, co dokazuje, kdy podpis již existoval. Jedná se tedy o důkaz o existenci (v čase), anglicky *proof of existence*.[297] S tím ale logicky musí být zafixován i obsah dokumentu, aby bylo možné detekovat jakékoli případné změny. Jak již bylo zmíněno v kapitole 4.2.8, nejlepším prostředkem pro tento účel je kvalifikované elektronické časové razítko, a to jak přímo u elektronického podpisu či pečeti, tak na dokumentu, případně na kontejneru či datové zprávě.

Jako důkaz o existenci v čase však mohou sloužit i jiné skutečnosti, například záznam podatelny o dodání dokumentu, záznam v transakčním protokolu, či jiná spolehlivá digitální stopa. Technická specifikace pro ověřování elektronických podpisů proto specifikuje základní principy pro ověřování jejich platnosti, nicméně současně umožňuje, aby příslušné nástroje a služby používaly vlastní nastavení a kritéria pro hodnocení, co je ještě přípustné, a co již nikoli.[298] To však v praxi vede k tomu, že různé nástroje či služby vyhodnocují stejné dokumenty, respektive příslušné elektronické podpisy, pečetě či časová razítka, odlišně. Je proto vhodné vědět, jak daný nástroj či služba funguje či jak je nastavená. V případě kvalifikovaných služeb pro ověřování platnosti by měla být vydávána tzv. validační politika. Jako příklad lze uvést politiku Národní certifikační autority,[299] či validační algoritmus služby DSS.[300] Problematické jsou však nástroje a služby jiné než kvalifikované. Ty totiž nemají

[296] PETERKA, Jiří. *Jak na digitální kontinuitu (11): K jakému časovému okamžiku se mají ověřovat elektronické podpisy?* Online. Dostupné z: https://www.lupa.cz/clanky/jak-na-digitalni-kontinuitu-11-k-jakemu-casovemu-okamziku-se-maji-overovat-elektronicke-podpisy/. [cit. 2023-12-15].
[297] ETSI TS 102 853 V1.2.1 (2014-12), s. 33, 9.1. dostupné zde: https://www.etsi.org/deliver/etsi_ts/102800_102899/102853/01.02.01_60/ts_102853v010201p.pdf.
[298] ETSI TS 102 853 V1.2.1 (2014-12), s. 28 s násl. 5, dostupné zde https://www.etsi.org/deliver/etsi_ts/102800_102899/102853/01.02.01_60/ts_102853v010201p.pdf.
[299] SPRÁVA ZÁKLADNÍCH REGISTRŮ. *NCA – Politika ověřování podpisu NCA QVerify v 1.0.1*. Online. Dostupné z: https://www.narodni-ca.cz/Dokumenty/NCA_Politika_kvalif_sluzby_overovani_platnosti_QVerify_1v01.pdf. [cit. 2023-12-18].
[300] EUROPEAN COMMISSION. *CEF eSignature DSS, Version 1.03, Qualified electronic signature (QES) validation algorithm*. Online. Dostupné z: https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/Qualified+electronic+signature+-+QES+validation+algorithm?preview=/467109151/467109153/Qualification%20algorithm.pdf. [cit. 2023-12-18].

povinnost popisovat způsob fungování, a pokud tak učiní, rozsah a způsob není jakkoli regulován. Příkladem může být popis od společnosti Adobe.[301]

Nařízení eIDAS používá ve vztahu k času podpisu pouze termín „*okamžik podpisu*“ bez dalšího.[302] Technická specifikace ETSI pak tvrzený čas podpisu označuje jako „*čas tvrzený podepisující osobou, který sám o sobě neposkytuje nezávislý důkaz skutečného času podpisu*“.[303] Při popisu postupu ověřování podpisů s časovým údajem technická specifikace pracuje s termínem nejlepšího okamžiku podpisu, tedy nejdřívějšího okamžiku, kdy se algoritmus ověřování může spolehnout na existenci podpisu. Děje se tak jak na základě důkazu o existenci v čase či v situaci, kdy tento okamžik vyplývá z validační politiky, nebo byl určený správcem či uživatelem[304] (například okamžik, kdy byl dokument doručen orgánu veřejné moci). Výše zmíněný validační algoritmus služby DSS k dané problematice přistupuje totožně.[305] Pokud tedy při připojení elektronického podpisu k dokumentu dojde k pozměnění času operačního systému a zároveň k připojení kvalifikovaného elektronického časového razítka, budou se tyto časové údaje lišit. Služba DSS však čas ověří právě podle certifikátu připojeného ke kvalifikovaného elektronickému časovému razítku, neboť jde o důkaz o existenci v čase a jde o nejlepší okamžik podpisu. Nicméně službu DSS, stejně jaké jiné validační procesy, lze nastavit i jinak, tedy aby ignorovaly důkazy o existenci v čase, a vycházely pouze z aktuálního času.[306]

Obecně lze říci, že ověřování k pozdějšímu časovému okamžiku není problematické. Logicky platí, že pokud lze ověřit podpis jako platný později, musely být splněny všechny podmínky i k časovému okamžiku předchozímu. Podle příslušné technické specifikace totiž podpisy nemohou vzniknout před platností certifikátu, tj. není možné vydávat certifikáty před začátkem jejich řádné doby platnosti.[307] V situaci, kdy se nemůžeme spoléhat na čas vzniku podpisu,

---

[301] ADOBE. *Ověření digitálních podpisů*. Online. Dostupné z: https://helpx.adobe.com/cz/acrobat/using/validating-digital-signatures.html. [cit. 2023-12-18].
[302] Článek 32 odst. 1 písm. h) nařízení eIDAS.
[303] ETSI EN 319 102-1 V1.3.1 (2021-11), s. 11, dostupné z: https://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.03.01_60/en_31910201v010301p.pdf ,
[304] *Ibid*, s. 59, 5.5.4.
[305] EUROPEAN COMMISSION. *CEF eSignature DSS, Version 1.03, Qualified electronic signature (QES) validation algorithm*. Online. Dostupné z: https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/Qualified+electronic+signature+-+QES+validation+algorithm?preview=/467109151/467109153/Qualification%20algorithm.pdf. [cit. 2023-12-18], s. 4.
[306] PETERKA, Jiří. *Jak na digitální kontinuitu (11): K jakému časovému okamžiku se mají ověřovat elektronické podpisy?*, op. cit. 296.
[307] ETSI TS 119 172-4 V1.1.1 (2021-05), dostupný z: https://www.etsi.org/deliver/etsi_ts/119100_119199/11917204/01.01.01_60/ts_11917204v010101p.pdf

nebo jej neznáme, dává smysl podpis ověřovat až k okamžiku pozdějšímu, kdy si budeme jisti tím, že podpis již existoval. V tomto případě se však může stát, že řádná doba platnosti certifikátu skončí, nebo nastala jeho revokace.

Program Adobe Acrobat Reader umožňuje nastavení času ověření s použitím (i) času vytvoření podpisu, (ii) do podpisu vložených zabezpečených časových razítek, nebo (iii) aktuálního času. Oproti službě DSS je zde první možnost, tedy deklarovaný čas podpisu. Pokud však dokument detekuje důkaz o existenci v čase, bude vycházet z času uvedeného v něm.

I čas ověření je tak klíčový pro posouzení autenticity a pravosti. Jak již bylo zmíněno výše v kapitole 4.2.2, i pokud se ověření z důvodu přerušení aktuální digitální kontinuity nepodaří, je zde stále možnost potenciální digitální kontinuity, která může vést k ověření autenticity i pravosti, avšak komplikovanější cestou.[308]

4.2.11. Jaké dokumenty lze elektronicky podepsat a jakými formáty podpisů

Jak již bylo popsáno v kapitole 4.2.10.1, elektronické podpisy, pečetě a časová razítka lze připojit k jakémukoli otisku dokumentu (*hashi*). Nejde však podepsat datový proud či jakákoli jiná data, která se v čase mění, např. audiovizuální přenos. V tomto případě je zapotřebí počkat na jejich finální podobu, a podepsat až výsledný celek dat. Ne všechna data se ovšem podepisují stejně. Existuje několik formátů elektronických podpisů, které se odvíjejí od formátu podepisovaného dokumentu, a několik způsobů zapouzdření, tedy jakým způsobem jsou elektronické podpisy s dokumentem spojeny.

Formáty elektronických podpisů jsou čtyři. Prvním formátem je XAdES (*XML Advanced Electronic Signature*), který slouží jako elektronický podpis pro dokumenty ve formátu XML.[309] Druhým formátem je PAdES (*PDF Advanced Electronic Signature*), kterým lze podepisovat dokumenty ve formátu PDF.[310] Třetím formátem je CAdES (*CMS Advanced Electronic Signature*),[311] jehož výhodou je, že s ním lze podepsat dokumenty v jakémkoli

[308] PETERKA, Jiří. *Jak na digitální kontinuitu (11): K jakému časovému okamžiku se mají ověřovat elektronické podpisy?*, op. cit. 296.
[309] ETSI EN 319 132-1 V1.2.1 (2022-02), s. 8, dostupný z: https://www.etsi.org/deliver/etsi_en/319100_319199/31913201/01.02.01_60/en_31913201v010201p.pdf
[310] ETSI EN 319 142-1 V1.1.1 (2016-04), s. 6, dostupný z: https://www.etsi.org/deliver/etsi_en/319100_319199/31914201/01.01.01_60/en_31914201v010101p.pdf ,
[311] ETSI EN 319 122-1 V1.2.1 (2021-10), s. 8, dostupný z: https://www.etsi.org/deliver/etsi_en/319100_319199/31912201/01.02.01_60/en_31912201v010201p.pdf

formátu, resp. jakákoli binární data. Posledním formátem je JAdES (*JSON Advanced Electronic Signatures*),[312] určený zejména pro elektronické transakce.

Elektronické podpisy pak mohou v závislosti na formátech být ve vztahu k dokumentu buď odpojené (*detached*), obalující (*enveloping*) nebo zabalené (*enveloped*). Odpojené elektronické podpisy představují samostatný objekt vůči dokumentu, ke kterému se vztahují. Pro odpojený elektronický popis je možné použít formáty XAdES a CAdES (v tomto formátu jsou i odpojené podpisy k dokumentům ve formátu PDF). V případě obalujícího elektronického podpisu je to, co je podepisováno, vnořeno do podpisu samotného. Pro použití obalujícího elektronického podpisu pak připadají v úvahu formáty XAdES a CAdES. Naopak v případě zabalených elektronických podpisů je podpis vnořen do podepisovaného dokumentu. K tomu lze použít formáty PAdES a XAdES.[313]

Odpojené elektronické podpisy jsou problematické, neboť netvoří s podepisovaným dokumentem jeden celek. Elektronický podpis a dokument tak lze teoreticky oddělit. Dalším problémem je vzájemná logická vazba. Odpojené elektronické podpisy totiž existují vedle sebe a mohou být vytvářeny nezávisle na sobě. Může tak nastat nejistota v jejich pořadí a počtu. Nařízení eIDAS právě pro tento případ počítá s řešením ve formě ASiC kontejnerů.[314] Ty umožňují zahrnout více souborů a odpojených elektronických podpisů ve formátech XAdES či CAdES do jednoho souboru (ZIP) a současně popsat vztah jednotlivých elektronických podpisů a dokumentů. Jak již bylo zmíněno výše v textu této práce, praktické použití je bohužel v České republice problematické. ASiC kontejnery totiž nejsou vedeny jako výstupní datové formáty ve vyhlášce o podrobnostech výkonu spisové služby,[315] nelze je přenášet prostřednictvím datových schránek, a neporadí si s nimi ani spisové služby a elektronické podatelny.[316]

Úrovně podpisů

[312] ETSI TS 119 182-1 V1.1.1 (2021-03), s. 5, dostupný z: https://www.etsi.org/deliver/etsi_ts/119100_119199/11918201/01.01.01_60/ts_11918201v010101p.pdf
[313] PETERKA, Jiří. *Jak na digitální kontinuitu (12): Proč mají elektronické podpisy různé profily, formáty a úrovně?* Online. Dostupné z: https://www.lupa.cz/clanky/jak-na-digitalni-kontinuitu-12-proc-maji-elektronicke-podpisy-ruzne-profily-formaty-a-urovne/. [cit. 2023-12-20].
[314] ETSI EN 319 142-1 V1.1.1 (2016-04).
[315] § 23 vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby.
[316] PETERKA, Jiří. *Jak na digitální kontinuitu (12): Proč mají elektronické podpisy různé profily, formáty a úrovně?*, op. cit. 313.

U všech výše uvedených podpisových formátů, tedy XAdES, PAdES, CAdES, JAdES a stejně tak i u ASiC kontejnerů, existuje více úrovní podpisů a pečetí. Ty se liší podle toho, co vše je k elektronickému podpisu či pečeti přidáno. První úrovní je B-B (*Basic Signature*), která je tvořena pouze elektronickým podpisem či pečetí. Ty mohou být ověřeny, pouze pokud je podpisový certifikát platný (není revokován nebo nevypršela jeho platnost).[317] Druhou úrovní je B-T (*Signature with Time*) a jedná se o podpis úrovně B-B doplněný o podpisové či dokumentové časové razítko. Tento podpis tedy dokazuje, že podpis v daném okamžiku existoval.[318] Třetí úrovní je B-LT (*Signature with Long-Term Validation Material*). V tomto případě se jedná o podpis úrovně B-T doplněný o validační informace (úplná data o certifikátu a jeho revokaci) pro pozdější ověření podpisu a časového razítka. Tento podpis zajišťuje dlouhodobou dostupnost validačních informací tím, že zahrnuje všechna data nebo odkazy na data potřebné pro ověření podpisu.[319] Poslední úrovní je LTA (*Signature providing Long Term Availability and Integrity of Validation Material*). Jedná se o úroveň podpisu B-LT doplněnou o dokumentové časové razítko či časová razítka, jež fixují validační informace a vytváří důkaz, že tyto informace existovaly v uvedeném čase. Tato úroveň umožňuje dlouhodobou dostupnost a integritu validačních informací a pokud jsou zavedena vhodná opatření (např. periodická obnova časových razítek), podpis na této úrovni může být stále validován i dlouho poté, co již nebudou kryptografické algoritmy použité pro jeho vytvoření považovány za dostatečně bezpečné, nebo jednodušeji po vypršení platnosti validačních informací.[320]

Všechny tyto úrovně odpovídají referenčním formátům dle prováděcího rozhodnutí Evropské komise.[321] Na tomto místě je však vhodné podotknout, že existují i starší formáty založené na jiných než ETSI standardech. Například aplikace Adobe Acrobat Reader je na tyto starší referenční formáty přednastavena. Je tedy vhodné v nastavení aplikace namísto výchozího formátu podepisování „PKCS#7 – Odpojeno“ vybrat „Ekvivalent rozšíření CAdES“.

Úrovně lze v průběhu existence dokumentu měnit. Z úrovně B-B lze přidat elektronické časové razítko a povýšit elektronický podpis či pečeť na úroveň B-T nebo při přidání elektronického časového razítka zahrnout i validační informace a povýšit elektronický podpis či pečeť na

[317] ETSI EN 319 102-1 V1.3.1 (2021-11), článek 4.3.2.
[318] *Ibid*, článek 4.3.3.
[319] *Ibid*, článek 4.3.4.
[320] *Ibid*, článek 4.3.5.
[321] 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 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu.

úroveň B-LT. Zvýšení úrovně je však vždy nutné učinit, dokud jsou validační informace standardním způsobem dostupné, tedy před koncem platnosti certifikátu, na kterém jsou elektronický podpis či pečeť založeny. Pokud by se tak mělo stát po konci jeho platnosti, ověření validačních informací již nemusí být k dispozici či věrohodné. To samé platí pro zvýšení úrovně na LTA. Tento proces lze opakovat po dobu, po kterou je zapotřebí udržovat aktuální digitální kontinuitu podepsaného dokumentu.[322]

4.2.12. Dílčí závěr

Aktuální a potenciální digitální kontinuita je v praxi ve většině případů zanedbávána. Většina orgánů veřejné moci anebo soukromých subjektů se často spoléhá na pouhý automatizovaný výstup určitých programů či systému ověřujícího platnost elektronických podpisů, pečetí či razítek bez dalšího. Jak však bylo v této kapitole rozebráno, tato ověření nemusí být vždy přesná. Jinými slovy, jako platně podepsaný a aktuálně digitálně kontinuální může být shledán dokument, který tak shledán být nemá, a naopak. To v praxi může vést k vážným následkům, kdy určitá právní jednání mohou být některými autory a soudy, analogicky stejně jako u prostých elektronických podpisů (byť chybně), shledávána jako neplatná.

Pro ověření elektronických dat je klíčová jejich integrita a autenticita. Zatímco autenticitou rozumíme integritu dokumentu, tedy jeho nezměněnou podobu, pravost spočívá v původu dokumentu od osoby, která jím projevuje svou vůli. Udržování digitální kontinuity pak v praxi naráží na mnoho praktických úskalí rozebraných v kapitole 4.2.3. Řešením by mohla být služba úschovy elektronický notář, která by fungovala jako notářská úschova listinných dokumentů, avšak v elektronické podobě. S podobnou službou počítá revize nařízení eIDAS.[323]

V rámci práce byla také popsána možnost ověřování elektronických podpisů a jeho praktické aspekty. Právě kvůli těm není v praxi tolik využívána, nicméně to by se mělo v dohledné době novelou vyhlášky a následné podpory kontejnerů ASiC datovými schránkami změnit.

České právo operuje s vyvratitelnou domněnkou spolehlivosti záznamu, jejíž náležitosti analogicky odpovídají požadavkům na autenticitu dokumentu. Pro účely práce s elektronickými dokumenty a udržování digitální kontinuity je pak zapotřebí rozlišovat mezi

[322] PETERKA, Jiří. *Jak na digitální kontinuitu (13): Pomáháme si vlastními silami*. Online. Dostupné z: https://www.lupa.cz/clanky/jak-na-digitalni-kontinuitu-13-pomahame-si-vlastnimi-silami/. [cit. 2023-12-21].
[323] Článek 45g návrhu revize nařízení eIDAS.

archivací, jejíž úprava směřuje na elektronické dokumenty jako celek, a uchováváním, které směřuje právě na zajištění digitální kontinuity.

Ideálním řešením zajištění uchovávání či archivace by byla bezplatná automatická služba, která by automaticky připojovala jak časová razítka, tak uchovávala potřebné validační informace. Služba by například mohla být pro fyzické osoby zabudována v Portálu občana a v případě právnických osob a orgánů veřejné moci v jejich spisových službách a úložištích elektronických dokumentů. To by zajisté přineslo větší právní jistotu a správnou péči o elektronické dokumenty, resp. dodržování digitální kontinuity. S tím souvisí i očekávaný růst užívání vyšších úrovní podpisů, který s největší pravděpodobností bude taktéž důsledkem revize nařízení eIDAS, k tomu více v kapitole 6.1. Vzhledem k nákladům a společenské poptávce je tato možnost spíše teoretická, avšak dle autora této práce vhodná. Archivace však s největší pravděpodobností bude i nadále poskytována soukromými subjekty, a to i s ohledem na plánovanou revizi nařízení eIDAS, které počítá se zřízením poskytování kvalifikovaných služeb v oblasti elektronické archivace či prostřednictvím placené služby datových schránek.

S problematikou digitální kontinuity při použití vyšších úrovní elektronických podpisů úzce souvisí elektronická časová razítka. Ta v kvalifikované formě umožnují objektivně ověřit čas připojení podpisu a při správném opětovném připojení udržování řetězce aktuální digitální kontinuity. Jak bylo rozebráno výše, právě toto ověření však nemusí vždy být dle automatizovaných programů správné. Opět tedy nastává situace, kdy tyto aspekty nejsou brány dostatečně v potaz, a může v praxi docházet jak ze strany soudů či jiných orgánů veřejné moci, ale i soukromoprávních subjektů k nesprávným závěrům, a to teoreticky i o platnosti právního jednání jako v případě prostého elektronického podpisu (byť nesprávně). Naopak kontejnery či datové zprávy nejsou pro udržování digitální kontinuity v současném prostředí vhodné.

