



Adam Jareš, František Kasl  
a Pavel Loutocký

# SOUČASNÉ VÝZVY A PŘÍLEŽITOSTI UZAVÍRÁNÍ SMLUV ONLINE

MASARYKOVA  
UNIVERZITA

ACTA UNIVERSITATIS BRUNENSIS IURIDICA  
EDITIO SCIENTIA

**MUNI**  
PRESS

**MUNI**  
LAW

Anetě, Benjaminovi, Bartolomějovi a Metodějovi;  
Sabině, Martinovi a Adélce;  
Katce, Viktorce a Tondovi.  
Bez vás bychom to nezvládli.

# SOUČASNÉ VÝZVY A PŘÍLEŽITOSTI UZAVÍRÁNÍ SMLUV ONLINE

Adam Jareš, František Kasl, Pavel Loutocký



Masarykova univerzita  
Brno 2024

Vzor citace

JAREŠ, Adam; KASL, František a Pavel LOUTOCKÝ. *Současné výzvy a příležitosti uzavírání smluv online*. 1. vyd. Brno: Masarykova univerzita, 2024, 239 s. Spisy Právnické fakulty Masarykovy univerzity, Edice Scientia, sv. č. 757. ISBN 978-80-280-0522-1 (print), 978-80-280-0523-8 (online, pdf)

CIP - Katalogizace v knize

Jareš, Adam

Současné výzvy a příležitosti uzavírání smluv online / Adam Jareš, František Kasl, Pavel Loutocký – 1. vydání. -- Brno: Masarykova univerzita, 2024. 239 stran. -- Spisy Právnické fakulty Masarykovy univerzity, Edice Scientia, sv. č. 757. ISBN 978-80-280-0522-1 (print), 978-80-280-0523-8 (online, pdf)

347.44\* 004-027.22\* 347.135.224:004\* 346.548\* (048.8:082)\*

- smluvní právo
- digitální technologie
- elektronický podpis
- ochrana spotřebitele
- kolektivní monografie

347 – Soukromé právo [16]

Tato publikace vznikla na Masarykově univerzitě v rámci projektu Právo a technologie XII č. MUNI/A/1529/2023 podpořeného z prostředků účelové podpory na specifický vysokoškolský výzkum, kterou poskytlo MŠMT v roce 2024.

Právní stav byl zohledněn ke dni 15. 3. 2024.

Recenzenti:

JUDr. Eva Fialová, LL.M., Ph.D.

Mgr. Ing. Zbyněk Loebel, LL.M.

Gratis Open Access – <https://www.press.muni.cz/open-access>

© 2024 Masarykova univerzita

ISBN 978-80-280-0523-8 (online ; pdf)

DOI <https://doi.org/10.5817/CZ.MUNI.M280-0523-2024>

# OBSAH

O autorech.....	11
Abstrakt a klíčová slova.....	13
Seznam použitých zkratk.....	15
Předmluva Radima Polčáka.....	17
Úvod.....	21

## I. Teoretická východiska uzavírání smluv online

1 Uzavírání smluv online jako projev virtualizace právního jednání.....	29
2 Specifika elektronického zachycení obsahu smluvního ujednání.....	33
3 Význam uzavírání smluv online v digitalizované společnosti.....	35

## II. Role digitálních technologií při vyjednávání a uzavírání smluv online

4 Specifika elektronické kontraktace a možná úskalí při identifikaci smluvních stran.....	39
4.1 Delokalizace smluv uzavíraných online.....	39
4.2 <i>Click-wrap</i> a <i>click-through</i> smlouvy.....	40
4.3 Úskalí při identifikaci smluvních stran.....	43
4.4 Dílčí závěr.....	44
5 Požadavky kladené na projev vůle zachycený elektronickým podpisem.....	45
5.1 Vlastnoruční podpis.....	45
5.2 Funkce plnění podpisem a požadavkem formy.....	47

5.3	Zachování písemné formy při využití elektronických prostředků	50
5.4	Naplnění písemné formy bez elektronického podpisu	54
5.5	Elektronické právní jednání jako projev zásad občanského práva	59
<b>6</b>	<b>Řešení nedostatků a vad smlouvy</b>	<b>63</b>
6.1	Náležitosti právního jednání	63
6.1.1	Písemná forma	63
6.1.2	Přísná písemná forma	66
6.2	Neplatnost elektronicky podepsané smlouvy	66
<b>7</b>	<b>Elektronický podpis</b>	<b>69</b>
7.1	Základní východiska a právní základ elektronického podpisu	69
7.2	Úrovně elektronického podpisu	72
7.2.1	Prostý elektronický podpis	72
7.2.2	Vyšších úrovně elektronických podpisů	76
7.2.3	Zaručený elektronický podpis	80
7.2.4	Kvalifikovaný elektronický podpis	81
7.2.5	Zaručený podpis založený na kvalifikovaném certifikátu	84
7.2.6	Uznávaný elektronický podpis	84
7.3	Srovnání vlastnoručního a elektronického podpisu	87
7.4	Úředně ověřený elektronický podpis	90
7.4.1	Zákon o právu na digitální služby	91
7.4.2	Ověření oprávněnou osobou	92
7.4.3	Záznam informačního systému veřejné správy	92
7.4.4	Využití údajů v základním registru obyvatel	93
7.4.5	Ověření elektronického podpisu na plné moci	93
7.4.6	Aktuální relevantní rozhodovací praxe	95
7.5	Vybrané varianty užití elektronických podpisů při soukromoprávním jednání	96
7.5.1	Uvedení jména v elektronickém dokumentu a e-mailu	96
7.5.2	Naskenovaný vlastnoruční podpis	99
7.5.3	Dynamický biometrický podpis	101
7.5.4	PIN a heslo	107
7.5.5	Click-wrap a click-through smlouvy	108
7.5.6	Elektronický podpis v datových schránkách	109
7.6	Právní rámec pro vzdálené podepisování	111

<b>8 Elektronické nástroje využívané pro uzavírání smluv online</b> .....	115
8.1 Kontraktační platformy a jiné nástroje pro uzavírání smluv online.....	115
8.2 Užití bankovní identity při uzavírání smluv online .....	117
8.3 Evropská peněženka digitální identity a elektronické podepisování.....	120
8.4 Využití protokolu <i>blockchain</i> pro uzavírání smluv .....	124
8.4.1 Přiblížení specifické povahy protokolu blockchain .....	125
8.4.2 Podstata smart kontraktů.....	127
8.4.3 Závislost smart kontraktu na „oracles“ jako jeho základní limitace.....	130
8.4.4 Zákonnost zachycení smluvního jednání pouze formou smart kontraktu.....	131
8.4.5 Závěrem k využitelnosti smart kontraktů při uzavírání smluv online.....	133
8.4.6 Automatizace plnění smlouvy skrze smart kontrakt .....	134
<b>9 Doručování elektronických právních jednání</b> .....	137
9.1 Evropské doporučené doručování.....	137
9.2 Soukromoprávní jednání prostřednictvím datových schránek.....	138
9.2.1 Obecné výkladové otázky při doručování pomocí datových schránek.....	139
9.2.2 Fikce doručení.....	143
9.2.3 Teorie dojití .....	145
9.2.4 Poměr teorie dojití k fikci doručení datové zprávy.....	147
9.3 Specifika doručování v pracovním právu.....	148
<b>10 Ochrana spotřebitele při uzavírání elektronických smluv</b> .....	153
10.1 Obecně k povinnostem podnikatele při uzavírání smlouvy se spotřebitelem.....	153
10.2 Ochrana spotřebitele před překvapivými obchodními podmínkami.....	155
10.3 Přípustnost poskytování obchodních podmínek hypertextovým odkazem.....	156
10.4 Ochrana spotřebitele v souvislosti s digitálním obsahem.....	157



## III. Využití digitálních technologií po uzavření smlouvy

<b>11 Rostoucí potenciál uplatnění digitálních technologií po uzavření smlouvy</b> .....	161
11.1 Smlouvy o poskytování digitálního obsahu.....	162
11.2 Smlouvy na nákup zboží přes e-shop.....	163
11.3 Smlouvy na poskytování služeb či personalizovaného plnění.....	164
11.3.1 Organizační a plánovací nástroje.....	164
11.3.2 Asistenční komunikační nástroje a nástroje pro online řešení sporů.....	165
11.3.3 Nástroje pro vytváření či zajištění vlastního předmětu plnění.....	166
11.4 Rostoucí význam digitální stopy smluvního vztahu.....	167
<b>12 Elektronická archivace právních jednání</b> .....	169
12.1 Obecně k elektronické archivaci.....	169
12.2 Další relevantní služby vytvářející důvěru.....	170
12.2.1 Elektronická pečeť.....	170
12.2.2 Elektronické časové razítko.....	173
12.3 Záznamy o právních jednáních při archivaci.....	174
12.4 Revize nařízení eIDAS a elektronická archivace.....	175
12.4.1 Elektronická archivace jako nová služba vytvářející důvěru.....	175
12.4.2 Využití protokolu blockchain a podobných technologií pro archivaci.....	177
<b>13 Vymáhání závazků z elektronicky podepsaných smluv</b> .....	181
13.1 Úvod.....	181
13.2 Elektronické důkazy.....	181
13.2.1 Volné hodnocení důkazů a další zásady.....	182
13.2.2 Nařízení eIDAS a elektronické důkazy.....	183
13.2.3 Zásada nediskriminace.....	184
13.3 Dokazování elektronickými podpisy, pečetěmi a razítky.....	186
13.4 Důkazní břemeno při dokazování pravosti podpisu.....	189

<b>14 Rozhodovací praxe z posledních let</b> .....	191
14.1 Nelze uzavřít smlouvou jen výměnou e-mailů .....	191
14.2 Oferta a akceptace dle dřívější právní úpravy .....	193
14.3 Elektronický podpis prostý ve formě unikátního ID.....	194
14.4 Potvrzení smluvních podmínek a zadání kódu z SMS .....	195
14.4.1 K písemnému právnímu jednání lze použít telefax .....	196
14.5 Doručení předžalobní výzvy e-mailem.....	198
14.6 E-mail musí být podepsán elektronickým podpisem.....	199
14.7 Elektronický podpis prostý sám neobstojí .....	199
14.8 Písemnost jen s uznávaným elektronickým podpisem.....	201
14.9 PIN jako elektronický podpis smlouvy .....	203
14.10 Uznání pouze kvalifikovaných a zaručených podpisů .....	203
14.11 Neplatnost smlouvy podepsané vložení SMS kódu .....	204
14.12 Prokázání identity podepisujícího a integrity dokumentu .....	206
<b>15 Soudy, smlouvy uzavřené online a elektronické důkazy</b> .....	209
15.1 Shrnutí k aktuálním trendům soudního rozhodování .....	212
<b>Závěr</b> .....	215
<b>Summary</b> .....	219
<b>Literatura a další použité zdroje</b> .....	223
Komentáře.....	223
Monografie a učebnice.....	224
Články a elektronické zdroje .....	226
Koncepční dokumenty Evropské unie.....	232
Rozhodovací praxe .....	233
Zahraniční.....	233
Česká a Československá.....	233
Právní předpisy .....	236
Zahraniční a unijní.....	236
Vnitrostátní .....	237



## O AUTORECH

**Adam Jareš** je ředitel Odboru právního a legislativního Digitální a informační agentury. Absolvoval magisterské a doktorské studium na Fakultě právnické Západočeské univerzity a rigorózní zkoušku ve specializaci Právo informačních a komunikačních technologií na Právnické fakultě Masarykovy univerzity. Rigorózní práci obhájil s tématem „Soukromoprávní úprava kryptoměn a perspektivy jejich regulace“ a disertační práci s tématem „Smlouva podepsaná elektronickým podpisem“. Má za sebou zkušenosti z advokacie, soukromého i neziskového sektoru, státní správy i samosprávy. Pravidelně publikuje a na vysokých školách je v oblasti práva informačních technologií zapojen do akademického výzkumu a výuky.

**František Kasl** působí jako odborný pracovník v Centru vzdělávání, výzkumu a inovací v oblasti informačních a komunikačních technologií na Fakultě informatiky a na Ústavu práva a technologií na Právnické fakultě Masarykovy univerzity. Podílí se na řadě národních i mezinárodních výzkumných projektů věnovaných mj. specifikům ochrany soukromí a osobních údajů ve zdravotnickém, energetickém a dopravním sektoru. Od roku 2017 přednáší specializovaná témata související mj. s kybernetickou bezpečností a ochranou osobních údajů. Je autorem nebo spoluautorem národních zpráv, výzkumných studií, knih a článků na tato a další témata. Je lektorem v programu LL.M. na Právnické fakultě Masarykovy univerzity, na Georg-August-Universität Göttingen a na Donau Universität Krems. V roce 2023 zahájil odbornou stáž na Information Society Law Center na Università degli Studi di Milano. Od roku 2017 byl zástupcem šéfredaktora časopisu *Revue pro právo a technologie* a od roku 2022 působí jako jeho šéfredaktor.

**Pavel Loutocký** je výzkumníkem a vedoucím úseku spolupráce na Fakultě informatiky Masarykovy univerzity, kde působí v rámci Centra vzdělávání, výzkumu a inovací v oblasti informačních a komunikačních technologií. Rovněž je odborným pracovníkem na Ústavu práva a technologií na Právnické fakultě Masarykovy univerzity a lektorem v rámci studijního programu *Kybernetická bezpečnost na Fakultě elektrotechniky a komunikačních*

technologií, Vysoké učení technické v Brně. Hlavním oblastem, kterým se věnuje výzkumně či výukově, je problematika elektronické identifikace a elektronických dokumentů, online ochrany spotřebitele, online řešení sporů, online platforem, elektronické kontraktace, doménových jmen, eJustice & eGovernmentu či kyberbezpečnosti a kyberkriminality. Úspěšně dokončil roční studia na University of Abertay, Dundee ve Skotsku a doktorská studia na Ústavu práva a technologií na Právnické fakultě Masarykovy univerzity. Od roku 2012 je pravidelným členem vybraných pracovních skupin fungujících v rámci Komise OSN pro mezinárodní obchodní právo (UNCITRAL). Působí rovněž jako externí lektor na Georg-August-Universität Göttingen či Donau Universität Krems.

# ABSTRAKT A KLÍČOVÁ SLOVA

## Abstrakt

Monografie se zaměřuje na elektronické uzavírání soukromoprávních smluv. Autoři se postupně zabývají předpoklady pro platné elektronické soukromoprávní jednání a překážkami pro jeho širší užití či relevantní rozhodovací praxí. V knize se věnují také dílčím aspektům, které v rámci elektronické kontraktace vyvstávají v soudobé společnosti, například alternativním technologiím a nástrojům souvisejícím s elektronickou kontraktací, a zaměřují se také na specifické subjekty (například na spotřebitele). V závěru se autoři zabývají vymáháním závazků z elektronicky podepsaných smluv v souvislosti s jejich důkazní spolehlivostí.

Na řešená témata autoři nenahlíží pouze z pozic českého právního řádu, ale věnují se jim prizmatem evropských předpisů, zejména nařízení eIDAS a jeho revize schválené v roce 2024. Téma je v knize zároveň vnímáno v kontextu strategických dokumentů Evropské unie a aktuálních trendů v oblasti elektronického právního jednání.

## Klíčová slova

Elektronické právní jednání; elektronický podpis; nařízení eIDAS; elektronická kontraktace; digitální dekáda; blockchain; virtualizace; spotřebitel; elektronická archivace.



# SEZNAM POUŽITÝCH ZKRATEK

## **DEPO**

Zákon č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci

## **DLT**

Technologie distribuované účetní knihy (*Distributed Ledger Technology*)

## **nařízení 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

## **notářský řád**

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

## **obč. zák. nebo občanský zákoník**

Zákon č. 89/2012 Sb., občanský zákoník

## **občanský soudní řád**

Zákon č. 99/1963 Sb., občanský soudní řád

## **občanský zákoník z roku 1964**

Zákon č. 40/1964 Sb., občanský zákoník

## **obecné nařízení**

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)

## **ODR**

Řešení sporů online (*Online Dispute Resolution*)



## **Úřad**

Úřadu pro ochranu osobních údajů

### **zák. o advokacii**

Zákon č. 85/1996 Sb., o advokacii

### **zák. o el. podpisu**

Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)

### **zák. o ověřování nebo zákon o ověřování**

Zákona č. 21/2006 Sb., o ověřování shody opisu nebo kopie s listinou a o ověřování pravosti podpisu a o změně některých zákonů (zákon o ověřování)

### **zák. o právu na digitální služby**

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

### **zák. o službách vytvářejících důvěru**

Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce

### **zák. práce nebo zákoník práce**

Zákon č. 262/2006 Sb., zákoník práce

## PŘEDMLUVA RADIMA POLČÁKA

Thomas Hobbes považuje za jednu z největších lidských slabostí nutkavou potřebu vzdorovat času. Tato potřeba se projevuje různě, od zájmu o plastické operace nebo určité typy zboží zaručeně řešící krizi středního (nebo jakéhokoli) věku, přes frenetickou snahu natáčet si nebo fotit jakékoli významné nebo zajímavé (ale z podstaty nenávratné) životní okamžiky až po nutkání zanechat po sobě nějaký pomník nebo alespoň totem.

Nikoli přímo iracionální, ale podobně sisyfovskou aktivitou snažící se vzdorovat času, je i dokazování. Jeho účelem je totiž přenést soud nebo jiný orgán autoritativně aplikující právo zpět v čas do okamžiku, kdy se stala právní skutečnost, která je předmětem řízení. Vypovídací hodnota a spolehlivost důkazu je tedy za situace, kdy je důkaz sám o sobě pravý, tím větší, čím lépe je příslušný důkazní prostředek schopen odolat času.

Snaží-li se člověk o právní jednání a má-li přitom, byť i jen sebemenší, podezření, že se takové jednání může někdy v budoucnosti stát předmětem rozhodování nějakého orgánu veřejné moci, je na místě pragmatický přístup. Je třeba se ptát, jak co nejvěrněji takovým jednáním vygenerovat kvalitní důkaz způsobilý spolehlivě přenést do minulosti orgán, který bude o něm rozhodovat a dát tomuto orgánu dostatečnou praktickou jistotou ohledně toho, co bylo jeho předmětem.

Tato knížka zabývá se tím, jak soukromoprávně jednat v online prostředí. To v právě zmíněném pragmatickém smyslu znamená, že hledá odpověď na otázku, jak elektronicky zachytit a dokumentovat právní jednání do formy důkazu, který v dostatečné míře praktické jistoty věrně a spolehlivě přeneseme zpět v čas toho, před kým bude proveden. Autoři se tedy nevěnují jen možností právního jednání upraveným obecnou nebo specifickou legislativou, ale rovněž rozebírají způsoby, kterými se s různými formami elektronického právního jednání s větším nebo menším úspěchem vypořádává rozhodovací praxe našich civilních soudů a dokonce naznačují způsoby, kterým se tato praxe může dále ubírat.

Výklad provedený v analytických částech této knížky poskytuje velmi solidní zázemí pro reflexi dvou problémů, které osobně ve vztahu k judičiální reflexi

elektronických forem právního jednání považují za zásadní. Prvním je oddělení otázek skutkových a právních – zde konkrétně právních otázek formy právního jednání a přípustnosti důkazu a skutkové otázky spolehlivosti takového důkazu. Autoři na podkladě poctivě analyzovaného souboru soudních rozhodnutí správně poukazují například na to, že ani dokument opatřený „pouze“ jednoduchým elektronickým podpisem nesmí soud *a priori* odmítnout jako písemnost nebo jako důkaz jen kvůli absenci „lepšího“ podpisu, ale musí se konkrétně zabývat jeho individuální důkazní spolehlivostí.

Druhým zásadním problémem, kterému je v této knížce věnována pozornost, a který je bezprostředním důsledkem virtualizace právního jednání, je netradiční řešení důkazní spolehlivosti elektronického dokumentu koherenční teorií pravdivosti. Zatímco listina je obvykle způsobilá k prokázání rozhodných skutečností i ověření své spolehlivosti sama o sobě prostou korespondenční teorií, může u elektronického dokumentu běžně docházet k tomu, že písemnost sice sama o sobě prokáže rozhodnou právní skutečnost (zde právní jednání), ale nelze z ní samotné ověřit její spolehlivost. Typickým příkladem mohou být smlouvy uzavírané v e-shopech, které jsou sice obvykle podepsány kliknutím na tlačítko, tj. důkazně *per se* nepříliš spolehlivým jednoduchým elektronickým podpisem. K jejich podpisu ale dochází v bezpečně autentizovaném prostředí, jehož obecné parametry a konkrétní metadata k předmětné transakci dodávají příslušné elektronické písemnosti kýženou důkazní spolehlivost.

Zajímavým zpestřením výkladu je v tomto směru i část věnovaná využití technologie *distributed ledger*. I v tomto případě se vlastně jedná o technologii zajišťující důkazní spolehlivost jinak relativně jednoduchého písemného právního jednání podepsaného prostým elektronickým odpisem. Velmi specifický rozměr této formě právního jednání ještě dodává možnost jeho technicky neoddělitelného spojení s předmětným plněním. Vcelku omezený prostor, který je této problematice v rámci knihy věnován, ale dokládá stále relativně omezený význam tohoto typu právního jednání v naší reálné praxi. Podobně vhodné, ale nikoli neúměrně rozsáhlé, jsou i exkurzy provedené v různých kapitolách do problematiky doručování, která má v našem právním prostředí až fetišistický či folklórní charakter.

Obecně lze říct, že především analýza naší prvostupňové rozhodovací praxe v různých částech této knihy ukazuje, že se můžeme u našich civilních soudů na jedné straně setkat s adekvátním pochopením elektronického právního jednání a jeho právní úpravy doprovázeným důkladnou a přesvědčivou právní i skutkovou argumentací. Na straně druhé ale tato knížka poukazuje i na případy, kdy mají naše soudy ještě určité rezervy i v chápání základních parametrů elektronického právního jednání nebo ve znalostech jeho obecné nebo speciální zákonné úpravy.

To jen dokládá, že i problematika, kterou se naše doktrína i praxe intenzivně zabývají již třetí dekádu, je z praktického hlediska stále ve vývoji a žádá si vedle soustavné pozornosti i specializovaných odborných publikací, mezi které patří i tato kniha. Doufám tedy, že vedle naší komerční praxe poslouží tato publikace i k inspiraci našim soudům, a že se nějakou cestou snad dostane na mapě naší civilní justice i do stinných míst, kam světlo technického a právního pokroku z nějakého důvodu ani za uplynulých pár desetiletí ještě zcela neproniklo.

*V Brně 3. 1. 2024*

*Radim Polčák*



# ÚVOD

Informační technologie přinášejí řadu možností pro usnadnění soukromoprávního styku, právního jednání a uzavírání smluv. Na internetu uzavíráme smlouvy pravidelně, ať již při nákupu v e-shopu nebo pro využití různých online služeb či platform. Komunikace a transakce probíhající na dálku jsou s užitím informačních technologií jednodušší. Díky tomu roste počet smluv uzavíraných elektronicky, a to především smluv uzavíraných se spotřebiteli. Tyto smlouvy nemusí být na internetu jen uzavírány, ale v případě různých online služeb také plněny (příkladem budiž poskytovatelé služeb sdílení obsahu online typu Youtube či služeb software as a service typu Google).<sup>1</sup>

Soukromoprávní úprava závazků představuje jeden ze základních kamenů našeho právního řádu, a to již od jeho římskoprávních kořenů.<sup>2</sup> Rozsáhlý korpus české právní doktríny<sup>3</sup> je věnován této oblasti a mapuje dynamický vývoj, kterým prošlo teoretické pojetí, dílčí instituty i potřeby praktické aplikace na měnící se společnost a její potřeby.

Římskoprávní tradici, stále znatelnou a vyučovanou v úvodu studia oboru práva, převzala a do značné míry překryla civilistická tradice, v českém právu pak jako historická inspirace slouží především německá a rakouská, reflektující postupně nový kontext společenských vztahů při zachování principů

---

1 Srov. KYSELOVSKÁ, T. Působnost práva na internetu. In: POLČÁK, R. a kol. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 41.

2 TELEČ, I. Předmluva k prvnímu vydání. In: TINTĚRA, T., PETR, P. *Základy závazkového práva. 1.díl. 2. vyd.* Praha: Leges, 2020, s. 17. ISBN 9788075024762, PELIKÁN, R., PELIKÁNOVÁ, I. In: ŠVESTKA, J., DVORÁK, J., FIALA, J. a kol. *Občanský zákoník. Komentář. Svazek V (§ 1721 až 2520)*. Praha: Wolters Kluwer, 2014, 1700 s., s. 1. ISBN 9788074786389, nebo TINTĚRA, T., PETR, P. *Základy závazkového práva. 1.díl. 2. vyd.* Praha: Leges, 2020, 288 s., s. 25. ISBN 9788075024762.

3 ŠVESTKA, J., DVORÁK, J., FIALA, J. a kol. *Občanský zákoník. Komentář. Svazek V (§ 1721 až 2520)*. Praha: Wolters Kluwer, 2014, 1700 s. ISBN 9788074786389, PRAŽÁK, Z., FIALA, J., HANDLAR, J. a kol. *Závazky z právních jednání podle občanského zákoníku. Komentář ke § 1721–2893 OZ*. Praha: Leges, 2017, 1680 s. ISBN 9788075021588, PETROV, J., VÝTISK, M., BERAN, V. a kol. *Občanský zákoník. Komentář. 2. vyd.* Praha: C. H. Beck, 2019, 3276 s. ISBN 9788074007477, TINTĚRA, T., PETR, P. *Základy závazkového práva. 1.díl. 2. vyd.* Praha: Leges, 2020, 288 s. ISBN 9788075024762, TINTĚRA, T., PETR, P. a kol. *Základy závazkového práva. 2.díl. 2. vyd.* Praha: Leges, 2023, 301 s. ISBN 9788075026675, či LAVICKÝ, P., POLIŠENSKÁ, P. *Vznik a obsah závazků*. Praha: Wolters Kluwer, 2015, s. 304. ISBN 9788074787546.

a podstaty.<sup>4</sup> Ta je stále doktrinálně směřodatným východiskem skrze právo prvorepublikové, k jehož tradici se současné české soukromé právo otevřeně hlásí.<sup>5</sup>

Nepominutelný a rostoucí vliv na české právo však má v důsledku reálné politické, právní i ekonomické provázanosti jak moderní kontinentální pojetí ovlivněné stále dalekosáhlejším dopadem práva Evropské unie,<sup>6</sup> tak v kontextu informačních a komunikačních technologií i zdánlivě vzdálená a oddělená tradice anglo-americká.<sup>7</sup>

Přestože základní pojetí a principy právního jednání ve formě závazků, potažmo smluv, je možné považovat za etablované a veskrze neměnné, setrvale narůstající složitost, rozmanitost a dynamika jednání a vztahů v moderní společnosti přinášejí nepřetržitý příliv výzev a příležitostí pro jejich výklad a dotváření.

Jak již výstižně vyjádřila a zachytila řada autorů napříč dílčími tématy, stěžejní proměna, kterou i závazkové právo v posledních několika dekáдах prochází, se váže k technologické proměně společnosti, kterou je možné označit pojmy elektronizace, digitalizace či digitální transformace.<sup>8</sup> Její dopady jsou dnes již zřejmé v převážné většině lidských činností a s jejím rozvojem vznikly zcela nová odvětví, služby a možnosti interakce, které se strhující rychlostí pronikly do naší i většiny ostatních společností a se vznikem nového virtualizovaného

<sup>4</sup> DVOŘÁK, J., ŠVESTKA, J., ZUKLÍNOVÁ, M. a kol. *Občanské právo hmotné. Svazek I. Díl první: Obecná část*. 2. aktualizované a doplněné vyd. Praha: Wolters Kluwer, 2016, 436 s., s. 57. ISBN 9788075521873, blíže viz HURDÍK, J., LAVICKÝ, P. a kol. *Změny soukromého práva v České republice a dalších evropských zemích*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2014, 122 s., s. 54. ISBN 9788021076020.

<sup>5</sup> ELIÁŠ, K. *Nový občanský zákoník s aktualizovanou důvodovou zprávou a rejstříkem*. Ostrava: Sagit, 2012, s. 33 a násl. ISBN 978-80-7208-922-2.

<sup>6</sup> DVOŘÁK, J., ŠVESTKA, J., ZUKLÍNOVÁ, M. a kol., 2016, op. cit., s. 48, blíže viz HURDÍK, J., LAVICKÝ, P. a kol. *Změny soukromého práva v České republice a dalších evropských zemích*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2014, 122 s., s. 9 a násl. ISBN 9788021076020.

<sup>7</sup> Srov. např. MAISNER, M. a kol. *Základy softwarového práva*. Praha: Wolters Kluwer, 2011, 356 s., s. 26. ISBN 9788073576387, popř. KMENT, V. *Elektronické právní jednání: Analýza s důrazem na využití elektronického podpisu podle práva EU, České republiky a Německa*. Praha: Wolters Kluwer, 2018, 460 s., s. 55. ISBN 9788075528148.

<sup>8</sup> Digitální budoucnost pro Evropu. *Rada Evropské unie* [online]. 2023 [cit. 23. 10. 2023]. Dostupné z: <https://www.consilium.europa.eu/cs/policies/a-digital-future-for-europe/>

prostoru – kyberprostoru<sup>9</sup>, přinesly nespočet nových kontextů, pro které bylo a je zapotřebí hledat vhodné zasazení do struktury závazkového práva.<sup>10</sup>

Katalyzátorem digitalizace právního styku byla pandemie nemoci COVID-19. Evropská unie nyní směřuje značné úsilí k urychlení vývoje v této oblasti. Před vydáním této monografie byl schválen text revize nařízení eIDAS<sup>11</sup>, od které si Evropská komise slibuje, že alespoň 80 % občanů Evropské unie bude mít do roku 2030 možnost využívat digitální identity založené na revizi stávajícího rámce k přístupu ke klíčovým veřejným službám v oblasti digitální identifikace. Revize však také směřuje na větší dostupnost služeb vytvářejících důvěru v rámci soukromoprávních transakcí a v této souvislosti zavádí nové služby vytvářející důvěru.

Tlak na digitalizaci je patrný i z koncepčních dokumentů Evropské unie. Evropská komise konstatovala již v roce 2019 ve sdělení nazvaném jako Zelená dohoda pro Evropu, že Evropa musí využít potenciálu digitální transformace, jež je klíčovým faktorem umožňujícím dosažení cílů Zelené dohody. Naráží také na to, že digitální technologie jsou rozhodujícím faktorem pro dosažení cílů udržitelnosti Zelené dohody v mnoha různých odvětvích. Komise zde naráží na opatření, jež zajistí, aby digitální technologie, například umělá inteligence, 5G sítě, cloud a *edge computing* a internet věcí, zrychlily a maximalizovaly dopad politik při řešení změny klimatu a ochraně životního prostředí.<sup>12</sup>

Evropský parlament a Rada na konci roku 2022 představily politický program „Digitální dekáda 2030“.<sup>13</sup> Mezi digitální cíle, kterých má být dosaženo

<sup>9</sup> K pojmu např. POLČÁK, R. *Internet a proměny práva*. Praha: Auditorium, 2012, s. 72. ISBN 9788087284223.

<sup>10</sup> Zmíněno již například v KOŠČÍK, M. Pojem a obsah právních úkonů na internetu. *Revue pro právo a technologie*. 2011, roč. 2, č. 4, s. 36. Dostupné z: <https://journals.muni.cz/revue/article/view/4089>

<sup>11</sup> Text revize nařízení eIDAS přijatý Evropským parlamentem je dostupný z: [https://www.europarl.europa.eu/doceo/document/TA-9-2024-0117\\_CS.pdf](https://www.europarl.europa.eu/doceo/document/TA-9-2024-0117_CS.pdf). Po vysázení textu této monografie byla revize nařízení eIDAS schválena i Radou a byla před zveřejněním v Úředním věstníku EU.

<sup>12</sup> EVROPSKÁ KOMISE. Sdělení Komise Evropskému parlamentu, Evropské radě, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů Zelená dohoda pro Evropu. *EUR-Lex* [online]. 2019 [cit. 11. 3. 2023]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A52019D0640&qid=1678544467235>

<sup>13</sup> Rozhodnutí Evropského parlamentu a Rady (EU) 2022/2481 ze dne 14. prosince 2022, kterým se zavádí politický program Digitální dekáda 2030. *EUR-Lex* [online]. 2022 [cit. 11. 3. 2023]. Dostupné z: <https://eur-lex.europa.eu/eli/dec/2022/2481/oj/ces>



do roku 2030, patří to, že 100 % klíčových veřejných služeb bude dostupných online a v relevantních případech bude pro občany a podniky Evropské unie možné komunikovat online s orgány veřejné správy, nebo cíl, že 100 % občanů Evropské unie bude mít přístup k některému z bezpečných prostředků pro elektronickou identifikaci uznávanému po celé Evropské unii, což jim umožní mít plnou kontrolu nad transakcemi zahrnujícími ověření totožnosti a sdílenými osobními údaji.<sup>14</sup> Míří se zde také na podporu evropské infrastruktury *blockchainových* služeb prostřednictvím projektů pro více zemí usnadňujících dosahování obecných a digitálních cílů.<sup>15</sup>

Podobný závazek vyplývá i z Evropského prohlášení o digitálních právech a zásadách pro digitální dekádu. Podle něj by každý měl mít online přístup ke klíčovým veřejným službám v Evropské unii a po nikom nebude požadováno, aby při přístupu k digitálním veřejným službám a jejich využívání poskytovat údaje častěji, než je nezbytné. Evropská komise se zde zavazuje, že zajistí, aby všem lidem žijícím v Evropské unii byla nabídnuta možnost využívat dostupnou, dobrovolnou, bezpečnou a důvěryhodnou digitální identitu umožňující přístup k široké škále online služeb.<sup>16</sup>

Tlak na digitální transformaci je patrný i v České republice. Lze jej spatřovat například v zákoně o právu na digitální služby přijatém v roce 2020<sup>17</sup> a navazujícím rozsáhlém novelizačním zákoně o další elektronizaci postupů orgánů veřejné moci<sup>18</sup>, zřízení Digitální a informační agentury či ve snahách o digitalizaci osobních dokladů<sup>19</sup>.

Tyto evropské a české dokumenty a předpisy sice míří především na veřejnoprávní styk, rozvoj elektronické identifikace a elektronických transakcí

<sup>14</sup> Rozhodnutí Evropského parlamentu a Rady (EU) 2022/2481 ze dne 14. prosince 2022, kterým se zavádí politický program Digitální dekáda 2030. *EUR-Lex* [online]. 2022, čl. 4 [cit. 11. 3. 2023]. Dostupné z: <https://eur-lex.europa.eu/eli/dec/2022/2481/oj/ces>

<sup>15</sup> *Ibid.*, Příloha.

<sup>16</sup> EVROPSKÁ KOMISE. Evropské prohlášení o digitálních právech a zásadách pro digitální dekádu 2023/C 23/01. *EUR-Lex* [online]. 2023, čl. 7 [cit. 11. 3. 2023] Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32023C0123%2801%29&qid=1678546597447>

<sup>17</sup> Zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů (dále „zák. o právu na digitální služby“).

<sup>18</sup> Zákon č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci (dále „DEPO“).

<sup>19</sup> V lednu 2024 došlo ke spuštění aplikace eDoklady, která slouží k využití digitálního stejnopisu průkazu (více viz <https://edoklady.gov.cz>).

v rámci veřejnoprávního styku však podle nás bude mít vliv na větší využívání a rozvoj služeb vytvářejících důvěru (a nejen jich) i v rámci soukromoprávního styku. I na tomto poli lze zaznamenat velké množství zahraničních, ale částečně i českých doktrinárních textů a soudních rozhodnutí.<sup>20</sup>

Přesto se domníváme, že jak pro laické, tak odborně znalé čtenáře v současnosti v českém právním diskurzu absentuje publikace, ve které by byly zevrubně a s vysokou mírou aktuálnosti pokryty klíčové právní důsledky digitalizace soukromoprávního jednání v souvislosti s uzavíráním smluv online.

Naší ambicí je v rámci této monografie právě takový zdroj informací čtenáři nabídnout a doplnit tak další díl do rozsáhlé mozaiky potřebné pro zdárné uchopení současného právního rámce pro soukromoprávní smluvní závazkové vztahy.

Věříme, že následující text bude shledán za přínosný při provedení touto problematikou s akcentem na nedávný vývoj na poli digitalizace společenských vztahů, legislativní a výkladový posun ve vztahu ke stěžejním prvkům elektronické kontraktace a důsledků virtualizace právního jednání.

Kniha je rozdělena na tři části. V té první mapujeme teoretická východiska pro diskuzi právních i mimoprávních souvislostí uzavírání smluv online. V druhé se zaměříme na právní rámec pro využití digitálních technologií při sjednávání a uzavírání soukromoprávních smluv. Zabýváme se v ní mimo jiné komunikací stran, identifikací smluvních stran, kontraktačními platformami a elektronickým podepisováním. Ve třetí části se přesouváme k právní úpravě využití digitálních technologií po uzavření smlouvy, tedy zejména k archivaci elektronicky uzavřených smluv, automatizaci smluvního plnění či vymáhání závazků z těchto smluv.

---

<sup>20</sup> K tomu srov. seznam literatury a užití rozhodovací praxe v této knize.



# **I. TEORETICKÁ VÝCHODISKA UZAVÍRÁNÍ SMLUV ONLINE**



# 1 UZAVÍRÁNÍ SMLUV ONLINE JAKO PROJEV VIRTUALIZACE PRÁVNÍHO JEDNÁNÍ

Moderní společnost je z perspektivy práva do značné míry protkána sítí právních jednání na základě soukromoprávních smluv. Od zakoupení nápoje v automatu přes cestu hromadnou městskou dopravou po užívání osobního počítače poskytnutého zaměstnavatelem nás smlouvy provází téměř na každém kroku. I na vnitřní uspořádání a fungování obchodní korporace lze nahlížet jako na systém vzájemně propojených smluv. Jak bylo nastíněno již v úvodu, byť je smluvní právo etablovanou a rozsáhle řešenou oblastí práva, dynamika současné doby a rostoucí podíl digitalizace s sebou i v této oblasti přinášejí nové možnosti, koncepty a nástroje, které je třeba reflektovat.

V této monografii máme za cíl pojednat o výseku problematiky, se kterou se úzce váže výkladové specifikum virtualizovaných právních jednání. Za smlouvy uzavírané online jsou v této monografii považovány takové smlouvy, u kterých je využíváno elektronických informačních a komunikačních technologií pro komunikaci a uzavření smlouvy na dálku.<sup>21</sup> Tím není zasaženo do principů a požadavků pro platné uzavření smlouvy, je však nutné přihlížet ke specifickým nástrojům, které jsou pro tyto účely využívány a přiměřeně tyto požadavky aplikovat či doplnit. Je-li tedy platnost smlouvy podmíněna náležitou identifikací smluvních stran, otevírá se s přenesením procesu kontraktace do prostředí kyberprostoru za využití elektronických nástrojů, jako jsou kontrakční platformy či elektronický podpis, řada nových výkladových otázek, které mají s rostoucím rozšířením těchto prostředků stále významnější dopad do praxe. Pro úvahy, které k nim v rámci následujících kapitol monografie nabízíme, je však významné mít na paměti teoretická východiska, která se s tímto okruhem právních jednání pojí.

Předně tedy platí, že právní jednání prostřednictvím informačních a komunikačních technologií je projevem fenoménu virtualizace. Tento pojem je používán již od antiky, a lze ho obecně definovat jako proces, při kterém zůstává zachována podstata daného, ale dochází k významné změně jeho formálních

<sup>21</sup> V dalším textu pracujeme zcela zaměnitelně s pojmy „elektronické uzavírání smluv“ a „elektronická kontraktace“.

znaků.<sup>22</sup> Hlavním smyslem virtualizace je zbavit starou formu s ní spojených problémů, přičemž problémy související s formou novou by měly být méně závažné.<sup>23</sup> Tento fenomén se stále intenzivněji projevuje i v oblasti závazkového, resp. smluvního práva. Uzavírání smluv prostřednictvím informačních technologií či obecně právní jednání za jejich použití je toho příkladným projevem.

Důsledkem virtualizace je, že se u daného institutu mění vnější jevové znaky při současném zachování jeho původní podstaty.<sup>24</sup> Virtualizaci lze chápat jako reakci na potřeby společnosti v oblasti efektivnosti procesů, rychlosti komunikace či procesní ekonomii. Neměla by tudíž vzbuzovat obavy a souhlasíme se Ščerbou, že představuje žádoucí vyjádření aktuálních potřeb společnosti, na které musí příslušná legislativa vhodně reagovat.<sup>25</sup>

Virtualizaci lze dle tradiční doktríny spojovat s identifikací podobnosti a rozdílů mezi fyzickou a virtuální formou sekundárních objektů právních vztahů, resp. různých dalších pro právo relevantních fenoménů.<sup>26</sup> Typickou otázkou podle Polčáka může být například to, „*zda a jaký je rozdíl platného práva rozdíl např. mezi listinou a elektronickým dokumentem nebo mezi urážkou v hospodě a na internetu.*“<sup>27</sup> Virtualitu není na místě chápat jako opak reality. Virtualizované fenomény sdílejí svoji podstatu s reálnými fenomény a liší se od nich jen svými pozitivními projevy. Klíčovým faktorem úspěchu virtualizace je pak adekvátní specifikace podstatných komponent příslušného fenoménu. Tedy u písemného právního jednání půjde primárně o určení zachyceného projevu vůle, nikoliv o jeho nosič.<sup>28</sup>

Pro podporu východiska úvodu této kapitoly lze odkázat na Ščerbu, který dochází k závěru, že právní úprava elektronického uzavírání smluv vychází prakticky ze stejného pojmového, materiálního, společenského a právního základu, ze stejných zásad a právních principů a ze stejných soukromoprávních

22 Srov. POLČÁK, R. Pojem a metoda práva informačních technologií. In: POLČÁK, R. a kol. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 8.

23 POLČÁK, R., KASL, F., LOUČOCKÝ, P., MÍŠEK, J., STUPKA, V. Virtualizace právních vztahů a nové regulatorní metody v pozitivním právu. *Právník*. 2019, č. 1, s. 86.

24 Srov. POLČÁK, R. Praxe elektronických dokumentů. *Bulletin advokacie*. 2011, č. 7–8, s. 54.

25 ŠČERBA, T. Právně teoretické aspekty elektronické kontraktační. *Revue pro právo a technologii*. 2012, č. 5, s. 38.

26 Viz POLČÁK, R. Protiprávní jednání a škoda online. *Bulletin advokacie*. 2021, č. 6, s. 16.

27 POLČÁK, R. Elektronické právní jednání – změny, problémy a nové možnosti v zákoně č. 89/2012 Sb. *Bulletin advokacie*. 2013, č. 10, s. 16.

28 Srov. POLČÁK, R. Odpovědnost umělé inteligence a informační útvary bez právní osobnosti. *Bulletin advokacie*. 2018, č. 11, s. 23.

institutů, na kterých obecně spočívá závazkové (obligační) právo jako takové.<sup>29</sup> Podobně Mason konstatuje, že užívání elektronického podpisu předcházelo jakékoliv legislativě a v posledním desetiletí 20. století soudci aplikovali zavedené právní principy na nové technologie, aby se vypořádali s elektronickými podpisy, stejně jako byli soudci v 19. století konfrontováni se vzrůstajícím užitím tisku, psacích strojů a telegramů bez toho, aby musela být přijata nějaká speciální právní úprava.<sup>30</sup> Vlastnoručně a elektronicky podepsané smlouvy však mají každá svá specifika, která rozebíráme dále.

Vývoj v oblasti praktických aspektů elektronické kontraktace je hnán kupředu především potřebou co nejvíce zjednodušit kontraktaci v rámci obchodního styku, a to především při uzavírání smluv se spotřebiteli. Jak zmiňuje Raban, snaha o generování zisku je hlavním motivátorem pro vyvíjení neustále sofistikovanějších metod spolupráce v obchodním prostředí. Tento vývoj přitom často předchází zakotvení pravidel v podobě zákonné úpravy, respektive často směřuje k nalézání cest, jak limity nastavené zákonnými pravidly překonat.<sup>31</sup>

Zjednodušení a zrychlení právního styku si všímá i Zuklínová. Ta nepovažuje za zajímavou skutečnost, že technické prostředky nahrazují po právu písemný projev, pokud jde pouze o právní jednání jedné osoby ve smyslu neadresovaného zveřejnění vůle. Za zajímavé lze podle ní považovat takové skutečnosti, kde jde o jednání jedné osoby vůči jiné osobě (několika jiným osobám), při kterém se za využití komunikačních technologií právní styk na dálku fakticky blíží spíše situaci obdobné osobnímu styku nežli právně tradičnímu styku na dálku v podobě výměny dopisů.<sup>32</sup>

Je otázka, nakolik právo, resp. rozhodovací praxe reflektuje praxi elektronické kontraktace. Účastníci soukromoprávních vztahů mají stále větší zájem uzavírat smlouvy elektronicky, a to i za cenu nižší právní jistoty. Dokladem je rozvoj *click-through* smluv, které zjednodušují uzavírání distančních smluv, přináší však také některá rizika diskutovaná v dalších kapitolách

<sup>29</sup> ŠČERBA, 2012, op. cit., s. 75.

<sup>30</sup> MASON, S. *Electronic Signatures in Law*. London: University of London, 2017, s. 223.

<sup>31</sup> RABAN, P. Obchodní závazky – obecné otázky. In: RABAN, P. a kol. *Obchodní právo*. Brno: Václav Klemm, 2020, s. 315.

<sup>32</sup> Srov. ZUKLÍNOVÁ, M. *Právní jednání podle občanského zákoníku č. 89/2012 Sb. Komentář, srovnání se zahraničím a vybraná platná judikatura*. 1. vyd. Praha: Linde, 2013, komentář k § 562. Dostupné z: <http://www.codexis.cz> [cit. 15. 2. 2022].



této knihy.<sup>33</sup> Zákodárce se na tento trend pokouší reagovat a aspiruje na budování důvěryhodnosti online prostředí a zvýšení důvěryhodnosti elektronických transakcí.<sup>34</sup> Jak ukážeme v částech tohoto textu věnovaným rozhodovací praxi soudů, zdá se však, že tento trend v současné chvíli příliš nereflektuje tradičně konzervativní soudní praxe, která je při nakládání s elektronicky podepsanými smlouvami zatím notně nejednotná.

Virtualizace právního jednání do podoby elektronických dokumentů nemá svůj význam pouze z pohledu konečného produktu – elektronicky podepsané smlouvy či jiného právního jednání. Přínos má i ve zjednodušení negociace finální podoby smlouvy. Strany si běžně několikrát vymění elektronický dokument, jehož různé verze lze prostřednictvím různých elektronických nástrojů porovnávat a pracovat například pouze s posledně provedenými změnami bez potřeby detailního opětovného zkoumání celého znění rozsáhlé smlouvy.<sup>35</sup>

Svou roli a z ní vyplývající přínos má však v rostoucí míře virtualizace také po uzavření smlouvy. S novými technologiemi se rozšiřují možnosti využití moderních technologií pro automatizaci plnění uzavřené smlouvy.<sup>36</sup> Řešení vad uzavřených smluv má v online prostředí také stále účinnější vlastní nástroje. Vyhledání konkrétní smlouvy a jejího určitého ustanovení je jednodušší při vyhledávání v rámci elektronické databáze smluv než v rozsáhlém archivu listinných vlastnoručně podepsaných smluv. Elektronickou smlouvu lze také bez větších problémů rychle sdílet se třetí stranou bez potřeby jejího kopírování či skenování. V neposlední řadě pak elektronické zachycení nejen vlastního textu smlouvy, ale řady doprovodných aspektů a kontextových informací má zásadní význam pro vymáhání závazků, jelikož za pomoci takto zachycených elektronických důkazů vzniká nesrovnatelně komplexnější zachycení příslušného právního jednání a jeho souvislosti.<sup>37</sup> Především pro lepší pochopení posledně zmíněné roviny je ovšem na místě nejprve přiblížit, jak se elektronicky uzavřená smlouva liší od tradičního ústního či písemného ujednání.

<sup>33</sup> Zejména v kapitole 3.2. Srov také JANOUŠEK, M. Prostý elektronický podpis umožňující uzavření smlouvy při elektronické kontraktaci. In: RÓNOVSKÁ, K., HAVEL, B., LAVICKÝ, P. *Pocťa prof. Janu Hurdíkovi k 70. narozeninám. Základní otázky života, práva a vůbec...* Brno: Masarykova univerzita, Právnická fakulta, 2021, s. 141.

<sup>34</sup> Bod odůvodnění č. 1 a 2 nařízení eIDAS.

<sup>35</sup> Srov. zejména část II této knihy.

<sup>36</sup> Viz také část II této knihy.

<sup>37</sup> K dokazování a vymáhání závazků srov. zejména část III této knihy.

## 2 SPECIFIKA ELEKTRONICKÉHO ZACHYCENÍ OBSAHU SMLUVNÍHO UJEDNÁNÍ

Rozdíl mezi vlastnoručně a elektronicky podepsanou smlouvou lze vhodně ilustrovat na rozdílném osudu elektronického dokumentu připraveného v textovém editoru na počítači a jeho podpisu vlastnoručním či elektronickým podpisem. Pokud je takový dokument vytištěn a vlastnoručně podepsán, nevyhnutelně ztrácí část informační bohatosti a kvality, kterou by mu jinak dal elektronický podpis. Jednoduchým příkladem je, že u vícestránkového dokumentu mohou být snadno vyměněny některé strany či jeho obsah jinak nedohledatelně pozměněn. Tomu naopak zabrání podepsání dokumentu takovým elektronickým podpisem, který při ověření podpisu indikuje změnu obsahu dokumentu oproti podepsané podobě (indikuje integritu dokumentu).

Pokud se k fyzickému dokumentu připojí vlastnoruční podpis, tento podpis mění, resp. doplňuje obsah dokumentu. Naproti tomu elektronický podpis představuje data připojovaná k jiným datům (podepisovanému dokumentu) a vlastní obsah dokumentu tudíž nemodifikuje.<sup>38</sup> Listinný dokument v sobě implicitně neobsahuje další pouhým okem viditelné informace. Bude z něj možné sejmout otisky prstů, potvrdit uváděné skutečnosti (např. datum připojení podpisu) svědeckou výpovědí, kamerovým záznamem apod. Elektronické dokumenty v sobě kromě čitelného obsahu obsahují i další související metadata, která k čitelnému obsahu doplňují další informace o původu dokumentu a jeho elektronické stopě. Vedle samotného elektronického podpisu bude elektronicky podepsaná smlouva tedy obsahovat rozsáhlá a užitečná metadata, která bývají charakterizována jako kontextová data s informační hodnotou o hlavních datech. Může jít o různá data vytvořená uživatelem anebo automaticky systémem, která obsahují například informace o datu vytvoření dokumentu, posledním přístupem, zda byl někdy vytištěn, o času stráveném úpravami, jaký uživatel učinil poslední změny apod. Metadata jsou zvláště hodnotná proto, že mohou být následně použita při dokazování pro podložení jinak snadno zpochybnitelných tvrzení

<sup>38</sup> Dle čl. 3 odst. 10 nařízení eIDAS jsou elektronickým podpisem data ve letronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která podepisující osoba používá k podepsání.

či poskytnutí detailů o smluvním jednání, které nejsou jinak zachytitelné. Další data jsou k elektronickému dokumentu připojena při jeho elektronickém podepsání, opatření elektronickým časovým razítkem či elektronickou pečeti. Při užití dynamického biometrického podpisu pak zahrnují také biometrické údaje podepisující osoby, v případě kvalifikovaných certifikátů podrobnosti o tomto certifikátu a jeho držiteli. Také u odeslaného e-mailu bude k dispozici více dat než v případě listinného dokumentu, a to včetně IP adres a dalších automaticky připojovaných metadat.<sup>39</sup> Ani metadata však nemusí pomoci vždy. Dokument může vytvořit uživatel označený jinak než svým jménem a na počítači nepřipojeném k jakékoliv síti. Dokazování zde však bude v rovině důvěryhodnosti dostupných dat, na rozdíl od vytištěné listiny podepsané nečitelným podpisem bez dalších údajů o podepisující osobě, kde hlavní překážkou bude jejich celková absence.

Pro ilustraci práce s metadaty e-mailu lze použít rozhodnutí Nejvyššího správního soudu ze dne 4. 2. 2009, sp. zn. 1 As 90/2008. Byť se rozhodnutí týká přestupkového řízení, je možné jej použít jako příklad, jak lze pracovat s metadaty jako důkazem. V řízení bylo k prokázání viny nashromážděno více důkazů včetně IP adresy pachatele, která byla považována za nepřímý důkaz. V případě většího množství důkazů pak je podle soudu třeba určit, jestli tyto důkazy tvoří „*ucelený logicky provázaný důkazní řetězec*“.

<sup>39</sup> KORBEL, F., MELZER, F. Písemnost, elektronický a biometrický podpis v elektronickém právním jednání. *Bulletin advokacie*. 2014, č. 12, s. 35.

### 3 VÝZNAM UZAVÍRÁNÍ SMLUV ONLINE V DIGITALIZOVANÉ SPOLEČNOSTI

S utvářením závazků skrze smluvní jednání online se pravidelně setkává většina z nás, a to zřejmě častěji, než je na první pohled zjevné. I z poměrně konzervativního pojetí (především v tom smyslu, že toto pojetí vylučuje služby, které jsou zdarma, které jsou v online prostředí všudypřítomné a jejich využití je zpravidla podmíněno uzavřením smlouvy), které volí ve svém dotazníkovém šetření z roku 2022 Eurostat,<sup>40</sup> vyplývá, že online smlouvu na zboží či službu v nedávné době uzavřeno přes 75 % našich spoluobčanů (ve věku 16 až 74 let), což je mírně nad průměrem výsledků v rámci celé EU (68 %).<sup>41</sup> I v důsledku vynucené změny, které do našich životů vnesla pandemie COVID-19 a s ní spojené bezprecedentní omezování tradičního přístupu k fyzickému nákupu zboží a využívání služeb,<sup>42</sup> byl umocněn dlouhodobý trend digitalizace naší společnosti a velká část z nás se buďto musela nově seznámit s online objednávání zboží a služeb nebo přistoupila k jejich častějšímu využívání.<sup>43</sup>

V důsledku toho lze dnes o to výrazněji sledovat význam uzavírání smluv online. Snadno pozorovatelný je na rostoucí roli online platform, ať již v poskytování stále širšího spektra služeb a zboží spotřebitelům, tak v rámci dodavatelských řetězců a kontraktace mezi podniky.<sup>44</sup> Smluvní ujednání,

<sup>40</sup> Objednávání zboží a služeb online jednotlivci se vztahuje na období 3 měsíců před průzkumem a zahrnuje pronajaté ubytování nebo dopravní služby, nákup finančních produktů, telekomunikačních služeb, videoher nebo softwaru, jakož i informační služby z internetu, které jsou přímo placeny. Zboží a služby, které jsou získávány prostřednictvím internetu zdarma, jsou vyloučeny. Vyloučeny jsou rovněž objednávky učiněné prostřednictvím individualizovaných e-mailů či zpráv psaných uživatelem.

<sup>41</sup> Digital economy and society statistics – households and individuals. *EUROSTAT* [online]. 2022 [cit. 15. 8. 2023]. Dostupné z: [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital\\_economy\\_and\\_society\\_statistics\\_-\\_households\\_and\\_individuals#Ordering\\_or\\_buying\\_goods\\_and\\_services](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals#Ordering_or_buying_goods_and_services)

<sup>42</sup> COVID-19 has changed online shopping forever, survey shows. *UNCTAD* [online]. 2020 [cit. 15. 8. 2023]. Dostupné z: <https://unctad.org/news/covid-19-has-changed-online-shopping-forever-survey-shows>

<sup>43</sup> COVID-19 Impact on e-commerce. *UNECE* [online]. 2022 [cit. 15. 8. 2023]. Dostupné z: [https://unece.org/sites/default/files/2022-01/ECE\\_TRADE\\_468E\\_1.pdf](https://unece.org/sites/default/files/2022-01/ECE_TRADE_468E_1.pdf)

<sup>44</sup> OECD. *An Introduction to Online Platforms and Their Role in the Digital Transformation* [online]. 2019 [cit. 15. 8. 2023]. Dostupné z: <https://www.oecd.org/innovation/an-introduction-to-online-platforms-and-their-role-in-the-digital-transformation-53e5f593-en.htm>

ke kterým je přistupováno v rámci utváření právních vztahů online mají různý význam, složitost a závažnost. Jak bylo nastíněno v úvodu, i registrace uživatele pro využití služby, která je zdarma, představuje uzavření smlouvy online, zpravidla adhezní, směřující k ujednání podmínek, za jakých je uživatel danou službu oprávněn využívat a jaká oprávnění (především ve vztahu k osobním údajům uživatele a údajům o využívání služby) nabývá její poskytovatel. Narůstá však i význam digitálních nástrojů pro uzavírání složitých smluv mezi právníckými osobami, které s sebou přinášejí nové výzvy pro výklad a aplikaci existujícího právního rámce. V následujících kapitolách budeme věnovat pozornost klíčovým výzvám, které jsou s uzavíráním smluv online spojené a jejich reflexi v aktuálním odborném diskurzu a judikatuře.

## **II. ROLE DIGITÁLNÍCH TECHNOLOGIÍ PŘI VYJEDNÁVÁNÍ A UZAVÍRÁNÍ SMLUV ONLINE**



## 4 SPECIFIKA ELEKTRONICKÉ KONTRAKTACE A MOŽNÁ ÚSKALÍ PŘI IDENTIFIKACI SMLUVNÍCH STRAN

Z předchozího textu je patrné, že nepominutelným trendem je digitalizace napříč společnostmi, která se významně odráží i v praxi uzavírání smluv. Převážná většina smluv je tak dnes uzavírána za určité míry pomoci informačních a komunikačních technologií, ať již jde o textový editor, ve kterém je sepsáno znění smluvního ujednání nebo dochází k platbě přiložením karty k čtecímu zařízení. Různorodost takto vymezeného zapojení technologií je nezměrná, specifika jejich použití se však nejzřetelněji projevují v situacích, kdy je jejich využití stěžejní, tedy když je smlouva uzavřena elektronicky.

K tomu může dojít i offline, v situaci, kdy strany sjednají a uzavřou, tedy podepíší, smlouvu sice za využití elektronických nástrojů, ale za přítomnosti všech smluvních stran v jednom okamžiku na jednom místě (tedy nedochází k uzavření smlouvy na dálku). Děje se tak například v bankách či na pobočkách mobilních operátorů při uzavírání adhezních smluv o poskytování příslušené služby či její úpravě formou smluvního dodatku.

### 4.1 Delokalizace smluv uzavíraných online

Převládající formou elektronické kontraktace však je uzavírání smlouvy online, tedy na dálku. Ta s sebou však přináší řadu specifík. Při sjednání smlouvy prostřednictvím sítě internet je velice jednoduché vstoupit do právního vztahu, který bude obsahovat mezinárodní prvek. V případě smluv uzavíraných online často některá ze stran (typicky spotřebitel) ani nepostřehne, že uzavírá smlouvu s osobou s bydlištěm či sídlem v zahraničí, nebo se nebude otázkou státu původu druhé smluvní strany vůbec zabývat. Lutz upozorňuje na to, že zvláštnosti internetové komunikace znesnadňují užití pravidel o určení rozhodného práva, které závisí především na geografických aspektech.<sup>45</sup> V důsledku slabého spojení s fyzickým místem, všudypřítomnosti a virtuality internetové komunikace je podle něj velmi složité

<sup>45</sup> LUTZI, T. Internet Cases in EU Private International Law – Developing a Coherent Approach. *International and Comparative Law Quarterly*. 2017, roč. 66, s. 688.



či nemožné skutečně lokalizovat místo, ve kterém došlo ke škodě či v kterém má dojít ke smluvnímu plnění.<sup>46</sup> V této souvislosti například Kyselovská hovoří o delokalizaci či denacionalizaci jako o rezignaci na základní vazbu mezi státem a právním řádem, který je platný na jeho území.<sup>47</sup> Lze nicméně souhlasit s Polčákem a jeho tvrzením, že delokalizaci společenských vztahů v prostředí informačních sítí není možné brát bez dalšího jako negativní jev. Ten nezatížení vzájemné komunikace teritoriální bariérou naopak hodnotí jako pozitivní důsledek moderních informačních technologií. Zároveň zde ale spatřuje jeden z naprosto zásadních problémů aplikace práva na internetu, a to rozpor faktické delokalizace společenských vztahů s konceptem místní působnosti ve spojení s principem státní suverenity jako jedním z nejstarších konceptů mezinárodního práva veřejného.<sup>48</sup>

## 4.2 *Click-wrap* a *click-through* smlouvy

Ze stejných důvodů je také nutné vzít v úvahu rizika při identifikaci druhé smluvní strany. To lze ilustrovat na příkladu *click-wrap*, resp. *click-through* smluv. Jejich smyslem je umožnit a zjednodušit smluvní proces při uzavírání smluv na dálku prostřednictvím informačních a komunikačních technologií. Výhodou je úspora času a transakčních nákladů. Postup uzavření smlouvy je podstatně zjednodušen oproti postupu, kdy by jedna ze stran smlouvy uzavírané mezi podnikatelem a spotřebitelem oslovila druhou smluvní stranu e-mailem s návrhem smlouvy podepsaným uznávaným elektronickým podpisem ve smyslu zák. o službách vytvářejících důvěru<sup>49</sup> a druhá smluvní strana by neprodleně přijetí této nabídky rovněž potvrdila e-mailem podepsaným svým uznávaným elektronickým podpisem.

„*Click-wrap*“ metoda bývá popisována jako projev souhlasu se smluvními podmínkami při uzavírání elektronických smluv kliknutím na tlačítko „Ano“,

<sup>46</sup> LUTZI, 2017, op. cit., s. 702.

<sup>47</sup> KYSELOVSKÁ, T. Působnost práva na internetu. In: POLČÁK, R. a kol. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 33.

<sup>48</sup> POLČÁK, 2012, op. cit., s. 103.

<sup>49</sup> Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce (dále „zák. o službách vytvářejících důvěru“).

„Přijímám“, „Souhlasím“ či s jinou obdobnou formou souhlasu.<sup>50</sup> „*Click-wrap*“ smlouvu lze tedy popsat jako projev vůle uzavřít smlouvu prostřednictvím elektronického prostředku, kdy vůle je projevována kliknutím na virtuální tlačítko vyjadřující souhlas, resp. zároveň se zaškrtnutím příslušného políčka se souhlasem. Název přitom vyplývá z anglického „*click*“ jako kliknutí myši či použití jiného obdobného zařízení, jako je *touchpad* nebo dotykový displej, a „*wrap*“, které sice doslovně znamená „zabalit“, ale v přeneseném významu je používáno pro „dokončení“, v tomto případě pro uzavření smlouvy. Předchůdcem tohoto způsobu uzavírání smluv byly takzvané „*shrink-wrap*“ smlouvy. Tímto způsobem řešili prodejci software uzavření licenční smlouvy s koncovým zákazníkem, kdy tuto smlouvu zákazník uzavřel porušením ochranné fólie nebo pečeti na obalu nosiče software.<sup>51</sup>

Přesněji lze dále popisovaný způsob uzavírání smluv označit jako „*click-through*“. Důvod je ten, že proces uzavření smlouvy nespočívá pouze v kliknutí na tlačítko se souhlasem, ale ve více krocích. Při nich zákazník například postupně prochází internetovým obchodem a různými fázemi objednávky – vybírá zboží, volí způsob dopravy, vyplňuje kontaktní, doručovací a fakturační údaje, projevuje souhlas s obchodními či jinými podmínkami apod. – a celý tento proces stvrdí a uzavře smlouvu kliknutím na příslušné tlačítko. Při textaci tohoto tlačítka či zaškrťovacího pole ve vztazích se spotřebiteli je třeba brát v úvahu směrnici o právech spotřebitelů<sup>52</sup>, která požaduje, aby spotřebitel při učinění objednávky výslovně vzal v potaz, že si je vědom toho, že se objednávkou zavazuje k zaplacení.<sup>53</sup> Ustanovení směrnice s tímto

<sup>50</sup> Např. KUNZ, Ch.L. a kol. Browse-Wrap Agreements: Validity of Implied Assent in Electronic Form Agreements. *The Business Lawyer*. 2003, roč. 59, č. 1, s. 279, BOYKIN, D. D. Survey of E-Contracting Cases: Browsewrap, Clickwrap, and Modified Clickwrap Agreements. *The Business Lawyer*. 2012, roč. 68, č. 1, s. 257.

<sup>51</sup> KOŠČÍK, M. Pojem a obsah právních úkonů na internetu. *Revue pro právo a technologie*. 2011, č. 4, s. 30 a násl.

<sup>52</sup> Směrnice Evropského parlamentu a Rady 2011/83/EU ze dne 25. 10. 2011 o právech spotřebitelů.

<sup>53</sup> „Obchodník zajišťuje, aby spotřebitel při učinění objednávky výslovně vzal na vědomí, že si je vědom toho, že se objednávkou zavazuje k zaplacení. Pokud je objednávka činěna kliknutím na tlačítko nebo podobnou funkci, musí být toto tlačítko či podobná funkce snadno čitelným způsobem označeny 'objedávka zavazující k platbě' nebo jinou odpovídající a jednoznačnou formulací, která upozorní na skutečnost, že podáním objednávky vzniká povinnost zaplatit obchodníkovi. Nedodrží-li obchodník ustanovení tohoto pododstavce, není spotřebitel smlouvou nebo objednávkou vázán.“ Čl. 8 odst. 2 směrnice o právech spotřebitelů.

požadavkem bylo transponováno s účinností od 6. 1. 2023 do občanského zákoníku. Požadavek této úpravy je takový, že je-li objednávka činěna použitím tlačítka nebo obdobného ovládacího prvku, musejí být označeny snadno čitelným nápisem „*Objednávka zavazující k platbě*“ nebo jinou odpovídající jednoznačnou formulací. Nesplní-li podnikatel tuto povinnost, je smlouva neplatná. Neplatnost však lze zhojit tím, že se spotřebitel takto uzavřené smlouvy dovolá.<sup>54</sup>

Přijetí nabídky a podmínek smlouvy je v případě „*click-through*“ smlouvy jednoznačné, nepodmíněné, nezměnitelné a často i nevratné. V angličtině je takový postup nazýván jako přístup „*take-it-or-leave-it*“, občanský zákoník používá pojem „smlouvy uzavírané adhezním způsobem“.<sup>55</sup> V případě adhezních smluv, jak upozorňuje Knapp, může být, a v současném obchodě a při poskytování služeb tomu tak často je, omezena svoboda jedné ze stran ujednat obsah smlouvy, kdy této straně zbývá jen volba nabídku přijmout či nepřijmout, jakákoliv negociace o podmínkách smlouvy je vyloučena.<sup>56</sup>

Ščerba k tomuto typu elektronických smluv konstatuje, že si od počátku získal přízeň soudů ve smyslu uznávání tohoto typu smluvního ujednání jako platné a vynutitelné smlouvy. Jako důvod pro vznik tohoto typu smluv jmenuje vytvoření možnosti uzavírat elektronické smlouvy jednoduchým kliknutím pomocí polohovacího zařízení, kterým dojde k vyjádření souhlasu se smlouvou a jejími jednotlivými parametry. Smyslem tak je umožnit širokému množství smluvních stran uzavírat smlouvy za účelem očekávaným smluvními stranami.<sup>57</sup>

V literatuře jsou také zmiňovány tzv. „*browse-wrap*“ smlouvy. Tímto způsobem jsou označovány smlouvy, při kterých strana smlouvy projevuje vůli řídit se jejím obsahem tím, že dále užívá webovou stránku druhé strany. Uživatel stránky tak přímo explicitně neprojevuje vůli, resp. přijetí smluvních podmínek nějakým výslovným úkonem, nicméně k jejich platnosti je třeba, aby s nimi měla smluvní strana skutečně možnost se seznámit. Druhá smluvní strana pak musí unést důkazní břemeno o tom, jakým způsobem se měl

<sup>54</sup> § 1826a obč. zák.

<sup>55</sup> ŠČERBA, 2012, op. cit., s. 36.

<sup>56</sup> KNAPP, 1998, op. cit., s. 145.

<sup>57</sup> ŠČERBA, 2012, op. cit., s. 98.

uživatel stránky možnost s podmínkami seznámit.<sup>58</sup> Dalo by se v jejich případě uvažovat o konkludentní formě souhlasu s uzavřením smlouvy. Ščerba jejich obecnou platnost v českém právním prostředí odmítá a případnou platnost lze podle něj přiznat pouze na základě konkrétních okolností *ad hoc*.<sup>59</sup>

Přestože je eliminaci určitých aspektů vzdálenosti mezi smluvními stranami možné přijímat kladně, může přinášet i svá negativa. Absentuje v případě těchto smluv fyzické ověření toho, která osoba je ve skutečnosti druhou smluvní stranou, ať již na straně prodávajícího či kupujícího.<sup>60</sup> Zde přitom elektronická komunikace často může poskytovat metadata, která mohou při případném dokazování výrazně pomoci dokreslit situaci na základě zachyceného kontextu. Nemusí tomu tak být však vždy a účastníci „*click-through*“ smluv musí být připraveni na skutečnost, že tyto smlouvy v tomto směru s sebou mohou nést nižší míru důkazní spolehlivosti. I zde totiž platí to, co se dá konstatovat o jiných způsobech právního jednání provedeného prostřednictvím elektronického prostředku – naplnění zákonných požadavků na platnost právního jednání neznamena automaticky důkazní spolehlivost.

### 4.3 Úskalí při identifikaci smluvních stran

Většina kroků smluvního procesu při uzavírání „*click-wrap*“ či „*click-through*“ smluv postrádá jednoznačnou identifikaci smluvních stran. Lze si představit, že kupující uvede při nákupu fiktivní údaje o své osobě. Neuvede své pravé jméno a bydliště, a při převzetí zboží zaplatí hotovostí. Pokud kupující zaplatí za zboží bankovním převodem či platební kartou k účtu znějícímu na stejné jméno, jaké bylo uvedeno v objednávce nebo se při převzetí zboží bude muset prokázat občanským nebo jiným průkazem, bude na tom smluvní strana s identifikací druhé smluvní strany samozřejmě lépe. V této souvislosti Mason konstatuje, že úkon spočívající v kliknutí na tlačítko vedoucí k objednávce zboží nebo služeb je považováno za méně bezpečné než vlastnoruční podpis. Důvěryhodnost této formy tak bude spočívat v dostatečné schopnosti jedné nebo druhé ze stran poskytnout dostatečné důkazy k prokázání,

<sup>58</sup> MASON, 2017, op. cit., s. 213 a 214.

<sup>59</sup> ŠČERBA, 2012, op. cit., s. 105.

<sup>60</sup> DONÁT, J., TOMÍŠEK, J. *Právo v síti: průvodce právem na internetu*. Praha: C. H. Beck, 2016, s. 139.