Pro vytvoření vyšší úrovně elektronických podpisů je nutné spojení tzv. soukromého a veřejného klíče (tím je zajištěna asymetrická kryptografie). Klíče jsou pak připojeny k otisku podepisovaných dat v elektronické podobě. Vytvoření otisku také podléhá technickým požadavkům, které se v čase vyvíjí. I těm je tak při ověření platnosti konkrétního dokumentu třeba věnovat pozornost.

Dalším relevantním aspektem je platnost certifikátů, kterou je zapotřebí vždy aktivně ověřit, a to včetně případné revokace. To platí i pro všechny certifikáty danému certifikátu nadřazené. V praxi by tak tento krok měl následovat po ověření, že nedošlo u elektronického podpisu,

pečeti či časového razítka k žádné změně, a nebyla tedy narušena autenticita dokumentu. Pokud se tak nestane, nelze elektronický podpis vyšší úrovně prohlásit za platný. V praxi lze mít opět pochyby, že je tento krok jednotlivými subjekty činěn.

Dalším relevantním aspektem je časový okamžik, ke kterému došlo k připojení elektronického podpisu, pečetě či razítka, tzv. důkaz o existenci v čase. Jak bylo rozebráno výše, časové údaje se mohou v elektronickém podpisu a připojeném časovém razítku lišit v závislosti na nastavení ověřovacího programu či systému. I této skutečnosti je tak v praxi zapotřebí věnovat pozornost a nejlépe vycházet z časového údaje v kvalifikovaném elektronickém časovém razítku. Posledním relevantním aspektem jsou pak rozdílné formáty a úrovně elektronických podpisů.

Z výše uvedeného tak vyplývají výhody vyšších úrovní elektronických podpisů oproti prostému elektronickému podpisu. Ty však vždy musí být zkoumány do detailu, aby platily jejich vyšší účinky ve srovnání s prostým elektronickým podpisem. Autor této práce má nicméně za to, že je povědomí o těchto aspektech nízké, a většina orgánů či subjektů argumentuje pouze vyšší formou elektronických podpisů bez jejich detailní znalosti a praktických důsledků.

4.3. Elektronické smlouvy

Elektronické podpisy jsou ruku v ruce spojeny také se způsobem kontraktace. Účelem této práce není jednotlivé typy online smluv či způsob kontraktace podrobně rozebírat, pro řešenou problematiku je však nutné téma alespoň základně nastínit. Na tomto místě je vhodné znovu zdůraznit, že je zapotřebí rozlišovat mezi nahrazením podpisu mechanickým prostředkem a uzavřením smlouvy konkludentně, kdy je obsah smluvních závazků písemnou formou pouze konkretizován.[324]

4.3.1. *Click-wrap* smlouvy

Prvním a zároveň nejčastějším typem on-line smluv jsou tzv. *click-wrap* smlouvy. Ty fungují na principu, kdy uživatel musí vyjádřit souhlas s podmínkami užívání před tím, než může službu nebo produkt užívat. Způsob udělení souhlasu se pak může lišit v závislosti na jednotlivé internetové stránce. Nejčastějším řešením je ovšem inkorporace dialogového okna, kde jsou zobrazeny smluvní podmínky nebo odkaz na ně a následné políčko pro zaškrtnutí vyjádření souhlasu s jejich zněním. Bez zaškrtnutí políčka (v angličtině právě ono kliknutí, „*click*“), které představuje z právního hlediska vyjádření vůle k uzavření smlouvy (opět

[324] POLČÁK, R. Praxe elektronických dokumentů, op. cit. 8, s. 57.

v angličtině v přeneseném významu „*wrap*“), pak zpravidla nelze v nákupu či jiné činnosti pokračovat. Důvodem vzniku této formy kontraktu bylo vytvoření možnosti uzavírat elektronické smlouvy na podkladě jednoduchého kliknutí pomocí polohovacího zařízení, čímž dojde k vyjádření souhlasu se smlouvou. Přesně proto historický vývoj ICT práva na dynamický vývoj elektronických kontraktací odpověděl právě etablováním tohoto smluvního typu e-kontraktace.[325]

Smyslem tohoto typu elektronických smluv je umožnění uzavírání smluv širokému okruhu veřejnosti, které je bezesporu časově daleko efektivnější než klasický způsob. Tento způsob je například často využíván při instalaci software, kdy je uzavření licenční smlouvy přímo součástí instalačního procesu. Pokud zákazníci s ustanoveními licenční smlouvy nesouhlasí, nelze software nainstalovat. Z právního pohledu jde o standardizovaná smluvní ustanovení (v angličtině SFC – *Standard Form Contracts*) a z pohledu českého práva se jedná o adhezní smlouvy.[326] V procesu uzavírání smlouvy je pak zapotřebí věnovat pozornost tomu, v jakém okamžiku dochází k uzavření smlouvy a jaké následky pro kontrahenta z uzavření plynou.[327]

4.3.2. *Click-through* smlouvy

Druhým typem online smluv jsou *click-through* smlouvy. Opět je zde prvek kliknutí („*click"*), ovšem tentokrát prostřednictvím něčeho či skrz něco („*through*“). V praxi si *click-through* smlouvy můžeme představit jako proklikání více kroky, které ve svém celku tvoří uzavření smlouvy. Jako příklad lze uvést výběr zboží, způsobu platby, dopravy atd. *Click-through* smlouvy je zapotřebí vnímat v souvislosti s předchozí kapitolou věnovanou problematice *click-wrap* smluv. Smlouvy jsou z čistě právního hlediska totožné. Rozdíl lze však nalézt z pohledu technického, kdy u *click-wrap* smluv dochází k jednorázovému zaškrtnutí políčka „Souhlasím“ či obdobnému projevu vůle. Oproti tomu u *click-through* smluv se jedná o komplexnější proces, neboť kontrahent musí zpravidla na příslušné internetové stránce proklikat více postupných kroků. Jedná se tak o složitější a časově náročnější proces, který lze ovšem považovat za bezpečnější a umožňující se spolehnout na větší míru pravděpodobnosti seznámení se kontrahenta s konkrétními aspekty uzavírané smlouvy.[328] Tento proces se

[325] ŠČERBA, Tomáš. *Elektronická kontraktace v právní praxi*. Rigorózní práce. Brno: Právnická fakulta Masarykovy Univerzity, 2008, s. 75-76.
[326] *Ibid,* s. 77.
[327] POLČÁK, Radim, Zsolt György BALOGH, Michael BOGDAN, Giovanni Maria RICCIO, Dan Jerker B. SVANTESSON a Andreas WIEBE. *Introduction to ICT Law (Selected Issues)*. Brno: Masarykova Univerzita, 2007. 185 s. AUBI, řada teoretická, 314. ISBN 978-80-210-4302-2, s. 74 – 78.
[328] ŠČERBA, Tomáš. *Elektronická kontraktace v právní praxi*, op. cit. 325, s. 85 – 86.

vyznačuje možností návratu k přechozím krokům a jejich úpravy. Kontrahent by si ovšem měl být vědom, v jakém okamžiku dochází k finálnímu uzavření smlouvy bez možnosti další změny.[329] Judikatura vztahující se k tomuto typu smluv je rozebrána v kapitole 5.1.6.

4.3.3. *Browse-wrap* smlouvy

Browse-wrap smlouvy jsou zpravidla uzavírány konkludentně. Na rozdíl od výše uvedených *click-wrap* a *click-through* typů online smluv není v případě *browse-wrap* smluv zapotřebí přímé zakliknutí souhlasu kontrahenta s danými podmínkami. Typickým příkladem je navštívení internetové stránky, kterým sám o sobě uživatel s danými podmínkami (smlouvou) souhlasí.[330] Smlouva však musí splňovat stejné náležitosti jako v případě *click-wrap* a *click-through* typů. Zejména musí být kontrahentovi zpřístupněny smluvní podmínky, musí být zřejmé, že dochází k uzavření smlouvy a souvisejících následků a souhlas musí být jasný a prokazatelný.[331] Jelikož se tento typ smluv může vyskytovat v mnoha variacích, nelze stanovit jasná univerzální kritéria pro jeho platnost. Je tak zapotřebí vycházet z obecných podmínek v občanském zákoníku upravujících uzavření smlouvy. Dle zahraniční rozhodovací praxe je zapotřebí vzít v potaz i technickou stránku, např. není možné umístit smluvní podmínky na jinou internetovou stránku a oznámení umístit na stránku malým písmem stejné barvy jako pozadí stránky[332] nebo po uživateli vyžadovat, aby smluvní podmínky sám aktivně vyhledával.[333]

4.3.4. *Shrink-wrap* smlouvy

Shrink-wrap smlouvy jsou v dnešní době již převážně překonaným typem. Povaha těchto smluv je spojena zejména s krabicovými počítačovými programy, který byl tradičně balen do průhledné plastové folie (*shrink wrap*). Jejich rozbalením uživatel vyjadřoval souhlas se smluvními podmínkami, se kterými se ovšem mohl seznámit až po rozbalení. To je z právního hlediska samozřejmě problematické, neboť uživatel vyjadřuje souhlas s podmínkami, které

[329] POLČÁK, Radim, Zsolt György BALOGH, Michael BOGDAN, Giovanni Maria RICCIO, Dan Jerker B. SVANTESSON a Andreas WIEBE. *Introduction to ICT Law (Selected Issues)*, op. cit. 327, s. 78 – 80.
[330] ŠČERBA, Tomáš. *Elektronická kontraktace v právní praxi*, op. cit. 325, s. 97.
[331] POLČÁK, Radim, Zsolt György BALOGH, Michael BOGDAN, Giovanni Maria RICCIO, Dan Jerker B. SVANTESSON a Andreas WIEBE. *Introduction to ICT Law (Selected Issues),* op. cit. 327, s. 81 – 84.
[332] Rozhodnutí Pollstar v. Gigmania, Ltd., United States District Court, D. California ze dne 17. října 2000, 981-982.
[333] Rozhodnutí Nguyen v. Barnes & Noble, Inc., United States Court of Appeals for the Ninth Circuit ze dne 18. srpna 2014 či Rozsudek ve věci Specht v. Netscape Comm. ze dne 1. října 2002.

nezná.[334] Rozhodovací praxe byla vůči tomuto typu smluv zpočátku velmi striktní a shledávala je za nevymahatelné, pozdější judikatura však mírnější a doposud není sjednocena.[335]

Obdobou *shrink wrap* smluv v současné doby jsou tzv. EULA (*end user license agreement*) upravující licenci mezi vlastníkem práv počítačového programu a koncovým uživatelem. Vzhledem k technologickému pokroku a změně povahy služeb jsou však tyto licenční smlouvy s koncovými uživateli přístupné na internetových stránkách distributorů počítačových programů, a koncoví uživatelé se s nimi mohou seznámit ještě před zakoupením licence daného počítačového programu.

4.3.5. *Blockchain* a *smart contracts*

Blockchain je speciálním druhem distribuované decentralizované databáze, která uchovává stále se rozšiřující počet záznamů (bloků), jež jsou chráněny proti neoprávněnému zásahu. Jedná se v podstatě o elektronickou účetní knihu (*electronic ledger* nebo *digital ledger*), která obsahuje úplnou digitální stopu, podle které lze zpětně dohledat veškeré transakce. Veškerý předchozí obsah je totiž ve formě kryptografického otisku (*hashe*) přidán k obsahu nově přidanému (zpravidla transakčním datům) spolu s časovým razítkem a dochází k jejich vzájemné fixaci. Jelikož každý blok obsahuje informaci o bloku předchozím, tvoří tak řetězec (*chain*). Díky principu decentralizace, tedy rozložení mezi více uzlů (výpočetních zařízení) v *peer-to-peer (P2P)* síti pak dochází ke garanci správnosti údajů a nemožnosti jejich neoprávněné změny jak z vnějšku, tak zevnitř P2P sítě, neboť každý uzel replikuje a ukládá identickou kopii dat účetní knihy a aktualizuje se nezávisle na ostatních uzlech na základě konsenzu.[336] Technologie je primárně využívána pro finanční transakce s kryptoměnami, avšak umožňuje použití i s elektronickými dokumenty, resp. jejich otisky (*hashe*). Bez ohledu na praktické aspekty, jako je uhlíková stopa a cena transakce, by právě z tohoto důvodu dle Peterky blockchain mohl být využíván jako nástroj k udržování digitální kontinuity, a to nejenom potenciální, ale i aktuální.[337] Jak bylo zmíněno výše v kapitole 4.2.6, *blockchain* technologie by měla splňovat požadavky § 562 odst. 2 občanského zákoníku.

---

[334] Více srov. ŠČERBA, Tomáš. *Elektronická kontraktace v právní praxi,* op. cit. 325, s. 62 a násl.
[335] KOŘÍNKOVÁ, Petra. *Internet a mezinárodní právo soukromé*. Diplomová práce. Praha: Univerzita Karlova v Praze Právnická fakulta, 2014.
[336] SHAAN, Ray. *The Difference Between Blockchains & Distributed Ledger Technology*. Online. Dostupné z: https://towardsdatascience.com/the-difference-between-blockchains-distributed-ledger-technology-42715a0fa92. [cit. 2023-12-27].
[337] PETERKA, Jiří. *Jak na digitální kontinuitu (3): Elektroničtí notáři, spisové služby, blockchain a vyvratitelné domněnky*, op. cit. 231.

S technologií *blockchain* souvisí *smart contracts* (v překladu chytré kontrakty). Jedná se o soubor příkazů ve zdrojovém kódu, jenž jsou automaticky vykonávány prostřednictvím počítačového programu.[338] Szabo uvádí jako příklad *smart contractu* situaci, kdy věřitel zapůjčí peníze na koupi automobilu. Automobil obsahuje zámek se *smart contractem* naprogramovaným tak, aby se zablokoval, pokud nedojde k řádnému splacení zápůjčky. Pokud tedy nedojde k řádnému splacení, nebude vydlužitel schopen automobil užívat. Naopak pokud dojde k splacení zápůjčky v celém rozsahu, *smart contract* bude navždy deaktivován.[339]

Aby byly *smart contracts* smlouvami, musí naplňovat obecné náležitosti dle občanského zákoníku. Na základě možnosti svobodné volby formy jednání[340] by neměl být problém s vyjádřením smlouvy prostřednictvím programovacího jazyku.[341] Dále musí dojít k nabídce, přijetí nabídky[342] a v případě distančního sjednávání smlouvy i k doručení přijetí nabídky nabízející straně.[343] Obsah nabídky ve *smart contract* musí tedy obsahovat alespoň podstatné náležitosti smlouvy tak, aby smlouva mohla být uzavřena jeho jednoduchým a nepodmíněným přijetím.[344] Pokud budou tyto náležitosti splněny, resp. obsaženy v počítačovém programu, a smluvní strany s nimi budou souhlasit, bude splněna podmínka vůle zřídit mezi sebou závazek a řídit se obsahem smlouvy.[345]

Je však otázkou, zda jsou v případě *smart contracts* splněny náležitosti písemné formy dle § 562 odst. 1 občanského zákoníku, tedy (i) zachycení obsahu právního jednání, (ii) určení jednající osoby. Jelikož je obsah zachycen v programovacím jazyku, je první podmínka splněna. Ohledně určení jednající osoby je však situace komplikovanější. Dle Kučery[346] záleží na konkrétních technických okolnostech. Pokud je osoba z technického pohledu jednoznačně určitelná nebo určitelná alespoň s určitou mírou pravděpodobnosti, měly by být smlouvy platné, a tím být splněna i druhá podmínka. Stejný názor zastává i Bratský, dle kterého každý uživatel vystupuje v databázi *blockchain* pod konkrétní kombinací veřejného a soukromého klíče, kterou disponuje vždy pouze jeden uživatel. Na základě kombinace klíčů lze tedy daného

---

[338] KUČERA, Zdeněk. *Smart contracts pohledem právníka*. Online. Dostupné z: https://www.pravniprostor.cz/clanky/obcanske-pravo/smart-contracts-pohledem-pravnika. [cit. 2023-12-27].
[339] SZABO, Nick. Formalizing and Securing Relationships on Public Networks. First Monday [online]. 1997 [cit. 2019-02-18]. ISSN 1396-0466. Dostupné z: https://ojphi.org/ojs/index.php/fm/article/view/548/469 .
[340] § 559 občanského zákoníku.
[341] BRATSKÝ, Pavel. Smart contract v českém právu. *Právní rádce*. 2019, roč. 2019, č. 3.
[342] § 1731 a násl. občanského zákoníku.
[343] § 570 občanského zákoníku.
[344] § 1732 občanského zákoníku.
[345] § 1724 odst. 1 občanského zákoníku.
[346] KUČERA, Zdeněk. *Smart contracts pohledem právníka*. Online. Dostupné z: https://www.pravniprostor.cz/clanky/obcanske-pravo/smart-contracts-pohledem-pravnika. [cit. 2023-12-27].

uživatele vždy jednoznačně určit a identifikovat. Dle Bratského lze navíc soukromý klíč považovat po jeho připojení i za prostý elektronický podpis. Takové jednání dle něj tedy splňuje písemnou formu i dle § 561 odst. 1 občanského zákoníku.[347]

4.4. Důkazní účinky elektronických podpisů *versus* (ne)platnost písemného právního jednání

Doposud se tato práce věnovala zejména otázce platnosti písemného právního jednání v případě prostého elektronického podpisu. Tu je však zapotřebí striktně odlišovat od potenciálního nesení důkazního břemene. Řada autorů[348] a soudních rozhodnutí, jak bude rozebráno v kapitole 5.1, dle názoru autora této práce a např. Korbela, Kováře a Amlera[349] tyto dvě oblasti ovšem bez dalšího zaměňují. Jak bylo rozebráno výše, různé úrovně elektronických podpisů budou mít bez pochyby různou míru důkazní spolehlivosti, avšak platnost písemného právního jednání bude dodržena i v případě prostého elektronického podpisu.[350] Rozdíl je pak zřejmý přímo i ze systematiky textu zákona, kdy platnost písemného právního jednání je řešena v ustanoveních § 561 a § 562 občanského zákoníku, zatímco důkazní účinky v ustanoveních § 565 a § 566 téhož zákona.

Opět je vhodné na tomto místě upozornit na zákaz diskriminace různých typů elektronických podpisů, tedy pravidlu, že elektronickému podpisu 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 že nesplňuje požadavky na kvalifikované elektronické podpisy.[351] O právních účincích elektronických dokumentů pojednává navíc přímo i nařízení eIDAS. Konkrétně stanoví, že „*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*“.[352] Dle této zásady platí, že příjemce by neměl, pokud tak nestanoví zvláštní právní přepis, požadovat dokument pouze v listinné podobě a odmítat dokument elektronický, jak je v praxi bohužel stále běžné. Z výše uvedeného vyplývá, že elektronický dokument, který není opatřen vyšší formou elektronických podpisů, nebo není opatřen podpisem vůbec,[353] by neměl být

[347] BRATSKÝ, Pavel. Smart contract v českém právu. *Právní rádce*. 2019, roč. 2019, č. 3.
[348] Srov např. PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra, op. cit. 9, nebo PETERKA, Jiří. *Zatímco technické obory přitvrzují, právo naopak měkne*, op. cit 91.
[349] KORBEL, František; KOVÁŘ, Dalibor a AMLER, Pavel. *Interpretace elektronického podpisu a související identifikace v soukromém právu*, op. cit. 29.
[350] K tomu srov. kapitolu 3.4.
[351] Článek 25 odst. 1 nařízení eIDAS.
[352] Článek 46 nařízení eIDAS. Srov. také články 25, 35, 41 a 43 nařízení eIDAS.
[353] § 566 odst. 1 a 2 občanského zákoníku.

příjemcem bez dalšího odmítnut, ale mělo by být zjištěno, zda z něj lze dovozovat zamýšlené účinky. Ke stejnému závěru dospívá i Polčák[354] a Korbel, Kovář a Jaroš.[355]

Dokument navíc sám o sobě je pouze důkazním prostředkem, nikoli důkazem samotným. Jeho obsah tedy nelze automaticky ztotožňovat s obsahem vůle jednajících osob. Také nelze dokument považovat za *a priori* spolehlivý. Jeho spolehlivost musí být vždy zkoumána v širším kontextu, tedy korelace obsahu a prokazované skutečnosti, obsahových a formálních parametrů a vztahu k ostatním okolnostem. To vše zejména s ohledem na zásadu materiální pravdy a zásadu volného hodnocení důkazů.[356] S ohledem na výše uvedené dává smysl vést polemiku o nejvhodnější úrovni elektronického podpisu sloužící k pozdější identifikaci podepisující osoby, nicméně nelze zpochybňovat platnost právního jednání v písemné formě.