že na tlačítko bylo skutečně kliknuto. I tak však dodává, že důvěryhodnost tohoto podpisu nemá vliv na jeho platnost.<sup>61</sup>

Obtíže s identifikací druhé smluvní strany však může pociťovat i kupující. Velmi snadno může dojít k překlepu v doménovém jménu, na jehož základě kupující připojí na internetovou stránku provozovanou jiným subjektem, přičemž tato stránka se mu pak svým vzhledem může jevit jako stránka obchodníka, od kterého původně zamýšlel provést nákup.<sup>62</sup> Taková záměrná registrace domény kolidující s jinou doménou v důsledku překlepů či neznalosti jazyka se nazývá *typosquatting*.<sup>63</sup> Občanský zákoník sice myslí na neplatnost právních jednání provedených při omylu. Problém v takovém případě však nemusí být posouzení platnosti právního jednání, ale spíše vymahatelnost vrácení zaplacených finančních prostředků.

Nad požadavkem identifikace se zamýšlí i Janoušek, který konstatuje, že v drtivě většině uzavíraných smluv není identita jednajících vůbec podstatná. Ověření identity se v naprosté většině případů nevyžaduje, protože to není potřebné ani žádoucí (například u běžného nákupu). Důvod požadavku identifikace pak vidí v ulehčení důkazního břemena při porušení smlouvy.<sup>64</sup>

#### 4.4 Dílčí závěr

Je patrné, že elektronické právní jednání a uzavírání smluv má svá specifika. Věnovali jsme se tomu, že díky internetu lze v právním styku velmi snadno překonat geografické bariéry, což však může přinášet i některé obtíže v souvislosti s určením rozhodného práva či vymahatelností právního jednání. V této souvislosti jsme hovořili také o úskalích při identifikaci smluvních stran při elektronické kontraktaci. V další kapitole proto na tyto úvahy navážeme textem zaměřeným na zákonné požadavky kladené na elektronické právní jednání. Největší pozornost bude věnována elektronickým podpisům, které mohou řešit některé z problémů, jenž mohou při kontraktaci na dálku vyvstat.

<sup>61</sup> MASON, 2017, op. cit., s. 208.

<sup>62</sup> DONÁT, TOMÍŠEK, 2016, op. cit., s. 140.

<sup>63</sup> HOSTAŠ, P. Doménová jména. In: POLČÁK, R. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 280.

<sup>64</sup> JANOUŠEK, 2021, op. cit., s. 144.

## 5 POŽADAVKY KLADENÉ NA PROJEV VŮLE ZACHYCNÝ ELEKTRONICKÝM PODPÍSEM

Nepominutelným prvkem většiny sporů vztahujícím se ke smluvnímu ujednání a jeho závaznosti pro určitou osobu je prokázání naplnění požadavku svobodného projevu vůle být vázán sjednaným obsahem smluvního závazku. Pro tyto účely v písemném právním jednání historicky nabyt stěžejní role vlastnoruční podpis. Jelikož při uzavírání smlouvy online dochází pouze k jinému vyjádření a zachycení virtualizované podstaty smluvního ujednání, podpis jako doložení projevu vůle je i zde klíčovým prvkem. Požadavky na něj kladené a důkazní hodnotu s ním spojenou je však nutné vykládat se zohledněním technologického kontextu jeho vytváření a zachycení. To s sebou přináší řadu specifických výkladových otázek, ke kterým se vztahuje stále se rozvíjející korpus judikaturních i odborných interpretací. Před přistoupením k pojednání o nich je však vhodné položit si zdánlivě banální otázku a rozvést, co je vlastně podpis.

### 5.1 Vlastnoruční podpis

Podpis jako takový totiž není právem nijak výslovně definován a lze se tedy věnovat jeho uchopení v právní teorii. Vlastnoruční podpis je podle Matese a Smejkal výsledkem určitého návyku v podobě individuálního a relativně stálého písemného projevu člověka. Vznik individuálnosti písma je podle nich důsledkem zažití si stereotypu psaní, který je závislý na přiměřeném procvičování.<sup>65</sup>

Polčák naráží na čistě obyčejový charakter nejen v českém právu. Hodnocení formální adekvátnosti podpisu a domněnka vyjádření vůle na jeho základě má tedy podle něj silný charakter obyčejové normy.<sup>66</sup>

Smejkal dále chápe podpis jako celospolečenskou konvenci či dohodu několika stran nebo skupiny obyvatel, jak vyjádřit souhlas s obsahem dokumentu či zprávy. K tomu pak dodává, že zavedený, ale právně nedefinovaný pojem

<sup>65</sup> MATEŠ, P., SMEJKAL, V. *E-government v České republice. Právní a technologické aspekty*. 2. podstatně přepracované a rozšířené vyd. Praha: Leges 2012, s. 271.

<sup>66</sup> Srov. POLČÁK, R. Elektronické právní jednání – změny, problémy a nové možnosti v zákoně č. 89/2012 Sb. *Bulletin advokacie*. 2013, č. 10, s. 34.

„vlastnoruční podpis“ by „klidně mohl být nabruzen pojmem ‚vlastnonožní podpis‘ či čimkoliv jiným, co by dané skupině obyvatel připadalo vhodné a užitečné.“<sup>67</sup> Český právní řád však v tomto není výjimkou a obyčejový charakter vlastnoručního podpisu je běžný i v jiných právních kulturách.<sup>68</sup>

Mason upozorňuje na to, že důvody pro uvedení podpisu na nějaký podklad se budou lišit v závislosti na tomto podkladu a vůli podepisující osoby. Podpis bude mít odlišnou funkci v případě podepsání kusu oblečení vlastnímu dítěti před cestou do školy, vyrytí jména na zhotovenou vázu, připojení podpisu na obraz nebo podepsání kupní smlouvy. Podpis v obecném vnímání však lze definovat jako připojení jména vlastní rukou na dokument, a to především formou vlastnoručního podpisu.<sup>69</sup> Funkce podpisu bude obecně určena druhem objektu či obsahem dokumentu, ke kterému je podpis připojován.<sup>70</sup>

Jako podpis bývá obvykle chápáno uvedení osobního jména a příjmení ve smyslu § 77 obč. zák. Podle tohoto ustanovení je za jméno člověka na místě považovat jeho osobní jméno a příjmení, popřípadě jeho další jména a rodné příjmení, která mu podle zákona náležejí. Každému člověku náleží právo užívat své jméno v právním styku. Tradičně je k podpisu používáno pouze příjmení, přičemž není ani vyžadována čitelnost podpisu. Na újmu platnosti právního jednání není podle § 79 obč. zák. ani použití pseudonymu v podpisu, je-li zřejmé, kdo jednal, a nemůže-li druhá strana mít pochybnost o osobě jednajícího.<sup>71</sup>

Nejvyšší soud dochází k závěru, že neuvedení jména a příjmení osoby jednající jménem smluvních stran (popř. za ně), nebo nečitelnost podpisu této osoby, nemá význam z hlediska dodržení zákonem požadované písemné formy právního úkonu.<sup>72</sup> Nejvyšší soud Československé republiky v roce 1926 dokonce dovodil, že lze připustit i podpis pouze křestním jménem: „Podpis křestním jménem vyhovuje v případě tomto, kde žena píše manželji svému a podepisuje se jak obvykle, předpisu § 578 obč. zák., a vylučuje každý omyl o totožnosti

67 SMEJKAL, V. Kryptografický a dynamický biometrický podpis podle platné právní úpravy. *Právní rozhledy* [online]. 2019, č. 10 [cit. 23. 1. 2022]. Dostupné z: <http://www.beck-online.cz>

68 POLČÁK, 2011, op. cit., s. 55.

69 MASON, 2017, op. cit., s. 5.

70 Ibid., s. 3.

71 ZUKLÍNOVÁ, 2013, op. cit., komentář k § 561.

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

*žůstavitelky*.<sup>73</sup> Podle Berana vždy postačí podpis příjmením, je ale přípustný i podpis křestním jménem, vztahovým označením („Tvůj otec“) nebo parafy tam, kde je to obvyklé a umožňuje to identifikovat jednajícího.<sup>74</sup>

Kovařík rozlišuje formální a materiální stránku podpisu. Formální stránka podpisu vyjadřuje, jestli grafický projev provedený na listině vykazuje zevní znaky vlastnoručního podpisu. Materiální stránka vyjadřuje, zda je tento podpis skutečně projevem vůle určité osoby.<sup>75</sup>

## 5.2 Funkce plnění podpisem a požadavkem formy

V souvislosti s teoretickým uchopením podpisu je vhodné se také věnovat funkcím plněným podpisem či právního požadavku na dodržení určité formy právního jednání. Rozlišování těchto funkcí není samoúčelné, ale tyto funkce by měly být vzaty v úvahu při rozhodování o platnosti a neplatnosti právního jednání v důsledku nedodržení předepsané formy a formálních náležitostí jednání.

Fuller v kontextu amerického práva v roce 1941 uváděl tři funkce náležitostí právních jednání, které lze přiřadit k písemné formě:

### 1. *Důkazní funkce*

Smysl písemné formy zde spočívá v důkazu existence a smyslu smlouvy v případě sporu. Potřebu zajištění této funkce lze naplnit požadavkem na písemnou formu či potvrzením notáře nebo jiné osoby.<sup>76</sup>

### 2. *Varovací funkce*

Tato funkce má sloužit jako pojistka před neuváženým jednáním. Původně takto mohla historicky sloužit pečeť.<sup>77</sup>

### 3. *Objasňující funkce*<sup>78</sup>

Tu považuje Fuller za jednu z nejdůležitějších funkcí a její význam ilustruje opět na pečeti. Ta připomínala slib a zvážení jeho projevu

<sup>73</sup> Rozhodnutí Nejvyššího soudu Československé republiky ze dne 3. 11. 1926, sp. zn. Rv II 161/26.

<sup>74</sup> BERAN, V. Komentář k § 562. In: PETROV, J., VÝTISK, M., BERAN, V. a kol. *Občanský zákoník. Komentář*. 2. vyd. Praha: C. H. Beck, 2019, s. 622.

<sup>75</sup> KOVAŘÍK, Z. *Směnka a šek v České republice*. 6. vyd. Praha: C. H. Beck, 2011, s. 46 a násl.

<sup>76</sup> FULLER, L. L. Consideration and Form. *Columbia Law Review*. Columbia Law Review Association, 1941, roč. 41, č. 5, s. 800.

<sup>77</sup> Ibid.

<sup>78</sup> Zde jde o velmi volný překlad, Fuller používá pojem „*Channelling function*“.



a zároveň to, že tento slib je vymahatelný. V této souvislosti byla pečeť v *common law* používána také v případě, že obchodník chtěl svůj slib učinit závazným. Písemná forma opatřená pečeti tak poskytovala prostředek k projevení vůle s právními účinky, když tato forma jednak potvrzovala projev vůle, objasňovala okamžik jejího projevu, ale také objasňovala obsah projevu.<sup>79</sup>

Fuller také uvádí, že všechny tři funkce jsou úzce propojené, a bude-li někdo chtít docílit některé z nich, bude mít zároveň sklon k docílení zbylých dvou funkcí.<sup>80</sup>

Česká komentářová literatura zmiňuje různé funkce písemné formy právního jednání, přičemž tyto funkce se dají přenést i na funkce podpisu. Tichý uvádí, že forma má řadu významných funkcí např. při dokazování, které vymezuje jako funkce důkazní, legitimační, informativní, varovnou a kontrolní.<sup>81</sup> Handlar pak uvádí ještě funkci poradní, kterou spojuje s veřejnou listinou, kdy by osoba, která veřejnou listinu sepisuje, měla být schopna poskytnout odborné poradenství v oblasti, které se listina týká.<sup>82</sup> Ščerba spatřuje v požadavku na formu varovnou, objasňující a důkazní funkci. Varovná má sloužit jako ochrana před ukvapeným jednáním, varovat a vzbudit ostražitost kontrahující strany. Objasňující funkce spočívá v možnosti objasnění sporných bodů a k ochraně bezpečí právního styku v průběhu kontraktace. Odděluje také kontraktační proces od vzniku právně závazné smlouvy. Důkazní funkce pak zlepšuje důkazní situaci v případě soudního, rozhodčího či jiného sporu.<sup>83</sup> Melzer kromě důkazní a varovací funkce uvádí také funkci zajišťovací, jejíž účel je zajištění nějaké významné hodnoty právního řádu, typicky právní jistoty. Zabezpečuje ochranu třetích osob a právní jistotu stanovením požadavku, že právní jednání má být sepsáno v písemné nebo nějaké přísnější

<sup>79</sup> FULLER, 1941, op. cit., s. 801.

<sup>80</sup> Ibid., s. 803.

<sup>81</sup> TICHÝ, L. Komentář k § 559. In: ŠVESTKA, J. a kol. *Občanský zákoník (zák. č. 89/2012 Sb.). Komentář. Svazek I (obecná část)*. 2. vyd. Praha: Wolters Kluwer, 2014, s. 1381.

<sup>82</sup> HANDLAR, J. § 559 [Forma právních jednání]. In: LAVICKÝ, P. a kol. *Občanský zákoník I. Obecná část (§ 1–654)*. 2. vyd. Praha: C. H. Beck, 2022, s. 1782.

<sup>83</sup> ŠČERBA, 2012, op. cit., s. 85.

formě, tím pádem také přístupné ostatním osobám, kterých se může právní jednání nějakým způsobem dotýkat.<sup>84</sup>

Podobné funkce bude možné dovodit pro vlastnoruční podpis. V české literatuře se hovoří zejména o třech funkcích podpisu:

- Funkci označovací jako označení toho, kdo činí právní jednání.
- Deklarační funkci, tedy potvrzení, že ten, kdo právní jednání učinil, ho učinit chtěl a že se jedná o projev jeho vůle.
- Důkazní funkci jako ověření totožnosti jednajícího a jako jeden z důkazů o tom, kdo učinil právní jednání.<sup>85</sup>

Korbel s Melzerem zmiňují také funkci krycí, podle které podpis pokrývá a prokazuje seznámení se s celým obsahem písemnosti. O jeho umístění nicméně rozhoduje zvyklost, v případě advokátů bývá podpis například na titulní straně.<sup>86</sup> Kment, který čerpá z německé literatury, upozorňuje i na další funkce vlastnoručního podpisu. Uvádí funkci ověřovací, identifikační, uzavírací, pravostní, varovací, zachovávací a důkazní.<sup>87</sup> Není to ale tak, že by byly nalézány jiné funkce než v literatuře naší, jen nejsou rozlišovány funkce písemné formy a podpisu.

Polčák podpis chápe jako nositele autentizační informace a jako nutnou formální náležitosti právně relevantní písemnosti. Dovojuje pro podpis tyto funkce: identifikaci osoby, deklaraci vůle a fixaci obsahu. Identifikace původce dokumentu pouhým podpisem však není dokonalá, a proto jsou užívány další pomůcky ke ztotožnění podpisu a konkrétní osoby. Deklaraci vůle pak považuje za čistě obyčejové právní pravidlo. Fixační funkce má smysl ve formálním uzavření dokumentu, k čemuž lze opět použít dalších prostředků.<sup>88</sup>

<sup>84</sup> MELZER, F. Neplatnost právního jednání v návaznosti na nedodržení formy. *Právní rádce*. 2013, č. 7, s. 31.

<sup>85</sup> ČERMÁK, K. Elektronický podpis – pohled soukromoprávní. *Bulletin advokacie*. 2002, č. 11.

<sup>86</sup> KORBEL, MELZER, 2014, op. cit., s. 32.

<sup>87</sup> KMENT, V. Nahradí elektronický podpis prostý ten tradiční vlastnoruční? *Bulletin advokacie*. 2016, č. 12.

<sup>88</sup> POLČÁK, 2011, op. cit., s. 55.

### 5.3 Zachování písemné formy při využití elektronických prostředků

V běžném vnímání je pro naplnění písemné formy právního jednání vyžadováno naplnění dvou náležitostí – písemnosti a podpisu. Byť má písemné elektronické právní jednání svá zásadní specifika, základ spočívá v zachycení obsahu právního jednání prostřednictvím textu. Na úvahy o vlastnoručním podpisu tedy navazujeme textem o chápání písemného právního jednání a o tom, do jaké míry je jeho přenesení do elektronické formy skutečně odlišné od jeho „papírového“ zachycení.

Je na místě zdůraznit, že podmínka písemnosti bude naplněna, bude-li právní jednání zachyceno v textu tak, aby jej bylo možné znovu přečíst či reprodukovat. Písemnost nepředstavuje vlastní projev vůle, ale pouze jeho vnější vyjádření. Písemný projev má tudíž podobu textu.<sup>89</sup> Z pohledu práva tak bude bez významu, zda bude hmotným nosičem textu papír či jiný pevný podklad anebo například elektronický dokument vytvořený a zobrazený textovým editorem.<sup>90</sup>

Ustanovení § 562 odst. 2 obč. zák. zavádí pravidlo, podle kterého je písemná forma zachována i při právním jednání učiněném elektronickými nebo jinými technickými prostředky umožňujícími zachycení jeho obsahu a určení jednající osoby. Taková právní jednání tedy nejsou zvláštní formou právního jednání ale typem písemné formy, je možné nazvat je spíše jako ekvivalenty (náhražky) písemné formy.<sup>91</sup> V úvahu je také nutné vzít § 3026 odst. 1 obč. zák., podle kterého, nevyklučuje-li to povaha písemnosti, platí ustanovení občanského zákoníku o listině obdobně i pro jinou písemnost bez zřetele na její podobu.

Je tedy vhodné vyjasnit, co je myšleno elektronickým prostředkem a jiným technickým prostředkem. Občanský zákoník tyto pojmy nijak nedefinuje a nečiní tak ani další předpisy. Výjimkou je zákon č. 480/2004 Sb., o některých službách informační společnosti. Pro účely tohoto zákona se elektronickými prostředky rozumí zejména síť elektronických komunikací, elektronická komunikační zařízení, automatické volací a komunikační systémy,

<sup>89</sup> Srov. POLČÁK, 2013, op. cit., s. 34.

<sup>90</sup> Srov. DONÁT, TOMÍŠEK, 2016, op. cit., s. 159.

<sup>91</sup> Srov. TICHÝ, L. Komentář k § 562. In: ŠVESTKA, J., DVORÁK, J., FIALA, J. a kol. *Občanský zákoník. Komentář. Svazek I.* Praha: Wolters Kluwer, 2014, s. 1391.

telekomunikační koncová zařízení a elektronická pošta.<sup>92</sup> Důvodová zpráva tohoto zákona konstatuje, že za elektronický prostředek je považován jak hardware, tak i softwarové aplikace. Ustanovení obsahuje demonstrativní výčet, jako příklad dalších elektronických prostředků důvodová zpráva uvádí také *messenger*<sup>93</sup> a jiné prostředky umožňující tento druh komunikace. Elektronická pošta, kterou zákon považuje také za elektronický prostředek, je 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.<sup>94</sup> Takto širokému vymezení elektronického prostředku odpovídá i jeho výklad pro účely § 561 a § 562 obč. zák. v odborné literatuře. Elektronickým či jiným technickým prostředkem se rozumí „*v podstatě kterýkoli prostředek umožňující komunikaci na dálku.*“<sup>95</sup> Hrdlička pod pojem „elektronický prostředek“ zahrnuje především internet, mobilní telefon a podobně. Jako „jiný technický prostředek“ chápe telegraf, telefax apod.<sup>96</sup> Odlišně však chápe „technický prostředek“ zákon o obchodních korporacích.<sup>97</sup> Ten umožňuje pro hlasování na valné hromadě užít také technických prostředků, které ale ve své důvodové zprávě spíše zaměňuje s „elektronickými prostředky“.<sup>98</sup>

Písemnou formu právního jednání lze provést prostřednictvím elektronických prostředků za splnění dvou podmínek:

1. musí být zachycen obsah právního jednání a
2. elektronický prostředek umožní určení jednající osoby.

<sup>92</sup> § 2 písm. c) zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů.

<sup>93</sup> Jako příklad *messengeru* důvodová zpráva uváděla aplikaci ICQ. Ta zřejmě nyní minimálně v České republice příliš využívána nebude. Aktuálně lze jako příklad uvést Messenger, WhatsApp, Viber a podobné aplikace.

<sup>94</sup> § 2 písm. b) zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů.

<sup>95</sup> KINDL, M., KINDL, T., KINDLOVÁ, M., ŠÍMA, A. a kol. *Občanský zákoník – Komentář s judikaturou. Svazek V – Právní skutečnosti (§ 545–654)*. [online]. [cit. 15. 2. 2022]. Ostrava: CODEXIS publishing, 2018, komentář k § 562. Dostupné z: <http://www.codexis.cz>

<sup>96</sup> HRDLIČKA, M. § 562 [Písemná forma právního jednání učiněného elektronickými prostředky]. In: LÁVICKÝ, P. a kol. *Občanský zákoník I. Obecná část (§ 1–654)*. 1. vyd. Praha: C. H. Beck, 2014, s. 2025.

<sup>97</sup> Srov. § 167 odst. 2 a § 398 odst. 2 zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích).

<sup>98</sup> VOSTOUPAL, J. Vybrané slabiny právní úpravy elektronických forem komunikace v obchodních korporacích v kontextu kybernetické bezpečnosti. *Obchodněprávní revue*. 2022, č. 1.

Je tedy nutné zajistit trvalost zaznamenané informace o právním jednání spolu s písemnou formou takového záznamu a jeho přičitatelnost jednáající osobě.<sup>99</sup> První podmínku nebude složité splnit např. prostřednictvím elektronického dokumentu uchovávaného na zařízení jednájících osob či jiném uložišti, prostřednictvím e-mailu, datových schránek a dalších prostředků elektronické komunikace. Jak uvádí Čech, text právního jednání v elektronické formě bude možné zachytit libovolným způsobem, například dokumentem v libovolném formátu, e-mailem nebo SMS zprávou.<sup>100</sup>

Druhou podmínku však již nemusí každý elektronický prostředek splňovat. Například e-mailovou adresu, na rozdíl třeba od datové schránky, není možné bez další identifikace spojit s konkrétní osobou. E-mailová adresa jan.novak@mujemail.cz negarantuje skutečnost, že jí disponuje skutečně osoba se jménem Jan Novák. A pokud ano, v České republice nepochybně nežije pouze jedna jediná osoba s tímto jménem. Problém identifikace osob jednájících prostřednictvím elektronických prostředků, zejména prostřednictvím sítě internet, je jedním ze základních problémů, které je třeba v případě právních jednání touto cestou řešit. Lze jej nicméně překlenout mimo jiné prostřednictvím služeb vytvářejících důvěru v elektronické transakce. Zároveň si lze klást otázku o vzájemném vztahu § 561 odst. 1 a § 562 odst. 1 obč. zák. – tedy zda je k platnosti písemné formy právního jednání učiněného prostřednictvím elektronického prostředku vždy třeba takové jednání opatřit elektronickým podpisem (k tomu viz následující podkapitola).

Pro další pojednání je třeba vymežit pojem „elektronický dokument“. Tichý k tomu uvádí, že „[e]lektronická 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.“<sup>101</sup>

Elektronické dokumenty představují základní předpoklad písemného elektronického právního jednání. Stejně tak jsou významné pro jakýkoliv další rozvoj

<sup>99</sup> VOSTOUPAL, 2022, op. cit., s. 55, POLČÁK, 2011, op. cit., s. 55.

<sup>100</sup> ČECH, P. Elektronická kontraktace. In: SEDLÁKOVÁ, J. a kol. *Softwarové smlouvy: Jejich specifiky a kontraktní proces*. Praha: C. H. Beck, 2021, s. 16.

<sup>101</sup> TICHÝ, L. Komentář k § 562. In: ŠVESTKA, J., DVOŘÁK, J., FIALA, J. a kol. *Občanský zákoník. Komentář. Svazek I*. Praha: Wolters Kluwer, 2014, s. 1391.

přeshraničních elektronických transakcí na vnitřním trhu Evropské unie.<sup>102</sup> Je však také třeba si uvědomit, že technologický vývoj do jisté míry boří běžnou představu o podobě dokumentu jako neměnného obsahu fixovaného k nějakému konkrétnímu okamžiku. Lze se stále častěji setkávat s dokumenty ukládanými na virtuálních úložištích (tzn. v *cloudu*), jejichž obsah se neustále (i v reálném čase) mění či které obsahují více vrstev informací.<sup>103</sup>

Pro účely archivnictví a spisové služby je dokument (i elektronický) definován v § 2 písm. e) zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, který dokumentem rozumí každou písemnou, obrazovou, zvukovou nebo jinou zaznamenanou informaci, ať již v podobě analogové či digitální. V kontextu zde řešené problematiky je nutné vzít v úvahu nařízení eIDAS, které dle svého čl. 3 bodu 35 rozumí elektronickým dokumentem jakýkoli obsah uchovávaný v elektronické podobě, zejména jako text nebo jako zvukovou, vizuální nebo audiovizuální nahrávku.

Pro diskuzi nad zachováním písemné formy právního jednání odhlédneme od skutečnosti, že pojem v sobě zahrnuje i zvukovou a audiovizuální nahrávku a berme za elektronický písemný dokument obsah uchovávaný v elektronické podobě jako text. Text je možné samozřejmě doplnit i vizuálními prvky, typicky obrázkem, nákresem apod. Pokud bude předmětem smlouvy například nemovitá věc, je zpravidla i v elektronické podobě na místě doplnit textovou smlouvu obrázkem s nákresem prostor nebo umístěním nemovité věci na katastrální mapě. Lze si však také představit spojení elektronicky podepsané smlouvy se zvukovou, vizuální nebo audiovizuální nahrávkou tvořící přílohu smlouvy.

Lze tak uzavřít, že při vnímání elektronické písemné formy je nutné se oprostit od představy, že elektronický dokument se ve svém základu co do obsahu zásadním způsobem odlišuje od právního jednání vyjádřeného na nějakém hmotném substrátu, nejčastěji na papíře. „Papírové“ právní jednání je pouze virtualizováno do podoby elektronického dokumentu. Základ obojího je však stejný, jen je elektronické právní jednání zbaveno této vnější papírové formy a je přeneseno do prostředí informačních technologií.

<sup>102</sup> DONÁT, J., PIFFL, R., MAISNER, M. *Nařízení eIDAS. Komentář*. Praha: C. H. Beck, 2017, s. 166.

<sup>103</sup> POLČÁK, 2011, op. cit., s. 54.

## 5.4 Naplnění písemné formy bez elektronického podpisu

Vyšší úrovně elektronického podpisu, ale i například dynamický biometrický podpis, který lze kvalifikovat pouze jako elektronický podpis prostý, přinášejí při uzavírání elektronických smluv řadu výhod pro jejich uživatele. Lze se však věnovat tomu, zda český právní řád pro platnost elektronického písemného právního jednání vyžaduje jeho podepsání elektronickým podpisem, či je možné platně jednat i bez elektronického podpisu.

Definice jednoduchého (prostého) elektronického podpisu dle č. 3 odst. 10 eIDAS je záměrně velice široká a bude ji za určitých okolností splňovat různorodá paleta typů elektronického podpisu.<sup>104</sup> Je nicméně stále na místě si klást otázku o vztahu mezi § 561 odst. 1 a § 562 odst. 1 obč. zák., tedy zda je k platnosti písemné formy právního jednání učiněného prostřednictvím elektronického prostředku vždy třeba takové jednání opatřit elektronickým podpisem. Zde existují zejména dva výkladové přístupy<sup>105</sup>:

1. Obě tato ustanovení občanského zákoníku upravují dvě odlišné kategorie právních jednání učiněných prostřednictvím elektronického prostředku. Do první kategorie patří právní jednání opatřená elektronickým podpisem a do druhé spadají právní jednání, která sice nebudou opatřena elektronickým podpisem, ale která i tak budou právně relevantní písemností, jelikož budou umožňovat zachycení obsahu právního jednání a také určení jednatelky osoby.
2. Písemné právní jednání učiněné elektronickými prostředky vyžaduje k zachování písemné formy vždy připojení elektronického podpisu.

V odborné literatuře a rozhodovací praxi se příležitostně objevují názory, že pro platnost elektronického právního jednání nestačí jeho podepsání prostým elektronickým podpisem a je třeba jej opatřit alespoň zaručeným

<sup>104</sup> Např. SMEJKAL, V., KODL, J., UŘIČAŘ, M. Elektronický podpis podle nařízení eIDAS. *Revue pro právo a technologie*. 2015, č. 11, s. 219, KMENT, V. Nahradí elektronický podpis prostý ten tradiční vlastnoruční? *Bulletin advokacie*. 2016, č. 12, s. 31–35, a KMENT, 2018, op. cit., s. 138–142.

<sup>105</sup> Viz např. BEZOUŠKA, P. § 562. Kdy je v případě e-mailu dodržena písemná forma právního jednání? In: BEZOUŠKA, P., HAVEL, B. *Občanský zákoník. Srovnávací komentář* [online]. Wolters Kluwer [cit. 4. 11. 2020] nebo KMENT, 2018, op. cit., s. 86–90.

elektronickým podpisem.<sup>106</sup> Lze soudit, že zastává-li někdo tento názor, nebude zřejmě akceptovat elektronické právní jednání bez jakéhokoliv elektronického podpisu.

Zdá se však, že v odborné literatuře převládá názor o vztahu speciality § 562 odst. 1 obč. zák. k § 561 odst. 1 obč. zák. Již v roce 2001 ve vztahu k občanskému zákoníku z roku 1964 a zák. o el. podpisu<sup>107</sup> konstatoval Matejka, že písemná forma právního úkonu zůstává zachována, je-li právní úkon učiněn elektronickými prostředky, jež umožňují zachycení obsahu právního úkonu a určení osoby, která právní úkon učinila. V této souvislosti zmiňuje, že „*nově upravené právo (nikoli tedy výslovnou povinností) jednající osoby, která učinila právní úkon elektronickými prostředky, podepsat jej elektronicky podle zvláštních předpisů. Jediným takovým platným zvláštním předpisem je v současné době pouze ZoEP [zák. o el. podpisu].*“<sup>108</sup>

Vzájemného poměru mezi § 561 odst. 1 a § 562 odst. 1 obč. zák. si všímá i Bezouška, který rozebírá oba přístupy a dochází k závěru, že každé z těchto ustanovení upravuje jiný druh právního jednání projeveného elektronickým prostředkem.<sup>109</sup> Obdobně Beran uvádí, že požadavek § 562 odst. 1 obč. zák. je vztažen k elektronickým právním jednáním, u kterých je písemná forma zachována, ač nejsou podepsána.<sup>110</sup> Zároveň konstatuje, že v případech uvedených v § 562 a § 563 obč. zák. není nezbytný podpis pro zachování písemné formy.<sup>111</sup>

<sup>106</sup> Např. MATULA, Z. Lze považovat e-mail bez zaručeného elektronického podpisu za písemné právní jednání? *Rekodifikace a praxe* [online]. 2014, č. 3 [cit. 22.2.2022]. Dostupné z: <http://www.noveaspi.cz>, HRDLÍČKA, M. § 562 [Písemná forma právního jednání učiněného elektronickými prostředky]. In: LAVICKÝ, P. a kol. *Občanský zákoník I. Obecná část (§ 1–654)*. 1. vyd. Praha: C. H. Beck, 2014, s. 2026, KINDL, M., KINDL, T., KINDLOVÁ, M., ŠÍMA, A. a kol. *Občanský zákoník – Komentář s judikaturou. Svazek V – Právní skutečnosti (§ 545–654)* [online]. Ostrava: CODEXIS publishing, 2018, komentář k § 561 [cit. 15.2.2022]. Dostupné z: <http://www.codexis.cz>

<sup>107</sup> Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu).

<sup>108</sup> MATEJKA, J. Úprava elektronického podpisu v právním řádu ČR. *Právník* [online]. 2001, č. 6, s. 557–586 [cit. 18.2.2022]. Dostupné z: <http://www.codexis.cz>

<sup>109</sup> BEZOUŠKA, P. § 562. Kdy je v případě e-mailu dodržena písemná forma právního jednání? In: BEZOUŠKA, P., HAVEL, B. *Občanský zákoník. Srovnávací komentář* [online]. Wolters Kluwer [cit. 4.11.2018]. Dostupné z: <http://www.noveaspi.cz>

<sup>110</sup> BERAN, Komentář k § 562, op. cit., s. 622.

<sup>111</sup> *Ibid.*, s. 621.



Donát s Tomíškem si vzájemného poměru § 561 odst. 1 a § 562 odst. 1 obč. zák. všimají také a konstatují, že písemného právního jednání v elektronické podobě lze dosáhnout i jinak než za pomoci elektronického podpisu. Odkazují pak právě na § 562 odst. 1 obč. zák. jako druhou variantu písemného právního jednání v elektronické podobě.<sup>112</sup>

I další autoři považují § 562 za významnou výjimku z podmínky naplnění písemné formy předpokládající existenci dvou náležitostí, a to písemnosti a podpisu.<sup>113</sup> Dochází přitom k závěru, že o jednání splňující požadavky písemné formy jde vždy, když k němu došlo za využití elektronického či jiného technického prostředku, který umožňuje zachycení obsahu jednání a určení jednajících osoby. Takovým prostředkem může přitom být v podstatě libovolný prostředek umožňující komunikaci na dálku. To může ve svém důsledku do značné míry eliminovat pravidlo obsažené v § 561 obč. zák.<sup>114</sup>

K závěru o vztahu speciality § 562 odst. 1 obč. zák. k § 561 odst. 1 dochází i Korbel s Melzerem, podle nichž § 562 odst. 1 upravuje případ, kdy elektronická forma naplní požadavek písemné formy i bez elektronického podpisu, pokud elektronický nebo jiný technický prostředek umožní alespoň zachycení obsahu právního jednání a určení jednajících osoby.<sup>115</sup> Shodný závěr konstatují Matejka s Güttlerem. Jako variantu pro určení jednajících osoby pak navrhují užití biometrických metod, které nebudou vyhovovat legislativnímu vymezení elektronického podpisu, ale budou plnit podobné funkce.<sup>116</sup> Ani podle Janouška se nevyžaduje, aby právní jednání učiněné v elektronické podobě splňující požadavky § 562 odst. 1 obč. zák. bylo podepsáno.<sup>117</sup>

K těmto závěrům se přikláníme také. Pokud by platil opak, pak by § 562 odst. 1 obč. zák. nepřinášel nic nového – písemná forma, byť provedená

<sup>112</sup> DONÁT, TOMÍŠEK, 2016, op. cit., s. 160.

<sup>113</sup> Srov. Např. rozhodnutí Nejvyššího soudu ze dne 29. 11. 2007, sp. zn. 29 Odo 965/2006.

<sup>114</sup> Srov. KINDL, M., KINDL, T., KINDLOVÁ, M., ŠÍMA, A. a kol. *Občanský zákoník – Komentář s judikaturou. Svazek V – Právní skutečnosti (§ 545–654)*. Ostrava: CODEXIS publishing, 2018, komentář k § 562. Dostupné z: <http://www.codexis.cz> [cit. 15. 2. 2022].

<sup>115</sup> KORBEL, MELZER, 2014, op. cit., s. 34.

<sup>116</sup> MATEJKA, J., GÜTTLER, V. Electronic Written Documents and Biometric Options of Their Signing – Problem of Evidentiary Reliability and Personal Data Protection. *The Lawyer Quarterly*. 2018, č. 1, s. 41.

<sup>117</sup> JANOUŠEK, M. § 562 [Písemná forma právního jednání učiněného elektronickými prostředky]. In: LAVICKÝ, P. a kol. *Občanský zákoník I. Obecná část (§ 1–654)*. 2. vyd. Praha: C. H. Beck, 2022, s. 1801.

prostřednictvím elektronického prostředku, musí být nepochybně nějakým způsobem zaznamenána. Konstatování o určení jednatelky osoby by bylo také zbytečné, protože určení jednatelky osoby by bylo možné učinit prostřednictvím adekvátního typu elektronického podpisu. Jinak řečeno, pokud by platilo, že písemné právní jednání učiněné elektronickými prostředky vyžaduje k zachování písemné formy vždy připojení elektronického podpisu, stačilo by použít § 561 odst. 1 ve spojení s § 3026 odst. 1 obč. zák.<sup>118</sup>. Zároveň by takový závěr zřejmě vylučoval použití prostého elektronického podpisu z toho důvodu, že ten by ve většině případů nesplňoval identifikační funkci. Je také možné argumentovat vývojem současné právní úpravy.<sup>119</sup> Pravidla uvedená v § 561 odst. 1 a § 562 odst. 1 obč. zák. byla v podstatě přejata z § 40 odst. 3 a 4 občanského zákoníku z roku 1964. Tato dvě ustanovení byla však do občanského zákoníku z roku 1964 vložena s účinností od 1. 1. 1992 zákonem 509/1991 Sb., kterým se mění, doplňuje a upravuje občanský zákoník. Do 30. 9. 2000 zněla takto:

*„(3) Písemný právní úkon je platný, je-li podepsán jednatelkou osobou; [...] Podpis může být nabrizen mechanickými prostředky v případech, kdy je to obvyklé.*

*(4) Písemná forma je zachována, je-li právní úkon učiněn telegraficky, dálkopisem nebo elektronickými prostředky, jež umožňují zachycení obsahu právního úkonu a určení osoby, která právní úkon učinila.“*

V té době v České republice neexistovala právní úprava elektronického podpisu. Ten byl do českého právního řádu zaveden až zák. o el. podpisu, a to s účinností od 1. 10. 2000. Tento zákon do výše uvedeného 3. odstavce vložil větu: *„Je-li právní úkon učiněn elektronickými prostředky, může být podepsán elektronicky podle zvláštních předpisů.“*

Lze tedy argumentovat tím, že mezi 1. 1. 1992 a 30. 9. 2000 bylo možné jednat prostřednictvím elektronických prostředků bez elektronického podpisu (úprava elektronického podpisu ani neexistovala) a 1. 10. 2000 byl novelizován § 40 odst. 3 občanského zákoníku z roku 1964 tak, že do něj byla přidána možnost podepsat právní úkon elektronickým podpisem (viz *„může být podepsán elektronicky“*).

<sup>118</sup> Toto ustanovení zní: *„Nevylučuje-li to povaha písemnosti, platí ustanovení tohoto zákona o listině obdobně i pro jinou písemnost bez zřetele na její podobu.“*

<sup>119</sup> Shodně BERAN, Komentář k § 562, op. cit., s. 623.

Předmětná ustanovení občanského zákoníku nyní zní:

1. Ustanovení § 561 odst. 1 obč. zák.: *„K platnosti právního jednání učiněného v písemné formě se vyžaduje podpis jednatelů. Podpis může být nabržen mechanickými prostředky tam, kde je to obvyklé. Jiný právní předpis stanoví, jak lze při právním jednání učiněném elektronickými prostředky písemnost elektronicky podepsat.“*
2. Ustanovení § 562 odst. 1 obč. zák.: *„Písemná forma je zachována i při právním jednání učiněném elektronickými nebo jinými technickými prostředky umožňujícími zachycení jeho obsahu a určení jednatelů.“*

Při zohlednění terminologických změn lze konstatovat, že tato ustanovení jsou s § 40 odst. 3 a 4 občanského zákoníku z roku 1964 Sb. téměř totožná. Navíc i v § 561 odst. 1 obč. zák. nalezneme příslovce „lze“ („může“ v dřívější úpravě) jako vyjádření možnosti, nikoliv povinnosti.

V úvahu je možné také vzít § 566 odst. 1 obč. zák., podle kterého není-li soukromá listina podepsána, je na tom, kdo ji použil, aby dokázal, že pochází od osoby, o níž to tvrdí. V případě elektronického právního jednání je však nutné rozlišit mezi naplněním náležitostí právního jednání a důkazní spolehlivostí provedeného právního jednání.

První nám známé rozhodnutí, ve kterém soud konstatoval totožný právní názor, je rozhodnutí Krajského soudu v Českých Budějovicích ze dne 27. 3. 2015, sp. zn. 24 Co 696/2015. Zde soud sice řešil naplnění požadavku písemnosti smlouvy podepsané elektronickým podpisem prostým prostřednictvím unikátních identifikačních údajů smluvní strany. Nad rámec svého závěru o platnosti takové podpisu však ale uvedl, že *„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 jednatelů.“*<sup>120</sup>

I přes tento závěr je na místě, aby ten, kdo provádí právní jednání prostřednictvím elektronického prostředku v zájmu zachování vyšší míry právní jistoty opatřil takové jednání elektronickým podpisem. A to nikoliv pouze prostým elektronickým podpisem, ale některou z vyšších úrovní elektronického

<sup>120</sup> Blíže viz kapitola 13 této knihy.

podpisu, která s sebou bude nést vyšší míru důkazní spolehlivosti a může do jisté míry skutečně plnit i identifikační funkci podpisu. Není však nutné (a zřejmě ani vhodné) spoléhat se pouze na vyšší úroveň elektronického podpisu. Identifikovat jednající osobu bude možné za použití dodatečných technik a důkazů, například při podpisu kódem předtím zasláným na mobilní telefon podepisujícího či v aplikaci, prostřednictvím které došlo k dostatečné identifikaci. Integritu smlouvy, resp. možnost zjistit její následné změny, lze pak zajistit například prostřednictvím kryptografie, při archivaci smlouvy prostřednictvím *blockchainu* či jiné DLT technologie nebo nějaké formy spisové služby s transakčním logem.<sup>121</sup>

## 5.5 Elektronické právní jednání jako projev zásad občanského práva

Český právní řád vychází z principu legální licence vyjádřené v Ústavě a Listině základních práv a svobod. Podle něj může každý činit, co není zákonem zakázáno, a nikdo nesmí být nucen činit, co zákon neukládá.<sup>122</sup> V soukromém právu se tento princip projevuje mimo jiné v podobě smluvní svobody spočívající ve svobodě rozhodnutí budoucích smluvních stran, zda smlouvu uzavřou, s kým ji uzavřou, jakým způsobem bude smlouva uzavřena, jakou zvolí formu smlouvy a také, jaký zvolí obsah vzájemných práv a povinností.<sup>123</sup>

Do současné právní úpravy se promítá zásada bezformálnosti, podle které má každý právo zvolit si pro právní jednání libovolnou formu, není-li ve volbě formy omezen ujednáním nebo zákonem.<sup>124</sup> Jednostranná a vícestranná právní jednání lze tedy činit – pokud zákon nestanoví jinak – bez ohledu na jejich formu. Zároveň se zde projevuje i zásada autonomie vůle, jelikož zákon nechává výběr konkrétní formy právního jednání v rukou jeho subjektů (samozřejmě opět, pokud nestanoví formu zákon). Jak konstatuje

<sup>121</sup> K tomu zejména kapitola 11 této knihy.

<sup>122</sup> Čl. 2 odst. 3 usnesení Předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, čl. 2 odst. 4 zákona č. 1/1993 Sb., Ústava České republiky.

<sup>123</sup> RABAN, P. a kol. *Závazkové právo*. Brno: Václav Klemm, 2019, s. 36.

<sup>124</sup> § 559 obč. zák.

Tichý, zásada svobody formy je důležitý faktor efektivity právního styku, významná zvláště při běžných právních jednáních každodenního života.<sup>125</sup>

K této efektivitě se přiléhavě vyjadřuje Fuller při odpovědi na otázku, ve kterých situacích má správná legislativa vyžadovat formalizované právní jednání. Odpovídá na ni tak, že požadavek formy je třeba použít pro relativně důležité úkony při zachování proporce mezi prostředkem a cílem, nikoliv zatěžovat běžné jednání nadbytečnými formalitami.<sup>126</sup> Upozorňuje také na to, že „*tam, kde se život již účinně organizuje, není třeba, aby zasahoval zákon.*“<sup>127</sup>

Podle Hurdíka je pro soukromé právo typická dispozitivnost právní úpravy, v rámci které je ponechán prostor uspořádání právních vztahů účastníky.<sup>128</sup>

Smlouvou dle občanského zákoníku projevují strany vůli zřídit mezi sebou závazek a řídit se obsahem smlouvy.<sup>129</sup> Lze ji tedy vymezit jako dvoustranné či vícestranné právní jednání, jímž její strany projevují vůli mezi sebou zřídit závazek a být vázány obsahem smlouvy. V § 1724 odst. 1 obč. zák., který takto smlouvu vymezuje, lze spatřovat projev zásady smluvní volnosti a autonomie vůle.<sup>130</sup> Byť je smluvní volnost projevem soukromoprávní svobody, autonomie vůle, upozorňují Pelikánová s Pelikánem, že rozsah smluvní svobody je determinován i právem veřejným. Pokud bylo dříve komunistickým režimem zakázáno podnikat, byla tím omezena i smluvní volnost, jelikož celou řadu smluv nemohla soukromá osoba uzavírat.<sup>131</sup>

Klíčová je zde svoboda stran se zavazovat. Knapp sice konstatuje, že definovat svobodu či definovat ji obecně není snadné. V obecném kontextu se o ní mluví jako o určitém postavení člověka ve společnosti, mluví se ale

<sup>125</sup> TICHÝ, L. Komentář k § 559. In: ŠVESTKA, J. a kol. *Občanský zákoník (zák. č. 89/2012 Sb.). Komentář. Svazek I (obecná část)*. 2. vyd. Praha: Wolters Kluwer, 2014, s. 1381.

<sup>126</sup> Srov. FULLER, 1941, op. cit., s. 805.

<sup>127</sup> *Ibid.*, s. 806.

<sup>128</sup> HURDÍK, J. Soukromé a občanské právo v systému práva. In: HURDÍK, J. a kol. *Občanské právo hmotné. Obecná část. Absolutní majetková práva*. Plzeň: Aleš Čeněk, 2018, s. 33.

<sup>129</sup> § 1724 obč. zák.

<sup>130</sup> GAŇO, J., JIRSA, J., ZOUBEK, H. a kol. *Občanský zákoník – Komentář s judikaturou. Svazek XI – Závazky – obecná část (§ 1721–2054)*. Ostrava: CODEXIS publishing, 2018, komentář k § 1724 Dostupné z: <http://www.codexis.cz> [cit. 15. 2. 2022].

<sup>131</sup> PELIKÁNOVÁ, I., PELIKÁN, R. Komentář k § 1724. In: ŠVESTKA, J., DVORÁK, J., FIALA, J. a kol. *Občanský zákoník. Komentář. Svazek V*. Praha: Wolters Kluwer. 2014, s. 8.

také o jejich specifických projevech, které se často nazývají jako autonomie vůle nebo autonomie chování, mezi které Knapp řadí i svobodu smluvní.<sup>132</sup> Fuller mezi základními koncepcemi smluvního práva jako nejrozšířenější a nepostradatelnou zásadu považuje autonomii vůle („*private autonomy*“). Ta podle něj jednoduše znamená, že právo považuje soukromé osoby za ty, které mají pravomoc v určitých mezích provádět změny ve svých právních vztazích.<sup>133</sup>

Smluvní strany se mohou svobodně rozhodnout, zda smlouvu uzavřou. V ní si mohou upravit svá vzájemná práva a povinnosti a ty měnit, rušit nebo s nimi jinak disponovat. Tato úprava je však do jisté míry limitována právním řádem a zároveň je dodržování smluvních podmínek státem vynutitelné.<sup>134</sup> Knapp tak hovoří o tom, že nezbytným předpokladem a požadavkem autonomie smluvní vůle je svoboda rozhodnutí o uzavření smlouvy. Významná je i svoboda „utvořit obsah“, která však může být omezena například při uzavírání adhezních smluv.<sup>135</sup>

Smluvní strany mezi sebou vytvářejí do jisté míry své vlastní, autonomní právo. Boguszak v této souvislosti konstatoval, že „[s]oukromoprávní sféra se vyznačuje dispozitivní autonomií subjektů, v jejichž kogentně určených mezích subjekty svými právními úkony, zejména smlouvami, jakoby vytvářejí své „autonomní právo“.“<sup>136</sup>

Vlastnoručně a elektronicky podepsaná právní jednání mají společný základ. Elektronickým právním jednáním do občanského práva není vnášeno nic zásadně nového, jen jsou rozšiřovány prostředky, jimiž lze právně jednat. Standardně lze právně jednat písemně, ústně, resp. konkludentně. Informační technologie postupně začaly umožňovat jednání i prostřednictvím elektronického prostředku.

Občanský zákoník vychází z principu autonomie vůle, smluvní svobody a bezformálnosti. Strany si mohou pro smlouvu zvolit libovolnou formu a prostředek jejího uzavření. Požadavek písemného právního jednání či písemné smlouvy je spíše výjimečný. Občanský zákoník zároveň nedělá v běžných

<sup>132</sup> KNAPP, V. *Teorie práva*. Praha: Beck, 1998, s. 15.

<sup>133</sup> FULLER, 1941, op. cit., s. 806.

<sup>134</sup> Srov. RABAN, 2019, op. cit., s. 35.

<sup>135</sup> KNAPP, 1998, op. cit., s. 145.

<sup>136</sup> BOGUSZAK, J. *Systém práva*. In: ČAPEK, J., BOGUSZAK, J. *Teorie práva*. Praha: Codex, 1997, s. 89.

právních vztazích rozdíl mezi písemností v listinné podobě podepsané vlastnoručním podpisem a v podobě elektronického dokumentu opatřeného elektronickým podpisem. Výjimkou je například nutnost podepsat závět' vlastní rukou.<sup>137</sup> Nadto se domníváme, že požadavek písemnosti naplní i právní jednání provedená elektronickým prostředkem, která nebudou opatřena elektronickým podpisem, bude-li takový prostředek umožňovat identifikaci jednající osoby a zjištění obsahu právního jednání.

K platnosti písemné formy v listinné podobě je vyžadován vlastnoruční podpis, který historicky plní funkci potvrzení projevu vůle jednající osoby a další funkce. Informační technologie k němu přinesly alternativu v podobě elektronického podpisu. V občanském právu uznáním rovnocennosti právního jednání učiněného elektronickým prostředkem s listinnou písemnou formou právního jednání či možností právní jednání elektronicky podepsat nedošlo k zavedení nových, revolučních institutů. Jen byly za platné uznány i jiné způsoby uzavření smlouvy a v souladu s principem smluvní svobody rozšířeny možnosti účastníků smluv při jejich kontraktaci. Navíc Ščerba v této souvislosti upozorňuje na to, že elektronické smlouvy nejsou tak nové, jak by se na první pohled mohlo zdát. „Elektronické“ smlouvy naopak považuje za fenomén 19. století, a to s ohledem na rozvoj telegrafu jako prostředku k přenosu informací.<sup>138</sup>

Pokud nebude pro konkrétní právní jednání stanoven, nyní spíše výjimečný, požadavek jeho provedení například ústně nebo výhradně s vlastnoručním podpisem či před notářem, pak si jednající osoba může pro právní jednání zvolit elektronický prostředek. Právo může virtualizaci právních vztahů a kontraktaci stanovit určité limity, nicméně obecně však zcela zapadá do systému zásad, na kterých stojí české soukromé smluvní právo.

<sup>137</sup> § 1533 a § 1534 obč. zák.

<sup>138</sup> ŠČERBA, 2012, op. cit., s. 80.

## 6 ŘEŠENÍ NEDOSTATKŮ A VAD SMLOUVY

V praxi se lze stále setkat s určitou mírou nedůvěry v elektronicky uzavřené smlouvy. To lze odůvodnit skepsí k zavádění nových nástrojů do právního styku, neporozuměním technologického pozadí elektronické kontraktace či aktuální rozhodovací praxí soudů. S posledním bodem nutně souvisí úvahy ohledně naplnění zákonných požadavků na dodržení písemné formy právního jednání a platnosti či neplatnosti právního jednání. Těmto oblastem se proto věnujeme v následujících pasážích.

### 6.1 Náležitosti právního jednání

Právní teorie obvykle uvádí, že právní jednání musí naplnit náležitosti subjektu, vůle, projevu této vůle, předmětu projevu vůle či vzájemného poměru vůle a jejího projevu.<sup>139</sup>

Projev vůle musí také naplnit některé podmínky. Musí být dostatečně určitý (jednoznačný), srozumitelný, a pokud tak stanoví zákon (nebo dohoda stran), je třeba dodržet určitou formu.<sup>140</sup> Pokud má být projev vůle projeven v určité formě, pak je forma takového právního jednání náležitostí právního jednání a podmínkou jeho platnosti.<sup>141</sup> Zároveň je třeba konstatovat, že je-li občanským zákoníkem určena konkrétní forma právního jednání, jde o ustanovení kogentní a účastníci právního jednání nemají na výběr a musí takovou formu dodržet.<sup>142</sup>

#### 6.1.1 Písemná forma

Písemná forma má mezi formami právního jednání výsadní postavení, jelikož jejím účelem je fixace obsahu právního jednání k určitému časovému okamžiku a jeho zachycení způsobem, který v čase přetrvá lépe než u ústního nebo konkludentního právního jednání.<sup>143</sup> Zákonodárcův požadavek

<sup>139</sup> ZUKLÍNOVÁ, M. Občanskoprávní skutečnost. In: DVOŘÁK, ŠVESTKA, ZUKLÍNOVÁ a kol., 2016, op. cit., s. 156.

<sup>140</sup> Ibid., s. 161.

<sup>141</sup> HANDLAR, J. § 559 [Forma právních jednání]. In: LAVICKÝ, P. a kol. *Občanský zákoník I. Obecná část (§ 1–654)*. 2. vyd. Praha: C. H. Beck, 2022, s. 1786.

<sup>142</sup> Ibid., s. 1782.

<sup>143</sup> DONÁT, TOMÍŠEK, 2016, op. cit., s. 158.



na zachování písemné formy u určitých právních jednání zasahuje do svobody volby účastníků právního jednání zvolit si pro toto jednání formu dle svého uvážení. Fuller uvádí, že bez ohledu na motiv zákonodárce, formální požadavek zákona na dodržení předepsané formy tenduje ke kategorizaci transakcí na právní a mimoprávní.<sup>144</sup>

Písemná forma je zachována za situace, kdy je právně jednáno prostřednictvím čitelné, tedy ve zrakem seznatelné podobě, přičemž podkladový materiál by měl vykazovat určitou trvalost. Materiál, na kterém je samotný text právního jednání zachycen, není určen. Typicky bývá jako příklad uváděn zápis vyrytý do kamene. Nemusí pak jít ani o zápis, který by byl skutečně napsán vlastní rukou – plně postačí text připravený na počítači v textovém editoru.<sup>145</sup>

Formální přísnost, tedy omezení autonomie vůle a prolomení zásady bezformálnosti a stanovení povinnosti provést právní jednání v písemné formě, není samoučelné a existuje pro ni několik důvodů. Podle Tichého má forma významnou úlohu zejména při dokazování a plní také významnou legitimační a informativní funkci. Krom toho plní také varovací a kontrolní funkci, přičemž požadavek povinné formy sleduje veřejný zájem i soukromý zájem stran.<sup>146</sup>

Toto konstatování se nevztahuje pouze k zákonné formě, tedy k právním jednáním, u nichž je písemná forma předepsána zákonem, ale může být důvodem, pro něž si písemnou formu právního jednání zvolí účastníci ze své vůle dohodou. Taková situace pak není omezením autonomie vůle, ale naopak jejím projevem. Jde o dohodnutou (smluvní) formu, kdy forma právního jednání závisí pouze na vůli účastníků. Podle § 1758 obč. zák. platí, že dohodnou-li se strany, že pro uzavření uijí určitou formu, má se za to, že nechtějí být vázány, nebude-li tato forma dodržena. To podle stejného ustanovení platí i tehdy, projeví-li jedna ze stran vůli, aby smlouva byla uzavřena v písemné formě.

Volba formy neznamená, že by tuto volbu účastníci právního jednání nemohli přehodnotit. To potvrdil Nejvyšší soud ve svém rozhodnutí ze dne

<sup>144</sup> FULLER, 1941, op. cit., s. 803.

<sup>145</sup> ZUKLÍNOVÁ, M. Forma právních jednání - I. *Právní prostor* [online]. 27. 7. 2015 [cit. 9. 7. 2022].

<sup>146</sup> TICHÝ, L. Komentář k § 559. In: ŠVESTKA a kol., 2014, op. cit., s. 1381.

22. 1. 2020, sp. zn. 26 Cdo 3501/2019. V něm se věnoval posouzení otázky písemně uzavřené smlouvy, v níž se účastníci dohodli, že bude měněna pouze písemnými dodatky s úředně ověřenými podpisy stran. K této smlouvě pak strany následně uzavřely tři písemné dodatky, ty byly nicméně podepsány bez úředního ověření podpisů. V této souvislosti soud konstatoval, že strany se nemohou do budoucna omezit tak, že by si úplně znemožnily se dohodnout jinak, a výhradu formy je tedy možno později opustit. Aktuálně projevená vůle stran má vždy přednost před vůlí projevou dříve a podle Nejvyššího soudu to platí i ohledně požadavku formy. Strany se mohou dohodou o opuštění dříve vyhrazené formy vyvázat, a to i v jiné formě. Podle soudu se však vyžaduje, aby strany učinily nejen neformální právní jednání samotné, nýbrž aby současně opustily (ať již v jakékoliv formě) i dříve ujednanou výhradu formy, což musí být prokázáno a doloženo. To může být součástí stejného aktu ve skutkovém smyslu, právně však půjde o dvě skutečnosti – dohodu o opuštění sjednané formy a samotné neformální právní jednání. Samotné neformální právní jednání pro opuštění sjednané formy podle soudu nepostačuje. Přesto se však soud také přiklonil 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 očekáváním a potřebami.“<sup>147</sup>

I písemná forma má své náležitosti, a to písemnost a podpis. Zde je možné odkázat na ustálenou judikaturu Nejvyššího soudu. Podle ní spočívá písemnost v tom, že projev vůle jednajícího zahrnuje všechny podstatné náležitosti zachycené v písemném textu listiny. Právně významný je tak pouze ten projev vůle jednajícího, který je vyjádřen v písemném textu. Písemný projev musí být zároveň podepsán, a je tak platný až po podpisu jednající osoby.<sup>148</sup>

Je však otázka, zda lze s ohledem na znění § 562 odst. 1 obč. zák. tento závěr bez dalšího vztáhnout i na právní jednání učiněná elektronickými nebo jinými technickými prostředky.<sup>149</sup>

<sup>147</sup> Rozhodnutí Nejvyššího soudu ze dne 22. 1. 2020, sp. zn. 26 Cdo 3501/2019.

<sup>148</sup> Srov. např. rozhodnutí ze dne 28. 5. 2008, sp. zn. 32 Odo 940/2006.

<sup>149</sup> K této otázce viz výše v kapitole 4.4.

Lze také s odkazem na rozhodnutí Nejvyššího soudu zde dne 28. 8. 2001, sp. zn. 29 Odo 14/2001, konstatovat, že pokud není písemná forma předepsána zákonem či některým účastníkem požadována, pak lze písemnou a ústní formu kombinovat. Pro hodnocení jednání účastníků je přitom rozhodující jejich vůle při uzavírání smlouvy.<sup>150</sup>

### 6.1.2 Přísná písemná forma

Zákon může pro některá právní jednání vyžadovat přísnější úroveň písemné formy, a to písemnou formu opatřenou úředně ověřeným podpisem či ve formě veřejné listiny. Veřejná listina je dle § 567 obč. zák. listina vydaná orgánem veřejné moci v mezích jeho pravomoci nebo listina, kterou za veřejnou listinu prohlásí zákon. Zároveň se jí dle § 3026 odst. 2 obč. zák. rozumí notářský zápis, popř. může být notářský zápis nahrazen rozhodnutím, kterým orgán veřejné moci v mezích své pravomoci schvaluje smír nebo jiný projev vůle, jehož povaha to nevylučuje.

Bližší se přísnou písemnou formou zabýváme v části věnované úřednímu ověření elektronických podpisů na elektronických dokumentech a elektronicky podepsané plné moci.<sup>151</sup>

## 6.2 Neplatnost elektronicky podepsané smlouvy

Při zvažování, zda smlouvu strany vlastnoručně či elektronicky podepíší, mohou mít strany obavy z nejistoty ohledně platnosti elektronicky uzavřené smlouvy pro nedodržení písemné formy (především v případě podpisu elektronickým podpisem prostým). Požadavek na dodržení písemné formy může mít dvojí podobu – může vyplývat ze zákona či z ujednání účastníků. Bude-li vyplývat z dohody mezi účastníky, pak lze neplatnost namítat pouze tehdy, pokud dosud nebylo plněno<sup>152</sup> či nebyl nedostatek formy dodatečně zhojen<sup>153</sup>. Zhojit nedostatek formy lze i v případě zákonem stanoveného požadavku formy.<sup>154</sup>

<sup>150</sup> Rozhodnutí Nejvyššího soudu ze dne 28. 8. 2001, sp. zn. 29 Odo 14/2001.

<sup>151</sup> Viz kapitola 6.4.

<sup>152</sup> § 582 odst. 2 obč. zák.

<sup>153</sup> § 582 odst. 1 obč. zák.

<sup>154</sup> Ibid.

Předně je nutné konstatovat, že na právní jednání je třeba spíše hledět jako na platné než jako na neplatné.<sup>155</sup> Právní jednání odporující zákonu (zde nedostatek formy) je navíc neplatné pouze tehdy, vyžaduje-li to smysl a účel zákona.<sup>156</sup> Nejvyšší soud v této souvislosti dovodil, že „[u]vedené omezení platí i pro posouzení důsledků nedodržení formy právního jednání vyžadované zákonem (§ 582 odst. 1 OZ). 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.“<sup>157</sup>

Neplatné tak nebude každé právní jednání provedené v rozporu s požadavkem písemné formy, ale bude třeba zkoumat v daném kontextu smysl a účel zákona. Pokud bude požadavek formy určen k ochraně třetích osob, a bude tedy plnit zajišťovací funkci, pak by právní jednání provedené v rozporu s tímto požadavkem mělo být shledáno jako absolutně neplatné a soud by měl k neplatnosti přihlídnout i bez návrhu.<sup>158</sup> Plní-li požadavek formy funkci varovací, tedy v tom smyslu, že varuje účastníka před neuvážlivým jednáním, pak by měla být neplatnost konstatována také, tentokrát však pouze na základě námítky osoby, jejíž zájem je příslušným zákonným ustanovením chráněn.<sup>159</sup>

Strany mohou mít také obavy z omezené platnosti certifikátu pro elektronický podpis. Neplatnost certifikátu je však třeba odlišit od neplatnosti podpisu či samotné smlouvy.<sup>160</sup>

Pokud nepůjde o smlouvu s obligatorní písemnou formou, může konstatovat soud závěr o jejím uzavření na základě jiné právní skutečnosti než na základě písemného právního jednání. Takto například Okresní soud v Kladně v níže rozebíraném rozhodnutí ze dne 31. 8. 2021, sp. zn. 208 C 115/2021, dospěl k závěru, že deficit písemnosti v dané věci byl bez významu, jelikož předmětnou smlouvu bylo možné uzavřít i v jiné než písemné formě.

Výše uvedené pak rozvádíme v dalších částech této monografie, včetně specifických požadavků na různé úrovně elektronických podpisů a dalších služeb vytvářejících důvěru.

<sup>155</sup> § 580 obč. zák.

<sup>156</sup> § 580 odst. 1 obč. zák.

<sup>157</sup> Rozhodnutí Nejvyššího soudu ze dne 27. 11. 2014, sp. zn. 29 Cdo 3919/2014.

<sup>158</sup> § 588 obč. zák.

<sup>159</sup> § 586 obč. zák. Blíže viz MELZER, 2013, op. cit., s. 32 a 33.

<sup>160</sup> K tomu blíže viz kapitolu 11 této knihy.



## 7 ELEKTRONICKÝ PODPIS

### 7.1 Základní východiska a právní základ elektronického podpisu

Možnost provádět transakce a uzavírat smlouvy elektronicky nemá přínos jen pro konkrétní smluvní strany, ale také pro ekonomiku. Bez nadnárodní regulace ale není možné využít jejich plný potenciál.<sup>161</sup> Internet umožňuje i svým běžným uživatelům zachovat vysokou míru anonymity. I v případě, že se uživatel rozhodne této anonymity vzdát, může pro něj být obtížné prokázat jiné osobě svou identitu tak, aby v takové prokázání měla dostatečnou důvěru. Strany také mohou mít obavy ze zachování autenticity, integrity, důvěryhodnosti či vymahatelnosti elektronicky podepsaných dokumentů. Tyto problémy se snaží adresovat legislativa regulující užití elektronických podpisů.<sup>162</sup>

Jako první zákon upravující komerční užívání elektronických podpisů je uváděn *The Utah Digital Signature Act* přijatý v roce 1995 v americkém státě Utah.<sup>163</sup> Tento zákon směřoval na to, aby byl v případě sporu dokument podepsaný elektronickým podpisem, dle požadavků zákona, přijat jako důkaz u soudu, aniž by bylo nutné předvolávat další svědky k prokázání pravosti podpisu. Důkazní břemeno podle něj leželo na podepisující osobě takového dokumentu, která musela prokázat, že dokument nepodepsala.<sup>164</sup>

Autentický vlastnoruční podpis je nedílně spojen s podepisující osobou. To je základní rozdíl oproti elektronickému podpisu. V jeho případě, vyjma dynamického biometrického podpisu a podobných podpisů, tomu tak nebude. Elektronickým podpisem podepisující osoba nepodepisuje žádný

<sup>161</sup> WOOD BRALEY, S. Why Electronic Signatures Can Increase Electronic Transactions and the Need for Laws Governing Electronic Signatures. *Law and Business Review of the Americas*. 2001, č. 7, s. 418.

<sup>162</sup> Srov. ibid.

<sup>163</sup> DUMORTIER, J. Legal Status of Qualified Electronic Signatures in Europe. In: PAULUS, S., POHLMANN, N., REIMER, H. (eds.). *ISSE 2004 – Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2004 Conference*. Wiesbaden: Vieweg+Teubner Verlag, 2004, s. 281.

<sup>164</sup> WIMS, M. D. Introduction to the Utah Digital Signature Act Editorial. *EDI Law Review*. 1995, roč. 2, č. 3, s. 156.

fyzický dokument, ale pouze připojuje elektronická data představující jeho elektronický podpis k jiným datům v elektronické podobě.<sup>165</sup>

Na evropské úrovni byly dříve elektronické podpisy upraveny směrnicí Evropského parlamentu a Rady 1999/93/ES o zásadách Společenství pro elektronické podpisy, nyní jsou regulovány nařízením eIDAS. Na rozdíl od původní směrnice nařízení eIDAS upravuje také elektronické pečete a elektronická časová razítka (v oblasti týkající se služeb vytvářejících důvěru), které byly dříve v české úpravě zák. o el. podpisu známy jako elektronické značky a časová razítka. Zároveň odstraňuje řadu nepřesností v oblasti elektronického podpisu ze směrnice 1999/93/ES a jednotlivých implementací této směrnice členskými státy.<sup>166</sup>

Nařízení eIDAS přiznává počátek a vývoj snah o unifikaci mezi členskými státy v oblasti elektronických transakcí kromě směrnice 1999/93/ES zejména ve:

- sdělení Komise ze dne 26. 8. 2010 s názvem „Digitální agenda pro Evropu“,
- ve výzvách Evropské rady Komisi k vytvoření jednotného digitálního trhu, usnadnění přeshraničního využívání online služeb a z bezpečné elektronické identifikace a autentizace z roku 2011,
- ve výzvě Rady Komisi z 27. 5. 2011 k vytvoření podmínek pro přeshraniční uznávání elektronické identifikace, dokumentů, podpisů a elektronického doručování, nebo
- v usnesení Evropského parlamentu ze dne 21. 9. 2010<sup>167</sup> o dotvoření vnitřního trhu pro elektronický obchod.<sup>168</sup>

Předmětem nařízení eIDAS je zajištění řádného fungování vnitřního trhu a odpovídající úrovně bezpečnosti prostředků pro elektronickou identifikaci a služeb vytvářejících důvěru. Z tohoto důvodu stanoví podmínky pro uznávání těchto prostředků a služeb mezi členskými státy, pravidla pro užití služeb vytvářejících důvěru zejména pro elektronické transakce a právní rámec pro služby vytvářející důvěru.<sup>169</sup> Jeho cílem je budování důvěryhodnosti online prostředí, zvýšení důvěryhodnosti elektronických transakcí na vnitřním trhu

<sup>165</sup> MASON, 2017, op. cit., s. 9.

<sup>166</sup> SMEJKAL, KODL, URČIČAŘ, 2017, op. cit., s. 192.

<sup>167</sup> Úř. věst. C 50 E, 21. 2. 2012, s. 1.

<sup>168</sup> Srov. bod odůvodnění 3 až 7 nařízení eIDAS.

<sup>169</sup> Srov. čl. 1 nařízení eIDAS.

Evropské unie a posílení efektivnosti veřejných a soukromých online služeb, elektronického podnikání a elektronického obchodu v Evropské unii.<sup>170</sup> Nařízení eIDAS nabídlo nové možnosti elektronické identifikace v právním styku. Jeho cílem je také zajištění uznávání elektronických identit napříč Evropskou unií, případně v dalších zemích.<sup>171</sup> Z čl. 14 nařízení eIDAS totiž vyplývá, že je na základě dohod uzavřených mezi Evropskou unií a třetími zeměmi možné uznávat služby vytvářející důvěru poskytované poskytovateli služeb vytvářejících důvěru usazených ve třetí zemi a uznaných jako kvalifikovaní poskytovatelé jako rovnocenné kvalifikovaným službám vytvářejícím důvěru, které jsou poskytovány kvalifikovanými poskytovateli služeb vytvářejících důvěru usazenými v Evropské unii.<sup>172</sup>

Evropská komise v hodnotící zprávě k nařízení eIDAS hodnotí toto nařízení jako průlom pro Evropskou unii, „jelikož zavedlo první přeshraniční rámec pro důvěryhodné digitální identity a služby vytvářející důvěru, který se nyní těší celosvětovému uznání.“<sup>173</sup> V této zprávě také připomíná důvody jeho přijetí, které Komise spatřuje ve zvýšení důvěryhodnosti elektronických transakcí na vnitřním trhu prostřednictvím poskytnutí společného základu pro bezpečnou a bezproblémovou elektronickou komunikaci, čímž mělo dojít k posílení efektivnosti mimo jiné i soukromých online služeb, elektronického podnikání a elektronického obchodu v Evropské unii.<sup>174</sup>

Do českého právního řádu bylo nařízení eIDAS adaptováno zák. o službách vytvářejících důvěru, u kterého zákonodárce zvolil při adaptaci relativně minimalistický přístup vzhledem k závaznosti, přímé použitelnosti a aplikační přednosti nařízení Evropské unie. Současně byl také přijat změnový zákon č. 298/2016 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce.

<sup>170</sup> Srov. bod odůvodnění 1 nařízení eIDAS.

<sup>171</sup> Srov. LOUTOCKÝ, P. eIDAS Regulation: A Step Forward? In: BALTHASAR, A. (ed.). *CEE e Dem and e Gov Days 2015: Independence day: time for a European Internet?* Wien: Österreichische Computer Gesellschaft, 2015, s. 106.