Určitelnost podepisující osoby totiž nezaručuje ani podpis vlastnoruční. Naopak, často se jedná o pouhou křivku, ze které nelze přečíst jméno ani příjmení. Tento poznatek vyplývá i z judikatury Nejvyššího správního soudu, dle kterého podpis neslouží primárně k identifikaci osoby.[357] Naopak slouží k potvrzení konečnosti a vážnosti vůle. Účelem elektronických podpisů pak je, stejně jako v případě vlastnoručního podpisu na fyzickém vyhotovení smlouvy, právě potvrzení konečnosti a vážnosti vůle. Identifikace smluvních stran, která je zpravidla uvedena v hlavičce smlouvy, by v opačném případě byla zcela nadbytečná. S tím souvisí i rozhodnutí Nejvyššího soudu, který shledal jako neplatnou smlouvu podepsanou jinou osobou oproti osobě uvedené jako zástupce právnické osoby v hlavičce smlouvy.[358] Vyšší úroveň elektronických podpisů navíc nemusí umožnit online okamžitou jednoznačnou identifikaci podepisující osoby, protože ani z kvalifikovaného certifikátu pro elektronický podpis plná identifikace nemusí vyplývat[359] a v případě zaručeného elektronického podpisu není identifikace podepisujícího ani možná.[360]

[354] POLČÁK, Radim. Praxe elektronických dokumentů, op. cit. 8, s. 56 a 57.
[355] KORBEL, František, KOVÁŘ, Dalibor a JAROŠ, Ján. Aktuální právní přístup k dynamickému biometrickému podpisu. *Pojistný obzor*. roč. 2021, č. 2, s. 13.
[356] POLČÁK, Radim. Praxe elektronických dokumentů, op. cit. 8, s. 54.
[357] Rozhodnutí Nejvyššího správního soudu ze dne 27. 7. 2017, sp. zn. 2 As 80/2017.
[358] Rozhodnutí Nejvyššího soudu ze dne 27. 8. 2013, sp. zn. 21 Cdo 2186/2012.
[359] Stejně jako z vlastnoručního podpisu. Dále srov. kapitolu 3.1 a DONÁT, Josef, Jan TOMÍŠEK a Ivan FENCL. *Je publikovaná judikatura k elektronickým podpisům skutečně relevantní?*, op. cit 26.
[360] JAREŠ, Adam. *SMLOUVA PODEPSANÁ ELEKTRONICKÝM PODPISEM*, op. cit. 6, s. 114.

5. Rozbor současné judikatury

Výše zmíněná problematika (ne)platnosti písemné formy právního jednání za použití prostého elektronického podpisu a ostatních výše zmíněných aspektů není čistě teoretická. Naopak, rozhodovací praxe soudů není sjednocena a v řadě případů dochází dokonce k paralelnímu vydávání rozhodnutí, která si vzájemně odporují. Důsledkem je vysoká míra právní nejistoty, která v praxi vede k vysokým nákladům. Není sporu o tom, že tento stav není ideální, dokonce je v rozporu se samotným nařízením eIDAS.[361] V této kapitole autor práce nastíní argumenty vybraných rozhodnutí soudů, vyloží, v čem rozpory spočívají, a předloží možné řešení nastalé situace. Většina rozhodnutí nižších soudů je dostupná v databázi okresních, krajských a vrchních soudů,[362] ostatní pak byly vyhledány prostřednictvím služeb beck-online a ASPI.

5.1. Analýza jednotlivých rozhodnutí a souvisejících rozporů

Nejdříve je vhodné rozebrat v krátkosti právní úpravu dokazování před soudy. Ta je jednak upravena v ustanovení § 125 osř, podle kterého za důkaz mohou sloužit všechny prostředky, jimiž lze zjistit stav věci. Široké vymezení pak nalezneme i v nařízení eIDAS, kde je pro účely dokazování v soudním a správním řízení užíván termín elektronický dokument, definovaný jako jakýkoli obsah uchovávaný v elektronické podobě, zejména jako text nebo zvuková, vizuální nebo audiovizuální nahrávka.[363] Nařízení eIDAS také stanovuje, že elektronickému podpisu, elektronické pečeti, elektronickému časovému razítku ani elektronickému dokumentu nesmějí být upírány právní účinky a nesmí být odmítány jako důkaz v soudním a správním řízení pouze z toho důvodu, že mají elektronickou podobu.[364] Podle zásady volného hodnocení důkazů je pak na soudu, jakou váhu jednotlivým důkazům soud přiloží.[365] Lze tedy dospět k závěru, že v tomto ohledu žádná formální limitace neexistuje a elektronické dokumenty včetně elektronických podpisů či dalších služeb vytvářejících důvěru jsou přípustné jako důkazy.[366]

[361] Srov. zejména recitál 1 a 2 nařízení eIDAS.
[362] Dostupné zde: https://rozhodnuti.justice.cz/soudnirozhodnuti/.
[363] Článek 3 odst. 35 nařízení eIDAS.
[364] Článek 25 odst. 1, článek 35 odst. 1, článek 41 odst. 1 a článek 46 nařízení eIDAS.
[365] § 132 osř.
[366] JAREŠ, Adam. *SMLOUVA PODEPSANÁ ELEKTRONICKÝM PODPISEM*, op. cit. 6, s. 139.

5.1.1. Email bez elektronického podpisu a požadavek písemné formy

Pravděpodobně největší kontroverze ve veřejném prostoru vyvolalo rozhodnutí Nejvyššího soudu ze dne 22. května 2019,[367] ve kterém soud dospěl k závěru, že „*prostý email bez elektronického podpisu nesplňuje požadavek písemného právního jednání*". Nejvyšší soud odkázal na své dřívější rozhodnutí,[368] dle kterého „*písemná forma právního jednání (ve smyslu § 561 a § 562 o. z.) předpokládá existenci dvou náležitostí, a to písemnosti a podpisu. Písemnost spočívá v tom, že projev vůle 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*".[369]

Nejvyšší soud v prvně citovaném rozhodnutí jednak uvedl, že k zachování písemné formy dle § 562 občanského zákoníku je zapotřebí připojení podpisu, a dále že předchozí úprava nebyla od té stávající odlišná. S prvním názorem autor této práce nesouhlasí. Jak bylo rozebráno v kapitole 4.1.6, ustanovení § 561 a § 562 občanského zákoníku jsou ve vztahu speciality, a podpis tedy v případě dodržení zákonných náležitostí v režimu § 562 odst. 1 zapotřebí není. Soud pak sice správně nevzal v úvahu nařízení eIDAS, které v rozhodnou dobu nebylo účinné, ale pouze platné, avšak vůbec se nezabýval definicí elektronického podpisu, resp. zda podané námitky nebyly podepsány alespoň prostým elektronickým podpisem (nehledě na to, v jakém předpisu byl definován), či zda se jednalo o zavedenou formu komunikace mezi stranami. Rozhodnutí vyvolalo značnou vlnu kritiky. Janošek například toto rozhodnutí označil za přepjatě formální a s jeho závěry se neztotožnil.[370] Donát s Tomíškem považují rozhodnutí za přežité.[371] K obdobným závěrům dospěl Nejvyšší soud již ve svých předchozích rozhodnutích.[372]

Oproti rozhodnutí citovanému výše nicméně Nejvyšší soud ve svém rozhodnutí ze dne 16. 5. 2019 shledal jako platnou rozhodčí smlouvu v písemné formě, která byla sjednána výměnou e-

[367] Rozhodnutí Nejvyššího soudu ČR ze dne 22. 5. 2019, sp. zn. 26 Cdo 1230/2019.
[368] Rozhodnutí Nejvyšší soudu ČR ze dne 1. 6. 2017, sp. zn. 20 Cdo 1741/2017.
[369] Nejvyšší soud dále odkazuje například na rozsudek Nejvyššího soudu ze dne 29. 1. 2009, sp. zn. 30 Cdo 1230/2007, nebo rozsudek Nejvyššího soudu ze dne 10. 4. 2014, sp. zn. 23 Cdo 1593/2012, jejichž závěry, byť se týkají formy právního úkonu podle ustanovení § 40 odst. 4 občanského zákoníku 1964, ve znění účinném do 31. 12. 2013, lze dle soudu aplikovat i na formu právního jednání podle ustanovení § 562 odst. 1 občanského zákoníku.
[370] JANOŠEK, Vladimír. *Prostý email a následky nedodržení písemné formy jednání alias přepjatý formalismus*. Online. Dostupné z: https://www.epravo.cz/top/clanky/prosty-email-a-nasledky-nedodrzeni-pisemne-formy-jednani-alias-prepjaty-formalismus-109790.html?mail. [cit. 2024-01-18].
[371] DONÁT, Josef a TOMÍŠEK, Jan. Právo v síti: průvodce právem na internetu, op. cit. 140, s. 160.
[372] Srov. např. rozhodnutí Nejvyššího soudu ČR ze dne 29. 1. 2009, sp. zn. 30 Cdo 1230/2007, nebo rozhodnutí Nejvyššího soudu ČR ze dne 10. 4. 2014, sp. zn. 23 Cdo 1593/2012.

mailů neobsahující kvalifikovaný elektronický podpis.[373] K obdobným názorům, tedy potvrzení písemné formy v případě prostého elektronického podpisu, pak dospěl Nejvyšší soud i ve svých jiných rozhodnutích.[374] Závěr o neplatnosti je navíc v rozporu s jiným rozhodnutím Nejvyššího soudu, dle kterého je právní jednání, které odporuje zákonu, včetně nedodržení formy právního jednání, neplatné, pouze vyžaduje-li to smysl a účel zákona.[375]

Z výše uvedeného vyplývá, že ani argumentace Nejvyššího soudu ohledně dodržení písemné formy právního jednání není jednotná. Ve vztahu k výše uvedeným rozhodnutím popírajícím platnost písemného právního jednání lze však argumentovat novou definicí elektronického podpisu v nařízení eIDAS, která neobsahuje požadavek ověření identity u prostého elektronického podpisu. Nicméně soudy nižších stupňů z těchto rozhodnutí (chybně) vycházejí i v případech, kdy bylo nařízení eIDAS již účinné.[376] Objevují se ovšem i rozhodnutí odkazující na předmětné rozhodnutí, které jeho závěry ovšem vykládají opačně.[377]

V jiných rozhodnutích soudů nižších stupňů lze pak najít argumentaci, dle které je dle ustanovení § 561 odst. 1 občanského zákoníku zapotřebí připojení podpisu, který splňuje všechny náležitosti uvedené v článku 26 nařízení eIDAS.[378] Jak již bylo rozebráno v kapitole

[373] Rozhodnutí Nejvyššího soudu ČR ze dne 16. 5. 2019, sp. zn. 23 Cdo 3439/2018. Konkrétně soud uvedl, „*že je na místě vykládat požadavek obsažení rozhodčí smlouvy „ve výměně dopisů nebo telegramů“ ve smyslu čl. II Newyorské úmluvy tak, že zahrnuje i výměnu komunikace prostřednictvím e-mailu“.*

[374] Rozhodnutí Nejvyššího soudu ČR ze dne 17. 12. 2013, sp. zn. 23Cdo 1308/2011 nebo rozhodnutí Nejvyššího soudu ČR ze dne 19. 10. 2016, sp. zn. 31 Cdo 1570/2015.

[375] Rozhodnutí Nejvyššího soudu ČR ze dne 27. 11. 2014, sp. zn. 29 Cdo 3919/2014. Soud konkrétně uvedl, že „*právní jednání odporující zákonu je neplatné pouze tehdy, vyžaduje-li to smysl a účel zákona (§ 580 odst. 1 o. z.). Uvedené omezení platí i pro posouzení důsledků nedodržení formy právního jednání vyžadované zákonem (§ 582 odst. 1 o. z.). Jinými slovy, není-li právní jednání učiněno ve formě stanovené zákonem, je (z tohoto důvodu) neplatné pouze tehdy, vyžaduje-li to smysl a účel zákona*.“

[376] Srov. např. rozhodnutí Obvodního soudu pro Prahu 9, ze dne 12. 6. 2023, č. j. 98 C 250/2017-649, ze dne 15. 5. 2023 č. j. 98 C 190/2022-64, ze dne 6. 1. 2023, č. j. 98 C 303/2020-275, ze dne 25. 10. 2022, č. j. 98 C 257/2019-309, ze dne 7. 7. 2022, č. j. 98 C 332/2020-245, rozhodnutí Obvodního soudu pro Prahu 7 ze dne 14. 9. 2022, č. j. 16 C 111/2021-198, rozhodnutí Obvodního soud pro Prahu 4 ze dne 13. 4. 2022, č. j. 28 C 48/2020-121, rozhodnutí Okresního soudu pro Prahu-východ ze dne 22. 2. 2022, sp. zn. 7 C 92/2021, rozhodnutí Okresního soudu v Litoměřicích ze dne 9. 8. 2021, sp. zn. 9 C 332/2019-218.

[377] Srov. např. rozhodnutí Obvodního soudu pro Prahu 2 ze dne 10. 11. 2021, č.j. 22 C 198/2020-223.

[378] Rozhodnutí Okresního soudu v Berouně ze dne 13. 9. 2023, sp. zn. 10 C 220/2023-59, obdobně pak v rozhodnutí Okresního soudu v Chomutově ze dne 6. 9. 2023, sp. zn. 7 C 248/2023, rozhodnutí Okresního soudu v Plzni – jih ze dne 7. 6. 2023, sp. zn. 1 C 62/2023, rozhodnutí Okresního soudu v Mostě ze dne 1. 9. 2023, č. j. 46 C 177/2023-24. Dle těchto rozhodnutí „*ve smyslu ustanovení § 561 odst. 1 o.z. je k platnosti smlouvy třeba, aby k ní žalovaný připojil svůj podpis. Elektronický podpis, jenž je postaven na roveň podpisu vlastnoručního, je ve smyslu přímo použitelného nařízení eIDAS pouze kvalifikovaný elektronický podpis (tj. podpisem vytvořeným kvalifikovaným prostředkem = v české terminologii rovněž označovaný jako„ kvalifikovaný elektronický podpis“). Ve smyslu článku 26 eIDAS lze za podpis, jenž důvěryhodně identifikuje osobu podepisující označit i zaručený elektronický podpis (= v českém terminologii označovaný „zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis“), jenž je jednoznačně spojen s podepisující osobou, umožňuje její jednoznačnou identifikaci, je vytvořen pomocí dat pro vytváření elektronických podpisů a je k podepisovanému dokumentu připojen tak, že je možné zjistit jakoukoliv následující změnu dat. Tedy takový podpis, který je v terminologii zákona č. č. 297/2016 Sb., podřazen pod termín uznávaný elektronický podpis. Jiné podpisy nelze*

4 výše, argumentace soudu je lichá. Ustanovení § 561 odst. 1 občanského zákoníku odkazuje na ZSVD, které elektronickým podpisem chápe i prostý elektronický podpis, stejně jako nařízení eIDAS. V tomto konkrétním případě se jednalo o úvěrové smlouvy, na které dopadá zákonný požadavek písemné formy dle ustanovení § 104 zákona o spotřebitelském úvěru.[379] Následkem nesplnění této podmínky však přímo dle znění tohoto ustanovení není neuzavření nebo neplatnost úvěrové smlouvy.[380] Ze znění zákona také nevyplývá povinnost vlastnoručního podpisu, kterou dovozují soudy ve výše uvedených případech.

Obdobně pak Okresní soud v Ostravě ve svém rozhodnutí[381] dospěl k závěru, že za podpis nelze považovat pouhé uvedení jména a příjmení žalovaného a dodatku o SMS verifikaci. Důvodem je dle soudu nedostatečná identifikace podepisující osoby. Obdobně pak rozhodl i Vrchní soud v Praze,[382] dle kterého „*nelze za „jiný typ elektronického podpisu“ považovat pouhé uvedení jména a příjmení osoby v textové části e-mailu bez spojení s dalším elektronickým prvkem (značkou), vylučujícím jednak záměnu jednající osoby s jinou, jednak poskytující jistotu její jednoznačné identifikace*“ (podtržení přidáno autorem).

K opačnému závěru ovšem dospěl např. ve svém rozhodnutí[383] Okresní soud v Blansku, dle kterého je v českém právu rozlišeno několik druhů elektronických podpisů a právní důsledky jsou spojeny s jakýmkoli z nich. Jako příklad soud uvedl naskenovaný vlastnoruční podpis, speciální kód v podobě PIN kódu, hesla, ID apod., ale i jméno a příjmení v samotném textu zprávy. Soud pak správně odlišil platnost písemného právního jednání a unesení důkazního břemene. K pozdějšímu soud uvedl, že žalobkyně sice tvrdila, že si žalovaný zřídil uživatelský

bez dalšího považovat za podpisy postavené na roveň vlastnoručního podpisu, resp. podpisy důvěryhodně identifikující podepisující osobu. Má-li být elektronický podpis uznán za podpis konkrétní osoby, musí být prokázáno, že splňuje všechny podmínky stanovené v článku 26 eIDAS“ (podtržení přidáno autorem).

[379] Zákon č. 257/2016 Sb. o spotřebitelském úvěru, ve znění pozdějších předpisů.

[380] K tomu srov. i rozhodnutí Krajského soudu v Praze ze dne 02. 3. 2022. č.j. 25 Co 1/2022 – 66.

[381] Rozhodnutí Okresního soudu v Ostravě ze dne 25. 01. 2022, sp. zn. 30 C 365/2021. Konkrétně soud uvedl následující: *Přestože elektronický podpis je vymezen velmi široce, nelze za něj považovat pouhé uvedení jména a příjmení žalovaného a dodatku o SMS verifikaci samo o sobě neumožňuje přesně identifikovat podepisující osobu. […] Soud tedy opakovaně konstatuje, že v řízení nevzal za prokázáno, že by mezi žalobkyní jako úvěrující a žalovanou jako úvěrovaným byla uzavřena smlouva o tvrzeném obsahu. Nedodržení písemné formy podle ust. § 104 zákona o spotřebitelském úvěru sice nemá za následek neplatnost smlouvy o úvěru, nicméně z této listiny se uzavření smlouvy žalovanou nepodává a v řízení nebylo prokázáno, že by text této listiny odpovídal projevu vůle žalované* (podtržení přidáno autorem).

[382] Rozhodnutí Vrchního soudu v Praze ze dne 23. 5. 2023, sp. zn. 4 Cmo 52/2023.

[383] Rozhodnutí Okresního soudu v Blansku ze dne 2. 12. 2021, sp. zn. 3 C 173/2021. Konkrétně soud uvedl, že „*české právo tedy nezná pouze jeden druh elektronického podpisu, ale rozlišuje různé druhy, přičemž právní důsledky spojuje s jakýmkoliv elektronickým podpisem. Obyčejným, prostým elektronickým podpisem může být nejen např. skenovaný vlastnoruční podpis, nebo speciální kód (PIN, heslo, ID apod.), kterým osoba disponuje, ale i řetězec jednotlivých znaků tvořících jméno a příjmení v textu zprávy zaslané z určité adresy elektronické pošty. Nicméně v rámci soudního řízení je nutné takové uzavření smlouvy prokázat“* (podtržení přidáno autorem).

účet, tato tvrzení však nebyla podložena důkazy. Z toho důvodu dle soudu nebylo v tomto konkrétním případě možné uzavřít, že by žalovaný byl smlouvou vázán.[384]

5.1.2. Předžalobní výzva doručená emailem

V dané problematice dále Krajský soud v Brně ve svém rozhodnutí[385] konstatoval, že předžalobní výzva doručená prostřednictvím emailu splňuje zákonný požadavek na její písemnou formu.

5.1.3. Možnost následné změny písemné formy

Dle rozhodnutí Nejvyššího soudu[386] je možné následně měnit písemnou formu jinou než dohodnutou formou. V posuzovaném případě se účastníci dohodli na změně uzavřené smlouvy pouze prostřednictvím dodatků opatřených úředně ověřenými podpisy stran. Následně však uzavřeli písemné dodatky, které byly podepsány bez úředně ověřených podpisů. Na základě této skutečnosti soud došel k závěru, že „*bude-li z okolností konkrétní věci zřejmé, že strany chtějí být uzavřeným právním jednáním vázány i při nedodržení smluvené formy, mělo by jít o vázanost platnou, neboť opačný důsledek je při úpravě obsažené v ustanovení § 1758 o. z. pro praxi do jisté míry nepředvídatelný a také v rozporu s jejími očekáváními a potřebami*“.