<sup>172</sup> Ibid., s. 108.

<sup>173</sup> 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), op. cit., s. 1.

<sup>174</sup> Ibid.



Adaptace byla dokončena v roce 2017 zákonem č. 250/20017, o elektronické identifikaci.<sup>175</sup>

Zákonodárce při adaptaci nařízení eIDAS s jednotlivými úrovněmi elektronických podpisů a pečeti nijak zvlášť dále nepracuje. Na nařízení eIDAS je v rámci uvedených zákonů odkazováno pouze v poznámkách pod čarou a v důvodových zprávách.

## 7.2 Úrovně elektronického podpisu

Jako základní východisko pro používání elektronického podpisu lze odkázat na čl. 25 eIDAS, který zavádí pravidlo, podle kterého „[e]lektronickému podpisu nesmí 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 nespĺňuje požadavky na kvalifikované elektronické podpisy.“ Zároveň předepisuje, že „[k]valifikovaný elektronický podpis má právní účinek rovnocenný vlastnoručnímu podpisu.“ Nařízení eIDAS výslovně upravuje tři úrovně elektronických podpisů – elektronický podpis prostý, zaručený a kvalifikovaný.

### 7.2.1 Prostý elektronický podpis

Starší česká právní úprava zák. o el. podpisu kladla na elektronický podpis přísnější požadavky. Rozuměla jím 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.<sup>176</sup> Přísnost, ve srovnání se současnou úpravou, lze vidět v požadavku na jednoznačné ověření identity podepsané osoby. Ten v současné úpravě absentuje. Nařízení eIDAS totiž jednoduchý elektronický podpis definuje v čl. 3 odst. 10 jako „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.“

Definice prostého (někdy jednoduchého) elektronického podpisu v čl. 3 odst. 10 nařízení eIDAS je záměrně široká. Matejka s Güttlerem ji hodnotí tak,

<sup>175</sup> Důvodová zpráva k zákonu o elektronické identifikaci uvádí, že „[z]ákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce byla započata adaptace na nařízení eIDAS. Zákonem o elektronické identifikaci bude tato adaptace dokončena.“

<sup>176</sup> § 2 písm. a) zák. o el. podpisu.

že potvrzuje tradiční respekt k autonomii vůle jako nenahraditelnou hodnotu pro strany soukromoprávního styku.<sup>177</sup> Požadavky bude za určitých okolností splňovat široká paleta různých typů elektronického podpisu jako třeba pouhé uvedení jména v závěru dokumentu či e-mailu, zadání PIN kódu apod.<sup>178</sup> Jako variantu elektronického podpisu prostého nabízí Smejkal, Kodl a Uříčar užití hlasu, který digitalizovat jde. Zároveň je jedinečný, čímž by podle nich bylo možné vytvořit vícefaktorovou autentizaci u základního typu elektronického podpisu.<sup>179</sup> Matejka s Güttlerem pak jako příklady elektronického podpisu prostého uvádí připojení naskenovaného podpisu, zadání specifického hesla nebo kódu či provedení jiného autentizačního postupu, a to včetně hlasu připojeného k písemnému dokumentu v elektronické podobě.<sup>180</sup> Za prostý elektronický podpis pak může být považován i podpis biometrický (o kterém pojednáváme dále).

Definice prostého elektronického podpisu neobsahuje jakýkoliv požadavek na identifikaci či prokázání totožnosti podepisující osoby.<sup>181</sup> Jediné spojení s podepisující osobou připadá v úvahu jen v případě části definice, která říká, že užitá data „*podepisující osoba používá ke podepsání*.“ Problematický aspekt této základní úrovně elektronického podpisu tak je ten, že vzhledem ke své definici nezaručuje, že v rámci vymáhání práv (nejen) v civilním procesu bude jeho prostřednictvím bez dalších tvrzení a důkazů prokázáno, že právní jednání bylo skutečně podepsáno osobou, o které je to tvrzeno. K prokázání této skutečnosti však bude možné použít další důkazy a typicky pak metadata zaznamenávána příslušným systémem. Účastník sporu se také zřejmě nebude moci úspěšně dovolávat toho, že smlouvu nepodepsal, pokud po podpisu začal na základě této smlouvy plnit závazek z ní vyplývající.

Nelze však možné obtíže při dokazování elektronickým podpisem prostým zaměňovat s otázkou jeho platnosti pro soukromoprávní jednání. Korbel s Kovářem a Jarošem proto upozorňují na to, že v praxi vznikne odlišná míra důkazní spolehlivosti různých úrovní podpisů, nicméně volba

<sup>177</sup> MATEJKA, GÜTTLER, 2018, op. cit., s. 50.

<sup>178</sup> Např. KMENT, V. *Elektronické právní jednání: Analýza s důrazem na využití elektronického podpisu podle práva EU, České republiky a Německa*. Praha: Wolters Kluwer, 2018, s. 142, nebo DONÁT, PIFFL, MAISNER, 2017, op. cit., s. 31.

<sup>179</sup> SMEJKAL, KODL, URÍČAR, 2017, op. cit., s. 219.

<sup>180</sup> MATEJKA, GÜTTLER, 2018, op. cit., s. 44.

<sup>181</sup> Ibid., s. 42.

konkrétní techniky elektronického podpisu je výhradně volbou jednajících osob na základě úvahy o dostatečnosti, efektivitě, jednoduchosti či ceně, nicméně volba nebude mít vliv na platnost právního jednání. Není proto podle nich žádoucí považovat prostý elektronický podpis za právně a fakticky nedůvěryhodný nebo neplatný podpis.<sup>182</sup> Podobně dříve Polčák upozorňoval na sporadicky se vyskytující praxi soudů spočívající v odmítání elektronických dokumentů opatřených pouze elektronickým podpisem prostým jako důkazů. Tu hodnotí tak, že je z podstaty vadná, jelikož soud sice může dospět k závěru, že předložený důkaz je nevěrohodný, nicméně se musí takovým důkazem alespoň zabývat a hodnotit jeho spolehlivost v řízení, ne takový důkaz bez dalšího odmítnout.<sup>183</sup>

Je však možné se setkat i odlišnými názory. Hrdlička s odkazem na rozhodnutí Nejvyššího soudu 33 Cdo 3210/2007 dochází k závěru, „*že ať zaručený elektronický podpis splňuje z hlediska bezpečnosti nároky na splnění písemné formy právního jednání. Tento závěr nic nemění na tom, že pokud nebude zákon ani dohoda účastníků vyžadovat písemnou formu, může být právní jednání učiněné elektronicky podepsáno „obyčejným“ elektronickým podpisem.*“<sup>184</sup> Zmíněnému rozhodnutí Nejvyššího soudu se blíže věnujeme v části věnované rozhodovací praxi, kde konstatujeme (stejně jako další autoři), že rozhodnutí považujeme vzhledem k definici jednoduchého elektronického podpisu za překonané. Domníváme se také, že „*hledisko bezpečnosti*“ této úrovně elektronického podpisu by nemělo být směřováno s otázkou naplnění zákonného požadavku písemnosti i za použití elektronického podpisu prostého.

V literatuře je možné se setkat i s názorem stojícím na pomezí paušálního odmítání elektronického podpisu prostého a jeho připuštění pro písemná

<sup>182</sup> KORBEL, F., KOVÁŘ, D., JAROŠ, J. Aktuální právní přístup k dynamickému biometrickému podpisu. *Pojistný obzor*. 2021, č. 2, s. 13.

<sup>183</sup> POLČÁK, 2011, op. cit., s. 56 a 57.

<sup>184</sup> HRDLIČKA, M. § 561 [Písemná forma právního jednání]. In: LAVICKÝ, P. a kol. *Občanský zákoník I. Obecná část (§ 1–654)*. 1. vyd. Praha: C. H. Beck, 2014. Dostupné z: <http://www.beck-online.cz> [cit. 15. 2. 2022]. Shodně také KINDL, M., KINDL, T., KINDLOVÁ, M., ŠÍMA, A. a kol. *Občanský zákoník – Komentář s judikaturou. Svazek V – Právní skutečnosti (§ 545–654)*. Ostrava: CODEXIS publishing, 2018. Dostupné z: <http://www.codexis.cz> [cit. 15. 2. 2022]. Komentář k § 561: „*K podepsování elektronickým podpisem lze přitom použít pouze uznaný elektronický podpis, jímž se podle § 6 odst. 2 zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, rozumí zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis nebo kvalifikovaný elektronický podpis.*“

právní jednání bez dalšího. K tomuto závěru dospívá na základě rekapitulace dříve publikovaných názorů Janoušek. Podle něj může elektronický dokument opatřený elektronickým podpisem prostým vyvolávat právní následky. To však pouze v případech, kdy se právní jednání dotýká jediné individuálních zájmů stran právního jednání. Nikoliv pak v případech, v nichž je potenciálně dotčen veřejný zájem, kdy je požadavkem písemné formy právního jednání sledována zajišťovací nebo kontrolní funkce právního jednání.<sup>185</sup>

Podle našeho názoru vyřešení otázky ohledně platnosti právního jednání opatřeného elektronickým podpisem prostým vězí ve znění § 561 odst. 1 obč. zák., podle nějž jiný právní předpis stanoví, jak lze při právním jednání učiněném elektronickými prostředky písemnost elektronicky podepsat. Toto ustanovení zde odkazuje na zák. o službách vytvářejících důvěru, který ve svém § 7 konstatuje, že lze použít i jiný typ elektronického podpisu, podepisuje-li se elektronický dokument, kterým se právně jedná vůči jiné osobě než veřejnoprávnímu podepisujícímu či další osobě při výkonu její působnosti. Zák. o službách vytvářejících důvěru již na rozdíl od zák. o el. podpisu neobsahuje požadavek na identifikaci podepisující osoby jejím podpisem. Postačí tedy naplnění nařízení eIDAS na základní úroveň elektronického podpisu. Účastníci by však měli zvážit užití některé z vyšších úrovní elektronického podpisu za účelem zachování vyšší míry důkazní spolehlivosti při využití technických výhod těchto elektronických podpisů.

Mimo právní řád České republiky se lze setkat i s odlišným přístupem. Například německý občanský zákoník vyžaduje pro platné nahrazení zákonem předepsané písemné formy elektronickou formou připojení jména jednající osoby a podepsání kvalifikovaným elektronickým podpisem. V případě smlouvy pak musí každá ze stran takto elektronicky podepsat totožný dokument.<sup>186</sup>

Specifickým druhem prostého elektronického podpisu je dynamický biometrický podpis. Ten sice nenaplní požadavky kladené na vyšší úroveň elektronických podpisů, jeho průkaznost je nicméně vyšší než u jiných druhů elektronického podpisu prostého. Věnovat se mu blíže budeme dále v této

<sup>185</sup> JANOUŠEK, 2021, op. cit., s. 151.

<sup>186</sup> Srov. § 126a Bürgerliches Gesetzbuch.

kapitole.<sup>187</sup> Na tomto místě je zmiňován z toho důvodu, že krom grafického znázornění vlastnoručního podpisu také vykazuje specifické vlastnosti, a na rozdíl od vlastnoručního podpisu je nositelem dalších biometrických dat pořízených při vyhotovení podpisu, které je možné při ověření podpisu či při dokazování využít. Pokud by byly akceptovány závěry o nepřijatelnosti elektronického podpisu prostého či jeho platnosti jen v některých případech (jak konstatuje například Janoušek citovaný výše), vylučovalo by to minimálně pro některá právní jednání i užití dynamického biometrického podpisu. To by byl s ohledem na jeho vlastnosti podle našeho názoru absurdní důsledek.

## 7.2.2 Vyšších úrovně elektronických podpisů

Strany elektronických transakcí mohou mít při jejich provádění obavy z naplnění požadavků na autenticitu, integritu, důvěrnost, nezpochybnitelnost a spolehlivost dat. Těmto obavám může předejít používání elektronických podpisů.<sup>188</sup> Většina technik prostých elektronických podpisů je ale nebude řešit adekvátně a nebude přinášet výhody vyšších úrovní elektronických podpisů. Polčák konstatuje, že prokázání nespolehlivosti jednoduchého elektronického podpisu může být vcelku jednoduché a často postačí i jen výpověď tvrzené podepisující osoby.<sup>189</sup> To může znamenat překážku (ať již v důsledku omylu či na základě úmyslného klamavého jednání podepisujícího) při elektronickém právním jednání či přímo finanční újmu. V soukromoprávním styku se proto prosazují a rozšiřují nástroje pro ověření identity jednajících osoby odpovídající vyšším úrovním důvěryhodnosti dle nařízení eIDAS.<sup>190</sup>

Výhodami vyšších úrovní elektronických podpisů je obvykle určitá míra ověření totožnosti původce podepsaného dokumentu nebo to, že tento dokument nebyl po jeho podepsání pozměněn (byla tedy zachována jeho integrita). Požadavky kladené právními předpisy na zaručený a kvalifikovaný elektronický podpis, resp. zaručený podpis založený na kvalifikovaném certifikátu rozebíráme dále. Nejprve je však vhodné stručně popsat jejich technologické pozadí.

<sup>187</sup> Viz podkapitulu 6.4 8.

<sup>188</sup> WOOD BRALEY, 2001, op. cit., s. 418.

<sup>189</sup> POLČÁK, 2011, op. cit., s. 56.

<sup>190</sup> Blíže LOUTOCKÝ, KASL, 2021, op. cit., s. 1047.

Elektronické podpisy v jejich současném běžném chápání jsou založeny na tzv. asymetrické kryptografii, která využívá k šifrování kombinaci tzv. soukromého a veřejného klíče. Smyslem je především zajištění autenticity a integrity dokumentu. Jako funkce kryptografie v této souvislosti bývají uváděny:

1. Autenticita jako zajištění důvěry v původ dokumentu.
2. Integrita ve smyslu zajištění toho, že obsah dokumentu odpovídá jeho původní podobě v okamžiku připojení vyšší úrovně elektronického podpisu.
3. Nezpochybnitelnost či nepopíratelnost, kterých lze v této souvislosti docílit prostřednictvím kroků, které musí podepisující osoba vykonat k vytvoření elektronického podpisu. V případě kvalifikovaného elektronického podpisu pak jde o znalost PIN kódu ke kvalifikovanému prostředku k vytváření elektronických podpisů a faktická dispozice s tímto prostředkem.<sup>191</sup>

O asymetrické kryptografii hovoříme právě proto, že je používán veřejný klíč, který může být zveřejněn komukoliv, a soukromý klíč, jenž by měl být známý pouze jeho vlastníkov. Při podepisování dokumentu je elektronický podpis spočítán pomocí soukromého klíče, což učiní pouze vlastník tohoto klíče. Skutečnost, že dokument skutečně podepsal vlastník pak může kdokoli ověřit prostřednictvím jeho veřejného klíče.

Zjednodušeně si lze podepisování soukromým a veřejným klíčem představit následujícím způsobem.<sup>192</sup> Podepisující osoba zašifruje dokument, resp. jeho jedinečný otisk (tzv. *hash*) soukromým klíčem. Tento otisk je představován daty odvozenými matematickou funkcí z šifrovaného dokumentu do podoby *hasbe* v předem stanovené délce. Při opakovaném matematickém výpočtu je ze stejného dokumentu vždy odvozen stejný *hash*. Nefunguje to ale oboustranně – z *hasbe* nelze odvodit obsah původního šifrovaného dokumentu. Smyslem *hashování* je jednodušší a rychlejší práce s dokumentem, jelikož má předem stanovenou délku.<sup>193</sup> Soukromým klíčem jsou ve smyslu nařízení eIDAS „*data pro vytváření elektronických podpisů*“, tedy jedinečná data,

<sup>191</sup> Blíže viz MASON, 2017, op. cit., s. 296.

<sup>192</sup> Jde o značné zjednodušení, jelikož text je zaměřen na právní, nikoliv technologické aspekty elektronického podepisování.

<sup>193</sup> ZAJÍČEK, Z. a kol. *Zákon o právu na digitální služby. Komentář*. Praha: C. H. Beck, 2021, s. 82.

kteřá podepisující osoba používá k vytváření elektronických podpisů.<sup>194</sup> Tato zašifrovaná podoba dokumentu je připojena k původnímu dokumentu.<sup>195</sup> Příjemce takového dokumentu pak prostřednictvím veřejného klíče podepisující osoby rozšiřuje připojený jedinečný otisk dokumentu, který je porovnán se samotným dokumentem. Veřejným klíčem lze rozumět v pojmosloví nařízení eIDAS „*data pro ověřování platnosti*“; tedy data, která se používají pro ověřování platnosti elektronického podpisu nebo elektronické pečeti<sup>196</sup> (fakticky je ale obdobného využíváno rovněž v případě kvalifikovaného časového razítka). Na základě tohoto porovnání je ověřeno, zda příjemce skutečně obdržel dokument v podobě, která byla podepsána.

V této souvislosti tak lze elektronický podpis, resp. jeho vyšší úroveň definované nařízením eIDAS, popsat jako data, která byla získána z původního dokumentu a za užití asymetrické kryptografie připojena k původnímu dokumentu.<sup>197</sup>

Elektronický podpis sám o sobě nezabrání změně elektronického dokumentu. Pokud je však nějaká změna provedena, projeví se to při ověření elektronického podpisu.<sup>198</sup> Ověření elektronického podpisu je zjednodušeně prováděno tak, že *hash* dokumentu zašifrovaný soukromým klíčem podepisujícího je rozšifrován pomocí veřejného klíče. Takto rozšifrovaný *hash* je porovnán s *hashem* dokumentu vytvořeným při ověření elektronického dokumentu, ke kterému má elektronický podpis náležet. Při shodě těchto dvou *hashů* je osobě provádějící ověření takto poskytnuto ověření integrity dokumentu, tedy shodné podoby mezi podepsaným a ověřovaným dokumentem. Zároveň z procesu ověření vyplývá jistota, že veřejný klíč použitý

<sup>194</sup> Čl. 3 bod 13 nařízení eIDAS.

<sup>195</sup> *Hashovací* funkce je převod vstupních dat (zde elektronického dokumentu) do relativně krátké sekvence znaků (Blíže viz PETERKA, J. *Báječný svět elektronického podpisu*. Praha: CZ.NIC, 2011, s. 70 a násl.). *Hash* lze také popsat jako jednocestnou matematickou funkci, „*která z libovolně velkých dat vypočítá krátký řetězec konstantní délky – hash hodnotu (nebo také pouze hash)*“ (ZAJÍČEK a kol., 2021, op. cit., s. 82.).

<sup>196</sup> Čl. 3 bod 40 nařízení eIDAS.

<sup>197</sup> EECKE, P. van. *The Legal Aspects of Digital Signatures*. In: D'HAENENS, L. (ed.). *Cyberidentities: Canadian & European Presence in Cyberspace*. Ottawa: University of Ottawa Press, 1999, s. 62.

<sup>198</sup> DONÁT, PIFFL, MAISNER, 2017, op. cit., s. 31.

pro dešifrování patří k soukromému klíči osoby, která elektronický podpis vytvořila.<sup>199</sup>

V této souvislosti bývá v zahraniční literatuře rozlišováno mezi elektronickým podpisem (*electronic signature*) a digitálním podpisem (*digital signature*). Digitální podpis je chápán jako data připojená k jiným datům či kryptografická transformace dat za účelem zajištění informace o původu a integritě podepsaných dat. Elektronický podpis je popisován jako cokoliv v elektronické formě, co lze použít k vyjádření vůle podepisující osoby v právním smyslu.<sup>200</sup>

V případě vyšších úrovní elektronických podpisů závisí jejich důvěryhodnost na použité technologii a certifikátu, resp. na poskytovateli služeb vytvářejících důvěru.<sup>201</sup> Dříve byl poskytovatel služeb vytvářejících důvěru označován jako poskytovatel certifikačních služeb (tzv. certifikační autorita).<sup>202</sup> Tito poskytovatelé jsou klíčoví pro spoléhání se na služby vytvářející důvěru, jelikož důvěra v ně je úměrná důvěře v poskytovatele certifikačních služeb.<sup>203</sup> Status kvalifikovaného poskytovatele udílí v členských státech Evropské unie orgány dohledu.<sup>204</sup> Poskytovatel může služby začít poskytovat však teprve poté, co jeho status bude zveřejněn v důvěryhodném seznamu vedeném podle čl. 22 nařízení eIDAS. Orgánem dohledu je v České republice v současnosti Digitální a informační agentura.<sup>205</sup> Kvalifikovaných poskytovatelů služeb vytvářejících důvěru je v České republice podle zveřejněných informací Digitální a informační agenturou ke dni 31. 8. 2023 osm.<sup>206</sup>

Dále rozebíráme jednotlivé vyšší úrovně elektronických podpisů ve smyslu nařízení eIDAS, resp. zák. o službách vytvářejících důvěru.

<sup>199</sup> ZAJÍČEK a kol., 2021, op. cit., s. 83.

<sup>200</sup> Srov. MASON, 2017, op. cit., s. 199.

<sup>201</sup> SMEJKAL, 2019, op. cit., s. 344.

<sup>202</sup> DONÁT, PIFFL, MAISNER, 2017, op. cit., s. 33.

<sup>203</sup> ZAJÍČEK a kol., 2021, op. cit., s. 83.

<sup>204</sup> Čl. 21 nařízení eIDAS.

<sup>205</sup> § 13 odst. 1 zák. o službách vytvářejících důvěru.

<sup>206</sup> Seznam kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru. *Digitální a informační agentura* [online]. [cit. 31. 8. 2023]. Dostupné z: <https://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/povinne-zverejnovane-informace/seznam-kvalifikovanych-poskytovatelu-sluzeb-vytvarejicich-duveru-a-poskytovanych-kvalifikovanych-sluzeb-vytvarejicich-duveru>



### 7.2.3 Zaručený elektronický podpis

Zaručený elektronický podpis naplňuje požadavky stanovené v článku 26 nařízení eIDAS. Těmito požadavky jsou:

- a) jednoznačné spojení elektronického podpisu s podepisující osobou;
- b) možnost identifikace podepisující osoby;
- c) vytvoření elektronického podpisu pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou; a
- d) připojení elektronického podpisu k podepisovaným datům takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat.

Jednoznačnou výhodou této úrovně elektronického podpisu oproti některým typům prostého elektronického podpisu a vlastnoručního podpisu je zajištění integrity podepsaných dat. Ta není – stejně jako v jiných diskutovaných případech – zajištěna tak, že by podepsaný dokument učinila nezměnitelným. Jakákoliv změna dokumentu se ale projeví při ověření elektronického podpisu a srovnání podepsaného dokumentu a dokumentu ověřovaného.

Zaručený elektronický podpis má zajišťovat identifikaci podepisující osoby. V nařízení eIDAS však není stanoveno, jak má k této identifikaci dojít či jakou míru důvěryhodnosti má tato identifikace mít. Lze tak vytvořit vlastní zaručený elektronický podpis založený na certifikátu bez ohledu na to, jaká osoba jej vytvořila ani pro jakou osobu byl vytvořen či jak byla tato osoba identifikována.<sup>207</sup> Je však třeba konstatovat, že plná identifikace podepisující osoby nevyplývá ani z kvalifikovaného certifikátu pro vytváření elektronických podpisů.<sup>208</sup>

Příkladem zaručeného elektronického podpisu je služba Bank iD Sign, která bude zmíněna dále v tomto textu v části věnované podepisování smluv prostřednictvím bankovní identity.<sup>209</sup> Dalším příkladem jsou tzv. komerční či podnikové certifikáty, které vydává pro ověření identity zaměstnavatel svým zaměstnancům.

<sup>207</sup> KORBEL, F. a kol. Elektronická identita při elektronickém (hmotně)právním jednání. *Právní rozhledy*. 2019, č. 18, s. 629. Srov. také např. ČECH, 2021, op. cit., s. 17.

<sup>208</sup> *Ibid.*, s. 630.

<sup>209</sup> Blíže kapitola 7.2 této knihy a také LOUTOCKÝ, KASL, 2021, op. cit., s. 1048.

## 7.2.4 Kvalifikovaný elektronický podpis

Kvalifikovaný elektronický podpis je nejvyšší úrovní elektronického podpisu. Účastníkům právního jednání potvrzuje s vysokou mírou jistoty, že osoba podepisující tímto elektronickým podpisem je skutečně ta osoba, které tento kvalifikovaný podpis náleží.<sup>210</sup> Jde tak o nejdůvěryhodnější úroveň elektronického podpisu, který lze použít pro jednoznačnou identifikaci nejen při veřejnoprávním jednání ale i v rámci soukromoprávního jednání.<sup>211</sup> To je zajištěno tím, že tento podpis je založen na kvalifikovaném certifikátu pro vytváření elektronických podpisů, který vydává pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru. Ten při vydání certifikátu ověří identitu osoby, které je certifikát vydáván. Zároveň je třeba, aby podepisující osoba při vytvoření elektronického podpisu disponovala krom certifikátu také kvalifikovaným zařízením, na kterém je certifikát uložen. Z běžně uváděných tří autentičacích faktorů – vlastnictví (zde např. čipová karta nebo *token*), znalost (např. heslo nebo PIN) a charakteristika (biometrické údaje)<sup>212</sup> – jsou v případě této úrovně podpisu užívány dvě (vlastnictví a znalost).

Další výhodou tohoto elektronického podpisu je jeho přeshraniční uznávání. Nařízení eIDAS jednak závazně stanovuje pro veškeré členské státy Evropské unie, že kvalifikovaný elektronický podpis má právní účinek rovnocenný vlastnoručnímu podpisu.<sup>213</sup> Zároveň se kvalifikovaný elektronický podpis založený na kvalifikovaném certifikátu vydaném v jednom členském státě uznává jako kvalifikovaný elektronický podpis ve všech ostatních členských státech.<sup>214</sup>

Kvalifikovaný podpis je *de facto* zaručeným elektronickým podpisem, který je dle čl. 3 odst. 12 vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů a který je založen na kvalifikovaném certifikátu pro elektronické podpisy.<sup>215</sup> Z požadavků kladených nařízením eIDAS

<sup>210</sup> DONÁT, TOMÍŠEK, 2016, op. cit., s. 142.

<sup>211</sup> LOUTOCKÝ, KASL, 2021, op. cit., s. 1048.

<sup>212</sup> SMEJKAL, V., KODL, J. Development Trends of Electronic Authentication. In: *Proceedings of the 42nd Annual Conference 2008 IEEE International Carnahan Conference on Security Technology*. 2008, s. 2.

<sup>213</sup> Čl. 25 odst. 2 nařízení eIDAS.

<sup>214</sup> Čl. 25 odst. 3 nařízení eIDAS.

<sup>215</sup> Rozvedením toho, co lze považovat za kvalifikovaný elektronický podpis a jaké jsou na něj kladeny požadavky se rovněž zabývá aktuálně Soudní dvůr Evropské unie v rozhodnutí ze dne 20. 10. 2022, ve věci „*Ekojrukt*“ *EOOD proti Direktor na Direktsia „Obžalvane i danačno-osiguritelna praktika“ – Veliko Tarnovo*, C-362/21.

na kvalifikované certifikáty a prostředky jsou patrné výhody, které pro své uživatele přináší. Prostředkem pro vytváření elektronických podpisů je konfigurované programové vybavení nebo technické zařízení, které se používá k vytváření elektronických podpisů. Kvalifikovaný je takový prostředek, který splňuje požadavky stanovené v příloze II nařízení eIDAS.<sup>216</sup> Kvalifikované prostředky podle ní vhodnými technickými prostředky a postupy musí zajistit alespoň minimální standard spočívající v tom, aby:

- a) byla přiměřeně zajištěna důvěrnost dat pro vytváření elektronických podpisů, která byla použita při vytváření elektronického podpisu;
- b) se data pro vytváření elektronických podpisů použítá při vytváření elektronického podpisu mohla prakticky vyskytnout pouze jednou;
- c) bylo přiměřeně zajištěno, že data pro vytváření elektronických podpisů použítá při vytváření elektronického podpisu nelze odvodit a že elektronický podpis je v současnosti dostupnými technickými prostředky spolehlivě chráněn proti paděláním;
- d) oprávněná podepisující osoba měla možnost data pro vytváření elektronických podpisů použítá při vytváření elektronického podpisu spolehlivě chránit před jejich zneužitím třetí osobou.

Kvalifikované prostředky pro vytváření elektronických podpisů zároveň nesmějí měnit podepisovaná data ani bránit tomu, aby byla tato data předložena podepisující osobě před vlastním podepsáním.

Kvalifikovaný elektronický podpis musí být také založen na kvalifikovaném certifikátu pro elektronické podpisy. Certifikátem pro elektronický podpis rozumí nařízení eIDAS elektronické potvrzení, které spojuje data pro ověřování platnosti elektronických podpisů s určitou fyzickou osobou a potvrzuje alespoň jméno nebo pseudonym této osoby.<sup>217</sup> Aby byl certifikát považovaný za kvalifikovaný musí podle přílohy č. I eIDAS obsahovat:

- a) označení, alespoň ve formě vhodné pro automatické zpracování, že se certifikát vydává jako kvalifikovaný certifikát pro elektronický podpis;
- b) soubor dat jednoznačně identifikujících kvalifikovaného poskytovatele služeb vytvářejících důvěru, který vydává kvalifikované certifikáty,

<sup>216</sup> Čl. 3 bod 22 a 23 nařízení eIDAS.

<sup>217</sup> Čl. 2 bod. 14 nařízení eIDAS.

- včetně alespoň členského státu, v němž je poskytovatel usazen, a v případě právnické osoby název a případné registrační číslo uvedené v úředních záznamech; v případě fyzické osoby jméno této osoby;
- c) alespoň jméno podepisující osoby nebo pseudonym. Je-li použit pseudonym, musí být tato skutečnost jasně vyznačena;
  - d) data pro ověřování platnosti elektronických podpisů, která odpovídají datům pro vytváření elektronických podpisů;
  - e) označení začátku a konce doby platnosti certifikátu;
  - f) identifikační číslo certifikátu, které musí být jedinečné pro daného kvalifikovaného poskytovatele služeb vytvářejících důvěru;
  - g) zaručený elektronický podpis nebo zaručenou elektronickou pečeť kvalifikovaného poskytovatele služeb vytvářejících důvěru, který certifikát vydává;
  - h) údaj o místě, kde je bezplatně k dispozici certifikát, na němž je založen zaručený elektronický podpis nebo zaručená elektronická pečeť podle písmene g);
  - i) údaj o umístění služeb, které lze využít k zjištění platnosti kvalifikovaného certifikátu;
  - j) pokud jsou data pro vytváření elektronických podpisů spojená s daty pro ověřování platnosti elektronických podpisů obsažena v kvalifikovaném prostředku pro vytváření elektronických podpisů, příslušnou poznámku, alespoň ve formě vhodné pro automatické zpracování.

Překážkou pro podepisování kvalifikovaným elektronickým podpisem může být to, že se běžnému uživateli může dané jevit jako složité<sup>218</sup>, navíc je třeba opatřit kvalifikovaný prostředek pro vytváření a požádat o vystavení kvalifikovaného certifikátu pro podepisování. Do budoucna má však Evropská komise záměr zpřístupnit elektronické podepisování širší mase běžných uživatelů, a to prostřednictvím evropských peněženek digitální identity, které by uživatelé mohli mít k dispozici i ve svých mobilních telefonech. Tato služba by podle návrhu Evropské komise měla uživatelům umožnit mimo jiné podepisovat kvalifikovanými elektronickými podpisy.<sup>219</sup>

<sup>218</sup> V tomto kontextu se jedná typicky o to, že certifikát je uložen na čipové kartě, je tedy nutno nadto disponovat příslušným čtecím zařízením.

<sup>219</sup> Ibid., s. 24, čl. 1 odst. 7.

### 7.2.5 Zaručený podpis založený na kvalifikovaném certifikátu

Zák. o službách vytvářejících důvěru v českém prostředí nad rámec eIDAS upravuje čtvrtou úroveň elektronického podpisu – zaručený elektronický podpis založený na kvalifikovaném certifikátu. Ten je určitým přechodem mezi zaručeným elektronickým podpisem a kvalifikovaným elektronickým podpisem. Certifikát pro tento podpis je shodný jako certifikát kvalifikovaného elektronického podpisu. Rozdíl je ten, že v případě zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu bude tento soukromý klíč uložen v zařízení uživatele (např. na disku počítače), které nebude splňovat požadavky na kvalifikovaný prostředek pro vytváření elektronických podpisů. Podle důvodové zprávy k zák. o službách vytvářejících důvěru je smyslem nad rámec nařízení eIDAS přiznat účinky vlastnoručního podpisu i jinému typu elektronického podpisu, než je kvalifikovaný, a to zejména z důvodu výše nákladů vynakládaných na pořízení kvalifikovaného prostředku pro vytváření kvalifikovaných elektronických podpisů.

Problematický je nyní tento podpis v rámci přeshraničního užívání (v současné chvíli takový podpis nebude v zahraničí bez dalšího uznán). Revize nařízení eIDAS má nicméně nyní ambice tento nedostatek překlenout a míří na výslovnou úpravu zaručených podpisů založených na kvalifikovaných certifikátech. Tato oblast v původním návrhu Evropské komise chyběla a do návrhu se dostala až v obecném přístupu Rady přijatého za českého předsednictví, možná také z toho důvodu, že česká úprava na tuto úroveň pamatuje. Revize tedy nově upravuje požadavky na ověřování zaručených elektronických podpisů založených na kvalifikovaných certifikátech. Komise má po přijetí revize nařízení eIDAS zároveň prostřednictvím prováděcích aktů stanovit specifikace a referenční čísla norem pro ověřování zaručených elektronických podpisů založených na kvalifikovaných certifikátech.

### 7.2.6 Uznávaný elektronický podpis<sup>220</sup>

Zák. o službách vytvářejících důvěru vzhledem k závaznosti, přímé použitelnosti a aplikační přednosti nařízení Evropské unie nijak blíže neupravuje

<sup>220</sup> Následující text vychází z dříve publikovaného textu JAREŠ, A. Nařízení eIDAS, elektronický podpis a pečeť v českém právním řádu. In: ŠEDLÁČEK, M., STŘELEČEK, T. a kol. *Právní jednání a procesní úkony (vzájemné vztahy a nové aspekty)*. Praha: Wolters Kluwer, 2019, s. 19–26.

jednotlivé úrovně elektronických podpisů. Naopak pouze stanoví, k jakým právním jednáním se použije konkrétní úroveň elektronického podpisu.

Uvedli jsme, že nařízení eIDAS upravuje prostý, zaručený a kvalifikovaný elektronický podpis. Zák. o službách vytvářejících důvěru nejprve v § 5 stanoví, které dokumenty je třeba opatřit kvalifikovaným elektronickým podpisem. Ustanovení § 6 odst. 1 pak uvádí, pro která jednání, resp. dokumenty se používá uznávaný elektronický podpis. Zdánlivě tak zákon zavádí jako další kategorii uznávaný elektronický podpis. Následující odstavec zákona však vysvětluje, že uznávaným elektronickým podpisem se rozumí zaručený elektronický podpis založený na kvalifikovaném certifikátu (tedy výše uvedené české specifikum) nebo kvalifikovaný elektronický podpis.

Zákonodárce tak namísto konstrukce typu „K podepisování lze použít pouze kvalifikovaný elektronický podpis a zaručený elektronický podpis založený na kvalifikovaném certifikátu“, zavádí kategorii (legislativní zkratku) „uznávaný elektronický podpis“ upravující tyto dva druhy elektronického podpisu. Tu navíc užívá ve svém textu dále jen jednou, a to hned v následujícím § 7. Podle něj je pro ostatní jednání mimo § 5 a § 6 možné použít zaručený elektronický podpis, uznávaný elektronický podpis, případně jiný typ elektronického podpisu. Zákonodárce si tak v případě zák. o službách vytvářejících důvěru pouze ušetřil jedno další výslovné uvedení kvalifikovaného elektronického podpisu. V případě § 7 lze navíc uvažovat o jeho nadbytečnosti. I bez něj by mělo být patrné, že k ostatním právním jednáním by bylo vzhledem k nařízení eIDAS přípustné použít jakýkoliv elektronický podpis včetně jednoduchého elektronického podpisu. Na druhou stranu, stanovuje-li § 561 odst. 1 obč. zák., že „[j]iný právní předpis stanoví, jak lze při právním jednání učiněném elektronickými prostředky písemnost elektronicky podepsat“, pak je zřejmě k vyloučení nejasností úprava § 7 zák. o službách vytvářejících důvěru vhodná.

Záměrem zákonodárce při zavedení pojmu „uznávaný elektronický podpis“ pravděpodobně bylo, aby s oběma typy v něm zahrnutých elektronických podpisů mohl do budoucna jednoduše pracovat i ve zvláštních zákonech. Takto byl tento pojem použit například v případě novely zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), zákonem č. 64/2017 Sb., který do insolvenčního zákona vložil § 80a používající

uznávaný elektronický podpis<sup>221</sup>, nebo novely zákona č. 164/2013 Sb., o mezinárodní spolupráci při správě daní<sup>222</sup>, zákonem č. 305/2017 Sb. Tomuto předpokladu odpovídá i důvodová zpráva k zákonu č. 298/2016 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce.

Důvodová zpráva uvádí, že v těch ustanoveních, ve kterých je to možné, je usilováno o vypuštění pojmů elektronický podpis, elektronická značka a elektronické časové razítko a jejich typů bez náhrady s tím, že bude využito subsidiarity procesních předpisů. Pokud takový postup není možný, dochází k náhradě obecnějšími, technologicky neutrálními pojmy, aby v budoucnu nemuselo docházet k novelizacím jednotlivých zákonů. V případě změny technologie tak bude třeba novelizovat pouze příslušná ustanovení zákona o službách vytvářejících důvěru, nikoliv další právní předpisy.

Pojem „uznávaný elektronický podpis“ navíc již používal původní zák. o el. podpisu, který ho ale definoval odlišným způsobem. Dle § 11 odst. 3 tohoto zákona se uznávaným elektronickým podpisem rozuměl:

- a) zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb a obsahujícím údaje, které umožňují jednoznačnou identifikaci podepisující osoby, a
- b) zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném za stanovených podmínek poskytovatelem certifikačních služeb, který je usazen mimo území České republiky.

S tímto pojmem také pracovali další zvláštní zákony. Při přijetí zák. o službách vytvářejících se tak zákonodárce vyhnul nutnosti dalších zásahů nad rámec novelizačních bodů zákona č. 298/2016 Sb.<sup>223</sup>

<sup>221</sup> „Osoby, kterým se podle zvláštního právního předpisu zřizuje datová schránka bez žádosti, činí podání včetně příloh v elektronické podobě do datové schránky soudu nebo v elektronické podobě podepsané uznávaným elektronickým podpisem. Není-li v odůvodněných případech možné učinit podání podle věty první, lze je výjimečně a s uvedením důvodu učinit v listinné podobě.“

<sup>222</sup> § 13zo odst. 1: „(1) Oznámení a obhlášení se podávají na tiskopise vydaném ministerstvem a činí se datovou zprávou a) podepsanou uznávaným elektronickým podpisem, nebo b) s ověřenou identitou podatele způsobem, kterým se lze přihlásit do jeho datové schránky.“

<sup>223</sup> Zákon 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.

### 7.3 Srovnání vlastnoručního a elektronického podpisu

V návaznosti na výše poskytnutý přehled úrovní elektronického podpisu a jejich kvalit z hlediska důvěryhodnosti se logicky nabízí otázka, jak si stojí elektronické způsoby podepisování v porovnání s tradičním vlastnoručním podpisem. Zde ovšem již Matejka s Chumem dovodili, že dosáhnout plnohodnotného srovnání je velmi nesnadné.<sup>224</sup> Ze zkušenosti lze říci, že vlastnoruční podpis je oproti elektronickému případ od případu zdánlivě nestálý a proměnlivý. Logicky navíc absentují doprovodná metadata. Měl by tak být především ve srovnání s vyššími úrovněmi elektronického podpisu relativně méně důvěryhodný.

Zde je ovšem na místě zohlednit dlouhou právní tradici vlastnoručního podpisu, přičemž platí, že byť grafologické posudky nejsou vždy zcela jednoznačné, lze se s takovými situacemi v rámci civilního procesu vypořádat. Vlastnoruční podpis ze své podstaty odpovídá vlastnostem a projevu konkrétní osoby. V této souvislosti Matejka s Chumem upozorňují na to, že u uznávaného elektronického podpisu jde naproti tomu o provedení nějakého úkonu, který je však pouze vázán na dostupnost prostředku pro vytvoření takového podpisu. Z hlediska dokazování tak podle nich nebude ani tak sporná skutečnost, zda byl právní úkon učiněn osobou, v jejíž dispozici byl podpisový prostředek, ale především identifikace té pravé osoby, která tento úkon učinila.<sup>225</sup>

V případě elektronických podpisů může dojít k prokázání skutečnosti, že elektronický podpis byl skutečně vytvořen tvrzenou podepisující osobou, prostřednictvím důkazu znalosti (PIN pro vytvoření kvalifikovaného elektronického podpisu), důkazu vlastnictvím (certifikát k vytváření elektronického podpisu) či důkazu vlastnostmi podepisujícího (data získaná při vytvoření dynamického biometrického podpisu).<sup>226</sup>

Certifikát pro zaručený elektronický podpis může vystavit v zásadě kdokoliv s dostatečným technickým zázemím a jeho důvěryhodnost je odvislá od důvěry v tohoto výstavce certifikátu. Tento problém řeší kvalifikovaný elektronický podpis, jelikož při vydání certifikátu dochází k dostatečně

<sup>224</sup> MATEJKA, J., CHUM, V. K právní úpravě elektronického podpisu. *Bulletin advokacie*. 2002, č. 3, s. 38.

<sup>225</sup> Ibid.

<sup>226</sup> Srov. MASON, 2017, op. cit., s. 303.



identifikaci žadatele a vystavuje jej certifikovaný kvalifikovaný poskytovatel služeb vytvářejících důvěru. Při vytvoření elektronického podpisu je zde kombinován důkaz vlastnictvím (podepisující osoba musí disponovat kvalifikovaným certifikátem a kvalifikovaným prostředkem pro vytváření elektronických podpisů) a důkaz znalostí (PIN pro vytvoření podpisu). Tato skutečnost však sama o sobě nutně nezaručuje, že právní jednání skutečně kvalifikovaným elektronickým podpisem opatřila tvrzená podepisující osoba. Rozdíl oproti vlastnoručnímu podpisu však v této souvislosti nemusí být při dokazování nijak zásadní. I tento elektronický podpis může být k dokumentu připojen neoprávněně. V rámci dokazování bude za užití správných důkazních prostředků možné prokázat, že vlastnoruční či kvalifikovaný elektronický podpis byl připojen jinou osobou, než je tvrzeno. Některé důkazní prostředky se mohou lišit, jiné, jako například svědecká výpověď, budou stejné.

Jako elektronický podpis lze užít také sken vlastnoručního podpisu připojený k elektronickému dokumentu. Ten bude možné jednoduše zneužít, postačí mít k dispozici grafické znázornění vlastnoručního podpisu tvrzené podepisující osoby. Kvalitativně na jiné úrovni se bude nacházet dynamický biometrický podpis, jehož složkou je také grafické znázornění vlastnoručního podpisu, je nicméně doplněn i o biometrické údaje podepisující osoby. Smejkal užívání dynamického biometrického podpisu hodnotí tak, že „[o]d podpisového vzoru v podobě neobratného a omylného srovnávání obrázků s podpisy (pozorováním ověřující osobou), poskytujícího minimální záruky, přes relativně bezpečné, ale komplikované postupy asymetrické kryptografie, jsme se opět vrátili ke podpisovým vzorům, ale vzorům ‚chytrým‘, skrývajícím oku neviditelnou a nezfalšovateľnou biometrickou vrstvu.“<sup>227</sup> Jeho užívání při právním jednání pak považuje za jednoduchou a neobtěžující formu autentizace podpisu podepisující osoby a za „vysoce přínosné jak při rutinním využívání, tak při zajištění integrity zpracovávaných podepsaných elektronických dokumentů.“<sup>228</sup>

V souvislosti s dynamickým biometrickým podpisem je uváděno, že biometrická stopa je v jeho případě pro každého jednotlivce unikátní a nelze ji v praxi reprodukovat padělatelem.<sup>229</sup> Maisner, Smejkal a Uříčar také k dále

227 SMEJKAL, V. Dynamický biometrický podpis a nařízení GDPR. *Revue pro právo a technologie*. 2017, roč. 8, č. 16, s. 92.

228 Ibid., s. 110.

229 MAISNER, M., SMEJKAL, V., UŘIČAŘ, M. Je používání dynamického biometrického podpisu v rozporu s GDPR. *Bulletin advokacie*. 2019, č. 9, s. 24.

rozebíranému rozhodnutí Úřadu pro ochranu osobních údajů<sup>230</sup> upozorňují, že návrat k používání pouhého obrázku jako podpisu zvyšuje riziko zhotovení padělku nebo popírání pravosti vlastního podpisu. Případný ústup od používání dynamického biometrického podpisu tak hodnotí jako rozporný se zájmem smluvních stran, ale i se současným požadavkem na zvyšování právní jistoty a bezpečnosti transakcí.<sup>231</sup>

Postupně přestalo být nutné využívat pro vytváření dynamických biometrických podpisů pouze speciální certifikované *signpady* a tablety, ale začala být využívána i jiná zařízení.<sup>232</sup> V praxi se prosazují softwarová řešení, která jsou nezávislá na použitém zařízení. Důkazní váha takto vyhotovených podpisů však bude proměnlivá podle parametrů použitých zařízení a prostředků.<sup>233</sup> Dynamický biometrický podpis lze však podle našeho názoru ve většině případů hodnotit jako důvěryhodnější než vlastnoruční podpis. Korbel, Kovář a Jaroš vnímají rozdílnou důvěryhodnost a míru důkazní spolehlivosti mezi dynamickým biometrickým podpisem a pouhým obrázkem podpisu (skicou, faksimilií). Poukazují přitom na to, že při dynamickém biometrickém podpisu dochází ke snímání a zaznamenávání podpisu vytvářeného vlastní rukou spolu s dalšími identifikačními prvky, které zajišťují vyšší právní jistotu jednání. Skica přitom nemá sama o sobě žádnou další důkazní hodnotu, jelikož jde pouze o naskenování obrazu podpisu. Dynamický biometrický podpis může být podkladem pro další písmoznalecké i technologické zkoumání pravosti podpisu.<sup>234</sup> Tento závěr lze užít dle našeho soudu i pro srovnání tohoto typu podpisu s vlastnoručním podpisem. Ten bude sice možné také podrobit písmoznaleckému zkoumání, nicméně již jej nebudou doprovázet další data, která jsou spojená s dynamickým biometrickým podpisem. Při vytváření dynamického biometrického podpisu je možné při užití dalších technologických postupů docílit zajištění integrity dokumentu podobným způsobem jako v případě asymetrické kryptografie.<sup>235</sup> Oproti vlastnoručnímu podpisu tak bude možné

<sup>230</sup> K němu blíže v kapitole 6.5.3.

<sup>231</sup> MAISNER, SMEJKAL, UŘIČAŘ, 2019, op. cit., s. 31.

<sup>232</sup> KORBEL, KOVÁŘ, JAROŠ, 2021, op. cit., s. 13.

<sup>233</sup> ZIMMER, J., FÜRST, T., HAUSER, T. Důkazní váha biometrického podpisu závisí na kvalitě použitého dotykového zařízení a na dostupnosti úplných podpisových dat. *Právní rozhledy*. 2021, č. 13–14.

<sup>234</sup> KORBEL, KOVÁŘ, JAROŠ, 2021, op. cit., s. 14.

<sup>235</sup> SMEJKAL, 2017, op. cit., s. 94.

zajistit i faktickou nezměnitelnost podepsaného dokumentu, resp. jakoukoliv změnu dokumentu zjistit při ověření podepsaného dokumentu a podpisu. Souhlasíme tedy se zmíněnými autory, kteří považují důkazní pozici osoby spoléhající na dynamický biometrický podpis za velmi silnou.<sup>236</sup>

## 7.4 Úředně ověřený elektronický podpis<sup>237</sup>

S ohledem na to, že v případě některých právních jednání nestačí takové právní jednání pouze podepsat, ale je třeba podpis rovněž úředně ověřit, zabýváme se dále úředním ověřením elektronického podpisu.

Úředním ověřením se rozumí legalizace ve smyslu § 10 zák. o ověřování<sup>238</sup>, kterou se na žádost ověřuje, že žadatel listinu před ověřující osobou vlastnoručně podepsal nebo podpis na listině uznal za vlastní, přičemž legalizací se nepotvrzuje ani správnost ani pravdivost údajů v listině uvedených.

Občanský zákoník, nařízení eIDAS, zák. o službách vytvářejících důvěru, ani jiný předpis dlouho neřešil obecným způsobem elektronické podepisování listiny v případě, kdy zákon vyžaduje úřední ověření podpisu umístěného na této listině.<sup>239</sup> Možnost elektronicky právně jednat i v případě, že zákon vyžaduje úřední ověření podpisu, musel umožnit zvláštní zákon. Bylo tomu tak například v případě zákona č. 256/2013 Sb., o katastru nemovitostí (katastrální zákon), resp. katastrální vyhlášky.<sup>240</sup> Podobně pak zákon o veřejných rejstřících právnických a fyzických osob umožnil namísto úředně ověřeného

<sup>236</sup> KORBEL, KOVÁŘ, JAROŠ, 2021, op. cit., s. 15.

<sup>237</sup> V podrobnostech viz JAREŠ, A. Nahrazení úředně ověřeného podpisu elektronickým dokumentem. *Soukromé právo*. 2020, č. 1, JAREŠ, A. Úřední ověření elektronického podpisu na plné moci. In: SEDLÁČEK, M., STŘELEČEK, T. a kol. *Zastoupení. Specifika a nové aspekty*. Praha: Wolters Kluwer, 2020.

<sup>238</sup> Zákona č. 21/2006 Sb., o ověřování shody opisu nebo kopie s listinou a o ověřování pravosti podpisu a o změně některých zákonů (zákon o ověřování) (dále „zákon o ověřování“ nebo „zákon o ověřování“).

<sup>239</sup> K tomu také například rozhodnutí Nejvyššího soudu ze dne 30. 7. 2019, sp.zn. 29 NSCR 133/2017.

<sup>240</sup> Dle § 64 odst. 1 vyhlášky č. 357/2013 Sb., o katastru nemovitostí (katastrální vyhláška), katastrální úřad považuje za prokázanou pravost elektronického podpisu na písemnosti obsahující právní jednání fyzické osoby (právní jednání právnických osob jsou nyní ponechána stranou), jestliže kvalifikovaný certifikát pro elektronický podpis obsahuje jméno a příjmení podepisující osoby a údaj, který umožňuje jednoznačnou identifikaci podepisující osoby, nebo podepsaná osoba uznala před katastrálním úřadem, že obsah písemnosti v elektronické podobě je projevem její vůle, a potvrdila, že je držitelem kvalifikovaného certifikátu pro elektronický podpis, kterým byla písemnost podepsána.

podpisu užít uznávaný elektronický podpis.<sup>241</sup> Lze také zmínit § 97 insolvenčního zákona<sup>242</sup> ve znění účinném do 18. 9. 2016, podle kterého musel být insolvenční návrh v listinné podobě opatřen úředně ověřeným podpisem, nebo v elektronické podobě uznávaným elektronickým podpisem, nebo zaslán prostřednictvím datové schránky podatele.

Byť se snahy o zavedení legalizace elektronického podpisu objevily již v roce 2006<sup>243</sup>, žádný předpis dříve tuto oblast obecně neupravoval. Před 31. 1. 2022 nadto zákon o ověřování<sup>244</sup> v § 13 písm. g) výslovně uváděl, že legalizace se neprovede, jde-li o legalizaci elektronického podpisu. Naproti tomu například slovenský občanský zákoník výslovně uvádí, že osvědčení pravosti podpisu se pro dokumenty podepsané uznávaným elektronickým podpisem nevyžaduje. Stanoví totiž, že „[n]a právne úkony uskutočnené elektronickými prostriedkami, podpísané zaručeným elektronickým podpisom alebo zaručenou elektronickou pečatou a opatrené časovou pečiatkou sa osvedčenie pravosti podpisu nevyžaduje.“<sup>245</sup>

#### 7.4.1 Zákon o právu na digitální služby

Tento nedostatek se pokusil vyřešit až zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů (dále „zák. o právu na digitální služby“). Podle něj, stanoví-li právní předpis požadavek úředního ověření vlastnoručního nebo uznávaného elektronického podpisu, považuje se za splněný při využití jednoho z následujících postupů:<sup>246</sup>

- a) elektronickým dokumentem nedílně spojeným s kvalifikovaným elektronickým podpisem osoby oprávněné provádět ověřování pravosti podpisu,
- b) elektronickým dokumentem nedílně spojeným se záznamem informačního systému veřejné správy,
- c) při podepsání uznávaným elektronickým podpisem, pokud lze s využitím údajů základního registru obyvatel nebo portálu veřejné správy ověřit, že kvalifikovaný certifikát patří podepisující osobě.

<sup>241</sup> § 22 odst. 3 zákona č. 304/2013 Sb., o veřejných rejstřících právnických a fyzických osob a o evidenci svěrenských fondů.

<sup>242</sup> Zákon č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon).

<sup>243</sup> ZAJÍČEK a kol., 2021, op. cit., s. 75.

<sup>244</sup> Zákon č. 21/2006 Sb., o ověřování shody opisu nebo kopie s listinou a o ověřování pravosti podpisu a o změně některých zákonů (zákon o ověřování).

<sup>245</sup> § 40 odst. 5 zákona č. 40/1964 Zb., občanský zákoník.

<sup>246</sup> Dle § 6 odst. 1 zák. o právu na digitální služby.

## 7.4.2 Ověření oprávněnou osobou

První možnost, jak lze podle zák. o právu na digitální služby místo vlastnoručního úředně ověřeného podpisu použít elektronický podpis, je opatřit elektronický dokument kvalifikovaným elektronickým podpisem osoby oprávněné provádět ověřování pravosti podpisu, která postupem podle jiného právního předpisu ověří, že podepisující osoba dokument před ní podepsala nebo podpis uznala za vlastní. Zároveň je třeba opatřit takový dokument kvalifikovaným elektronickým časovým razítkem.

Podle zákona o ověřování legalizaci provádí krajský, obecní a újezdní úřad, držitel poštovní licence (Česká pošta, s. p.) a Hospodářská komora České republiky. Podle notářského řádu úřední ověření podpisu vykonává také notář. Dle původní dikce návrhu zák. o právu na digitální služby mohlo být sporné, zda bude moci provést elektronické ověření podpisu i advokát. Tento nedostatek byl však v průběhu legislativního procesu napraven a § 6 odst. 1 písm. a) odkazuje na jiný právní předpis s výslovným uvedením zák. o advokacii v poznámce pod čarou.

Původ podepisovaného dokumentu a vůle dokumentem projevovaná bude v tomto případě tedy potvrzená elektronickým podpisem podepisující osoby. Zároveň bude nezměnitelnost dat tohoto dokumentu zaručena kvalifikovaným elektronickým podpisem a kvalifikovaným časovým razítkem osoby provádějící ověření podpisu tohoto dokumentu.

Oproti klasickému listinnému dokumentu s úředně ověřeným podpisem vykazuje takto ověřený elektronický dokument několik výhod. Jeho obsah je prakticky nezměnitelný (resp. každá jeho změna se projeví při ověřování kvalifikovaného elektronického podpisu a časového razítka). Odpadá také dřívější nutnost provedení autorizované konverze listinného dokumentu s ověřeným podpisem, pokud by ho chtěla podepisující osoba použít v elektronické podobě. Zároveň bude možné použít libovolné množství kopií takto elektronicky ověřeného dokumentu.

## 7.4.3 Záznam informačního systému veřejné správy

Zákon také předpokládá nahrazení úředně ověřeného podpisu dokumentem nedílně spojeným se záznamem informačního systému veřejné správy

o provedení elektronické identifikace podepisujícího prostřednictvím kvalifikovaného systému elektronické identifikace s úrovní záruky vysoká. Tento záznam pak musí být opatřený kvalifikovanou elektronickou pečeti a kvalifikovaným elektronickým časovým razítkem kvalifikovaného poskytovatele. Technické provedení samotného nástroje, kterým bude v tomto případě prováděna elektronická identifikace, a kterým bude realizován popsany proces, zák. o právu na digitální služby v souladu se zásadou technologické neutrality nijak neřeší a bude na každém správci systému, jaké technické řešení zvolí.<sup>247</sup>

#### 7.4.4 Využití údajů v základním registru obyvatel

V průběhu legislativního procesu návrhu zák. o právu na digitální služby došlo k významným zásahům do původního návrhu § 6 zavádějícího právo na úřední ověření elektronického podpisu. K druhé variantě ověření mělo původně docházet prostřednictvím záznamu kvalifikovaného poskytovatele o provedení elektronické identifikace podepisujícího uživatele. Do tohoto ustanovení byla také vložena další možnost vyhovění požadavku na úřední ověření podpisu. Podle zák. o právu na digitální služby se považuje tento za splněný také využitím uznávaného elektronického podpisu, pokud lze s využitím údajů základního registru obyvatel<sup>248</sup> nebo portálu veřejné správy ověřit, že kvalifikovaný certifikát pro elektronický podpis, na jehož základě podepisující vytvořil uznávaný elektronický podpis na dokumentu, patří podepisujícímu.

#### 7.4.5 Ověření elektronického podpisu na plné moci

Výše byly rozebrány tři způsoby splnění požadavku úředně ověřeného podpisu prostřednictvím elektronického dokumentu. Zák. o právu na digitální služby stanoví omezení pro nahrazení úředně ověřeného podpisu elektronickým dokumentem, a to pro plnou moc k právnímu jednání, pro které je vyžadována forma veřejné listiny.<sup>249</sup> Pro takové právní jednání totiž postačí

<sup>247</sup> Srov. § 13 zák. o právu na digitální služby.

<sup>248</sup> Certifikát lze jednoduše nahrát do registru obyvatel Portálu občana. Dostupné z: <https://portal.gov.cz>

<sup>249</sup> § 6 odst. 3 zákona o právu na digitální služby: „Ustanovení § 6 odst. 1 písm. b) a § 6 odst. 2 se nepoužijí pro plnou moc k právnímu jednání podle § 441 odst. 2 poslední věty občanského zákoníku.“

plná moc s úředně ověřeným podpisem, není třeba ji vyhotovit také ve formě veřejné listiny.<sup>250</sup> Takovou plnou lze vyhotovit s elektronickým podpisem pouze v případě, že je tento podpis ověřen notářem, advokátem nebo jinou osobou oprávněnou provádět legalizaci.<sup>251</sup>

Nemožnost elektronického ověření podpisu na plné moci pro právní jednání, pro něž je vyžadována forma veřejné listiny, byla do návrhu zákona vložena až v rámci legislativního procesu pozměňovacím návrhem. Ten byl odůvodněn tak, že principem úředního ověření je jeho provádění třetí nezávislou osobou. K ověření podpisu pro umožnění sepisu veřejné listiny notářem tedy podle něj není vhodná forma automatické identifikace podepisujícího a nelze tak připustit sepis veřejné listiny na základě plné moci, na které nebyla třetí nezávislou osobou ověřena totožnost podepisující osoby.<sup>252</sup>

Tento požadavek se může zdát jako zbytečně tvrdý a jevit se jako překážka elektronickému právnímu jednání. Postup při ověřování pravosti podpisu je upraven zákonem o ověřování<sup>253</sup>, notářským řádem<sup>254</sup> a zákonem o advokacii<sup>255</sup>. S ohledem na formální požadavky kladené na tento postup bude ověřený podpis na plné moci plnit důkazní, označovací i deklarační funkci. Sice platí, že osoba provádějící ověření neodpovídá za obsah samotné listiny,<sup>256</sup> při ověření podpisu notářem či advokátem však může podepsovaná listina v některých případech dobře plnit i funkci kontrolní a poradní. Vždy by ale měla být naplněna funkce varovná.

Domníváme se, že elektronickému právnímu jednání a elektronické kontrakci nemají být kladeny překážky. Na druhou stranu ale s ohledem na závažné právní následky právních jednání, pro která je vyžadována forma veřejné listiny, je vhodné stanovit formální požadavky pro podpis plné moci pro takové právní jednání. Požadavek na kvalifikovanou formu právního jednání (zde úředně ověřený podpis) nemá totiž smysl jen v zajištění spolehlivého důkazu.

<sup>250</sup> § 441 odst. 2 obč. zák.

<sup>251</sup> Viz § 6 odst. 3 zák. o právu na digitální služby.

<sup>252</sup> *Pozměňovací návrh poslance Mgr. Tomáše Koboutka, MBA k návrhu poslanců [...] na vydání zákona o právu na digitální služby a o změně některých zákonů* [online]. [cit. 20. 6. 2020]. Dostupné z: <http://www.psp.cz/sqw/text/orig2.sqw?idd=162341>

<sup>253</sup> § 11 a § 12 zák. o ověřování.

<sup>254</sup> § 74 notářského řádu.

<sup>255</sup> § 25a zák. o advokacii.

<sup>256</sup> § 74 odst. 4 notářského řádu, § 10 odst. 2 zák. o ověřování.

Spatřujeme jej také v tom, aby si jednající osoba byla skutečně vědoma následků podpisu a jeho závažnosti.

Jako zásadní funkce přísné písemné formy lze vidět varovnou, poradní a kontrolní funkci, které se dobře projeví v případě, kdy notář nebo advokát bude schopný poskytnout účastníkům právního jednání také odborné poradenství. U právního jednání prováděného formou notářského zápisu, které bude provádět zmocněnec na základě plné moci, se pro zmocnitele tyto funkce nenaplní natolik, jako by tomu bylo při jeho osobním jednání. Tyto funkce by tedy měly být alespoň do jisté míry suplovány při podpisu plné moci. Kontrolní a poradní funkce sice nebude splněna při podpisu na přepážce Czech POINT před úředníkem krajského nebo obecního úřadu či před zaměstnancem České pošty. Takový podpis bude ale stále dobře plnit varovací funkci. Už samotný formální postup při podepsání nebo uznání podpisu za vlastní před oprávněnou osobou by totiž měly podepisujícího varovat před tím, že jeho podpis má zásadní právní účinky. Přikláníme se tedy k názoru o správnosti požadavku na provedení ověření podpisu na plné moci pro diskutovaná právní jednání pouze před třetí osobou provádějící ověření podpisu, nikoliv pouze prostřednictvím elektronické identifikace či spojení elektronického podpisu s registrem osob nebo portálem veřejné správy.

## 7.4.6 Aktuální relevantní rozhodovací praxe

Mírný rozruch vzbudilo v kruzích právníků zaměřujících se na insolvenční rozhodnutí Vrchního soudu v Praze z roku 2023, které se zabývalo naplněním požadavku na úřední ověření podpisu insolvenčního návrhu uznávaným elektronickým podpisem.<sup>257</sup> Zde soud vyložil požadavky dřívější právní úpravy na podpis insolvenčního návrhu a plné moci spolu s požadavky účinného znění § 97 insolvenčního zákona. Podle soudu mají ustanovení § 97 odst. 2 a 3 insolvenčního zákona za cíl nezaměnitelným způsobem identifikovat osobu projevující vůli k podání insolvenčního návrhu, případně vůli jejího právního zástupce. Bylo by tak iracionální, pokud by v případě insolvenčního návrhu v listinné formě bylo trváno na úředním ověření podpisu, a při elektronickém podání by se soud spokojil s podáním s „*jakoukoliv kvalitou*

<sup>257</sup> Rozhodnutí Vrchního soudu v Praze ze dne 28. června 2023, sp.zn. 3 VSPH 610/2023-A-122.



*podpisu*“: Naplnění požadavku úředně ověřeného podpisu na insolvenčním návrhu tak lze docílit buď prostřednictvím autorizované konverze listiny s úředně ověřeným podpisem, anebo při splnění požadavků stanovených v § 6 zák. o právu na digitální služby.

Toto rozhodnutí navazuje na dřívější usnesení Ústavního soudu ze stejného roku, které se také týkalo insolvenčního řízení.<sup>258</sup> Ústavní soud zde konstatuje, že *„stěžovatelka nedoceňuje, že podmínkou pro využití elektronického podpisu jako alternativy k úředně ověřenému podpisu je, že si podepisující zapíše údaje o sériovém čísle kvalifikovaného certifikátu podpisu do příslušné databáze vedené veřejnou správou.“* Podle soudu pak právě toto sériové číslo kvalifikovaného certifikátu elektronického podpisu identifikuje podepisující osobu i *„vydavatele použitého elektronického podpisu.“*

## 7.5 Vybrané varianty užití elektronických podpisů při soukromoprávním jednání

Elektronický podpis může být proveden v různých formách. Jejich smysl je ale vždy stejný – vyjádřit vůli podepisujícího k ověření podepisovaných dat,<sup>259</sup> v kontextu našeho tématu vyjádřit vůli právně jednat. Dále uvádíme přehled variant elektronického podpisu používaných v praxi při elektronickém podepisování. Tento přehled si nemůže klást ambice na úplnost. Vychází pouze z nejčastějších způsobů elektronické kontraktace a elektronického podpisu používaných v praxi a rozebíraných v odborné literatuře či rozhodovací praxi.

### 7.5.1 Uvedení jména v elektronickém dokumentu a e-mailu

Definici prostého elektronického podpisu vyhoví i připojení jména a příjmení k textu elektronického dokumentu.<sup>260</sup> V odborné literatuře je dlouhá léta vedena diskuze k naplnění písemné formy podepsáním e-mailu jménem a příjmením.

<sup>258</sup> Usnesení Ústavního soudu ze dne 4. 4. 2023, sp. zn. III.ÚS 752/23.

<sup>259</sup> MASON, S. *Electronic Signatures in Law*. p. 258.

<sup>260</sup> Shodně BERAN, V. Komentář k § 561. In: PETROV, J., VÝTISK, M., BERAN, V. a kol. *Občanský zákoník. Komentář*. 2. vyd. Praha: C. H. Beck, 2019, s. 622. Zde se však navíc objevuje závěr, že elektronický podpis prostý lze použít pouze za situace, kdy bude umožňovat *„identifikace jednající osoby, včetně ověření její totožnosti“*.

K identifikaci jednatelky osoby může postačovat i uvedení jména v e-mailové adrese, a to obzvláště v případě e-mailu na doméně organizace (např. jmeno.prijmeni@nazevuniverzity.cz). V řadě právních řádů je kombinace jména a doménového jména v e-mailové adrese považována za formu elektronického podpisu.<sup>261</sup> V zahraničním textech bývá v souvislosti s tímto typem elektronického podpisu odkazováno na rozhodnutí australského soudu, ve kterém soud v roce 2013 konstatoval, že jedna ze stran sporu napsala své jméno v zápatí emailu, čímž se podle soudu podepsala, přičemž opačný závěr soud prohlásil za smrtící útok na zdravý rozum.<sup>262</sup>

Korbel s Melzerem konstatují, že datová zpráva v širším slova smyslu (tedy i e-mail) se považuje za podepsanou, pokud obsahuje elektronický podpis, a není tedy nutné užít zaručený elektronický podpis. V kontextu tehdy platného zák. o el. podpisu však podle nich pouhé napsání jména na klávesnici v těle e-mailu spíše nebylo elektronickým podpisem, jelikož obsahovalo tvrzení identity, nikoliv její ověření.<sup>263</sup> Domníváme se, že vzhledem k současné absenci požadavku na jednoznačné ověření identity podepsané osoby pro elektronický podpis v nařízení eIDAS by tento závěr dnes měl být odlišný, pokud bude možné určit jednatelky jiným způsobem. Tito autoři však zároveň dodávají, že i pokud by nebyl e-mail podepsán uvedením jména v jeho textu, šlo by o platné právní jednání. Podle okolností mohlo jít o obvyklou náhradu podpisu ve smyslu § 561 odst. 1 obč. zák., nebo o určitelnou osobu i bez podpisu jednatelky podle § 562 odst. 1 obč. zák.<sup>264</sup>

Matejka a Chum již za účinnosti tehdejšího zák. o el. podpisu považovali za elektronický podpis prostý i text připojený k datové zprávě odeslané z obvyklé e-mailové adresy.<sup>265</sup> Podle nich k připojení elektronického podpisu k takové datové zprávě postačoval jakýkoliv řetězec znaků umožňující ověření totožnosti podepsané osoby jako uvedení e-mailové či skutečné adresy, případně jména odesílatele, které adresát zná, aby bylo umožněno ověření totožnosti.<sup>266</sup> Ke shodnému závěru dochází i Polčák s konstatováním,

<sup>261</sup> MASON, 2017, op. cit., s. 256.

<sup>262</sup> *Stuart v Hisbon* [2013] NSWSC 766.

<sup>263</sup> KORBEL, MELZER, 2014, op. cit., s. 34.

<sup>264</sup> *Ibid.*

<sup>265</sup> MATEJKA, CHUM, 2002, op. cit., s. 31.

<sup>266</sup> *Ibid.*

že jakákoli data označující původce dokumentu mají základní účinky podpisu a elektronický dokument je takto podepsán, byť by se jednalo pouze o automaticky doplňovanou patičku v e-mailu.<sup>267</sup> Obdobně Černý dospěl k tomu, že prosté vložení jména na konec e-mailové zprávy naplní obecnou definici elektronického podpisu.<sup>268</sup>

Donát s Tomíškem upozorňují na dřívější spory o tom, zda prosté uvedení jména v e-mailu sloužilo jako elektronický podpis, a to vzhledem k dřívějšímu požadavku na jednoznačné ověření identity podepsané osoby. Nyní však dochází k závěru, že například odstoupení od kupní smlouvy zasláné e-mailem podepsaným jménem a příjmením zákaznice bude možné považovat za písemné odstoupení od smlouvy.<sup>269</sup>

Shodně také Čech konstatuje, že elektronický podpis může představovat i pouhá e-mailová adresa, pokud z ní lze dovodit identitu jednající osoby. Bude se podle něj jednat o písemné právní jednání, pokud se podepisující osoba podepíše pod text e-mailu, na sociálních sítích či v jakékoli jiné komunikační platformě<sup>270</sup>

K odlišnému závěru dochází například Beran, podle něhož uvedení jednající osoby prostým napsáním jména jako elektronický podpis nepostačuje. Napsané jméno podle něj plní pouze nepatrně autentizační funkci, neboť takto lze vytvořit podpis bez jakékoli součinnosti s podepsanou osobou či bez využití výsledků jejího projevu, jako je například sken vlastnoručního podpisu.<sup>271</sup>

Podle našeho názoru uvedení jména a příjmení v závěru e-mailu naplní definici elektronického podpisu prostého a ob stojí jako podpis ve smyslu § 561 odst. 1 obč. zák. Výkladem lze dospět k tomu, že elektronicky podepsané právní jednání má naplnit požadavky § 562 odst. 1 obč. zák. – má-li nepodepsané právní jednání umožňovat určení jednající osoby, tím spíše má určení jednající osoby umožnit jednání elektronicky podepsané. Nelze však dle našeho soudu dovodit, že by zákon vyžadoval i ověření totožnosti,

<sup>267</sup> POLČÁK, 2011, op. cit., s. 56.