5.1.4. Ustanovení § 561 a § 562 občanského zákoníku ve vztahu speciality

Vztah speciality ustanovení § 561 a 562 občanského zákoníku potvrdil ve svém rozhodnutí[387] Krajský soud v Českých Budějovicích, který konstatoval, že „*požadavek písemnosti je přitom splněn nejen prizmatem § 561 odst. 1 o.z., ale rovněž dle § 3 odst. 1 zákona o rozhodčím řízení,*

---

[384] Soud konkrétně uvedl, že: „*Žalobkyně tvrdila, že žalovaný se zaregistroval zadáním osobních údajů včetně telefonního čísla a e-mailové adresy, čímž zahájil kroky ke zřízení uživatelského účtu; následně byl žalovanému v rámci webového rozhraní zaslán návrh úvěrové smlouvy, což žalovaný odsouhlasil verifikačním kódem ([číslo]) s tím, že kód nahrazuje fyzický podpis smlouvy. K žádné z těchto tvrzených skutečností však žalobkyně nenavrhla důkazy, kterými by bylo možné prokázat, že k takovému průběhu událostí opravdu došlo. Mohl by např. být navržen důkaz počítačovým systémem, který obsahuje záznamy údajů o právních jednáních. Pokud by zároveň bylo prokázáno, že se záznamy provádějí se systematicky a posloupně a jsou chráněny proti změnám, mohla by se uplatnit vyvratitelná právní domněnka stanovená v § 562 odst. 2 o. z., že záznamy v takovém elektronickém systému jsou spolehlivé. Důkaz počítačovým systémem však navržen nebyl a z důkazů, které žalobkyně navrhla a předložila, nevyplývá, že by žalovaný (elektronickým) podpisem vyjádřil svůj souhlas se smlouvou. Proto není možné uzavřít, že by žalovaný byl smlouvou vázán“* (podtržení přidáno autorem)

[385] Rozhodnutí Krajského soudu v Brně ze dne 9. 11. 2017, sp. zn. 27 Co 86/2017. Konkrétně soud uvedl, „*že v situaci, kdy žalobce se žalovaným uzavřel smlouvu, jejíž splnění vymáhá soudně, prostřednictvím e-mailové komunikace, splňuje požadavky výzvy k plnění dle § 142a odst. 1 o. s. ř. i předžalobní výzva k plnění, kterou žalobce zaslal e-mailem žalovanému v předepsané lhůtě na elektronickou (e-mailovou) adresu udávanou žalovaným v obchodním styku účastníků*.“.

[386] Rozhodnutí Nejvyššího soudu ČR ze dne 22. 1. 2020, sp. zn. 26 Cdo 3501/2019.

[387] Rozhodnutí Krajského soudu v Českých Budějovicích ze dne 27. 3. 2015, sp. zn. 24 Co 696/2015.

respektive § 562 odst. 2 o.z., dle nichž se i nepodepsané elektronické dokumenty považují za podepsané, pokud zachycují obsah dokumentu a umožňují identifikaci jednající osoby".

Okresní soud Praha-východ,[388] Krajský soud v Praze[389] či Okresní soud v Karviné – pobočka v Havířově[390] však vztah ustanovení ve vztahu speciality ve většině svých rozhodnutí nechápou. Dle názoru autora této práce ustanovení ve vztahu speciality jsou, jak bylo rozebráno v kapitole 4.1.6.

5.1.5. Naskenovaný vlastnoruční podpis

Obvodní soud pro Prahu 6 ve svém rozhodnutí neakceptoval vyfocený vlastnoruční podpis vložený do smlouvy. Dle soudu byl podpis obrázkem podpisu, který byl sejmutý z jiného elektronického dokumentu a vložen do jiné smlouvy bez vůle tuto smlouvu podepsat.[391]

K opačným závěrům pak dospěl například ve svém rozhodnutí[392] Okresní soud v Blansku. Dle názoru autora této práce naskenovaný vlastnoruční podpis splňuje definici prostého elektronického podpisu a s ním související písemnou formu právního jednání. Z důkazního hlediska je však zapotřebí studovat spojení naskenovaného podpisu (dat v elektronické podobě) s podepisovaným obsahem (jinými daty v elektronické podobě).

5.1.6. Unikátní ID a *click-through* smlouvy

Krajský soud v Českých Budějovicích ve svém rozhodnutí[393] potvrdil, že prostým elektronickým podpisem mohou být i ID a heslo, kdy se při jejich zadání a následném vyplnění

[388] Rozhodnutí Okresního soudu Praha-východ ze dne 17. 5. 2021, sp. zn. 35 C 130/2021.
[389] Rozhodnutí Krajského soudu v Praze ze dne 17. 1. 2019, sp. zn. 27 Co 327/2018.
[390] Rozhodnutí Okresního soudu v Karviné - pobočka v Havířově ze dne 6. 12. 2022, sp. zn. 111 C 374/2022.
[391] Rozhodnutí Obvodního soudu pro Prahu 6 ze dne 13. 9. 2021, sp. zn. 18 C 198/2021. Konkrétně soud uvedl, že podpisy byly *„de facto jako obrázek podpisu sejmuty z jiné (elektronické) listiny a následně vloženy do písemností označených jako postupní smlouvy. Fakticky se tak nemuselo jednat ani o podpis osoby uvedené jako postupitel a tento obrázek podpisu mohl být dokonce sejmut z jiného dokumentu a bez vůle uvedené osoby podepsat postupní smlouvu mohl být vložen do předmětného dokumentu označeného jako postupní smlouva.“*.
[392] Rozhodnutí Okresního soudu v Blansku ze dne 2. 12. 2021, sp. zn. 3 C 173/2021.
[393] Rozhodnutí Krajského soudu v Českých Budějovicích ze dne 27. 3. 2015, sp. zn. 24 Co 696/2015. Konkrétně soud uvedl, že „*v předmětné věci došlo k uzavření smluv tak, že povinná obdržela na základě registrace unikátní přihlašovací údaje a následně se smluvními podmínkami vyslovila souhlas kliknutím na virtuální tlačítko. Tyto kontrakty bývají někdy nazývány jako tzv. „clickthrough smlouvy“ a je pro ně typický kontraktační proces, který kombinuje prostý elektronický podpis (ID, Heslo) s mechanickými prostředky (klik myší na příslušné tlačítko). Lze proto uzavřít, že povinná opatřila smlouvy včetně rozhodčí doložky prostým elektronickým podpisem, neboť po zadání unikátních identifikačních údajů vztahujících se výhradně k její osobě mechanickým prostředkem „kliknutí“ vyslovila souhlas s jejich zněním. Požadavek písemnosti je přitom splněn nejen prizmatem § 561 odst. 1 o.z., ale rovněž dle § 3 odst. 1 zákona o rozhodčím řízení, respektive § 562 odst. 2 o.z., dle nichž se i nepodepsané elektronické dokumenty považují za podepsané, pokud zachycují obsah dokumentu a umožňují identifikaci jednající osoby*."

click-through smlouvy jedná o písemnou formu, a to jak ve smyslu § 561 odst. 1, tak § 562 odst. 2 občanského zákoníku.

K obdobným závěrům, tedy že k uzavření spotřebitelské smlouvy stačí jiný typ elektronického podpisu, pak dospěl i Krajský soud v Českých Budějovicích v jiných rozhodnutích,[394] Krajský soud v Ostravě[395] nebo Krajský soud v Brně.[396] Tato rozhodnutí byla navíc vydána před účinností nařízení eIDAS. Dle autora této práce lze jejich závěry uplatnit o to více i dle současné úpravy, neboť, jak již bylo zmíněno výše, definice prostého elektronického podpisu byla oproti tehdejší úpravě nařízením eIDAS rozšířena.

5.1.7. Dvoufaktorové ověření v podobě SMS zprávy

Okresní soud v Hodoníně ve svém rozhodnutí[397] potvrdil platnost písemné formy kombinací zakliknutí pole ve webovém rozhraní a zadání unikátního SMS kódu. Ke stejnému závěru dospěl soud v obdobném případě i v jiném rozhodnutí.[398] Okresní soud v Hodoníně odkázal na rozhodnutí Krajského soudu v Ostravě[399] a Krajského soudu v Brně,[400] která byla rozebrána v kapitole 5.1.6, a potvrdil aplikovatelnost jejich závěrů i za účinnosti současné právní úpravy. K tomu dospěl i autor této práce v kapitole 2.3.

K obdobnému závěru dospěl i Obvodní soud pro Prahu 6, který ve svém rozhodnutí[401] shledal jako platnou smlouvu uzavřenou připojením elektronického podpisu do navrhované smlouvy prostřednictvím kódu zaslaného pomocí SMS. Obdobně rozhodl i Okresní soud v Mladé Boleslavi.[402]

---

[394] Rozhodnutí Krajského soudu v Českých Budějovicích ze dne 7. 8. 2015, sp. zn. 5 Co 639/2015 a ze dne 12. 5. 2015, sp. zn. 24 Co 1000/2015.
[395] Rozhodnutí Krajského soudu v Ostravě ze dne 28. 1. 2016 sp. zn. 37 ICm 4495/2014.
[396] Rozhodnutí Krajského soudu v Brně ze dne 5. 6. 2017, sp. zn. 33 Icm 547/2016.
[397] Rozhodnutí Okresního soudu v Hodoníně ze dne 14. 9. 2021, sp. zn. 13 C 67/2021. Konkrétně soud uvedl, že „*ze strany žalovaného došlo ke kontraktaci smlouvy způsobem, který lze považovat za jiný typ elektronického podpisu tvořený kombinací kliknutí na příslušné pole v chráněném webovém rozhraní právního předchůdce žalobkyně a zadání unikátního SMS kódu v tomto rozhraní. Dle závěrů soudobé judikatury je pro uzavření spotřebitelské smlouvy jiný typ elektronického podpisu (dříve prostý elektronický podpis) postačující a nevyžaduje se kvalifikovaný elektronický podpis*."
[398] Rozhodnutí Okresního soudu v Hodoníně ze dne 24. 11. 2022, sp. zn. 13 C 163/2022.
[399] Rozhodnutí Krajského soudu v Ostravě ze dne 28. 1. 2016, sp. zn. 37 ICm 4495/2014.
[400] Rozhodnutí Krajského soudu v Brně ze dne 5. 6. 2017, sp. zn. 33 Icm 547/2016.
[401] Rozhodnutí Obvodního soudu pro Prahu 6 ze dne 27. 10. 2021, sp. zn. 6 C 375/2021. Konkrétně „*za použití prostředků komunikace na dálku tak, že žalovaný prostřednictvím těchto prostředků požádal elektronickým podepsáním návrhu smlouvy žalobkyni o její uzavření s tím, že elektronický podpis tohoto návrhu byl připojen na základě zadaného kódu, který byl žalovanému zaslán prostřednictvím SMS a žalobkyně tento návrh akceptovala opatřením smlouvy elektronickým podpisem pověřeného pracovníka žalobkyně.*"
[402] Rozhodnutí Okresního soudu v Mladé Boleslavi ze dne 24. 5. 2022, sp. zn. 15 C 89/2022.

Okresní soud v Chomutově ve svém rozhodnutí[403] posuzoval, zda smlouva byla s podpisem spojena, resp. zda data v elektronické podobě (podpis) byla k jiným datům v elektronické podobě (smlouva) připojena. Soud tak správně připouští možnost podpisu i prostřednictvím prostého elektronického podpisu, avšak v tomto konkrétním případě nebylo ze strany žalobce uneseno důkazní břemeno o jeho připojení. Ve vztahu k otázce platnosti písemné formy právního jednání ovšem soud v daném rozhodnutí nad rámec zákonných požadavků požaduje integritu dokumentu.

Opačně ovšem rozhodl Okresní soud v Karviné v obdobném skutkovém případě. Ten ve svém rozhodnutí[404] dospěl k závěru, že PIN kód uvedený na smlouvě dostačujícím podpisem není, neboť nesplňuje podmínky stanovené pro kvalifikovaný (zaručený) elektronický podpis, a proto shledal smlouvu neplatnou. K obdobnému závěru dospěl ve svém rozhodnutí[405] i soud v České Lípě. Autor této práce s těmito rozhodnutími nesouhlasí, neboť není pravdou, že pouze kvalifikovaný (zaručený) elektronický podpis je jedinou formou podpisu vyžadovanou k písemné formě právního jednání. Tento fakt je navíc zapotřebí odlišovat od účinků vlastnoručního podpisu, resp. jeho elektronického ekvivalentu.

Ke stejnému závěru dospěl ve svém rozhodnutí[406] i Okresní soud v Berouně. V posuzovaném případě byla smlouva uzavřena zadáním podpisového SMS kódu do aplikace žalobkyně a následně zaslána na email žalovanému.[407] Soud však v tomto případě neměl za prokázané, že byla podepsána právě tato smlouva. Soud navíc kladl na podpis požadavky dle článku 26 nařízení eIDAS.[408] Závěry autora k předešlému rozhodnutí tak platí obdobně. Ani Okresní soud

---

[403] Rozhodnutí Okresního soudu v Chomutově ze dne 12. 1. 2022, sp. zn. 7 C 339/2021. Soud uvedl, že „*samotná úvěrová smlouva v elektronické podobě neobsahuje žádné záznamy o tom, že by k němu byly připojeny podpisy (tj. data v elektronické podobě, která by byla připojena k jiným datům – smlouvě), tj. žádné záznamy o tom, že by elektronická smlouva obsahovala kvalifikovaný či uznávaný elektronický podpis a ani údaje o připojení jakýchkoliv dalších dat ke smlouvě, jež by mohly být považovány za podpis. Kód měl být žalovaným připojen na smlouvu, ze smlouvy předložené žalobkyní však nevyplývá, kdy a jak k ní byl výše uvedený kód připojen, a že poté, kdy k ní byl tento kód připojen, je možné zjistit jakoukoliv dodatečnou změnu smlouvy. Dále nebylo prokázáno, že by kód byl připojen právě žalovaným, a že by právě žalovaný byl tím, kdo jej na smlouvu připojil.“* (zvýraznění přidáno autorem)

[404] Rozhodnutí Okresního soudu v Karviné ze dne 14. 1. 2022, sp. zn. 24 C 233/2021.

[405] Rozhodnutí Okresního soudu v České Lípě ze dne 17. 8. 2022, sp. zn. 48 C 189/2022.

[406] Rozhodnutí Okresního soudu v Berouně ze dne 21. 12. 2021, sp. zn. 18 C 225/2021.

[407] Konkrétně: „*žalovaný vyplnil požadované údaje a po automatizovaném schvalovacím procesu byla žádost žalovaného schválena. Žalobkyně následně žalovanému zaslala podpisový SMS kód na telefonní číslo, které žalovaný uvedl ve své žádosti a na internetových stránkách se objevil text smlouvy. Smlouva byla uzavřena po zadání podpisového SMS kódu žalovaným do aplikace žalobkyně a žalovanému zaslána na e-mailovou adresu, kterou žalovaný uvedl v žádosti*.“

[408] Soud uvedl, že „*Samotná úvěrová smlouva v elektronické podobě – tj. soudu předložený PDF dokument – neobsahuje žádné záznamy o tom, že by k němu byly připojeny podpisy (tj. data v elektronické podobě, která by byla připojena k jiným datům – smlouvě), tj. žádné záznamy o tom, že by elektronická smlouva obsahovala kvalifikovaný či uznávaný elektronický podpis (a ani údaje o připojení jakýchkoliv dalších dat ke smlouvě, jež by*

v Českém Krumlově,[409] Městský soud v Brně,[410] Obvodní soud pro Prahu 3,[411] nebo Krajský soud v Praze[412] ve svých rozhodnutích neshledaly kód zaslaný formou SMS na telefonní číslo jako dostatečný.

Opět se tedy můžeme setkat s rozhodnutími soudů, které si vzájemně odporují. Dle názoru autora této práce je vzhledem k definici prostého elektronického podpisu a splnění náležitosti písemné formy, jak byly rozebrány v této práci výše, zapotřebí dojít k názoru, že prostý podpis může být tvořen i kódem zaslaným prostřednictvím SMS v podobě dvoufaktorového ověření. Naopak má, dle názoru autora této práce, tato forma prostého elektronické podpisu vyšší důkazní sílu oproti jednodušším formám prostého elektronického podpisu, je však zapotřebí z důkazního hlediska zkoumat konkrétní okolnosti spojení (dat v elektronické podobě) s podepisovaným obsahem (jinými daty v elektronické podobě).

5.1.8. Podpis myší do prázdného pole na internetové stránce

Městský soud se ve svém rozhodnutí[413] zabýval platností postoupení smlouvy, kdy si její účastníci zvolili písemnou formu. V tomto případě byla smlouva podepsána pomocí myši do prázdného pole na obrazovce a podpis pak byl přenesen datovou formou na předmětný dokument (formulář), který dle soudu účastnice přímo nepodepsala. Hlavním problémem byla dle soudu nedostatečná identita podepisující a neprokázání projevu vůle k uzavření smlouvy.

mohly být považovány za podpis ve smyslu ustanovení článku 26 eIDAS).“ Soud dále uvedl, že mu není „*zjevné, jak je možné do elektronického dokumentu pojmout vlastnoruční podpis, tedy opět může jíž pouze o grafickou podobu, tentokrát vlastnoručního podpisu, která byla vložena přímo do dat dokumentu, nikoliv k datům obsahujícím smlouvu připojený.“*

[409] Rozhodnutí Okresního soudu v Českém Krumlově ze dne 26. 11. 2021, sp. zn. 2 C 164/2021.

[410] Rozhodnutí Městského soudu v Brně ze dne 19. 9. 2023, č. j. 47 C 178/2023 – 30, ze dne 23. 5. 2023, č. j. 47 C 92/2023 – 39, nebo ze dne 03. 2. 2023, č. j. 47 C 85/2022 – 54.

[411] Rozhodnutí Obvodního soudu pro Prahu 3 ze dne 16. 8. 2022, sp. zn. 19 C 230/2022 nebo ze dne 4. dubna 2023 č. j. 16 C 16/2023-28.

[412] Rozhodnutí Krajského soudu v Praze ze dne 20. 1. 2022, sp. zn. 24 Co 243/2021.

[413] Rozhodnutí Městského soudu v Praze ze dne 8. 7. 2020, sp. zn. 18 Co 187/2020. Soud konkrétně uvedl: „*že jen tyto podpisy (kvalifikované, zaručené a uznávané, pozn. autora) umožňují českému soudu identifikovat podepsanou osobu se značnou úrovní důvěry. Jiné elektronické podpisy již identitu podepsané osoby nikterak nezaručují. Tímto jiným, tj. nezaručeným elektronickým podpisem je i údajný podpis postupitelky nároku D. J.G., který byl de facto jako obrázek podpisu sejmut z jiné (elektronické) listiny a následně vložen do písemnosti označené jako postupní smlouva. Fakticky se tak nemuselo jednat ani o podpis osoby uvedené jako postupitelka a tento obrázek podpisu mohl být dokonce sejmut z jiného dokumentu a bez vůle uvedené osoby podepsat postupní smlouvu mohl být vložen do předmětného dokumentu označeného jako postupní smlouva. Zásadní tvrzení žalobce, že poškozená osoba projevila vůli na něj převést pohledávku tvrzenou postupní elektronickou smlouvou, tedy prokázáno nebylo*.“

K obdobným závěrům dospěl i Krajský soud v Ostravě,[414] Okresní soud v Novém Jičíně[415] nebo Obvodní soud pro Prahu 6.[416]

Soudy se ovšem nezabývaly definicí prostého elektronického podpisu. Dle názoru autora této práce tak nelze závěry z těchto rozhodnutí generalizovat, ale vnímat je prizmatem neunesení důkazního břemene v daném konkrétním případě.[417] Jinými slovy, soudy by měly v případě prostých elektronických podpisů požadovat důkazy o dalších okolnostech, pouze pokud je pravost podpisu zpochybněna.[418]

5.1.9. Prostý elektronický podpis je (ne)dostačující ke splnění písemné formy

Okresní soud v Kladně ve svém rozhodnutí[419] řešil obdobnou situaci, kdy se žalovaný nejprve elektronicky registroval jako zájemce o půjčku vyplněním formuláře na internetových stránkách a vyplnil své identifikační údaje. Pod takto získanou elektronickou identitou pak elektronicky (kliknutím) vybral požadovanou částku a vyjádřil i souhlas se smluvními podmínkami na předem připraveném předtisku smlouvy a obchodních podmínek.

Vzhledem k tomu, že nebyla stranami ani zákonem vyžadována písemná forma, soud se nezabýval tím, zda smlouva byla uzavřena elektronicky v písemné formě alespoň v souladu s § 562 občanského zákoníku. Uvedl však, že nebyly využity žádné elektronické služby důvěryhodné identifikace a autentizace[420] a že z předložených dokumentů nevyplývá, zda k danému právnímu jednání došlo v elektronickém systému, v němž jsou záznamy prováděny systematicky a posloupně a jsou chráněny proti změnám, a že je zřejmé, že smlouva nebyla podepsána ve smyslu § 561 občanského zákoníku. Soud se však v tomto případě spokojil s faktem, že výplata finančních prostředků byla prokázána výpisem z účtu právního předchůdce žalobkyně. Samotná registrace v systému by dle soudu k uzavření smlouva však nepostačovala.[421]

---

[414] Rozhodnutí Krajského soudu v Ostravě ze dne 28. března 2022, č.j. 11 Co 338/2020–161.
[415] Rozhodnutí Okresního soudu v Novém Jičíně ze dne 29. 9. 2020, č. j. 12 C 23/2020-86 a sp. zn. 7 C 261/2019.
[416] Rozhodnutí Obvodního soudu pro Prahu 6 sp. zn. 18 C 79/2019, 18 C 29/2019.
[417] Srov. ustanovení § 565 občanského zákoníku.
[418] Stejně jako např. v případě podpisu vlastnoručního.
[419] Rozhodnutí Okresního soudu v Kladně ze dne 31. 8. 2021, sp. zn. 208 C 115/2021.
[420] V úrovni vysoké nebo alespoň značné.
[421] Dle soudu „*tím byla potvrzena totožnost osoby, která registraci provedla, jakož i skutečnost, že podle sjednaných podmínek převzala půjčenou částku, jinak by totiž žalobkyně neměla důvod konkrétní osobě peníze zasílat a žalovaný neměl důvod peníze přebírat, zejména pokud sám žalovaný nic netvrdil o jiném důvodu či o jiných podmínkách pro převzetí peněz v daném místě a čase. Je tedy zřejmé, že důvodem plnění byla v dokumentaci popsaná půjčka. Samotná (zcela anonymní) registrace (elektronická identita) by naproti tomu pro uzavření*

Ačkoli by bylo možné z argumentace soudu usuzovat, že by prostý elektronický podpis nebyl dostačující, v tomto případě se soud spokojil vzhledem k chybějícímu požadavku písemné formy s ostatními důkazy. Obdobně pak rozhodl Okresní soud v Plzni.[422] Jak bylo již zmíněno výše v této práci, je vždy zapotřebí přihlížet při posouzení platnosti právního jednání v písemné formě i k ostatním okolnostem, a ne pouze k podpisu samotnému. K opačnému závěru ohledně identifikace uživatele zasláním bankovní platby ovšem dospěl Okresní soud ve Zlíně[423] nebo Okresní soud v Nymburce,[424] které ve svých rozhodnutích rozlišovaly mezi autentizací dané osoby v systému a potvrzením obsahu smlouvy.

K obdobným závěrům dospěl Obvodní soud pro Prahu 10. Ten ve svém rozhodnutí[425] uvedl, že prostý elektronický podpis nelze použít k podepsání písemného právního jednání, a to z důvodu nejednoznačného ověření identity podepsané osoby a nemožnosti zjistit následnou změnu podepsaných dat. Jak bylo rozebráno výše, jednoznačné ověření identity a zachování integrity nejsou náležitostmi všech elektronických podpisů. Stejně není na místě ani argument soudu o tom, že v případě kvalifikovaného podpisu lze vždy spojit podpis s konkrétní podepisující osobou, resp. že lze osobu vždy jednoznačně bez dalšího identifikovat.[426]

Soud v rozhodnutí dále argumentoval, že pro veškeré procesní úkony je vyžadován uznávaný elektronický podpis, a to samé by mělo platit pro úkony hmotněprávní.[427] Autor této práce

---

smlouvy právě se žalovaným nepochybně v dostatečné míře nesvědčila, stejně jako tvrzené (a jinak nedoložené) uzavření smlouvy kliknutím."

[422] Rozhodnutí Okresního soud v Plzni ze dne 30. 8. 2023, sp. zn. 16 C 77/2023.

[423] Rozhodnutí Okresního soudu ve Zlíně ze dne 10. 11. 2021, sp. zn. 26 C 62/2021.

[424] Rozhodnutí Okresního soudu v Nymburce ze dne 14. 8. 2023, sp. zn. 6 C 137/2023.

[425] Rozhodnutí Obvodního soudu pro Prahu 10 ze dne 20. 12. 2021, sp. zn. 9 C 104/2021. Konkrétně soud uvedl „*že písemné právní jednání (písemnost) v elektronické podobě nelze platně podepsat tzv. prostým elektronickým podpisem, ale pouze zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu a vytvořeným pomocí prostředku pro bezpečné vytváření podpisu, resp. uznávaným elektronickým podpisem. Jiná (nižší) úroveň elektronického podpisu zjevně neumožňuje dosáhnout na základě tohoto elektronické podpisu „jednoznačného ověření" identity podepsané osoby a už vůbec neumožňuje zjistit jakoukoli následnou změnu dat. Uvedená jednoznačnost je ale nejen zákonným znakem všech úrovní elektronického podpisu, ale i účelem, proč je podpis vyžadován, obdobně jako u vlastnoručního podpisu. To vše s tím rozdílem, že nyní užívaná technologie elektronického podepisování na bázi asymetrické kryptografie skutečně umožňuje při plnění zákonných požadavků na užívání dat a prostředků pro vytváření elektronického podpisu dosáhnout ještě vyšší úroveň jistoty o totožnosti podepsané osoby, než v případě vlastnoručního podpisu. Jde právě o zjištění v rovině „jednoznačnosti" (100%, tedy ano/ne), nikoli v rovině převažující pravděpodobnosti. […] Tato technologie umožňuje prostřednictvím asymetrické kryptografie jednoznačně spojit elektronický podpis (vypočítané číslo) s konkrétní podepisující osobou prostřednictvím dat pro vytváření podpisu (soukromého klíče), které podepisující osoba může a musí udržet pod svou výhradní kontrolou (jako tajemství). Je také umožněno v případě připojení takového elektronického podpisu k datové zprávě zjistit (při ověření elektronického podpisu) jakoukoliv následnou změnu podepsaných dat, což jiné technologie zatím neumožňují."* (podtržení přidáno autorem).

[426] K tomu srov. např. DONÁT, Josef, Jan TOMÍŠEK a Ivan FENCL. *Je publikovaná judikatura k elektronickým podpisům skutečně relevantní?*, op. cit 26 a kapitolu 3.1.

[427] Konkrétně soud uvedl, že „*z hlediska výkladu § 561 odst. 1 o. z., ve spojení s adaptačním zákonem nelze odhlédnout ani od toho, že pro veškeré procesní úkony je v českém právním řádu podle § 5 a § 6 adaptačního*

tento argument shledává jako nepřesvědčivý. Pokud by se totiž měl argument aplikovat, byla by nadbytečná i úprava zaručeného elektronického podpisu, který je výslovně upraven v ZSVD i nařízení eIDAS. Podle soudu se pak v případě vypsání jména a příjmení v datové zprávě (emailu), zadání přihlašovacího jména a hesla, odeslání SMS zprávy, telefonického potvrzení nebo odeslání finančních prostředků z určitého účtu nejedná o elektronický podpis, neboť není umožněna jednoznačná identifikace podepsané osoby a není zajištěna integrita dokumentu.[428]

Na závěr soud uvádí, že písemná forma je zachována pouze při zachycení jejího obsahu a určení jednající osoby. Navíc dle názoru soudu mohou být přihlašovací údaje použity kýmkoli.[429] Závěr soudu tak lze chápat jako vzájemnou aplikaci ustanovení § 561 a § 562 OZ, nikoli ve vztahu speciality, jak jej chápe širší odborná veřejnost.[430] Ani v tomto prizmatu se však nelze ztotožnit s výše uvedenými argumenty, jak bylo rozebráno pod jednotlivými pasážemi rozhodnutí.

---

zákona a podle všech procesních předpisů vyžadován tzv. uznávaný elektronický podpis, tedy ještě vyšší kvalita elektronického podpisu, než je zaručený elektronický podpis. Je proto logické, aby pro hmotně právní jednání v elektronické podobě, kterým se právní vztahy v písemné formě zakládají, mění nebo ruší, byla vyžadována nejméně stejná kvalita elektronického podpisu jako pro procesně právní jednání, kterým se práva a povinnosti pouze vymáhají." (podtržení přidáno autorem).

[428] Soud konkrétně uvedl: *„proto nelze za platný elektronický podpis považovat vypsání jména a příjmení v datové zprávě (emailu, např. formou tzv. emailové patičky), nebo uvedení přihlašovacího jména (tzv. ID nebo login) a zadání hesla ([příjmení]) spojené s následným„ odkliknutím" určitého dokumentu na konkrétní internetové stránce, popřípadě odeslání SMS zprávy z mobilního telefonu určité osoby, telefonické potvrzení souhlasu nebo identity (prokazované nahrávkou hlasu), odeslání finančních prostředků z určitého účtu, zjištění IP adresy použité pro připojení k internetu a podobně. Nic z toho totiž z hlediska technologických vlastností samo o sobě objektivně neumožňuje jednoznačnou identifikaci podepsané osoby, vytvoření takových „podpisů" není pod výhradní kontrolou konkrétní (identifikované a autentizované) osoby. Nejsou také s podepsanými daty nijak pevně technicky spojeny, natož ve smyslu ověření integrity (nezměnitelnosti) podepsaných dat (zpětného určení obsahu jednání). Opačným výkladem by za písemné právní jednání opatřené elektronickým podpisem bylo možné považovat nejen prosté emaily, SMS zprávy, ale i sdělení na sociálních i komunikačních sítích nejrůznějšího druhu (např. Facebook, WhatsApp apod.), kde jednotlivé fyzické osoby mohou vystupovat pod smyšlenými nebo cizími identitami, tyto libovolně měnit či množit. Bylo by nutné rezignovat na požadavek jistoty o zachování původního obsahu písemného jednání i na požadavek jistoty o podepsané osobě (jednoznačnost). Ve světě elektronických dokumentů je navíc padělání identity a nezjistitelné změny obsahu dokumentů mnohem snazší, než ve světě listinných dokumentů a tomu musí odpovídat i výklad příslušných ustanovení tak, aby byl zachován účel a smysl zákona (§ 2 o. z.)."* (podtržení přidáno autorem).

[429] Soud uvedl, že *„při právním jednání učiněném elektronickými prostředky je písemná forma zachována umožňuje-li zachycení jejího obsahu a určení jednající osoby. V daném případě byly přihlašovací údaje známy jak žalovanému, tak i právní předchůdkyni žalobkyně, případně správci sítě. Ze skutečnosti, že byly případně přihlašovací údaje zadány do webové aplikace, proto nelze s jistotou dovozovat, že je tam zadal právě žalovaný. Jestliže nebylo možno určit jednající osobu, nebyla dodržena písemná forma smlouvy o spotřebitelském úvěru a právní předchůdkyni žalobkyně, jakož ani následně žalobkyni, nevznikl nárok na zaplacení jiných částek než jistiny dluhu*." (podtržení přidáno autorem).

[430] K tomu srov. kapitolu 4.1.6.

Ani v rozhodnutí Okresního soudu v Berouně[431], Okresního soudu v České Lípě[432], Krajského soudu v Praze,[433] Krajského soudu v Plzni[434] či Krajského soudu v Ústí nad Labem[435] není prostý elektronický podpis soudem shledán jako dostatečný ke splnění písemné formy právního jednání. Proti nim však stojí např. rozhodnutí Krajského soudu v Českých Budějovicích[436] či Krajského soudu v Ústí nad Labem.[437]

Okresní soud ve Frýdku Místku pak ve svém rozhodnutí[438] dospěl k závěru, že smlouva podepsaná pouze číselným kódem nesplňuje zákonné náležitosti, neboť postrádá autentizační či verifikační prvek. Dle tohoto rozhodnutí tedy nepostačí jako důkaz text smlouvy jako takový, ale je potřeba prokázat jeho přijetí.

Okresní soud v Jihlavě ve svém rozhodnutí[439] shledal jako neplatnou smlouvu v jiném formátu, než ve kterém byla uzavřena, neboť nebyla jasná autenticita dokumentu. Je proto vhodné nastavit interní systémy na správu smluvní dokumentace tak, aby podepsané dokumenty byly ve finální formě.

[431] Rozhodnutí Okresního soudu v Berouně ze dne 28. 12. 2021, sp. zn. 10 C 305/2021.
[432] Rozhodnutí Okresního soudu v České Lípě ze dne 20. 10. 2021, sp. zn. 48 C 347/2021.
[433] Rozhodnutí Krajského soudu v Praze sp. zn. 27 Co 327/2018, 28 Co 387/2015, In: PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra, op. cit. 9.
[434] Rozhodnutí Krajského soudu v Plzni, sp. zn. 64 Co 485/2015, In: PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra, op. cit. 9.
[435] Rozhodnutí Krajského soudu v Ústí nad Labem, sp. zn. 10 Co 577/2015, sp. zn. 9 Co 702/2014, In: PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra, op. cit. 9.
[436] Rozhodnutí Krajského soudu v Českých Budějovicích ze dne 27. 3. 2015, sp. zn. 24 Co 696/2015.
[437] Rozhodnutí Krajského soudu v Ústí nad Labem, sp. zn. 14 Co 268/2014, sp. zn. 11 Co 703/2014, In: PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra, op. cit. 9.
[438] Rozhodnutí Okresního soudu ve Frýdku Místku ze dne 08. 11. 2022, sp. zn. 16 C 208/2022. Konkrétně soud uvedl, že „*smlouva o úvěru postrádá podpis žalovaného i mechanický prostředek podpis nahrazující. Zahrnuje pouze číselný kód, který měl podle žalobkyně podpis nahradit. Avšak elektronický dokument zachycující úvěrovou smlouvu postrádá jakýkoli autentizační či verifikační prvek a zároveň žalobkyně nepředložila žádný důkaz, jenž by zachycoval proces kontraktace*."
[439] Rozhodnutí Okresního soudu v Jihlavě ze dne 19. 9. 2023, sp. zn. 18 C 81/2023. Konkrétně soud uvedl, že „*žalobkyně soudu předložila znění předmětné smlouvy ve formátu elektronického souboru.pdf, tedy v jiném formátu, než v jakém měla být smlouva v prostředí webového rozhraní uzavřena. Z této skutečnosti nelze dospět k závěru, že znění této smlouvy v okamžiku její akceptace žalovaným bylo totožné se zněním poskytnutým soudu, tudíž že nedošlo k jeho následné změně. Není totiž zřejmé, kdo, kdy a jak tyto dokumenty vytvořil. Žalobkyně tudíž neprokázala, že forma jednání, kterou zvolila, umožnila zachycení obsahu a jeho nezměnitelnost. V takovém případě je však nutno uzavřít, že nebyla prokázána vůle žalovaného uzavřít předmětnou smlouvu o úvěru v podobě předložené soudu, neboť tato smlouva nebyla žalovaným podepsána, a že současně nebyla dodržena písemná forma smlouvy*."

Okresní soud Brno-venkov ve svém rozhodnutí[440] neshledal jako dostatečné k potvrzení obsahu smlouvy logy, a to z důvodu, že z výpisu databázového logu není zjistitelný obsah smlouvy ani projev vůle.

Dle Okresního soudu v Mostě[441] není k dodržení písemné formy dostatečný autorizační kód, ale biometrický podpis již ano. Dle autora této práce soud opět zaměňuje důkazní účinky jednotlivých podpisů, neboť jak bylo rozebráno v kapitole 3.5, biometrický podpis je z právního hlediska prostým elektronickým podpisem stejně jako autorizační kód.

5.1.10. Neplatné elektronické podpisy a platně uzavřená smlouva

Okresní soud v Jihlavě ve svém rozhodnutí[442] shledal smlouvu za platně uzavřenou v písemné formě v situaci, kdy byly připojené elektronické podpisy neplatné. Dle soudu totiž bylo potvrzeno, že byla zachována autenticita dokumentu a aktivita v mobilní aplikaci odpovídala době vzniku podpisu. Soud tak správně přihlédnul k souvisejícím okolnostem, ze kterých dovodil dostatečné důkazy potřebné k prokázání nutných okolností v daném případě.

5.1.11. Záměna požadavku písemné formy a identifikace

Okresní soud v Chomutově ve svém rozhodnutí[443] specificky dovodil nedostatek písemné formy z nedostatku jednoznačné identifikace ve webovém rozhraní Správce financí. Soud tak

---

[440] Rozhodnutí Okresního soudu Brno-venkov ze dne 15. 11. 2022, sp. zn. 41 C 150/2022. Konkrétně soud uvedl, že „*v posuzovaném případě však žalobkyní navrženými důkazy nelze prokázat, že by k jí tvrzenému průběhu událostí (žalovaná uzavřela smlouvu zadáním zaslaného SMS kódu zaslaného žalobkyní na telefonní číslo žalované) došlo. Výpis z interního systému žalobkyně projev vůle žalované k uzavření žalobkyní tvrzené smlouvy o úvěru se, žalobkyní tvrzeným obsahem, nezachycuje a její uzavření právě se žalovanou nijak neprokazuje. Z výpisu z databázového logu žalobkyně není zjistitelný obsah žalobkyní tvrzené smlouvy o úvěru, zjistitelné není ani to, že s tvrzeným zněním smlouvy o úvěru byla žalovaná seznámena a že projevila vůči žalobkyni vůli k jejímu zavření se žalobkyní tvrzeným obsahem. Žalobkyní navržené důkazy neprokazují, že by žalovaná (elektronickým) podpisem vyjádřila svůj souhlas s jí tvrzenou smlouvou a že by jí tedy byla vázána*."

[441] Rozhodnutí Okresního soudu v Mostě ze dne 7. 9. 2021, sp. zn. 32 C 59/2021.

[442] Rozhodnutí Okresního soudu v Jihlavě ze dne 26. 1. 2022, sp. zn. 20 C 214/2021. Konkrétně soud uvedl, že „*ačkoliv elektronické podpisy jsou v elektronické verzi smlouvy označené jako neznámé, resp. neplatné, považuje soud za podstatné to, že potvrzují, že se smlouva od jejich aplikace nezměnila. Současně podpis žalované časově koreluje její aktivitě v mobilní aplikaci [jméno] [příjmení]. Pokud současně poskytnutým úvěrem byl z valné části hrazen jiný úvěr žalované, který do té doby řádně splácela ze svého běžného účtu, je vysoce pravděpodobné, že smlouvu opravdu podepsala žalovaná. Byly tak dodrženy požadavky § 562 odst. 1 občanského zákoníku*."

[443] Rozhodnutí Okresního soudu v Chomutově ze dne 7. 12. 2022, sp. zn. 9 C 125/2022. Soud uvedl, že „*v projednávané věci k uzavření smlouvy mělo dojít prostřednictvím komunikace na dálku, a to prostřednictvím Správce financí, webového rozhraní žalobkyně, jenž je obdobou internetového bankovnictví. Tato forma uzavírání smluv nesplňuje požadavek na jednoznačnou identifikaci osoby, která smlouvu sjednává, neboť <u>se tak děje bez uznávaného elektronického podpisu</u>, respektive jiného jednoznačného identifikátoru v rámci uceleného systému zabezpečených internetových stránek. V projednávaném případě tak smlouva, v níž měl být sjednán tvrzený úvěr, <u>trpí nedostatkem písemné formy</u>. A protože zákon spojuje tuto podmínku s platností právního jednání (§ 561 odst. 1 ObčZ), je podle názoru soudu <u>smlouva o úvěru neplatná</u>*" (zvýraznění přidáno autorem).

zaměnil požadavek identifikace podepisující osoby s požadavky elektronického podpisu, jehož nižší formy tento požadavek neobsahují.