<sup>268</sup> ČERNÝ, J. E-commerce. In: MAISNER, M. a kol. *Základy softwarového práva*. Praha: Wolters Kluwer, 2011, s. 213.

<sup>269</sup> DONÁT, TOMÍŠEK, 2016, op. cit., s. 163.

<sup>270</sup> ČECH, 2021, op. cit., s. 16.

<sup>271</sup> BERAN, Komentář k § 561, 2019, op. cit., s. 622.

autentizaci, jednající osoby.<sup>272</sup> Nařízení eIDAS autentizaci definuje jako „*elektronický postup, který umožňuje potvrdit elektronickou identifikaci fyzické či právnické osoby nebo původ a integritu dat v elektronické podobě*“.<sup>273</sup> Požadavek na určení jednající osoby v § 562 odst. 1 obč. zák. je tedy odlišný od požadavku autentizace. Nedomníváme se tak, že by elektronický podpis, aby jím bylo možno podepsat právní jednání, měl přímo autentizovat jednající osobu či jinak ověřovat její totožnost. Autentizaci podepisujícího neposkytuje ani zaručený elektronický podpis. Ten v souladu s čl. 26 písm. b) nařízení eIDAS pouze umožňuje identifikaci podepisující osoby. Podle písmena c) téhož článku má zajistit, že data pro vytvoření podpisu podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou. To však neznamená, že by při vytvoření zaručeného elektronického podpisu musela být podepisující osoba autentizována. Ani při vydání certifikátu pro zaručený elektronický podpis nemusí být totožnost držitele certifikátu ověřena. To neplatí při vydání kvalifikovaného certifikátu pro elektronický podpis, kdy kvalifikovaný poskytovatel služeb vytvářejících důvěru totožnost žadatele ověří a ověřit ji musí.

## 7.5.2 Naskenovaný vlastnoruční podpis

Naskenování či jiný způsob převedení vlastnoručního podpisu do jeho elektronického ztvárnění je běžně používáno například v obchodních vztazích, především na marketingových materiálech.<sup>274</sup> Problém tohoto podpisu je jeho snadné neoprávněné použití bez vědomí údajné podepisující osoby. To vyplývá z procesu jeho získání. Postačí pouze například naskenovat či vyfotit vlastnoruční podpis a přenést jej na podepisovaný elektronický dokument. Přesto jde v jeho případě o prostý elektronický podpis – jde o data v elektronické podobě, která podepisující osoba užívá k podepisování a připojuje je k jiným (podepisovaným) datům. Bez ohledu na bezpečnost by stále měl být takový podpis považován za prostý elektronický podpis.<sup>275</sup> Shodně Čech dochází k závěru, že i připojením naskenovaného podpisu lze v běžných soukromoprávních vztazích uzavírat smlouvy.<sup>276</sup>

<sup>272</sup> Odlišně BERAN, Komentář k § 561, op. cit., s. 622.

<sup>273</sup> Čl. 3 odst. 5 nařízení eIDAS.

<sup>274</sup> MASON, 2017, op. cit., s. 287.

<sup>275</sup> Srov. např. KORBEL, MELZER, 2014, op. cit., s. 35.

<sup>276</sup> ČECH, 2021, op. cit., s. 16.

Je však třeba říci, že současná rozhodovací praxe nižších soudů se může stát – stejně jako k dalším typům elektronického podpisu prostého – k tomuto typu elektronického podpisu spíše negativně. Takto například Obvodní soud pro Prahu 6 v rozhodnutí ze dne 13. 9. 2021, sp. zn. 18 C 198/2021, odmítl uznat za platnou postupní smlouvu, ke které bylo připojeno foto vlastnoručního podpisu. Konstatoval, že podpisy postupidelů 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 postupidel a tento obrázek podpisu mohl být dokonce sejmuto z jiného dokumentu a bez vůle uvedené osoby podepsat postupní smlouvu mohl být vložen do předmětného dokumentu označeného jako postupní smlouva.*“

Je také možné klást otázku, zda lze považovat za elektronicky podepsaný také elektronický dokument, který byl nejprve vytištěn, podepsán vlastnoručním podpisem a následně naskenován. Z našeho pohledu je totiž sporné, zda v takém případě nejde spíše o prostou kopii vlastnoručně podepsaného listinného dokumentu, či zda lze takový dokument mít za elektronicky podepsaný. Těto otázce je vhodné se věnovat i vzhledem k dříve rozebíranému rozhodnutí Nejvyššího soudu ze dne 27. 4. 2022, sp. zn. 21 Cdo 2061/2021, ve kterém došlo k uzavření dohody o narovnání tak, že jedna strana nejprve zaslala druhé takto připravený návrh dohody, kterou druhá strana stejným způsobem akceptovala.

K této situaci lze přistupovat dvěma způsoby. U prvního přístupu nejde vůbec o elektronicky podepsaný dokument, ale pouhou prostou elektronickou kopií listinného a vlastnoručně podepsaného dokumentu. V takovém případě by právní jednání bylo zaznamenáno na listinném a vlastnoručně podepsaném dokumentu, jehož existence byla druhé straně prokázána e-mailem zaslanou elektronickou kopií dokumentu. K připojení elektronického podpisu by nedošlo, jelikož pojmově jsou elektronickým podpisem elektronická data připojena k jiným datům (či s těmito daty jinak logicky spojena),<sup>277</sup> přičemž k tomuto připojení či spojení by tímto výkladovým přístupem nedošlo. E-mail ani dokument by zde nepředstavoval elektronický

<sup>277</sup> Viz čl. 3 odst. 10 nařízení eIDAS: „*elektronickým podpisem* [jsou] *data v elektronické podobě, která jsou připojena ke jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která podepisující osoba používá k podepsání*“.

prostředek, prostřednictvím kterého byla dohoda uzavřena, a e-mail by sloužil pouze jako prostředek pro předání kopie podepsané dohody. Fungoval by podobně, jako kdyby jedna strana zaslala druhé v obálce poštou prostou kopii dohody.

Při druhém výkladovém přístupu by mohl být elektronický dokument připravený tímto způsobem považovaný za elektronicky podepsaný. Nedošlo by zde sice k přímému připojení dat představujících elektronický podpis k jiným –podepisovaným – datům, nicméně elektronický dokument s naskenovaným vlastnoručním podpisem by představoval logické spojení elektronického podpisu s podepisovanými daty.

Podle nás by v obou případech měla být takto uzavřená smlouva považována za platnou. V prvním případě by smlouva byla uzavřena v listinné podobě podepsané vlastnoručním podpisem a zasláný sken dokumentu by představoval pouze prostou kopii tohoto listinného dokumentu. Jedna strana by tak druhé straně naskenovaným dokumentem potvrzovala akceptaci nabídky, resp. uzavření smlouvy připojením vlastnoručního podpisu. V druhém případě by smlouva byla platně uzavřena také, jen by byla považována za elektronicky podepsanou. Volba výkladového přístupu však bude hrát roli v případech soudů, které by nepřístupovaly k elektronickému podpisu prostému příliš otevřeně. Pokud by totiž takový soud nedospěl k závěru o způsobu uzavření smlouvy dle prve uváděného výkladového přístupu, pak by nemusel dokument považovat ani za elektronicky podepsaný, což by přivedlo další výkladová rizika (přestože je pak takový přístup neodůvodnitelný, bohužel se stále v praxi poměrně rigidní názory v tomto smyslu objevují<sup>278</sup>).

Bezpečnost vlastnoručního podpisu přeneseného do elektronické podoby zvyšuje dynamický biometrický podpis, v jehož případě osoba na elektronickém zařízení provede svůj podpis připojovaný k dokumentu.

### 7.5.3 Dynamický biometrický podpis

Při vytváření elektronického podpisu lze užít dotykovou obrazovku či podložku, na které podepisující osoba provede svůj vlastnoruční podpis, přičemž zařízení může kromě vzhledu podpisu zaznamenat například rychlost,

<sup>278</sup> Např. usnesení Nejvyššího soudu ze dne 22. 5. 2019, sp. zn. 26 Cdo 1230/2019-175.

rytmus, sílu, návyk, sled tahů a dynamiku, které jsou pro podepisující osobu jedinečné v době, kdy podpis vytvoří.<sup>279</sup> Takový podpis spolu s těmito doprovodnými údaji je nazýván jako dynamický biometrický podpis. Ten vzniká tak, že při užití digitalizačního snímače jsou zaznamenána data umožňující analyzovat statické a dynamické vlastnosti spojené s typickým chováním podepisující osoby.<sup>280</sup> Původně bylo možné vyhotovovat dynamické biometrické podpisy pouze na speciálních certifikovaných *signpadech* a tabletech. Vývoj v této oblasti však postupně začal umožňovat i využívání vlastních zařízení podepisujících.<sup>281</sup>

Biometrií lze rozumět způsob identifikace osoby pomocí informačních technologií založený na biologických charakteristikách této osoby.<sup>282</sup> Je možné ji také vymezit jako soubor vědních poznatků založených na zkoumání a praktickém využití měřitelných charakteristik živých organismů za účelem jejich jednoznačné identifikace.<sup>283</sup> Dynamický biometrický podpis má po vytvoření dvě složky. První je grafické vyjádření podpisu a druhou jsou doprovodné údaje s informací o způsobu, jakým byl podpis vytvořen, která odpovídá charakteristickým znakům podepisující osoby, jejím návykům a projevům chování.<sup>284</sup> Jako příklad různých návyků při vytvoření podpisu lze uvést to, že někdo doplní diakritiku po vyhotovení celého podpisu, někdo v průběhu podepisování.<sup>285</sup>

Při vytvoření dynamického biometrického podpisu jsou snímány různé údaje související s pohybem a tlakem ruky při vytvoření „vlastnoručního“ podpisu. V případě těchto – ale i jiných – biometrických údajů nebude jejich snímání vždy vykazovat stejné hodnoty. Čím bližší získané hodnoty jsou, tím je větší pravděpodobnost, že tyto hodnoty náleží stejné osobě. Je tak třeba při využívání biometrických údajů správně zvážit, jaké odchylky lze ještě připustit k učinění závěru, že tyto údaje pochází od stejné osoby. Čím přesnější hodnoty budou vyžadovány, tím více bude eliminováno riziko podvodu. To ale na druhou stranu může vést k tomu, že byt' budou údaje pocházet od správné

<sup>279</sup> MASON, 2017, op. cit., s. 292.

<sup>280</sup> SMEJKAL, KODL, UŘIČAŘ, 2019, op. cit., s. 23.

<sup>281</sup> KORBEL, KOVÁŘ, JAROŠ, 2021, op. cit., s. 13.

<sup>282</sup> GRIJPINK, J. Biometrics and Privacy. *Computer Law & Security Report*. 2001, č. 3, s. 154.

<sup>283</sup> SMEJKAL, 2017, op. cit., s. 91.

<sup>284</sup> SMEJKAL, KODL, UŘIČAŘ, 2019, op. cit., s. 24.

<sup>285</sup> MATEJKA, GÜTTLER, 2018, op. cit., s. 39.

osoby, systém je vyhodnotí jako nesprávné.<sup>286</sup> V souvislosti s dynamickým biometrickým podpisem je však uváděno, že biometrická stopa je v jeho případě pro každého jednotlivce unikátní a nelze ji v praxi reprodukovat padělatelem.<sup>287</sup> I tak ale podepisující osoba může později narážet na skutečnost, že její motorika při podepisování se mění s věkem.<sup>288</sup>

I přes svou charakteristiku a odlišnost oproti ostatním typům elektronického podpisu prostého bude dynamický biometrický podpis představovat pouze tuto základní úroveň elektronického podpisu. Nebude jej tedy možné užívat při úkonech vůči veřejnoprávním podepisujícím a jiným osobám při výkonu jejich působnosti. To i přesto, že Smejkal uvádí, že při vytváření dynamického biometrického podpisu lze docílit zajištění integrity dokumentu podobně jako v případě asymetrické kryptografie. Ta nicméně není užitá na straně podepisující osoby, ale může být otázkou technického řešení užitého systému.<sup>289</sup> K biometrickým údajům jsou při tom také připojeny další údaje jako sériové číslo použitého zařízení a časové razítko, což zajistí, že je možné zjistit následné zneužití biometrických údajů.<sup>290</sup> Zneužití biometrických údajů či jejich užití pro zfalšování podpisu v jiných případech však vyloučit nelze a je tak třeba dbát zvýšené ochrany údajů získaných při vytváření těchto podpisů.<sup>291</sup> To souvisí i s tím, že bude-li zneužit běžný certifikát pro vytváření elektronických podpisů, lze certifikát zneplatnit. V případě „odcizení“ biometrických dat a jejich zneužití situace již tak jednoduchá nebude a podepisující osobě zřejmě nezůstane nic jiného než změnit svůj podpisový vzor.<sup>292</sup>

Dynamický biometrický podpis se může zdát vzhledem k metadatům k němu připojovaným jako ideální forma prostého elektronického podpisu. Může však narážet na limity ochrany osobních údajů. Pojem „biometrický údaj“ je definován na úrovni práva Evropské unie jako osobní údaj vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje

<sup>286</sup> GRIJPINK, 2001, op. cit., s. 155 a 156.

<sup>287</sup> SMEJKAL, KODL, UŘIČAŘ, 2019, op. cit., s. 24.

<sup>288</sup> PETERKA, J. Elektronický podpis na rozcestí. Lupa.cz [online]. 6. 6. 2011 [cit. 22. 2. 2022]. Dostupné z: <https://www.lupa.cz/clanky/elektronicky-podpis-na-rozcesti/>

<sup>289</sup> SMEJKAL, 2017, op. cit., s. 94.

<sup>290</sup> Ibid., s. 95.

<sup>291</sup> Srov. MATEJKA, GÜTTLER, 2018, op. cit., s. 45.

<sup>292</sup> Ibid., s. 46.



jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje.<sup>293</sup> Patří tak do zvláštní kategorie osobních údajů, jejichž zpracování je zásadně zakázáno. Možné je jejich zpracování pouze v úzce vymezených případech, přičemž jedním z nich je i výslovný souhlas se zpracováním pro jeden nebo více stanovených účelů.<sup>294</sup>

Objevují se sice názory, že dynamický biometrický podpis je využíván podobně jako klasický podpis a jeho užití tedy není spojeno s dalším automatickým zpracováním těchto údajů. Neměl by tak sloužit k identifikaci, ale pouze ke stvrzení identifikace podepisující osobou.<sup>295</sup> Dne 21. března 2019 však Úřadu pro ochranu osobních údajů (dále „Úřad“) vydal rozhodnutí č. j. UOOU-10138/18-8, ve kterém účastníkovi řízení udělil pokutu 250 000 Kč mimo jiné také za jednání spočívající v tom, že při uzavírání smluv s klienty týkajících se poskytování úvěru v elektronické podobě za účelem uzavření a uchování smluvní dokumentace a zjednodušení tohoto procesu užíval též biometrický podpis klientů. Ten podle Úřadu nebyl nezbytný pro uzavření příslušné smlouvy ani pro její plnění. Tím došlo k porušení zásady minimalizace údajů, podle které musí být zpracovávané osobní údaje přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány.<sup>296</sup>

V řízení bylo prokázáno, že účastník řízení zpracovává při uzavření smlouvy v elektronické formě také dynamické biometrické podpisy klientů, kteří s tímto zpracováním vyslovili svůj souhlas. Podle něj byl biometrický podpis zpracováván za účelem uzavření a uchování smluvní dokumentace a zjednodušení tohoto procesu. Úřad však nedospěl k závěru, že biometrický podpis klienta účastníka řízení byl pro účely uzavření a uchování smluvní dokumentace či zjednodušení tohoto procesu nezbytný. Pro tento účel je podle Úřadu dostatečné zpracovávat pouze prostý obraz podpisu klientu na dematerializované smluvní dokumentaci, který je podle Úřadu srovnatelný s podpisem na smluvní dokumentaci v listinné formě. Úřad v rozhodnutí nadto

<sup>293</sup> Čl. 3 odst. 14 nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále „obecné nařízení“).

<sup>294</sup> Srov. čl. 9 obecného nařízení.

<sup>295</sup> SMEJKAL, 2017, op. cit., s. 109 a 110.

<sup>296</sup> Dle čl. 5 odst. 1 písm. c) obecného nařízení.

konstatoval, že ani souhlas subjektu údajů nezavazuje povinnosti dodržovat všechny zásady zpracování osobních údajů. Soulad sledovaného účelu a k němu se vztahujícího minimálního rozsahu osobních údajů je podle něj nutno hodnotit objektivně, nikoliv subjektivně jako možný předmět dohody uzavřené mezi účastníkem řízení a subjektem údajů.

Lze si klást otázku, zda je možné toto rozhodnutí natolik zobecnit, že by jeho závěry generálně vylučovaly užívání dynamického biometrického podpisu. Pokuta nebyla nicméně uložena jen pro zpracování biometrických podpisů v rozporu se zásadou minimalizace osobních údajů, ale také za uchovávání záznamů telefonických rozhovorů v rozporu se zásadou omezeného uložení osobních údajů.

Z rozhodnutí dále vyplývá, že účastník řízení stanovil jako účel zpracování biometrických údajů uzavření a uchování smluvní dokumentace a zjednodušení tohoto procesu. Je otázka, zda dynamický biometrický podpis skutečně nějak zjednoduší proces uzavření smlouvy a její uchování. Jistě pomůže, pokud účastník smlouvu podepíše digitálně na elektronickém zařízení. K tomu ale není třeba zpracovávat také biometrické údaje. Dynamický biometrický podpis bude mít zásadní přínos pro případné dokazování při sporu vyplývajícím ze smlouvy, ve kterém bude účastník popírat platnost podpisu. V předmětném sporu nicméně na účastníka řízení dopadaly mimo jiné povinnosti identifikace klienta v souladu se zákonem č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu. Od klienta tak byl v souvislosti s uzavíráním smlouvy vyžadován široký rozsah osobních údajů, včetně rodného čísla či údaje o dokladu totožnosti (druh, číslo, datum a místo vydání, platnost). Byla také pořizována a uchovávána kopie občanského průkazu, v některých případech i druhého dokladu totožnosti. I bez biometrických údajů tak účastník řízení klienta dostatečně identifikoval. Ze souhlasu se zpracováním osobních údajů mělo také vyplývat to, že v případě nutnosti odborník v porovnání s jiným podpisem určí, zda podpis učinila táž osoba či nikoliv. To je však opět možné učinit i bez zpracování biometrických údajů.

Matejka s Gütlerem stanovili kritéria, která by měla být před zpracováním biometrických údajů zvážena. Podle nich je třeba zvážit, zda:

- je zpracování biometrických údajů nezbytné pro dosažení stanoveného cíle nebo potřeby,
- jde o nejefektivnější způsob dosažení daného cíle nebo potřeby,
- ztráta soukromí spojená s určitým způsobem zpracování biometrických údajů je přiměřená k zásahu do soukromí ve srovnání s přínosem získaným takovým zpracováním biometrických údajů,
- neexistuje jiný vhodný způsob dosažení stanoveného cíle, který by představoval menší zásah do soukromí dotčených osob.<sup>297</sup>

Domníváme se, že pokud by účastník řízení před zpracováním zvažoval tato kritéria, mohl by dospět k závěru, že biometrické údaje klientů zpracovávat nemusí. Z našeho pohledu skutečně zřejmě zpracovával biometrické údaje získané prostřednictvím dynamického biometrického podpisu nadbytečně, a to vzhledem ke stanovenému účelu zpracování a v kontextu široké palety dalších osobních údajů zpracovávaných o klientech. Pokud by tyto osobní („nebiometrické“) údaje, včetně kopie dokladů totožnosti, účastník řízení nezpracovával a neuchovával, popř. by účel zpracování biometrických údajů určil jiným způsobem, mohl by podle našeho soudu teoreticky Úřad ve vztahu ke zpracování biometrických údajů přistoupit jinak.

Korbel, Kovář a Jaroš uvádí, že Úřad od doby vydání rozebíraného rozhodnutí podobné rozhodnutí nevydal, ani nevydal stanovisko s podobným závěrem.<sup>298</sup> Jediné nám známé rozhodnutí Úřadu s podobným závěrem, je příkaz ze dne 3. 3. 2021, č. j. UOOU-00982/21-5.<sup>299</sup> Podle našeho názoru tedy není vhodné toto rozhodnutí příliš zobecňovat a činit na základě něj závěr o nemožnosti užití dynamického biometrického podpisu v České republice.<sup>300</sup>

Lze konstatovat, že bude možné užít dynamického biometrického podpisu v případech, kdy půjde o zcela nahodilé užití osobních údajů, na které se nebude obecné nařízení vztahovat. Nařízení se totiž vztahuje na zcela nebo částečně automatizované zpracování osobních údajů a na neautomatizované

<sup>297</sup> MATEJKA, GÜTLER, 2018, op. cit., s. 48.

<sup>298</sup> KORBEL, KOVÁŘ, JAROŠ, 2021, op. cit., s. 12.

<sup>299</sup> Příkaz je dostupný na webových stránkách Úřadu z: [https://www.uouu.cz/assets/File.ashx?id\\_org=200144&cid\\_dokumenty=49941](https://www.uouu.cz/assets/File.ashx?id_org=200144&cid_dokumenty=49941)

<sup>300</sup> Shodně ibid., s. 16.

zpracování těch osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny.<sup>301</sup> Neuplatní se například na zpracování osobních údajů prováděné fyzickou osobou v průběhu výlučně osobních či domácích činností.<sup>302</sup> Výhody dynamického biometrického podpisu se však projeví zejména při jeho pravidelném užívání při uzavírání velkého množství smluv. V takovém případě je nicméně nutné zvážit například výše uvedená kritéria Matejky s Güttlerem, důkladně formulovat účel zpracování a dbát všech zásad zpracování osobních údajů. Je přitom zejména třeba vzít v úvahu, zda je zpracování biometrických údajů pro daný účel nezbytné. V případě zpracování uvedeného ve výše zmíněném příkazu Úřadu účastník řízení konstatoval, že účelem zpracování bylo stvrzení platnosti právního jednání učiněného v písemné formě, zjednodušení procesu poskytování služeb a jeho atraktivnění pro klienty a zároveň potvrzení a uchování smluvní dokumentace včetně nepochybného „ověření/verifikace“ klienta.<sup>303</sup> Účastník řízení ale zároveň v řízení potvrdil, že biometrické údaje doprovázející dynamický podpis nikdy u žádného klienta nijak dále nepoužil.<sup>304</sup>

#### 7.5.4 PIN a heslo

Zadání PIN kódu považuje česká literatura za elektronický podpis.<sup>305</sup> Mason jej považuje za pravděpodobně nejstarší formu elektronického podpisu, který je široce používán zejména k přihlášení k účtu v bankomatu nebo při potvrzení transakce s kreditní nebo debetní kartou.<sup>306</sup>

V českém prostředí konstatoval o specifickém PIN kódu například Krajský soud v Českých Budějovicích v rozhodnutí ze dne 27. 3. 2015, sp. zn. 24 Co 696/2015, že představuje elektronický podpis.<sup>307</sup> Za formu elektronického

<sup>301</sup> Čl. 2 odst. 1 obecného nařízení.

<sup>302</sup> Čl. 2 odst. 2 písm. c) obecného nařízení.

<sup>303</sup> Příkaz Úřadu ze dne 3. 3. 2021, č. j. UOOU-00982/21-5, s. 2.

<sup>304</sup> Ibid., s. 5.

<sup>305</sup> KMENT, V. *Elektronické právní jednání: Analýza s důrazem na využití elektronického podpisu podle práva EU, České republiky a Německa*. Praha: Wolters Kluwer, 2018, s. 142, nebo DONÁT, PIFFL, MAISNER, 2017, op. cit., s. 31, SMEJKAL, KODL, URČIČAŘ, 2017, op. cit., s. 219.

<sup>306</sup> MASON, 2017, op. cit., s. 215.

<sup>307</sup> Blíže k tomuto rozhodnutí v kapitole 13 věnované rozhodovací praxi.

podpisu ho prohlašují také například americké soudy.<sup>308</sup> K závěru, že zadání specifického PIN kód nebo jiného autentizačního nástroje představuje písemnost s prostým elektronickým prostředkem, dochází v české literatuře dále také například Korbel s Melzerem.<sup>309</sup> Z rozhodovací praxe – zatím pouze nižších soudů – však vyplývá, že soudy jsou v přijímání tohoto typu podpisu nejednotné, a v současné době se zdá, že jej spíše odmítají uznat za platný podpis. V těchto rozhodnutích soudy vyžadují, aby elektronický podpis poskytl identifikaci jednající osoby a zajistil ochranu proti následné změně obsahu uzavřené smlouvy. Tyto požadavky však z evropské legislativy ani českého právního řádu podle našeho názoru nevyplývají a tato soudní je trvale neudržitelná.<sup>310</sup>

### 7.5.5 Click-wrap a click-through smlouvy

Za jednu z forem elektronického podpisu je považováno i zaškrtnutí políčka a kliknutí na příslušné tlačítko při potvrzení právního jednání. K tomu dochází v případě tzv. „*click-wrap*“, resp. „*click-through*“ smluv, o kterých byla zmínka již výše v podkapitole 5.2. Uživatelé se s nimi mohou běžně setkat zejména při nákupu skrze e-shop či jinou platformu. Ščerba dříve konstatoval, že při uzavření „*click-wrap*“ a „*click-through*“ smlouvy není použit elektronický podpis, ale dochází k nahrazení podpisu jiným mechanickým prostředkem ve smyslu § 561 odst. 1 obč. zák., ve kterém je uvedeno, že „*podpis může být nahrazen mechanickými prostředky tam, kde je to obvyklé*“<sup>311</sup>, resp. ve smyslu § 40 odst. 3 občanského zákoníku z roku 1964, který obsahoval obdobný text. Jeho text však vznikl v době před přijetím nařízení eIDAS a zák. o službách vytvářejících důvěru, tedy před potvrzením možnosti použít pro podepsání i jednoduchý elektronický podpis. O tomto výkladu hovoří i Polčák, když zmiňuje, že pro „klikací smlouvy“ byla zavedena interpretace, podle které se dříve v jejich případě nejednalo o elektronický podpis, protože není splněna podmínka identifikace, ale o mechanický prostředek

<sup>308</sup> Např. United States Court of Appeals, District of Columbia Circuit. *U.S. v. Miller*, 70 F.3d 1353, 1355 (D.C. Cir. 1995): „*What he did do, however, was to enter Rolark's PIN, which acts as a sort of electronic signature authorizing an ATM to release available funds.*“

<sup>309</sup> KORBEL, MELZER, 2014, op. cit., s. 35.

<sup>310</sup> Blíže viz také podkapitolu 13 této monografie.

<sup>311</sup> ŠČERBA, 2012, op. cit., s. 33 a násled.

standardně nahrazující elektronický podpis.<sup>312</sup> Podobně se lze setkat se závěrem, že „za konkludentní jednání je možno považovat i v internetovém obchodu kliknutí na příslušné políčko, vyjadřující souhlas s nabídkou (click wrap contract)“.<sup>313</sup> Obdobně Donát s Tomíškem považují stisknutí tlačítka při uzavření „click-wrap“; resp. „click-through“ smlouvy za projev vůle, se kterým je spojen právní následek, jelikož ve fyzickém i elektronickém světě jsou právní jednání, která nevyžadují podpis.<sup>314</sup>

S ohledem na vývoj právního rámce je ovšem dle našeho názoru na místě konstatovat, že forma i metoda projevení souhlasu s obsahem smluvního ujednání „click-wrap“, resp. „click-through“ představuje prostý elektronický podpis.

### 7.5.6 Elektronický podpis v datových schránkách

Užívání datové schránky k právnímu jednání v rámci veřejného práva přináší zásadní výhodu – úkon učiněný osobou oprávněnou k přístupu do datové schránky nebo pověřenou osobou prostřednictvím datové schránky má dle zák. o el. úkonech stejné účinky jako úkon učiněný písemně a podepsaný.<sup>315</sup> Při absenci požadavku na podpis právního jednání se elektronický právní styk zásadně zrychluje a zjednodušuje. Tato fikce podpisu se však uplatní pouze při právním jednání vůči orgánu veřejné moci.

Pokud tedy bude právně jednáno datovou schránkou v oblasti soukromého práva, pak se fikce podpisu dle § 18 odst. 2 zák. o el. úkonech neuplatní. To nicméně nemusí být překážka pro soukromoprávní jednání datovou schránkou. Ve vztahu k dříve platnému zák. o el. Podpisu Korbel a Melzer konstatovali, že použití datové schránky naplňuje definici prostého elektronického podpisu a požadavek podpisu pro soukromoprávní jednání dle § 561 odst. 1 obč. zák. kvůli jednoznačnému ověření identity osoby přihlášené do datové schránky ve vztahu k odeslané datové zprávě.<sup>316</sup>

<sup>312</sup> POLČÁK, R., Nové směry v elektronické dokumentaci právního jednání. *Právní prostor* [online]. [cit. 13.10.2019]. Dostupné z: <https://www.pravniprostor.cz/clanky/obcanske-pravo/nove-smery-v-elektronicke-dokumentaci-pravniho-jednani>

<sup>313</sup> RABAN, 2019, op. cit., s. 41.

<sup>314</sup> DONÁT, TOMÍSEK, 2016, op. cit., s. 141.

<sup>315</sup> § 18 odst. 2 zák. o el. úkonech.

<sup>316</sup> KORBEL, F., MELZER, F. Písemnost, elektronický a biometrický podpis v elektronickém právním jednání. *Bulletin advokacie*. 2014, č. 12, s. 36.

S ohledem na dříve uvedené závěry k elektronickému podpisu prostému by podle nás mělo být právní jednání učiněné datovou schránkou považováno za podepsané i v případě, že nebude opatřeno některou z vyšších úrovní elektronického podpisu.

Předchozí závěr bude nicméně nutné modifikovat v případě, že prostřednictvím datové schránky bude jednat právnická osoba s kolektivním statutárním orgánem a zakladatelské právní jednání bude vyžadovat jednání více osob.<sup>317</sup> V takovém případě bude nutné právní jednání opatřit alespoň prostým elektronickým podpisem všech osob, jejichž podpis je v případě konkrétní obchodní korporace požadován. I v případě fikce podpisu pro veřejnoprávní jednání obchodní korporace (resp. i dalších právnických osob) totiž zák. o el. úkonech zavádí výjimku. Stanovuje totiž, že se fikce podpisu neuplatní, pokud „jiný právní předpis nebo vnitřní předpis požaduje společný úkon více z uvedených osob.“<sup>318</sup>

Specifická situace nastává při doručování právního jednání prostřednictvím „cizí“ datové schránky.<sup>319</sup> K elektronickému podpisu při jednání prostřednictvím datové schránky odlišné osoby než skutečně jednající osoby, je na místě zmínit rozhodnutí Nejvyššího soudu ze dne 27. 10. 2020, sp. zn. 27 Cdo 143/2020. V něm se soud zabýval otázkou, zda lze přiznat právní účinky podání k rejstříkovému soudu od společenství vlastníků jednotek, které bylo zasláno z datové schránky předsedy výboru společenství vlastníků jednotek a nebylo ani opatřeno uznávaným elektronickým podpisem předsedy. V této věci nejprve soud prvního stupně a poté i odvolací soud vycházely z toho, že úkon učiněný jinou osobou prostřednictvím „cizí“ datové schránky nemá právní účinky, které zákon jinak dokumentu doručenému prostřednictvím datové schránky přiznává. V kontextu předmětné věci tedy z toho, že opravený návrh podaný prostřednictvím informačního systému datových schránek z datové schránky předsedy výboru není podepsaný způsobem, se kterým jiný právní předpis spojuje účinky vlastnoručního podpisu. Toto právní posouzení však Nejvyšší soudu nepovažoval za správné.<sup>320</sup> Konstatoval,

<sup>317</sup> Srov. § 164 odst. 2 obč. zák.

<sup>318</sup> § 18 odst. 2 zák. o el. úkonech.

<sup>319</sup> Přípustnost tohoto postupu lze dovodit například z bodů 38 a 40 stanoviska Nejvyššího soudu ze dne 1. 5. 2017, sp. zn. Pls 1/2015.

<sup>320</sup> Bod 38 rozhodnutí Nejvyššího soudu ze dne 27. 10. 2020, sp. zn. 27 Cdo 143/2020.

že fyzická osoba oprávněná jednat jménem právnické osoby, může jménem právnické osoby učinit elektronické podání i ze své datové schránky. V takovém případě je podle soudu podání podepsáno touto fyzickou osobou a je-li přitom z podání zřejmé, že je činí jménem právnické osoby, například jako předseda jejího statutárního orgánu, jde o podání této právnické osoby učiněné a podepsané fyzickou osobou oprávněnou jednat za dotčenou právnickou osobu.<sup>321</sup>

Lze tedy uzavřít, že datové schránky lze užívat nejen v rámci veřejnoprávní komunikace s orgány veřejné moci, ale také v rámci soukromoprávního styku. V jeho případě se sice neuplatní veřejnoprávní fikce podpisu ve smyslu zák. o el. úkonech, nicméně vzhledem k jednoznačné identifikaci osoby, pro kterou byla datová schránka zřízena, lze datovou zprávu považovat za elektronicky podepsanou i bez jejího opatření některou z vyšších úrovní elektronického podpisu. To nicméně nebude bez dalšího platit v případě užití datové schránky pro doručování právního jednání odlišné osoby od té, pro kterou byla datová schránka zřízena. V takovém případě bude třeba zvažovat, za dokument obsahující právní jednání obsahuje alespoň elektronický podpis prostý.

## 7.6 Právní rámec pro vzdálené podepisování

Původně se předpokládalo, že kvalifikovaný prostředek pro vytváření kvalifikovaných elektronických podpisů bude přímo v dispozici podepisující osoby v podobě například tokenu nebo čipové karty a její čtečky. Je však také možné v souladu s nařízením eIDAS vytvářet elektronický podpis na dálku, kdy bude prostředek k vytváření kvalifikovaného podpisu v dispozici kvalifikovaného poskytovatele služeb vytvářejících důvěru.<sup>322</sup> Smysl může spočívat jak v úspoře nákladů na pořízení kvalifikovaného prostředku pro vytváření podpisů, tak ve větší uživatelské přívětivosti užívání kvalifikovaných elektronických podpisů.

Využívání vzdáleného elektronického podepisování předpokládá nařízení eIDAS již ve svých bodech odůvodnění. Konstatují totiž, že „[p]odepisující

<sup>321</sup> Bod 37 rozhodnutí Nejvyššího soudu ze dne 27. 10. 2020, sp. zn. 27 Cdo 143/2020.

<sup>322</sup> KMENT, V. *Elektronické právní jednání: analýza s důrazem na využití elektronického podpisu a elektronické pečeti podle práva EU, České republiky a Německa*, s. 149.