5.2. Návrh sjednocení přístupu českých soudů

Výše popsané rozpory judikatury vytvářejí značnou právní nejistotu. Řešením by mohlo být sjednocující stanovisko Nejvyššího soudu, které však dle názorů některých soudců obecně není vhodnou praxí, zejména s ohledem na západní jurisdikce, které od podobných postupů upouštějí. Navíc by takové stanovisko s největší pravděpodobností znamenalo i výklad nařízení eIDAS, který by však vyžadoval objasnění v rámci řízení o předběžné otázce u Soudního dvora EU.

Je také obtížné přesně dovodit, jaký je poměr případů, kdy soud prostý elektronický podpis shledá jako dostačující ke splnění písemné formy právního jednání, a kdy nikoli, neboť v mnoha případech soud závěr o splnění požadavků může mít za prokázaný bez dalšího a ve svých rozhodnutích se k této problematice nevyjadřovat. U úvěrových smluv, které jsou nejčastěji předmětem soudních rozhodnutí, hraje navíc roli další aspekt spotřebitele a zvláštní nutnosti identifikace pro posouzení úvěru. Soudy v praxi usilují o ochranu spotřebitele, nicméně cestou, kterou nelze považovat za vhodnou, tj. nesprávným hodnocením písemného právního jednání jako neplatné, aniž by pro to byl podklad v právu.

Z výše uvedených závěrů lze abstrahovat následující argumentaci, která se v rozhodnutích opakuje. Aby byla splněna písemná forma právního jednání, je nutné připojení vyšší formy elektronického podpisu. Tento závěr byl vyvrácen v kapitole 3.4 této práce. Dále z rozhodnutí vyplývá požadavek identifikace jednající osoby. Jak bylo rozebráno v kapitolách 3.1 a 4.4, úplná identifikace není vždy jistá ani u nejvyšší formy elektronického podpisu (kvalifikované) či u vlastnoručního podpisu a není zákonnou náležitostí u prostého elektronického podpisu. I tento závěr judikatury je tak nesprávný. Soudy také v části rozhodnutí argumentují tím, že podpis má zajistit autenticitu (integritu) dokumentu. Ta je sice žádoucí, nicméně opět není zákonnou náležitostí prostého elektronického podpisu, a jedná se tak o otázku důkazní, nikoli platnosti právního jednání. Dalším požadavkem kladeným na všechny formy písemného právního jednání je připojení elektronického podpisu k danému dokumentu, resp. datům v elektronické podobě. Tento argument je samozřejmě relevantní, avšak z pohledu projevu vůle samotné a unesení důkazního břemene. Není nezbytnou náležitostí prostého elektronického podpisu jako takového.

Právní úprava je v současném českém právním řádu dle autora této práce dostatečná. V případě, kdy se Nejvyšší soud ČR k vydání sjednocujícího stanoviska staví zdrženlivě, připadá v úvahu pouze jeho rozhodnutí, které by předmětné otázky stanovilo na jisto. Avšak ani samotné rozhodnutí by nebylo pramenem práva, nicméně ostatní soudy by jej měly brát v potaz a rozhodovat obdobně.[444] Žádoucí je také postupná erudice všech soudních instancí širší odbornou i veřejnou diskuzí o tomto tématu, která umožní sjednocení jejich praxe.

[444] § 13 občanského zákoníku.

6. Perspektiva elektronických podpisů v budoucím vývoji

Na některé z nejasností vyplývajících z předchozích kapitol reagují návrhy revizí právní úprava, a to jak na úrovni Evropské Unie, tak v českém prostředí. Nejedná se však o legislativní změny ve vztahu k prostým elektronickým podpisům jako takovým, změny se dotýkají vyšších úrovní podpisů. Nicméně na jejich základě lze očekávat daleko častější využití právě těchto vyšších forem, které by v praxi mohly vést ke zvýšení právní jistoty. Bude však zapotřebí brát o to více v potaz aspekty digitální kontinuity rozebrané v kapitole 4.2.

6.1. Možné dopady eIDAS 2.0

Vzhledem k výše zmíněným problematickým oblastem Evropská Komise od roku 2021 diskutuje o revizi nařízení eIDAS, populárně známé pod označením eIDAS 2.0. V červnu 2021 zveřejnila zprávu o hodnocení,[445] ve které dospěla k závěru, že je „*potřeba zlepšit účelnost, účinnost, soudržnost a relevanci nařízení eIDAS, aby mohlo plnit nové politické cíle, očekávání uživatelů a uspokojit poptávku na trhu i s ohledem na nejnovější vývoj v oblasti digitalizace*“. Zpráva také konstatuje, že „*kromě řešení v oblasti identity, která nespadají do oblasti působnosti nařízení eIDAS, jako jsou řešení nabízená poskytovateli sociálních médií a finančními institucemi, vyvolávají obavy o ochranu soukromí a údajů. Nemohou účinně reagovat na nové požadavky trhu a postrádají přeshraniční dosah, aby byla schopná řešit zvláštní odvětvové potřeby v případech, kdy je identifikace citlivá a vyžaduje vysoký stupeň jistoty*“. Cílem revize eIDAS má dle této zprávy být „*zvýšit jeho účinnost, rozšířit jeho působnost na soukromý sektor a prosazovat důvěryhodné digitální identity pro všechny občany a podniky EU*“.

Cílem navrhované revize nařízení eIDAS[446] je, aby alespoň 80 % občanů mělo do roku 2030 možnost využívat k přístupu ke klíčovým veřejným službám řešení v oblasti digitální identifikace, bezpečnost a kontrola poskytované evropským rámcem digitální identity byly na dostatečné úrovni a byla zajištěna kontrola toho, kdo má přístup ke svému digitálnímu dvojčeti a k jakým konkrétním údajům. V reakci na dynamiku trhů a technologický vývoj navrhovaná revize dále rozšiřuje stávající seznam služeb vytvářejících důvěru v rámci nařízení eIDAS o tři nové kvalifikované služby vytvářející důvěru, a to (i) poskytování služeb elektronické

[445] EVROPSKÁ KOMISE, *ZPRÁVA KOMISE EVROPSKÉMU PARLAMENTU A RADĚ o hodnocení nařízení (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (nařízení eIDAS)*. Dostupná zde: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52021DC0290.

[446] Návrh nařízení Evropského Parlament a Rady, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu.

archivace, (ii) elektronických účetních knih a (iii) správu prostředků pro dálkové vytváření elektronických podpisů a pečetí. Návrh navíc „*znamená posun pro vydavatele řešení v oblasti evropské digitální identity a poskytuje společnou technickou architekturu, referenční rámec a společné normy, které mají být vypracovány ve spolupráci s členskými státy. Harmonizovaný přístup je nezbytný, aby se zabránilo tomu, že vývoj nových řešení v oblasti digitální identity v členských státech způsobí další roztříštěnost vyvolanou používáním odlišných vnitrostátních řešení*".

Dochází také k představení nového institutu evropské digitální peněženky. Na základě konzultací o revizi nařízení eIDAS se zúčastněnými stranami jsou peněženky digitální identity vnímány veřejným a soukromým sektorem jako nejvhodnější nástroj umožňující uživatelům vybrat si, kdy a s kterým soukromým poskytovatelem služeb sdílet různé atributy. Digitální identity založené na digitálních peněženkách bezpečně uložených na mobilních zařízeních byly identifikovány jako hlavní aktivum v hledání řešení schopného obstát v budoucnosti. Soukromý trh (např. Apple, Google, Thales) i vlády se tímto směrem již ubírají. Dle revidovaného neřízení eIDAS bude uživatel použitím evropské peněženky digitální identity moci kontrolovat množství údajů poskytnutých spoléhajícím se stranám a bude informován o atributech požadovaných k poskytování konkrétní služby, aniž by byly dotčeny předpisy o ochraně osobních údajů.[447] Dle recitálu 9 revidovaného nařízení eIDAS by pak všechny evropské peněženky digitální identity měly uživatelům umožnit přeshraniční elektronickou identifikaci a autentizaci online a offline pro přístup k široké škále veřejných a soukromých služeb. Z pohledu této práce je však nejdůležitější možnost vytvářet a používat kvalifikované elektronické podpisy a pečetě, které jsou přijímány v celé EU.[448] To by mělo vést k častějšímu používání vyšších forem elektronických podpisů a nepřímé eliminaci problémů rozebraných v této práci. Naopak ale bude aktuálnější téma dodržování digitální kontinuity, taktéž rozebrané v kapitole 4.2.

Je také zavedena nová kvalifikovaná služba správy prostředků pro vytváření elektronických podpisů na dálku. Tato nová kvalifikovaná služba, jak již název napovídá, má umožnit vytvářet, spravovat a kopírovat data pro vytváření elektronických podpisů jménem podepisující

[447] Zejména nařízení GDPR.
[448] Článek 6a odst. 3 písm. p) návrhu revidované verze nařízení eIDAS.

osoby prostřednictvím kvalifikovaného poskytovatele služeb vytvářejících důvěru, který poskytuje tuto kvalifikovanou službu.[449]

Poskytování služeb elektronické archivace bylo rozebráno v kapitole 4.2.7. Na tomto místě je však vhodné upozornit na to, jaký bude vztah této služby a ustanovení § 562 odst. 2 občanského zákoníku. Dle názoru autora této práce bude nutná v případě kolize norem revize tohoto ustanovení. Návrh revize nařízení je stále v legislativním procesu, na jeho finální znění tak bude nutné ještě vyčkat.

6.2. eDoklady

K vývoji dochází v mezidobí ovšem i v České republice. Zde byla nedávno spuštěna služba eDoklady,[450] která umožňuje nahrání relevantních dokladů do aplikace a následné prokazování totožnosti právě prostřednictvím této aplikace bez nutnosti předložení fyzického dokladu.

Od 20. 1. 2024 je možné do aplikace nahrát jako první doklad občanský průkaz. Tím se lze v první vlně prokazovat před ústředními správními úřady od 1. 7. 2024 u dalších státních orgánů a od 1. 1. 2025 u ostatních orgánů veřejné moci i soukromých osob.[451] Aplikace je tak národní obdobou digitální peněženky ve smyslu revidovaného nařízení eIDAS. Není však doposud jisté, zda bude splňovat jeho náležitosti, či nikoli (avšak lze s největší pravděpodobností očekávat, že ano). Vytváření vyšších forem elektronických podpisů však prozatím aplikace neumožňuje.

[449] Článek 29 odst. 1a návrhu revidované verze nařízení eIDAS.
[450] Více informací lze nalézt zde: https://edoklady.gov.cz.
[451] Kompletní seznam včetně harmonogramu je dostupný zde: https://edoklady.gov.cz/podpora-obcanu/clanky-a-navody/prehled-mist-kde-lze-edoklady-pouzit.

7. Závěr

Autor se v této práci věnoval problematice elektronických právních jednání, která jsou běžnou součástí každodenní praxe a vzhledem k trendu technologického pokroku lze očekávat jejich další rozvoj. I přes fakt, že elektronické podpisy jsou upraveny na úrovni Evropské unie,[452] tak i české národní legislativy[453] již od 90. let 20. století, je v této oblasti řada sporných otázek. Přestože od té doby došlo k novelizaci, novelizovaná úprava je v relevantních aspektech obdobná úpravě předchozí.[454] Řadu rozhodnutí soudů přijatých za předchozí právní úpravy tak lze aplikovat i na současnou úpravu, jak mimo jiné bylo potvrzeno odbornou veřejností i judikaturou.

Současná úprava elektronických podpisů, pečetí a časových razítek je obsažena v nařízení eIDAS a v českém implementačním zákoně, tj. ZSVD. Zatímco elektronické podpisy mohou užívat pouze fyzické osoby a jde o projev právního jednání,[455] elektronické pečetě mohou užívat pouze právnické osoby a slouží k zaručení původu a integrity.[456] Elektronická časová razítka jsou pak důkazem o existenci v čase.[457]

Nařízení eIDAS upravuje kvalifikovaný elektronický podpis, zaručený elektronický podpis a prostý elektronický podpis. ZSVD pak přidává čtvrtou úroveň podpisu v podobě zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu. Nejvíce diskutovaným je prostý elektronický podpis v jeho nejjednodušší podobě (např. uvedením jména na konci emailu či v textovém editoru), a to zejména z pohledu dodržení písemné formy.

Náležitosti písemné formy jsou upraveny v ustanoveních § 561 a § 562 občanského zákoníku. Dle ustanovení § 561 odst. 1 je k právním jednáním v písemné formě zapotřebí podpis jednajícího. Ten může být nahrazen mechanickými prostředky tam, kde je to obvyklé. Ohledně náležitostí podpisu odkazuje ustanovení na ZSVD. Ustanovení § 562 odst. 1 pak stanoví, že je písemná forma zachována i při právním jednání učiněném elektronickými nebo jinými technickými prostředky umožňujícími zachycení jeho obsahu a určení jednající osoby. Ve druhém odstavci je pak stanovena vyvratitelná domněnka spolehlivosti záznamu.

[452] Směrnice EU pro elektronické podpisy.
[453] § 40 občanského zákoníku 1964 a § 24a hospodářského zákoníku.
[454] Nařízení eIDAS naopak pojem elektronického podpisu ještě rozšířilo.
[455] Článek 3 odst. 9 nařízení eIDAS.
[456] Článek 3 odst. 24 a 25 nařízení eIDAS.
[457] Článek 3 odst. 33 nařízení eIDAS.

Právě na tuto problematiku, tedy zda je prostý elektronický podpis dostatečný k dodržení písemné formy právního jednání, směřuje první výzkumná otázka této práce. Dle názorů odborné veřejnosti by měla být odpověď kladná. Vyskytují se však i názory opačné, a to i v určitých soudních rozhodnutích. Vždy totiž záleží na konkrétních okolnostech a prostředcích, jakými byl prostý elektronický podpis vytvořený. Mělo by být vždy jednoznačně prokázáno, jakým způsobem byl elektronický podpis připojen a že se jedná o projev vůle dané osoby. Identifikace osoby, resp. její vysoká míra, však není náležitostí prostého elektronického podpisu a pro platné právní jednání může vyplývat z jiných okolností. Právě identifikace vyplývající přímo z podpisu bývá často odbornou veřejností a některými soudními rozhodnutími nesprávně vyžadována. Dalším důležitým aspektem je pak podepisování finální verze dat v elektronické podobě.

Jako podkategorie prostého elektronického podpisu byl rozebrán i biometrický podpis, který může mít mnoho podob. S ním je pak spojena ve většině případů větší míra jistoty o určitelnosti konkrétní osoby, na druhé straně vystávají otázky spojené s ochranou osobních údajů a s ní spojenou zásadou minimalizace. S biometrickým podpisem je také spojeno vyšší riziko v případě jeho zneužití, neboť data bývají zpravidla po dobu života člověka neměnná, a problematika jeho ověření. Je proto vždy vhodné zvážit konkrétní okolnosti, pro které má být podpis použit.

Druhá výzkumná otázka, tedy zda může být písemná forma právního jednání splněna i bez připojení podpisu, pak směřuje právě na ustanovení § 562 občanského zákoníku. Ačkoli by se odpověď mohla zdát jako jednoznačná, s ohledem na nejasný vztah ustanovení § 561 a § 562 občanského zákoníku tomu tak nutně není. Z převažujících názorů a některých soudních rozhodnutí lze však mít za to, že jsou tato ustanovení ve vztahu speciality. Mělo by tedy být možné písemně právně jednat i bez připojení podpisu, avšak za splnění zákonných podmínek, tedy při zachycení obsahu a určení jednající osoby. Jak bylo rozebráno v této práci, bohužel ani tyto pojmy, resp. jejich náležitosti, nejsou v praxi vždy zcela jasné.

Není-li požadavek dán zákonem, je na subjektech soukromého práva, jakou formu právního jednání si sjednají. Obecně lze tak doporučit vyšší míru elektronických podpisů, nejlépe kvalifikovaných, u právně významných jednáních s přihlédnutím k praktickým a ekonomickým aspektům. S tímto tématem souvisí třetí výzkumná otázka, tedy jaké jsou výhody vyšších úrovní elektronických podpisů oproti prostému elektronickému podpisu a zda jsou vždy brány v potaz. Kvalifikovaný podpis s připojením kvalifikovaného elektronického

razítka je nařízením eIDAS jako jediná forma podpisu uznán s účinky vlastnoručního podpisu (toto však může být na úrovni členských států modifikováno, ZSVD k této problematice mlčí), a měl by zajistit funkci integrity podepsaných dat a identifikaci podepisující osoby.[458]

S vyššími úrovněmi elektronických podpisů pak úzce souvisí udržování digitální kontinuity, která je v praxi často zanedbávána. Většina orgánů veřejné moci anebo soukromých subjektů se často spoléhá na pouhý automatizovaný výstup určitých programů či systému ověřujícího platnost elektronických podpisů, pečetí či razítek bez dalšího, což může vést k nepřesným výstupům a závažným následkům. V kapitole 4.2. byly rozebrány všechny relevantní aspekty, zejména rozlišena aktuální a potenciální digitální kontinuita, integrita a autenticita dokumentů, ověřování elektronických podpisů, vyvratitelná domněnka spolehlivosti záznamu, služba archivace, a to i ve světle navrhované novely nařízení eIDAS, elektronická časová razítka a kontejnery, princip asymetrické kryptografie a s ním související platnost certifikátů a času připojení. Tyto aspekty však dle názoru autora této práce nejsou v praxi zkoumány do detailu. Odpověď na druhou část výzkumné otázky je tedy negativní.

V práci byly také popsány jednotlivé typy online smluv, konkrétně *click-wrap*, *click-through*, *browse-wrap* a *shrink wrap* smlouvy. Až na poslední kategorii mohou podle odborných názorů a judikatury tyto typy smluv splňovat písemnou formu právního jednání, samozřejmě s přihlédnutím ke konkrétním okolnostem daného případu. Stejný závěr pak platí i pro *blockchain* a *smart contracts*.

V návaznosti na poslední výzkumnou otázku pak po teoretickém rozboru jednotlivých aspektů byly v práci rozebrány relevantní soudní rozhodnutí za účelem zjištění, zda je současná úprava soudy správně aplikována. Pozornost byla věnována zejména otázkám v oblastech emailu bez elektronického podpisu a (ne)splnění požadavku písemné formy, vztahu ustanovení § 561 a § 562 občanského zákoníku, povaze naskenovaného vlastnoručního podpisu, unikátního ID a *click-through* smluv, dvoufaktorového ověření v podobě SMS zprávy, podpisu myší do prázdného pole na internetové stránce, požadavku na vyšší formy elektronických podpisů ke splnění písemné formy a záměně požadavku písemné formy a identifikace. Z analyzovaných rozhodnutí vyplývá, že soudní praxe není v těchto otázkách sjednocena. Obecně lze dovodit, že některé soudy i na prostý elektronický podpis kladou nároky podpisu zaručeného, tedy že má zaručovat autenticitu (integritu) dokumentu a identifikovat jednající osobu. Řešením by

[458] Avšak jak bylo rozebráno v kapitole 3.1 a 4.4, ne vždy zcela jednoznačnou.

pak bylo vydání sjednocujícího stanoviska Nejvyššího soudu ČR, případně judikatura zabývající se těmito otázkami. Alternativou je širší odborná i veřejná diskuze vedoucí k erudici nižších soudů. Je pak obtížné s přesností posoudit, jaký je podíl soudních rozhodnutí prosté elektronické podpisy uznávající, neboť ty mohou být v praxi akceptovány soudem bez výslovného odůvodnění. Dokud však judikatura zejména nižších soudů nebude sjednocena, bude převládat právní nejistota, která je spojena se značnými náklady. Současný stav tak není žádoucí.

Na závěr této práce byla rozebrána plánovaná revize nařízení eIDAS, která by měla přinést mimo jiné službu správy prostředků pro dálkové vytváření elektronických podpisů a pečetí a evropské peněženky digitální identity. To by v praxi mělo vést k usnadnění užívání kvalifikovaných elektronických podpisů, čímž by byla vyřešena část rozporných otázek. Udržování digitální kontinuity by ovšem získalo na větším významu. Konkrétní aspekty budou známé po přijetí finální verze navrhované revize a případné národní implementaci. V mezidobí byl v České republice představen obdobný projekt eDoklady, který však prozatím možnost vytvářet kvalifikované elektronické podpisy neumožňuje.

Vzhledem k aktuálnosti i vzrůstající komplexnosti tématu elektronického právního jednání je na místě, aby dané problematice byla věnována stále větší pozornost jak v akademické, tak praktické sféře. Jak bylo v této práci dovozeno, současnou právní úpravu lze považovat za dostatečnou a problematickým aspektem je především její rozporuplná interpretace, což je nepříznivé z hlediska právní jistoty. Sjednocení výkladové praxe je tak nasnadě za pomoci sjednocujícího stanoviska Nejvyššího soudu, respektování rozhodnutí vyšších soudů, která lze v dohledné době očekávat, popřípadě i neformálních diskuzí odborné veřejnosti.

SEZNAM POUŽITÝCH ZKRATEK

eIDAS – 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;

hospodářský zákoník – zákon č. 109/1964 Sb., hospodářský zákoník;

notářský řád – zákon č. 358/1992 Sb., o notářích a jejich činnosti (notářský řád);

občanský zákoník – zákon č. 89/2012 Sb., občanský zákoník;

občanský zákoník 1964 – zákon č. 40/1964 Sb., občanský zákoník;

osř – zákon č. 99/1963 Sb. občanský soudní řád;

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

zákon o advokacii – zákon č. 85/1996 Sb., o advokacii, ve znění pozdějších předpisů;

zákon o archivnictví – zákon č. 499/2004 Sb., o archivnictví a spisové službě, ve znění pozdějších předpisů;

zákon o elektronickém podpisu – zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů;

zákon o ověřování – zákon č. 21/2006 Sb., o ověřování shody opisu nebo kopie s listinou a o ověřování pravosti podpisu a o změně některých zákonů, ve znění pozdějších předpisů;

zákon o právu na digitální služby – zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů;

ZSVD – zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.

Seznam zdrojů

1. **Komentářová literatura, monografie a odborné články z časopisů**

BAJURA, J., ČÁP, Z., ČERNÁ, S., DOLANSKÁ BÁNYAIOVÁ, L., DVOŘÁK, J., DVOŘÁK, T., ELIÁŠ, J., ELISCHER, D., FIALA, J., FIALA, V., FRINTA, O., HAAS, K., HAJN, P., HOLČAPEK, T. a kol. Občanský zákoník: Komentář, Svazek VI, (§ 2521-3081). [Systém ASPI]. Wolters Kluwer [cit. 2023-7-26]. ASPI_ID KO89_f2012CZ., ISSN 2336-517X, § 3026.

BERAN, Vladimír. § 561 [Písemná forma]. In: PETROV, Jan, VÝTISK, Michal, BERAN, Vladimír a kol. Občanský zákoník. 2. vydání (1. aktualizace). Praha: C. H. Beck, 2022.

BERAN, Vladimír. § 562 [Elektronické a jiné technické prostředky]. In: PETROV, Jan, VÝTISK, Michal, BERAN, Vladimír a kol. Občanský zákoník. 2. vydání (1. aktualizace). Praha: C. H. Beck, 2022.

BERAN, Vladimír. § 568 [Důkazní síla veřejné listiny]. In: PETROV, Jan, VÝTISK, Michal, BERAN, Vladimír a kol. Občanský zákoník. 2. vydání (2. aktualizace). Praha: C. H. Beck, 2023.

BERAN, Vladimír. § 3026 [Písemnosti a veřejné listiny]. In: PETROV, Jan, VÝTISK, Michal, BERAN, Vladimír a kol. Občanský zákoník. 2. vydání (2. aktualizace). Praha: C. H. Beck, 2023

BEZOUŠKA, P., HAVEL, B. Občanský zákoník: Srovnávací komentář. [Systém ASPI]. Wolters Kluwer [cit. 2023-6-3]. ASPI_ID KO89_p12012CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X, § 562.

BĚHOUNKOVÁ, Tereza. *Písemná forma právního jednání v elektronickém obchodu*. Diplomová práce. Praha: Právnická fakulta Univerzity Karlovy, 2023.

BRATSKÝ, Pavel. Smart contract v českém právu. *Právní rádce*. 2019, roč. 2019, č. 3.

ČERMÁK, Karel. Elektronický podpis – pohled soukromoprávní. *Bulletin advokacie*. 2002, roč. 2002, č. 11 - 12, s. 64 - 77.

DONÁT, Josef, Jan TOMÍŠEK a Ivan FENCL. *Je publikovaná judikatura k elektronickým podpisům skutečně relevantní?* [online]. [cit. 2023-06-18]. Dostupné z: https://www.epravo.cz/top/clanky/je-publikovana-judikatura-k-elektronickym-podpisum-skutecne-relevantni-116077.html.

DONÁT, Josef a TOMÍŠEK, Jan. Právo v síti: průvodce právem na internetu. V Praze: C.H. Beck, 2016. ISBN 978-80-7400-610-4.

HANDLAR, Jiří. § 582 [Nedostatek formy]. In: LAVICKÝ, Petr a kol. Občanský zákoník I. Obecná část (§ 1−654). 2. vydání. Praha: C. H. Beck, 2022.

HULMÁK, Milan. Elektronický právní styk. Právní rozhledy, 2005, č. 7, s. 229-234.

HRDLIČKA, Miloslav. § 562 [Písemná forma právního jednání učiněného elektronickými prostředky]. In: LAVICKÝ, Petr a kol. Občanský zákoník I. Obecná část (§ 1−654). 1. vydání. Praha: C. H. Beck, 2014.

JANOŠEK, Vladimír. *Prostý email a následky nedodržení písemné formy jednání alias přepjatý formalismus*. Online. Dostupné z: https://www.epravo.cz/top/clanky/prosty-email-a-nasledky-nedodrzeni-pisemne-formy-jednani-alias-prepjaty-formalismus-109790.html?mail. [cit. 2024-01-18].

JANOUŠEK, Michal. § 561 [Písemná forma právního jednání]. In: LAVICKÝ, Petr a kol. Občanský zákoník I. Obecná část (§ 1−654). 2. vydání. Praha: C. H. Beck, 2022.

JANOUŠEK, Michal. § 562 [Písemná forma právního jednání učiněného elektronickými prostředky]. In: LAVICKÝ, Petr a kol. Občanský zákoník I. Obecná část (§ 1−654). 2. vydání. Praha: C. H. Beck, 2022.

JAREŠ, Adam. *SMLOUVA PODEPSANÁ ELEKTRONICKÝM PODPISEM*. Plzeň, 2022. Disertační práce. Západočeská univerzita v Plzni Fakulta právnická.

KMENT, Vojtěch. *Elektronické právní jednání: Srovnávací analýza s důrazem na využití elektronického podpisu podle práva EU, České republiky a Německa*. Praha, 2018. Disertační práce. Právnická fakulta Univerzity Karlovy.

KORBEL, František a MELZER, Filip. Písemnost, elektronický a biometrický podpis v elektronickém právním jednání. *Bulletin advokacie*. 2014, roč. 2014, č. 12, s. 31 - 36.

KORBEL, František; KOVÁŘ, Dalibor a AMLER, Pavel. *Interpretace elektronického podpisu a související identifikace v soukromém právu*. Online. Dostupné z: https://www.pravniprostor.cz/clanky/obcanske-pravo/interpretace-elektronickeho-podpisu-souvisejici-identifikace-v-soukromem-pravu. [cit. 2023-06-18].

KORBEL, František; KOVÁŘ, Dalibor; NEŠPŮREK, Robert a OTEVŘEL, Richard. *Dynamický biometrický podpis nově vždy jako zvláštní kategorie osobních údajů*. Online. Dostupné z: https://www.pravniprostor.cz/clanky/pravo-it/dynamicky-biometricky-podpis-nove-vzdy-jako-zvlastni-kategorie-osobnich-udaju. [cit. 2023-08-24].

KORBEL, František, KOVÁŘ, Dalibor, POTOČŇÁK, Štefan: Elektronická identita při elektronickém (hmotně)právním jednání, *Právní rozhledy*, 18/2019, č. 18

KORBEL, František. *Aktuální novinky českého e-Governmentu a digitálních služeb*. Online. Dostupné z: https://www.pravniprostor.cz/clanky/spravni-pravo/aktualni-novinky-ceskeho-e-governmentu-digitalnich-sluzeb. [cit. 2023-11-29].

KORBEL, František, KOVÁŘ, Dalibor a JAROŠ, Ján. Aktuální právní přístup k dynamickému biometrickému podpisu. *Pojistný obzor*. roč. 2021, č. 2.

KOŘÍNKOVÁ, Petra. *Internet a mezinárodní právo soukromé*. Diplomová práce. Praha: Univerzita Karlova v Praze Právnická fakulta, 2014.

KUČERA, Zdeněk. *Smart contracts pohledem právníka*. Online. Dostupné z: https://www.pravniprostor.cz/clanky/obcanske-pravo/smart-contracts-pohledem-pravnika. [cit. 2023-12-27].

KUNT, M. – LECHNER, T. *Spisová služba*. 2., aktualizované vydání. Praha: Leges, 2017

LAVICKÝ, Petr. § 568 [Pravost a správnost veřejné listiny]. In: LAVICKÝ, Petr a kol. Občanský zákoník I. Obecná část (§ 1−654). 2. vydání. Praha: C. H. Beck, 2022

MATEJKA, Ján a Vojen GÜTTLER. *Electronic Written Documents and Biometric Options of Their Signing – Problem of Evidentiary Reliability and Personal Data Protection*, Vol. 8, No 1 (2018), s. 38 - 50.

MATEJKA, Ján. Úprava elektronického podpisu v právním řádu ČR. Právník. roč. 2001, č. 6. s. 557–586 [online] dostupné z právního informačního systému CODEXIS [cit. 2023-09-18].

MATEJKA, Ján a CHUM, Václav. K PRÁVNÍ ÚPRAVĚ ELEKTRONICKÉHO PODPISU. *Bulletin advokacie*. 2002, roč. 2002, č. 3, s. 27 - 41.

MATEJKA, J., MATES, P. Zákon o právu na digitální služby. Komentář. [Systém ASPI]. Nakladatelství Leges [cit. 2023-4-21]. ASPI_ID KO12l2020CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X, § 6.

MELZER, F., TÉGL, P. a kol. Občanský zákoník. Velký komentář. Sv. III. § 419-654. Praha: Leges, 2014, komentář k § 561 odst. 1.

PETERKA, Jiří. *Elektronický podpis na rozcestí*. Online. Dostupné z: https://www.lupa.cz/clanky/elektronicky-podpis-na-rozcesti/. [cit. 2023-10-11].

PETERKA, Jiří. *Jak rozumět dynamickým biometrickým podpisům?* Online. Dostupné z: https://www.lupa.cz/clanky/jak-rozumet-dynamickym-biometrickym-podpisum/. [cit. 2023-09-11].

PETERKA, Jiří. *Zatímco technické obory přitvrzují, právo naopak měkne*. Online. Dostupné z: https://www.pravniprostor.cz/clanky/spravni-pravo/zatimco-technicke-obory-pritvrzuji-pravo-naopak-mekne. [cit. 2023-07-14].

PETERKA, Jiří. *Jak na digitální kontinuitu (nejenom) v datových schránkách?* Online. Dostupné z: https://www.lupa.cz/clanky/jak-na-digitalni-kontinuitu-nejenom-v-datovych-schrankach/. [cit. 2023-11-18].

PETERKA, Jiří. *Jak na digitální kontinuitu (2): Co když platnost elektronického podpisu už nejde ověřit?* Online. Dostupné z: https://www.lupa.cz/clanky/jak-na-digitalni-kontinuitu-2-co-kdyz-platnost-elektronickeho-podpisu-uz-nejde-overit/. [cit. 2023-11-22].

PETERKA, Jiří. *Jak na digitální kontinuitu (3): Elektroničtí notáři, spisové služby, blockchain a vyvratitelné domněnky*. Online. Dostupné z: https://www.lupa.cz/clanky/jak-na-digitalni-kontinuitu-3-elektronicti-notari-spisove-sluzby-blockchain-a-vyvratitelne-domnenky/. [cit. 2023-11-25].

PETERKA, Jiří. *Jak na digitální kontinuitu (4): Jak aktivně pečovat o starší dokumenty a datové zprávy*. Online. Dostupné z: https://www.lupa.cz/clanky/jak-na-digitalni-kontinuitu-4-jak-aktivne-pecovat-o-starsi-dokumenty-a-datove-zpravy/. [cit. 2023-11-30].

PETERKA, Jiří. *Jak na digitální kontinuitu (7): Co (ne)umí Czech POINTy, co elektronické podatelny a co Adobe Reader*. Online. Dostupné z: https://www.lupa.cz/clanky/jak-na-digitalni-kontinuitu-7-co-ne-umi-czechpointy-co-elektronicke-podatelny-a-co-adobe-reader/. [cit. 2023-12-05].

PETERKA, Jiří. *Jak na digitální kontinuitu (8): Proč kryptografické algoritmy oslabují a elektronické dokumenty stárnou?* Online. Dostupné z: https://www.lupa.cz/clanky/jak-na-digitalni-kontinuitu-8-proc-kryptograficke-algoritmy-oslabuji-a-elektronicke-dokumenty-starnou/. [cit. 2023-12-09].

PETERKA, Jiří. *Jak na digitální kontinuitu (9): Co jsou certifikáty a proč je musíme pravidelně obměňovat?* Online. Dostupné z: https://www.lupa.cz/clanky/jak-na-digitalni-kontinuitu-9-co-jsou-certifikaty-a-proc-je-musime-pravidelne-obmenovat/. [cit. 2023-12-10].

PETERKA, Jiří. *Jak na digitální kontinuitu (10): Co je revokace certifikátu a jak komplikuje digitální kontinuitu*. Online. Dostupné z: https://www.lupa.cz/clanky/jak-na-digitalni-kontinuitu-10-co-je-revokace-certifikatu-a-jak-komplikuje-digitalni-kontinuitu/. [cit. 2023-12-14].

PETERKA, Jiří. *Jak na digitální kontinuitu (11): K jakému časovému okamžiku se mají ověřovat elektronické podpisy?* Online. Dostupné z: https://www.lupa.cz/clanky/jak-na-digitalni-kontinuitu-11-k-jakemu-casovemu-okamziku-se-maji-overovat-elektronicke-podpisy/. [cit. 2023-12-15].

PETERKA, Jiří. *Jak na digitální kontinuitu (12): Proč mají elektronické podpisy různé profily, formáty a úrovně?* Online. Dostupné z: https://www.lupa.cz/clanky/jak-na-digitalni-kontinuitu-12-proc-maji-elektronicke-podpisy-ruzne-profily-formaty-a-urovne/. [cit. 2023-12-20].

PETERKA, Jiří. *Jak na digitální kontinuitu (13): Pomáháme si vlastními silami*. Online. Dostupné z: https://www.lupa.cz/clanky/jak-na-digitalni-kontinuitu-13-pomahame-si-vlastnimi-silami/. [cit. 2023-12-21].

PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra. *Advokátní deník* [online]. 2020 [cit. 2023-04-11]. Dostupné z: https://advokatnidenik.cz/2020/05/04/podepisovani-soukromych-listin-vcera-dnes-a-zitra/.

POLČÁK, Radim. Praxe elektronických dokumentů. *Bulletin advokacie*. 2011, č. 7–8, s. 53 - 61.

POLČÁK, Radim. Elektronické právní jednání – změny, problémy a nové možnosti v zákoně č. 89/2012 Sb. *Bulletin advokacie*, 2013, č. 10.

POLČÁK, Radim. *Internet a proměny práva*. Téma (Auditorium). Praha: Auditorium, 2012. ISBN 978-80-87284-22-3.

POLČÁK, Radim, Zsolt György BALOGH, Michael BOGDAN, Giovanni Maria RICCIO, Dan Jerker B. SVANTESSON a Andreas WIEBE. *Introduction to ICT Law (Selected Issues)*. Brno: Masarykova Univerzita, 2007. 185 s. AUBI, řada teoretická, 314. ISBN 978-80-210-4302-2.

ROZUMNÉ PRÁVO. *Platforma Rozumné právo: Je třeba zjednodušit elektronické právní jednání*. Online. Dostupné z: https://www.pravniprostor.cz/clanky/ostatni-pravo/platforma-rozumne-pravo-je-treba-zjednodusit-elektronicke-pravni-jednani. [cit. 2023-08-14].

SHAAN, Ray. *The Difference Between Blockchains & Distributed Ledger Technology*. Online. Dostupné z: https://towardsdatascience.com/the-difference-between-blockchains-distributed-ledger-technology-42715a0fa92. [cit. 2023-12-27].

SMEJKAL, Vladimír, Jindřich KODL a Miroslav UŘIČAŘ. Elektronický podpis podle nařízení eIDAS, *Revue pro právo a* technologie, roč. 6, č. 11, roč. 2015.

SMEJKAL, Vladimír. Kryptografický a dynamický biometrický podpis podle platné právní úpravy, *Právní rozhledy* č. 10/19, s. 343.

SZABO, Nick. Formalizing and Securing Relationships on Public Networks. First Monday [online]. 1997 [cit. 2019-02-18]. ISSN 1396-0466. Dostupné z: https://ojphi.org/ojs/index.php/fm/article/view/548/469.

ŠČERBA, Tomáš. *Elektronická kontraktace v právní praxi*. Rigorózní práce. Brno: Právnická fakulta Masarykovy Univerzity, 2008.

TICHÝ, Luboš. Komentář k § 562. In: ŠVESTKA, Jiří, Jan DVOŘÁK, Josef FIALA a kol. *Občanský zákoník. Komentář. Svazek I*. Praha: Wolters Kluwer ČR, 2014.

TOMÁNEK, Jaroslav. *Biometrický podpis - mýty a fakta*. DSM 2012. Online. Dostupné z: https://www.ica.cz/Userfiles/files/zpravy/Biometricky_podpis.pdf. [cit. 2023-09-14].

VALÁŠEK, Michal. *Nahradí dynamické biometrické podpisy ty současné elektronické?* Online. Dostupné z: https://www.lupa.cz/clanky/nahradi-dynamicke-biometricke-podpisy-ty-soucasne-elektronicke/. [cit. 2023-08-26].

ZUKLÍNOVÁ, Michaela. Právní jednání podle občanského zákoníku č. 89/2012 Sb. Komentář, srovnání se zahraničím a vybraná platná judikatura. 1. vyd. Praha: Linde, 2013. [online] dostupné z právního informačního systému CODEXIS [cit. 2023-04-12]. Komentář k § 561.

ZUKLÍNOVÁ v DAVID, O., DEVEROVÁ, L., DOLANSKÁ BÁNYAIOVÁ, L., DVOŘÁK, J., DVOŘÁK, T., FIALA, J., FRINTA, O., HOLČAPEK, T., HURDÍK, J., KINDL, T., MACKOVÁ, A., PAULY, J., PAVLÍK, P., PELIKÁN, R. a kol. Občanský zákoník: Komentář, Svazek I, (§ 1-654). [Systém ASPI]. Wolters Kluwer [cit. 2023-6-3]. ASPI_ID KO89_a2012CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X, § 561.

ZUKLÍNOVÁ v DAVID, O., DEVEROVÁ, L., DOLANSKÁ BÁNYAIOVÁ, L., DVOŘÁK, J., DVOŘÁK, T., FIALA, J., FRINTA, O., HOLČAPEK, T., HURDÍK, J., KINDL, T., MACKOVÁ, A., PAULY, J., PAVLÍK, P., PELIKÁN, R. a kol. Občanský zákoník: Komentář, Svazek I, (§ 1-654). [Systém ASPI]. Wolters Kluwer [cit. 2023-10-4]. ASPI_ID KO89_a2012CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X, § 562.

2. Ostatní články, stanoviska a normy

I. CERTIFIKAČNÍ AUTORITA. *Následný certifikát*. Online. Dostupné z: https://www.ica.cz/Nasledny-certifikat. [cit. 2023-12-13].

ADOBE. *Ověření digitálních podpisů*. Online. Dostupné z: https://helpx.adobe.com/cz/acrobat/using/validating-digital-signatures.html. [cit. 2023-12-18].

BÁJEČNÝ SVĚT. *Příklad ztráty digitální kontinuity*. Online. Dostupné z: https://www.bajecnysvet.cz/priklady/priklad010.php. [cit. 2023-11-25].

ČESKÁ NÁRODNÍ BANKA. *K některým ustanovením zákona č. 257/2016 Sb., o spotřebitelském úvěru*. Online. Dostupné z: https://www.cnb.cz/cs/dohled-financni-trh/legislativni-zakladna/stanoviska-k-regulaci-financniho-trhu/RS2017-02/. [cit. 2023-12-18], otázka č. 11.

ČESKÁ POŠTA. *Časová razítka*. Online. Dostupné z: https://www.ceskaposta.cz/sluzby/certifikacni-autorita-postsignum/casova-razitka. [cit. 2023-12-13].

EUROPEAN COMMISSION. *CEF eSignature DSS, Version 1.03, Qualified electronic signature (QES) validation algorithm*. Online. Dostupné z: https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/Qualified+electronic+signature+-+QES+validation+algorithm?preview=/467109151/467109153/Qualification%20algorithm.pdf. [cit. 2023-12-18].

EVROPSKÁ KOMISE, *ZPRÁVA KOMISE EVROPSKÉMU PARLAMENTU A RADĚ o hodnocení nařízení (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (nařízení eIDAS)*. Dostupná zde: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52021DC0290

ETSI TS 102 853 V1.2.1 (2014-12)

ETSI EN 319 142-1 V1.1.1 (2016-04)

ETSI EN 319 162-1 V1.1.1 (2016-04)

ETSI EN 319 162-2 V1.1.1 (2016-04)

ETSI TS 119 511 V1.1.1 (2019-06)

ETSI TS 119 512 V1.1.1 (2020-01)

ETSI TS 119 182-1 V1.1.1 (2021-03)

ETSI TS 119 172-4 V1.1.1 (2021-05)

ETSI EN 319 122-1 V1.2.1 (2021-10)

ETSI EN 319 102-1 V1.3.1 (2021-11)

ETSI EN 319 132-1 V1.2.1 (2022-02)

NÁRODNÍ ARCHITEKTONICKÝ PLÁN - ARCHITEKTURA EGOVERNMENTU ČR. *Systémy správy dokumentů*. Online. Dostupné z: https://archi.gov.cz/nap:system_spravy_dokumentu?do=#digitalni_kontinuita. [cit. 2024-01-18].

NÁRODNÍ ARCHIV. *Spisová služba v otázkách a odpovědích*. Online. Dostupné z: https://www.nacr.cz/verejnost/2-predarchivni-pece/verejnopravni-puvodci/spisova-sluzba-otazky-odpovedi#transakce7. [cit. 2023-11-28].

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD. *Prohlášení NBÚ k využívání hashovacích funkcí*. Online. Dostupné z: https://web.archive.org/web/20090226093652/http:/www.nbu.cz/cs/ochrana-utajovanych-informaci/kryptograficka-ochrana/informace/. [cit. 2023-12-10].

POSTSIGNUM. *Obnova certifikátů PostSignum*. Online. Dostupné z: https://www.postsignum.cz/obnova_certifikatu.html. [cit. 2023-12-13].

SPRÁVA ZÁKLADNÍCH REGISTRŮ. *NCA – Politika ověřování podpisu NCA QVerify v 1.0.1*. Online. Dostupné z: https://www.narodni-ca.cz/Dokumenty/NCA_Politika_kvalif_sluzby_overovani_platnosti_QVerify_1v01.pdf. [cit. 2023-12-18].

Stanovisko odboru archivní správy a spisové služby k užívání časového razítka v souvislosti s odesíláním a ukládáním dokumentů v digitální podobě, ze dne 6. dubna 2010 č. j. MV-36491-1/AS-2010, dostupné zde: https://www.mvcr.cz/soubor/uzivanicasrazstanas-pdf.aspx

Výkladové stanovisko ÚOHS k novele zákona o významné tržní síle, § 3b, s. 20 – 21, dostupné zde: https://www.uohs.cz/cs/vyznamna-trzni-sila/metodicka-cinnost/vykladova-stanoviska-a-doporuceni.html

3. Seznam použitých právních předpisů

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

Návrh nařízení Evropského Parlament a Rady, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu

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 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu.

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

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

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

Zákon č. 109/1964 Sb., hospodářský zákoník, ve znění pozdějších předpisů

Zákon č. 358/1992 Sb., o notářích a jejich činnosti (notářský řád), ve znění pozdějších předpisů

Zákon č. 634/1992 Sb., o ochraně spotřebitele, ve znění pozdějších předpisů

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

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

Zákon č. 365/2000 Sb. o informačních systémech veřejné správy

Zákon č. 37/2004 Sb., o pojistné smlouvě, ve znění pozdějších předpisů

Zákon č. 256/2004 Sb., o podnikání na kapitálovém trhu, ve znění pozdějších předpisů

Zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), ve znění pozdějších předpisů

Zákon č. 499/2004 Sb., o archivnictví a spisové službě, ve znění pozdějších předpisů

Zákon č. 21/2006 Sb., o ověřování shody opisu nebo kopie s listinou a o ověřování pravosti podpisu a o změně některých zákonů, ve znění pozdějších předpisů

Zákon č. 253/2008 Sb. o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů

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

Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

Zákon č. 186/2016 Sb. o hazardních hrách, ve znění pozdějších předpisů

Zákona č. 257/2016 Sb., o spotřebitelském úvěru, ve znění pozdějších předpisů

Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů

Zákon č. 250/2017 Sb. o elektronické identifikaci, ve znění pozdějších předpisů

Zákon č. 370/2017 Sb., o platebním styku, ve znění pozdějších předpisů

Zákon č. 170/2018 Sb., o distribuci pojištění a zajištění (IDD), ve znění pozdějších předpisů

Zákon č. 12/2020 Sb. o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů

Zákon č. 159/2020 Sb., o kompenzačním bonusu v souvislosti s krizovými opatřeními v souvislosti s výskytem koronaviru SARS CoV-2

Zákon č. 269/2021 Sb. o občanských průkazech, ve znění pozdějších předpisů

Nařízení vlády č. 317/2021 Sb., o postupu notáře při legalizaci elektronického podpisu

Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby

4. Seznam použité judikatury

Rozhodnutí Nejvyššího soudu ČR ze dne 29. 11. 2007, sp. zn. 29 Odo 965/2006.

Rozhodnutí Nejvyššího soudu ČR ze dne 29. 1. 2009, sp. zn. 30 Cdo 1230/2007.

Rozhodnutí Nejvyššího soudu ČR ze dne 17. 12. 2013, sp. zn. 23Cdo 1308/2011.

Rozhodnutí Nejvyššího soudu ČR ze dne 10. 4. 2014, sp. zn. 23 Cdo 1593/2012.

Rozhodnutí Nejvyššího soudu ČR ze dne 27. 8. 2013, sp. zn. 21 Cdo 2186/2012.

Rozhodnutí Nejvyššího soudu ČR ze dne 27. 11. 2014, sp. zn. 29 Cdo 3919/2014.

Rozhodnutí Nejvyššího soudu ČR ze dne 19. 10. 2016, sp. zn. 31 Cdo 1570/2015.

Rozhodnutí Nejvyššího soudu ČR ze dne 30. 11. 2016, sp. zn. 22 Cdo 2526/2016.

Rozhodnutí Nejvyšší soudu ČR ze dne 1. 6. 2017, sp. zn. 20 Cdo 1741/2017.

Rozhodnutí Nejvyššího soudu ČR ze dne 16. 5. 2019, sp. zn. 23 Cdo 3439/2018.

Rozhodnutí Nejvyššího soudu ČR, ze dne 18. 12. 2018, sp. zn. 21 Cdo 682/2018.

Rozhodnutí Nejvyššího soudu ČR ze dne 22. 5. 2019, sp. zn. 26 Cdo 1230/2019.

Rozhodnutí Nejvyššího soudu ČR ze dne 22. 1. 2020, sp. zn. 26 Cdo 3501/2019.

Rozhodnutí Nejvyššího soud ČR – senát ze dne 15. 8. 2023, č.j. 23 ICdo 60/2022 – 76.

Rozhodnutí Nejvyššího správního soudu ze dne 27. 7. 2017, sp. zn. 2 As 80/2017.

Rozhodnutí Nejvyššího správní soudu ze dne 28. 6. 2013, sp. zn. 5 As 1/2011.

Rozhodnutí Vrchního soudu v Olomouci ze dne 13. 10. 2022, č.j. 5 Cmo 111/2022-378.

Rozhodnutí Vrchního soudu v Praze ze dne 28. 6. 2023, č. j. 3 VSPH 610/2023-A-122, ze dne 23. 5. 2023, sp. zn. 4 Cmo 52/2023.

Rozhodnutí Městského soudu v Praze ze dne 8. 7. 2020, sp. zn. 18 Co 187/2020.

Rozhodnutí Krajského soudu v Brně ze dne 9. 11. 2017, sp. zn. 27 Co 86/2017, ze dne 5. 6. 2017, sp. zn. 33 Icm 547/2016.

Rozhodnutí Krajského soudu v Českých Budějovicích ze dne 27. 3. 2015, sp. zn. 24 Co 696/2015, ze dne 7. 8. 2015, sp. zn. 5 Co 639/2015, ze dne 12. 5. 2015, sp. zn. 24 Co 1000/2015.

Rozhodnutí Krajského soudu v Praze ze dne 2. 3. 2022. č. j. 25 Co 1/2022 – 66, ze dne 17. 1. 2019, sp. zn. 27 Co 327/2018, ze dne 20. 1. 2022, sp. zn. 24 Co 243/2021.

Rozhodnutí Krajského soudu v Ostravě ze dne 28. 3. 2022, sp. zn. 11 Co 338/2020, ze dne 28. 1. 2016 sp. zn. 37 ICm 4495/2014.

Rozhodnutí Obvodního soudu pro Prahu 2 ze dne 10. 11. 2021, č. j. 22 C 198/2020-223.

Rozhodnutí Obvodního soudu pro Prahu 3 ze dne 16. 8. 2022, sp. zn. 19 C 230/2022 nebo ze dne 4. dubna 2023 č. j. 16 C 16/2023-28.

Rozhodnutí Obvodního soud pro Prahu 4 ze dne 13. 4. 2022, č. j. 28 C 48/2020-121.

Rozhodnutí Obvodního soudu pro Prahu 6 ze dne 13. 9. 2021, sp. zn. 18 C 198/2021, ze dne 27. 10. 2021, sp. zn. 6 C 375/2021, sp. zn. 18 C 79/2019, sp. zn. 18 C 29/2019.

Rozhodnutí Obvodního soudu pro Prahu 7 ze dne 14. 9. 2022, č. j. 16 C 111/2021-198.

Rozhodnutí Obvodního soudu pro Prahu 9, ze dne 12. 6. 2023, č. j. 98 C 250/2017-649, ze dne 15. 5. 2023 č. j. 98 C 190/2022-64, ze dne 6. 1. 2023, č. j. 98 C 303/2020-275, ze dne 25. 10. 2022, č. j. 98 C 257/2019-309, ze dne 7. 7. 2022, č. j. 98 C 332/2020-245.

Rozhodnutí Obvodního soudu pro Prahu 10 ze dne 20. 12. 2021, sp. zn. 9 C 104/2021.

Rozhodnutí Okresního soudu Praha-východ ze dne 22. 2. 2022, sp. zn. 7 C 92/2021, ze dne 17. 5. 2021 sp. zn. 35 C 130/2021.

Rozhodnutí Městského soudu v Brně ze dne 19. 9. 2023, č. j. 47 C 178/2023 – 30, ze dne 23. 5. 2023, č. j. 47 C 92/2023 – 39, nebo ze dne 03. 2. 2023, č. j. 47 C 85/2022 – 54.

Rozhodnutí Okresního soudu v Berouně ze dne 13. 9. 2023, sp. zn. 10 C 220/2023, ze dne 21. 12. 2021, sp. zn. 18 C 225/2021, ze dne 28. 12. 2021, sp. zn. 10 C 305/2021.

Rozhodnutí Okresního soudu v Blansku ze dne 2. 12. 2021, sp. zn. 3 C 173/2021.

Rozhodnutí Okresního soudu Brno-venkov ze dne 15. 11. 2022, sp. zn. 41 C 150/2022.

Rozhodnutí Okresního soudu v České Lípě ze dne 17. 8. 2022, sp. zn. 48 C 189/2022, ze dne 20. 10. 2021, sp. zn. 48 C 347/2021.

Rozhodnutí Okresního soudu v Českém Krumlově ze dne 26. 11. 2021, sp. zn. 2 C 164/2021.

Rozhodnutí Okresního soudu ve Frýdku Místku ze dne 08. 11. 2022, sp. zn. 16 C 208/2022.

Rozhodnutí Okresního soudu v Hodoníně ze dne 14. 9. 2021, sp. zn. 13 C 67/2021, ze dne 24. 11. 2022, sp. zn. 13 C 163/2022.

Rozhodnutí Okresního soudu v Chomutově ze dne 6. 9. 2023, sp. zn. 7 C 248/2023, ze dne 12. 1. 2022, sp. zn. 7 C 339/2021, ze dne 7. 12. 2022, sp. zn. 9 C 125/2022.

Rozhodnutí Okresního soudu v Jihlavě ze dne 19. 9. 2023, sp. zn. 18 C 81/2023, ze dne 26. 1. 2022, sp. zn. 20 C 214/2021.

Rozhodnutí Okresního soudu v Karviné ze dne 14. 1. 2022, sp. zn. 24 C 233/2021.

Rozhodnutí Okresního soudu v Karviné – pobočka v Havířově ze dne 6. 12. 2022, sp. zn. 111 C 374/2022.

Rozhodnutí Okresního soudu v Kladně ze dne 31. 8. 2021, sp. zn. 208 C 115/2021.

Rozhodnutí Okresního soudu v Kladně ze dne 27. 2. 2024, sp. zn. 208 C 179/2023.

Rozhodnutí Okresního soudu v Litoměřicích ze dne 9. 8. 2021, sp. zn. 9 C 332/2019-218.

Rozhodnutí Okresního soudu v Mladé Boleslavi ze dne 24. 5. 2022, sp. zn. 15 C 89/2022.

Rozhodnutí Okresního soudu v Mostě ze dne 1. 9. 2023, č. j. 46 C 177/2023-24, ze dne 7. 9. 2021, sp. zn. 32 C 59/2021.

Rozhodnutí Okresního soudu v Novém Jičíně ze dne 29. 9. 2020, č. j. 12 C 23/2020-86 a sp. zn. 7 C 261/2019.

Rozhodnutí Okresního soudu v Nymburce ze dne 14. 8. 2023, sp. zn. 6 C 137/2023.

Rozhodnutí Okresního soudu v Ostravě ze dne 25. 01. 2022, sp. zn. 30 C 365/2021.

Rozhodnutí Okresního soud v Plzni ze dne 30. 8. 2023, sp. zn. 16 C 77/2023.

Rozhodnutí Okresního soudu v Plzni – jih ze dne 7. 6. 2023, sp. zn. 1 C 62/2023.

Rozhodnutí Okresního soudu ve Zlíně ze dne 10. 11. 2021, sp. zn. 26 C 62/2021.

Rozsudek Soudního dvora EU ze dne 27. ledna 2010, ve věci E-4/09.

Rozsudek Soudního dvora EU ze dne 25. ledna 2017, ve věci C-375/15.

Rozhodnutí Court of King’s Bench v kanadské provincii Saskatchewan v případu South West Terminal Ltd v Achter Land and Cattle Ltd [2023 SKKB 116].

Rozhodnutí Pollstar v. Gigmania, Ltd., United States District Court, D. California ze dne 17. října 2000, 981-982.

Rozhodnutí Nguyen v. Barnes & Noble, Inc., United States Court of Appeals for the Ninth Circuit ze dne 18. srpna 2014

Rozsudek ve věci Specht v. Netscape Comm. ze dne 1. října 2002

Elektronická právní jednání se zaměřením na prostý elektronický podpis

Abstrakt

Práce je členěna do šesti kapitol. První kapitola je tvořena úvodem. Ve druhé kapitole je představena obecná úprava a význam podpisu se stručným historickým exkurzem potřebným pro posouzení možné aplikovatelnosti dřívějších závěrů na aktuální právní úpravu.

Třetí kapitola je věnována současné úpravě a jednotlivým druhům elektronických podpisů, tedy dělení na kvalifikovaný elektronický podpis, zaručený elektronický podpis a prostý elektronický podpis a české specifikum v podobě zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu pro elektronické podpisy, obecně známého jako uznávaný elektronický podpis. Na závěr kapitoly je také rozebrán v praxi stále šířeji užívaný biometrický podpis.

Čtvrtá kapitola se věnuje písemné formě právního jednání, tedy podrobnému rozboru ustanovení § 561 a § 562 občanského zákoníku, a to včetně jejich vzájemného vztahu. Dále jsou rozebrány aspekty digitální kontinuity u vyšších forem elektronických podpisů a jejich komparace s prostým elektronickým podpisem. V poslední části kapitoly je věnována pozornost různým typům elektronických smluv a rozdílům mezi důkazními účinky jednotlivých typů elektronických podpisů a (ne)platnosti písemného právního jednání.

V páté kapitole se autor práce věnuje rozboru současné judikatury, respektive jejím rozporům zejména v otázkách emailu bez elektronického podpisu a (ne)splnění požadavku písemné formy, vztahu ustanovení § 561 a § 562 občanského zákoníku, povahy naskenovaného vlastnoručního podpisu, unikátního ID a *click-through* smluv, dvoufaktorového ověření v podobě SMS zprávy, podpisu myší do prázdného pole na internetové stránce, požadavku na vyšší formy elektronických podpisů ke splnění písemné formy a záměny požadavku písemné formy a identifikace. V poslední části kapitoly je rozebráno možné řešení pro sjednocení soudní praxe.

V šesté kapitole je nastíněna perspektiva elektronických podpisů v budoucím vývoji, zejména s ohledem na plánovanou novelu nařízení eIDAS, známou pod označením eIDAS 2.0. a nedávno spuštěnou aplikaci eDoklady.

Klíčová slova: elektronický podpis, písemné právní jednání, digitální kontinuita

Electronic legal transactions with a focus on simple electronic signatures

Abstract

The thesis is divided into six chapters. The first chapter consists of an introduction. The second chapter presents the general regulation and the meaning of the signature with a brief historical background necessary to assess the possible applicability of earlier conclusions to the current legal regulation.

The third chapter is devoted to the current regulation and individual types of electronic signatures, *i.e.* the division into qualified electronic signature, advanced electronic signature and simple electronic signature and the Czech specificity in the form of advanced electronic signature based on a qualified certificate for electronic signatures, commonly known as recognised electronic signature. The chapter also concludes with a discussion of biometric signature, which is increasingly used in practice.

The fourth chapter deals with the written form of legal transactions, *i.e.* a detailed analysis of the Sections 561 and 562 of the Civil Code, including their interrelation. Furthermore, aspects of digital continuity in higher levels of electronic signatures and their comparison with simple electronic signature are discussed. In the last part of the chapter, different types of electronic contracts and the differences between the evidentiary effects of different types of electronic signatures and the (in)validity of a written legal transactions are discussed.

In the fifth chapter, the author of the thesis analyses the current case law and its contradictions, in particular on the issues of email without electronic signature and (non-)fulfilment of the requirement of written form, the relationship between the provisions of Sections 561 and 562 of the Civil Code, the nature of scanned handwritten signature, unique ID and click-through contracts, two-factor authentication in the form of SMS message, mouse signature in a blank field on a website, the requirement of higher levels of electronic signatures to fulfil the written form and the confusion between the requirement of written form and identification. The last part of the chapter discusses possible solutions to unify court practice.

The sixth chapter outlines the future prospects for electronic signatures, particularly in light of the planned amendment to the eIDAS regulation, known as eIDAS 2.0, and the recently launched eDoklady application.

Key words: electronic signature, written legal transactions, digital continuity