*osoba by měla mít možnost svěřit kvalifikované prostředky pro vytváření elektronických podpisů do péče třetí straně, pokud jsou zavedeny odpovídající mechanismy a postupy, které zajišťují, že podepisující osoba má výhradní kontrolu nad používáním svých dat pro vytváření elektronických podpisů, a použitím tohoto prostředku jsou splněny požadavky na kvalifikovaný elektronický podpis.*<sup>323</sup> Další také uvádí, že vytváření elektronického podpisu na dálku přináší mnohé ekonomické výhody a předpokládá jeho stále častější užití.<sup>324</sup>

Přímo příloha II nařízení eIDAS, která obsahuje požadavky na kvalifikované prostředky pro vytváření elektronických podpisů, obsahuje přímo dovolení, podle kterého data pro vytváření elektronických podpisů může jménem podepisující osoby vytvářet nebo spravovat pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru.<sup>325</sup>

Revizi nařízení eIDAS na rozdíl od původního textu nařízení eIDAS blíže pamatuje na vzdálené podepisování a zavádí novou službu vytvářející důvěru – správu prostředků pro vytváření elektronických podpisů na dálku nebo prostředků pro vytváření elektronických pečeti na dálku. Kvalifikovaným prostředkem pro vytváření elektronických podpisů na dálku revize rozumí „*kvalifikovaný prostředek pro vytváření elektronických podpisů, který jménem podepisující osoby v souladu s článkem 29a spravuje kvalifikovaný poskytovatel služeb vytvářejících důvěru.*“<sup>326</sup>

Smyslem vzdáleného podepisování dle nařízení eIDAS je to, aby podepisující osoba u sebe nemusela mít žádný kvalifikovaný prostředek (například čipovou kartu). Certifikát pro podpis bude uložený na kvalifikovaném prostředkem ve správě kvalifikovaného poskytovatele služeb vytvářejících důvěru a k podpisu bude využito webového rozhraní nebo aplikace poskytovatele.

<sup>323</sup> Bod odůvodnění 51 nařízení eIDAS.

<sup>324</sup> Bod odůvodnění 52 nařízení eIDAS.

<sup>325</sup> Odstavec 3 přílohy II nařízení eIDAS.

<sup>326</sup> EVROPSKÝ PARLAMENT. Legislativní usnesení Evropského parlamentu ze dne 29. února 2024 o návrhu nařízení Evropského parlamentu a Rady, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu (COM(2021)0281 – C9-0200/2021 – 2021/0136(COD)) [online]. 2024 [cit. 15. 3. 2024]. Dostupné z [https://www.europarl.europa.eu/doceo/document/TA-9-2024-0117\\_CS.pdf](https://www.europarl.europa.eu/doceo/document/TA-9-2024-0117_CS.pdf)

S ohledem na zachování právní jistoty vítáme, že revize nařízení eIDAS míří blíže i na tuto oblast a na stanovení souvisejících technických a provozních specifikací a referenčních norem.

Co se týče soukromých poskytovatelů služeb vytvářejících důvěru, kteří zprostředkovávají podepisování zaručeným nebo prostým elektronickým podpisem, nic jim nebrání poskytovat tyto služby i dálkově a mnohdy tak i činí.



## 8 ELEKTRONICKÉ NÁSTROJE VYUŽÍVANÉ PRO UZAVÍRÁNÍ SMLUV ONLINE

V předchozí kapitole bylo pojednáno o elektronickém podpisu jako ústředním nástroji, který umožňuje zvýšit důvěryhodnost elektronického právního jednání. Jak ovšem vyplývá z diskutovaných variant, kterých může elektronický podpis nabývat, tento nástroj je při dnešním jednání v online prostředí často téměř nezatelně zakomponován do uživatelského prostředí tak, že návštěvník e-shopu při odeslání objednávky nemusí užití tohoto nástroje zaznamenat. Zvyšování uživatelské přívětivosti za současného uplatňování nástrojů, které vytváření důvěry v právní jednání online je přitom všeobecně vítáno a směřuje k němu jak vývoj právního rámce, tak nabídka služeb a řešení, které zajišťují či zprostředkovávají elektronickou kontraktaci a transakce v online prostředí obecně. V této kapitole se proto budeme podrobněji věnovat kontraktačním platformám a dalším nástrojům pro uzavírání smluv online, především pak možnému uplatnění bankovní identity a očekáváním spojeným s připravovanou evropskou peněženkou digitální identity či službami na bázi protokolu *blockchain*.

### 8.1 Kontraktační platformy a jiné nástroje pro uzavírání smluv online

Pojem kontraktačních platform je možno chápat různě. Může jít o aplikace zprostředkovávající přístup k širokému spektru zboží či služeb, a to formou jejich koupě, sdílení, pronájmu apod. Typickým příkladem jsou online tržiště, platformy zprostředkující krátkodobé ubytování, služby sdílené dopravy či platformy pro komunitní financování. Kontraktační platformy odlišuje od jiných zprostředkovatelských platform to, že jejich účelem je celkové zprostředkování směny předmětných statků v online prostředí, nikoli pouze poskytnutí dat potřebných pro realizaci transakcí tohoto typu.<sup>327</sup>

Pro účely této monografie nicméně za vhodnější vymezení kontraktační platformy považujeme, že se jedná o takovou platformu, která zprostředkovává uživatelsky přívětivé prostředí podporující strany při provedení a dokončení elektronické transakce. S výše uvedeným vymezením se toto do značné míry

<sup>327</sup> Obdobně pojem kontraktační platformy vnímá Polčák (srov. POLČÁK, R. Odpovědnost ISP. In: POLČÁK a kol., 2018, op. cit., s. 98 a násl.).

překrývá, podstatné nicméně je, že pro naše pojetí není rozhodující, zda se jedná pouze o dílčí funkcionalitu či o jádro obchodního modelu daného poskytovatele. Je pro nás tedy bez významu, zda jde o uživatelská rozhraní e-shopu, kde je zákazníkovi umožněno zakoupit na základě formulářového uzavření smlouvy zboží vybrané z online katalogu v předchozím kroku, anebo o specializované kontraktační platformy, které nabízejí kontraktační služby a online prostředí pro uzavření smlouvy jako primární produkt (příkladem uveďme poskytovatele DocuSign<sup>328</sup> či DigiSign<sup>329</sup>).

Pro tyto platformy je důležitý § 562 odst. 2 obč. zák. týkající se důkazní spolehlivosti záznamů. Jde o zásadní ustanovení, které naplnění jeho podmínek přináší důkazní spolehlivost při prokazování aspektů souvisejících s kontraktačním procesem.<sup>330</sup> Druhým podstatným přínosem kontraktační platformy může být možnost (spolehlivé) identifikace podepisujícího. V tomto směru je silným benefitem těchto nástrojů, že umožňují stranám smlouvy překonávat nejistoty spojené s transakcemi napříč jurisdikcemi. Například DocuSign tak poskytuje všechny úrovně elektronického podpisu upravené nařízením eIDAS.<sup>331</sup> Ještě výraznější je pak přínos při uzavírání smlouvy se stranami mimo EU, na které úprava nařízení eIDAS přímo nedopadá. Platforma nabízí nástroje, které jsou přizpůsobené požadavkům a úpravě jurisdikcí mimo EU (především USA) a zvyšuje tak právní jistotu při elektronické kontraktaci napříč kyberprostorem.

Je přitom vhodné zdůraznit, že i na elektronickou kontraktaci se stále uplatní základní soukromoprávní principy, především zásady bezformálnosti právního jednání a autonomie vůle. Není tak zdaleka nutné, aby k platnému uzavření smlouvy online, byť s mezinárodním prvkem, docházelo za využití kontraktační platformy, ať v pojetí online tržiště nebo specializované služby jako je DocuSign. V online prostředí naopak může docházet a dochází k uzavírání smluv velmi různorodými, mnohdy na první pohled ne zcela snadno odhalitelnými, způsoby.

<sup>328</sup> DocuSign. *DocuSign* [online]. 2023 [cit. 23.10.2023]. Dostupné z: <https://www.docusign.com/>

<sup>329</sup> Ibid.

<sup>330</sup> Ustanovení je více rozebíráno dále v kapitole 11.3.

<sup>331</sup> DocuSign Standards-Based Signatures for the European Union. *DocuSign* [online]. 2019 [cit. 20.8.2023]. Dostupné z: [https://www.docusign.com/sites/default/files/DocuSign\\_Standards\\_Based\\_Signatures.pdf](https://www.docusign.com/sites/default/files/DocuSign_Standards_Based_Signatures.pdf)

Škála služeb a nástrojů dostupných přes internet, prostřednictvím kterých k uzavření smlouvy může dojít, je tak překvapivě široká, byť se v řadě případů (už) nemusí jednat o příliš frekventované prostředky. Například sociální síť Facebook sice primárně k obchodování nabízí přihlášeným uživatelům specifickou službu s označením Marketplace<sup>332</sup>, nic ovšem těmto uživatelům nebrání v tom, aby spolu uzavřeli např. smlouvu o prodeji použitého nábytku za využití synchronního komunikačního nástroje, který je do této sociální sítě integrován a nese označení Messenger<sup>333</sup>. Stejně tak může dojít k veřejné nabídce prodeje tohoto použitého nábytku tím, že prodávající jako přihlášený uživatel bude sdílet odpovídající výzvu prostřednictvím veřejné zprávy, která se ostatním uživatelům této sociální sítě zobrazí skrze funkci News Feed<sup>334</sup> a k uzavření smlouvy dojde zprávou protistrany vyjadřující akceptaci veřejně směřovanou reakcí na tento příspěvek.

K uzavření smlouvy online tak může dojít v zásadě skrze jakýkoli nástroj pro online komunikaci, ať se jedná o e-mailového klienta, mobilní aplikaci pro zaslání zpráv přes internet (např. WhatsApp), kontraktační platformu či komentářovou sekci pod článkem na zpravodajském serveru.

Konkrétní případ s sebou může nést specifické výkladové výzvy, na které se snažíme alespoň částečně upozornit a reagovat napříč touto monografií.

## 8.2 Užítí bankovní identity při uzavírání smluv online

Primární překážka, která stojí proti širšímu uplatnění nástrojů vyšší úrovně důvěryhodnosti pro ověření identity smluvní strany při uzavírání smluv online, je mnohdy jejich relativní uživatelská nepřívětivost a potřeba značné iniciativy jednotlivce. I proto je využití zaručených či kvalifikovaných elektronických podpisů ze strany fyzických osob při soukromoprávním jednání stále notně marginální záležitostí.

<sup>332</sup> META. Marketplace. *Facebook* [online]. 2023 [cit. 23. 10. 2023]. Dostupné z: [https://www.facebook.com/marketplace/learn-more/?locale=cs\\_CZ](https://www.facebook.com/marketplace/learn-more/?locale=cs_CZ)

<sup>333</sup> META. Messenger. *Facebook* [online]. 2023 [cit. 23. 10. 2023]. Dostupné z: [https://www.messenger.com/?locale=cs\\_CZ](https://www.messenger.com/?locale=cs_CZ)

<sup>334</sup> ČTK. Proč vidím tento příspěvek? Facebook vysvětlí, jak řadí položky v kanálu news feed. *Aktuálně.cz* [online]. 1. 4. 2019 [cit. 25. 10. 2023]. Dostupné z: <https://zpravy.aktualne.cz/ekonomika/proc-vidim-tento-prispevek-facebook-vysvetli-jak-radi-polozk/r~634f6b3254b611e998d70cc47ab5f122/>

Relativně nedávno však přibyla nová alternativa, která směřuje k překlenutí této hlavní rezistence skrze využití etablovaného rámce ověřených identit velké části společnosti, kterými pro poskytování bankovních služeb disponují banky. Tento koncept stojí na tom, že banky mohou formou specifické identifikační služby posílit právní jistotu při elektronickém právním jednání tím, že potvrdí identitu jednatelů jiné osobě, jelikož při založení bankovního účtu ověří identitu této osoby.<sup>335</sup> S účinností od června 2021 lze tak jako nástroj při uzavření soukromoprávní smlouvy online v rostoucí míře využít také tzv. bankovní identity (Bank iD).<sup>336</sup>

Ta byla zavedena novelizačním zákonem 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, přičemž záběr této úpravy je notně širší a možnost využití bankovní identity pro zvýšení právní jistoty stran při soukromoprávním jednání online je spíše doprovodnou funkcí, byť se značným potenciálem praktické využitelnosti.

Zjednodušeně lze bankovní identitu popsat jako relativně nově dostupný nástroj elektronické identifikace umožňující online přístup do systému veřejné správy nebo ke službám soukromého sektoru včetně soukromoprávního poskytování identifikačních služeb.<sup>337</sup> Nejedná se však o nový nástroj, protože v podstatě představuje pouze rozšíření oprávnění bank při využívání existující ověřené identity klienta (kterou u některé banky disponuje většina populace). Zákon č. 49/2020 Sb. přinesl do zákona č. 21/1992 Sb., o bankách nový povolený předmět činnosti spočívající v poskytování elektronické identifikace, autentizace a služeb vytvářejících důvěru.<sup>338</sup> Poskytovatelem identifikačních služeb se v tomto zákoně nově rozumí osoba, která není bankou, je na základě jiného právního předpisu oprávněna poskytovat identifikační služby a ve které mají podíl pouze banky nebo pobočky zahraničních bank.<sup>339</sup>

<sup>335</sup> DONÁT, TOMÍŠEK, 2016, op. cit., s. 141.

<sup>336</sup> O Bank iD. *Bank iD* [online]. 2023 [cit. 23. 10. 2023]. Dostupné z: <https://www.bankid.cz/o-nas>

<sup>337</sup> LOUTOCKÝ, P., KASL, F. Potenciál a identifikačních služeb bankovní identity. *Právník*. 2021, č. 12, s. 1042.

<sup>338</sup> Srov. § 1 odst. 4 zákona č. 21/1992 Sb., o bankách.

<sup>339</sup> § 38aa odst. 2 zákona č. 21/1992 Sb., o bankách.

Tou je v současné chvíli společnost Bankovní identita, a. s., jejímiž akcionáři je deset největších bank působících na českém trhu.<sup>340</sup>

Za touto službou vnímáme ambici přinést do elektronické kontraktace vyšší míru důvěryhodnosti o identitě jednající osoby. Hlavní využití shledáváme především ze strany poskytovatelů služeb k tomu, aby pro ně snížila rizika plynoucí z možného nepřikázaného jednání či vadného plnění v důsledku mylného ztotožnění jednající osoby, ať již v podobě ztížené vymahatelnosti vzniklé pohledávky či potenciálním škodním nárokem poškozené osoby.<sup>341</sup>

Dalším přínosem bankovní identity pro elektronickou kontraktaci je skutečnost, že ji lze využít v rámci vzdáleného prokazování totožnosti účastníka notářem. Z novely notářského řádu provedené zákonem č. 300/2021 Sb.<sup>342</sup> vyplývá, že ke vzdálenému prokázání totožnosti může dojít podle nově vloženého § 64a odst. 1 notářského řádu spojením videokonference se současným využitím prostředků pro elektronickou identifikaci. Jako prostředek pro elektronickou identifikaci lze přitom užít i bankovní identitu.<sup>343</sup> Vzdáleného ověření totožnosti pomocí bankovní identity tak bude možné provést i při legalizaci elektronického podpisu.<sup>344</sup>

Nejnovější, a potenciálně velmi zajímavou službu spojenou s bankovní identitou je služba Bank iD SIGN, prostřednictvím které je možné podepisovat dokumenty zaručeným elektronickým podpisem.<sup>345</sup>

Jak ve svém příspěvku podrobně přibližuje Peterka, je nutné službu Bank iD SIGN od vlastní Bank iD odlišovat co do účelu, funkcionalit i dostupnosti.<sup>346</sup>

<sup>340</sup> Otázky, na které se často ptáte. *BankID.cz* [online]. [cit. 10. 12. 2021]. Dostupné z: <https://www.bankid.cz/faq>

<sup>341</sup> Blíže viz LOUTOCKÝ, KASL, 2021, op. cit., s. 1047.

<sup>342</sup> Zákon č. 300/2021 Sb., kterým se mění zákon č. 358/1992 Sb., o notářích a jejich činnosti (notářský řád), ve znění pozdějších předpisů, a zákon č. 634/2004 Sb., o správních poplatcích, ve znění pozdějších předpisů.

<sup>343</sup> § 64a odst. 2 písm. b) notářského řádu.

<sup>344</sup> § 74a odst. 1 notářského řádu.

<sup>345</sup> Pro firmy. *BankID.cz* [online]. [cit. 10. 12. 2021]. Dostupné z: <https://www.bankid.cz/pro-firmy>

<sup>346</sup> PETERKA, J. Není BankID jako BankID Sign aneb Jak se elektronicky podepisuje s bankovní identitou? *Lupa.cz* [online]. 20. 6. 2022 [cit. 25. 10. 2023]. Dostupné z: <https://www.lupa.cz/clanky/neni-bankid-jako-bankid-sign-aneb-jak-se-elektronicky-podepisuje-s-bankovni-identitou/>



V současné době je služba v počáteční fázi nasazení a rozsah,<sup>347</sup> ve kterém najde uplatnění je proto do značné míry nejistý.

Pokud by měla být do budoucna bankovní identita širěji používána pro elektronické podepisování a uzavírání smluv, prospělo by jí, pokud by bylo jejím prostřednictvím možno podepisovat kvalifikovaným elektronickým podpisem. To by mimo jiné vedlo i k přeshraničnímu uznávání elektronického podpisu. Kvalifikovaný elektronický podpis založený na kvalifikovaném certifikátu vydaný v jednom členském státě se totiž uznává jako kvalifikovaný elektronický podpis ve všech ostatních členských státech.<sup>348</sup>

### 8.3 Evropská peněženka digitální identity a elektronické podepisování

V kontrastu k myšlenkám o možném širším uplatnění národního nástroje bankovní identity s kvalifikovaným elektronickým podpisem v rámci Jednotného trhu stojí unijní iniciativa rozvoje elektronických nástrojů pro zjištění vysoké míry důvěryhodnosti, především pak připravované zavedení nástroje evropské peněženky digitální identity skrze revizi a rozšíření nařízení eIDAS.

Evropská komise ve zprávě o hodnocení nařízení eIDAS z června 2021<sup>349</sup> připomíná, že služby vytvářející důvěru, jako např. elektronické podpisy, slouží ke zvýšení bezpečnosti, praktičnosti a efektivity online transakcí.<sup>350</sup> Komise upozorňuje také na to, že zprostředkovatelé internetových služeb, jako jsou například velké platformy sociálních médií a internetových prohlížečů, působí v roli „strážců identity“ nabízejících službu BYOI („bring your own identity“). Jejím prostřednictvím uživatelům umožňují autentizaci na internetových

<sup>347</sup> Česká spořitelna jako první banka umožňuje digitální podpis firmám přes bankovní identitu. *Česká spořitelna* [online]. 6. 6. 2023 [cit. 25. 10. 2023]. Dostupné z: <https://www.csas.cz/cs/o-nas/pro-media/tiskove-zpravy/2023/06/06-1/ceska-sporitelna-jako-prvni-banka-umoznuje-digitalni-podpis-firmam-pres-bankovni-identitu>

<sup>348</sup> Dle čl. 25 odst. 3 nařízení eIDAS se kvalifikovaný elektronický podpis založený na kvalifikovaném certifikátu vydaném v jednom členském státě uznává jako kvalifikovaný elektronický podpis ve všech ostatních členských státech Evropské unie.

<sup>349</sup> 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). *Evropská komise* [online]. 2021 [cit. 1. 2. 2022]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52021DC0290>

<sup>350</sup> *Ibid.*, s. 3.

stránkách a u služeb třetích stran pomocí jednoho uživatelského profilu zřízeného u těchto zprostředkovatelů. To však může vést ke ztrátě kontroly nad zpřístupněnými osobními údaji. Tyto prostředky elektronické identifikace však nejsou spojeny s ověřenou fyzickou totožností a objevuje se zde riziko hrozeb podvodů a kybernetických bezpečnostních hrozeb.<sup>351</sup> Komise v hodnotící zprávě dochází k závěru, že stávající podoba nařízení eIDAS nemůže splnit nové požadavky trhu v oblasti elektronické identity. Naopak by mělo dojít k jeho úpravě, aby mohlo být naplněno očekávání uživatelů, uspokojena poptávka na trhu a aby byl sledován nejnovější vývoj v oblasti digitalizace.<sup>352</sup>

Přímo v návrhu revize nařízení eIDAS Komise konstatovala, že „[p]řevážná většina potřeb v oblasti elektronické identity a dálkové autentizace zůstává v soukromém sektoru, zejména v oblastech, jako jsou bankovníctví, telekomunikace a provozovatelé platform, od nichž zákon vyžaduje, aby ověřovali totožnost svých zákazníků.“ Přidaná hodnota nařízení eIDAS v oblasti elektronické identity je podle návrhu omezena vzhledem k jeho nízkému pokrytí, přijímání a používání.<sup>353</sup>

Revize v této souvislosti zavádí evropské peněženky digitální identity, které by měly sloužit k přeshraniční elektronické identifikaci a autentizaci pro přístup k veřejným, ale i soukromým službám. Ty by také měly umožnit vytvářet a používat kvalifikované elektronické podpisy a pečete přijímané v celé Evropské unii.<sup>354</sup>

Návrh Evropské komise evropskou peněženku digitální identity vymezoval jako produkt a službu, které uživatelé umožňují uchovávat údaje o totožnosti, pověření a atributy spojené s jeho totožností, poskytovat je na požádání spoléhajícím se stranám a používat je pro autentizaci, online i offline, pro službu v souladu s článkem 6a<sup>355</sup> a k vytváření kvalifikovaných elektronických podpisů a pečeti.<sup>356</sup>

<sup>351</sup> Návrh nařízení Evropského Parlamentu a Rady, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu, op. cit., s. 2.

<sup>352</sup> 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), op. cit., s. 7.

<sup>353</sup> Návrh nařízení Evropského Parlamentu a Rady, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu, op. cit., s. 5.

<sup>354</sup> Ibid., s. 13.

<sup>355</sup> Jde o nově vkládaný článek věnovaný podrobné úpravě evropské peněženky digitální identity.

<sup>356</sup> Návrh nařízení Evropského Parlamentu a Rady, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu, op. cit., s. 24, čl. 1 odst. 3 písm. i).

Mírně odlišně ji definovala Rada ve svém obecném přístupu. Součástí definice už není to, že by mělo jít o produkt a službu, ale o prostředek pro elektronickou identifikaci, který uživateli umožňuje nejen uchovávat ale i vyhledávat údaje o totožnosti, včetně osobních identifikačních údajů, elektronických potvrzení atributů spojených s jeho totožností, poskytovat je na požádání spoléhajícím se stranám a používat je pro autentizaci, online a případně offline, pro službu v souladu s článkem 6a také a umožňuje podepisovat kvalifikovanými elektronickými podpisy a pečeti kvalifikovanými elektronickými pečeti.<sup>357</sup>

V textu revize schválené Evropským parlamentem se evropskou peněženkou digitální identity rozumí prostředek pro elektronickou identifikaci, který uživateli umožňuje bezpečně ukládat, spravovat a ověřovat osobní identifikační údaje a elektronická potvrzení atributů za účelem jejich poskytnutí spoléhajícím se stranám a dalším uživatelům evropských peněženek digitální identity a podepisovat prostřednictvím kvalifikovaných elektronických podpisů nebo pečeti prostřednictvím kvalifikovaných elektronických pečeti.<sup>358</sup>

Těžiště záměru je prostřednictvím evropských peněženek digitální identity zjednodušit uživatelům přístup k prostředkům elektronické identifikace k přístupu k veřejným službám. Zároveň mají sloužit jako alternativa soukromým identifikačním službám, které poskytuje například Google<sup>359</sup> nebo Facebook<sup>360</sup>, a bude možné je používat i při elektronické identifikaci mimo

<sup>357</sup> Nově vkládaný bod 42 nařízení eIDAS dle obecného přístupu Rady. Zdá se však, že penženka může být nakonec definována ještě jinak. V předběžné politické dohodě je vymezena takto: „*‘European Digital Identity Wallet’ means an electronic identification means, which allows the user to securely store, manage and validate identity data and electronic attestations of attributes, to provide them to relying parties and to other users of European Digital Identity Wallets, and to sign by means of qualified electronic signatures or to seal by means of qualified electronic seals.*“ (ITRE. European Digital Identity – Provisional Agreement. *Evropský parlament* [online]. 2023 [cit. 20. 12. 2023]. Dostupné z: <https://www.europarl.europa.eu/committees/cs/european-digital-identity-provisional-ag/product-details/20231116CAN72103>).

<sup>358</sup> Legislativní usnesení Evropského parlamentu ze dne 29. února 2024 o návrhu nařízení Evropského parlamentu a Rady, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu (COM(2021)0281 – C9-0200/2021 – 2021/0136(COD)). *Evropský parlament* [online]. 2024 [cit. 15. 3. 2024]. Dostupné z: [https://www.europarl.europa.eu/doceo/document/TA-9-2024-0117\\_CS.pdf](https://www.europarl.europa.eu/doceo/document/TA-9-2024-0117_CS.pdf)

<sup>359</sup> Google Identity. *Google for developers* [online]. 2023 [cit. 25. 10. 2023]. Dostupné z: <https://developers.google.com/identity>

<sup>360</sup> Facebook Identity Provider | Login with Facebook. *Fusion.Auth Docs* [online]. 2023 [cit. 25. 10. 2023]. Dostupné z: <https://fusionauth.io/docs/v1/tech/identity-providers/facebook>

veřejný sektor při běžném využívání soukromých služeb vyžadujících identifikaci. Revize nařízení eIDAS tím poskytuje uživatelům větší kontrolu nad sdílenými osobními a jinými údaji při přihlašování k různým online službám. Stojí totiž na principu tzv. *self sovereign identity*, podle kterého uživatel apriori nesdílí veškeré své údaje s poskytovatelem služeb digitální identity ani se službou, ke které se přihlašuje, ale jen údaje vybrané uživatelem, resp. ty, které jsou potřebné k identifikaci příslušnou službou.

Peněženka by měla také uchovávat takzvané atributy spojené s totožností uživatele. Dle návrhu má být atributem rys, vlastnost, právo nebo povolení fyzické nebo právnické osoby nebo předmětu. Může jít například o dosažené vzdělání, různá potvrzení, doklady o očkování, řidičská oprávnění apod. Uživatel by pak měl mít kontrolu nad tím, jaký atribut či osobní údaj bude sdílet s druhou (spoléhající) stranou. Zjednodušeně řečeno – k prokázání věku není nutné předložit celý občanský průkaz s datem narození, rodným číslem či bydlištěm, ale postačí sdílet údaj o věku, pokud bude potřeba prokázat bydliště, naopak již není nutné sdílet rovněž údaj o věku.

Jádro použitelnosti peněženky tak míří do jisté míry mimo zaměření této monografie. Zmiňujeme ji nicméně v souvislosti s tím, že měla umožnit vytváření a používání kvalifikovaných elektronických podpisů přijímaných v celé Evropské unii. To je důležitý moment pro budoucí širší uplatnění kvalifikovaných elektronických podpisů v soukromoprávním styku. Kvalifikovaný elektronický podpis je v současnosti nejdůvěryhodnější formou elektronického podpisu. Při vytvoření podpisu je identita podepisující osoby ověřena vlastnictvím kvalifikovaného prostředku pro vytváření podpisů a znalostí (typicky PINu) k tomuto prostředku.

Nutnost použít kvalifikovaný prostředek pro vytvoření podpisu má svůj přínos ve vyšší bezpečnosti a důvěryhodnosti této úrovně elektronického podpisu. Běžného uživatele ale může snadno odradit, pokud má u sebe pro tyto účely neustále nosit *USB token*, čipovou kartu či jiný kvalifikovaný prostředek. I pokud bude soukromý klíč pro podpis uložený na čipu občanského průkazu, stále nestačí jen občanský průkaz a je třeba disponovat i čtečkou čipových karet.

Tato zvýšená manipulační náročnost je vedle složitosti a relativní nákladnosti pořízení dle našeho názoru klíčovým důvodem, proč nejsou kvalifikované

elektronické podpisy příliš používány fyzickými osobami v soukromoprávním styku. Pokud ovšem dojde k posunu od současných kvalifikovaných prostředků k aplikacím evropské peněženky v telefonu nebo jiném zařízení, očekáváme, že s vyšší uživatelskou přívětivostí a přístupností vzroste i používání kvalifikovaných podpisů v tomto kontextu. Tím by mohla být nejen zvýšena úroveň zabezpečení údajů podepisující osoby, ale též postupně překonány nedostatky právní jistoty spojené s dnes převládajícím využíváním prostých elektronických podpisů.<sup>361</sup>

Toto zjednodušení a větší dostupnost prostředků pro elektronickou identifikaci a elektronické podepisování prostřednictvím evropské peněženky digitální identity nebude bez překážek. Každý bude moci využívat bezpečnou aplikaci pro elektronickou identifikaci, sdílení svých elektronických atributů a vytváření elektronických podpisů. To však nemusí být jen pozitivní. Je zásadní, aby samotná aplikace evropské peněženky digitální identity s ohledem na svou centrální roli pro prokázání identity nositele spolehlivě a konzistentně splňovala vysoké bezpečnostní požadavky. Používána bude ale na telefonech různých výrobců, včetně těch, před kterými v roce 2018 varoval Národní úřad pro kybernetickou a informační bezpečnost.<sup>362</sup> Zpracování a naplnění bezpečnostních standardů a důvěra uživatelů v příslušnou aplikaci tak bude stěžejní pro přijetí, rozšíření a výsledný dopad tohoto připravovaného unijního nástroje digitální identifikace.<sup>363</sup>

## 8.4 Využití protokolu *blockchain* pro uzavírání smluv

V právu lze sledovat tendence ke zjednodušení a jisté míře automatizaci služeb či realizaci právního jednání. Specifický soubor inovativních prostředků, které lze ve stále širší míře při elektronické kontraktaci využít, jsou založeny na protokolu *blockchain*. V tomto prostředí lze smlouvy jednak uzavřít, ale též, jak bude popsáno dále, v rostoucí míře také automatizovat její vykonání

<sup>361</sup> K tomu blíže v kapitole věnované vymáhání závazků a rozhodovací praxi.

<sup>362</sup> Software i hardware společností Huawei a ZTE je bezpečnostní hrozbou. In: *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 9. 6. 2023]. Dostupné z: <https://www.nukib.cz/cs/infoservis/aktuality/1303-software-i-hardware-spolecnosti-huawei-a-zte-je-bezpecnostni-hrozbou/>

<sup>363</sup> SCHWALM, S., ALBRECHT, D., ALAMILLO-DOMINGO, I. *eIDAS 2.0: Challenges, perspectives and proposals to avoid contradictions between eIDAS 2.0 and SSI*. 2022, s. 24. DOI: [http://doi.org/10.18420/OID2022\\_05](http://doi.org/10.18420/OID2022_05)

anebo její obsah spolehlivě archivovat. Smlouvy uzavřené prostřednictvím protokolu blockchain mohou představovat alternativu ke smlouvám v jejich běžném vnímání. Oproti vlastnoručně podepsaným listinným smlouvám, ale i obvyklým elektronicky uzavřeným smlouvám, vykazují tyto smlouvy řadu odlišností. Pro orientaci v této problematice pak příliš nepřispívá, že se v tomto kontextu rozšířilo užívání pojmu „chytré smlouvy“ (*smart contracts*), který ovšem nevychází z právního pojetí smlouvy s jejími náležitostmi, ale jde o samovykonatelný program vedoucí při splnění stanovených podmínek ke změně záznamů v databázi (např. převodu virtuálního aktiva mezi uživatelskými účty).

### 8.4.1 Přiblížení specifické povahy protokolu blockchain

Pro pochopení fungování protokolu *blockchain* je třeba nejprve vyjasnit jeho specifika a některé pojmy. Základem jeho fungování je specifický způsob ukládání dat prostřednictvím technologie distribuované účetní knihy (v angličtině *Distributed Ledger Technology*, dále „DLT“), resp. dle českého překladu návrhu nařízení Evropského parlamentu a Rady o trzích s kryptoaktivy „technologie sdíleného registru“.<sup>364</sup> V jeho případě jsou data ukládána prostřednictvím účetní knihy či databáze distribuované mezi uživatele.<sup>365</sup> Záznamy mohou být vedeny nepřetržitě nebo uspořádány v blocích jako v případě *blockchainu*.<sup>366</sup>

Ne všechny DLT jsou založeny na záznamech uspořádávaných a zapisovaných do bloků. Proto jde v případě DLT o širší pojem než *blockchain*.<sup>367</sup> Protokol *blockchain* je druh DLT, ve kterém jsou všechny evidované transakce zachyceny ve formě „řetězu“ vzájemně propojených bloků dat o provedených transakcích. Při jeho vytvoření je nový blok připojen k předchozím blokům prostřednictvím procesu, kterým je v souladu s pravidly sítě prováděno

<sup>364</sup> Návrh nařízení Evropského parlamentu a Rady o trzích s kryptoaktivy a o změně směrnice (EU) 2019/1937. COM(2020)593 final. *Evropská komise* [online]. [cit. 1. 2. 2020]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A52020PC0593&qid=1619174354936>

<sup>365</sup> Advice on “Initial Coin Offerings and Crypto-Assets”. *ESMA* [online]. 2019, s. 9 [cit. 4. 11. 2020]. Dostupné z: [https://www.esma.europa.eu/system/files\\_force/library/esma50-157-1391\\_crypto\\_advice.pdf?download=1](https://www.esma.europa.eu/system/files_force/library/esma50-157-1391_crypto_advice.pdf?download=1)

<sup>366</sup> BASHIR, I. *Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained*. 2. vyd. Birmingham: PACKET Publishing, 2018, s. 31.

<sup>367</sup> *Ibid.*

ověřování transakcí. Ověřovací proces a propojení s předchozími záznamy zajišťuje nezměnitelnost vedené databáze. Kopie aktuální verze databáze pak může být distribuována mezi všechny uživatele této databáze.

Bejček popisuje *blockchain* jako rozptýlenou, distribuovanou a sdílenou datovou strukturu, která umožňuje transparentní a bezpečné internetové uchovávání a přenos informace bez nutnosti spoléhání na třetí osobu stojící mimo *blockchain*. Pro kontraktaci podle něj *blockchain* představuje velký přínos, jelikož ji značně zrychluje a zvyšuje její kredibilitu. To je umožněno řadou autentizovaných a zřetězených elektronických záznamů nezpochybnitelně dokládajících smluvní úkony či jiné skutečnosti.<sup>368</sup>

Pro svou nezměnitelnost a distribuovaný charakter je *blockchain* ideálním způsobem evidence záznamů. Nejznámějším způsobem využití *blockchainu* jsou kryptoměny, což je druh kryptoaktiva, resp. virtuální měny<sup>369</sup>. Vlastnictví jednotek kryptoměny se prokazuje pouze prostřednictvím kryptografie, její vlastnictví je evidováno v *blockchainu*, a s ohledem na neexistenci jejich hmotné alternativy lze převody kryptoměny provádět pouze elektronicky prostřednictvím konkrétního protokolu *blockchain*.<sup>370</sup> Například Szostek konstatuje, že kryptoměny, resp. *blockchain* představují revoluční nástroj informačních technologií. Důvodem je, že vývoj nových technologií, globalizace a digitalizace ekonomiky, otevřenost trhů či jednoduchost uzavírání smluv online s relativně vysokými náklady na platby musely vést k novým alternativním, levným a globálním způsobům plateb. A jako příklad potenciálního řešení chápe síť Bitcoin.<sup>371</sup>

S ohledem na charakter protokolu *blockchain* jako distribuované a zabezpečené databáze záznamů jej lze využít i pro evidenci vlastnictví jiných věcí, než jsou kryptoměny. Je diskutováno nebo testováno například využití této technologie také pro evidenci vlastnických a jiných práv k nemovitým věcem. Jako příklady implementace protokolu *blockchain* pro evidenci nemovitých

<sup>368</sup> BEJČEK, J. Chytré smlouvy jakožto smlouvy „chytře“ protiprávní. In: SUCHOŽA, J., HUSÁR, J., HUČKOVÁ, R. (eds.). *Právo, Obchod, Ekonomika IX*. Košice: Univerzita P.J. Šafárika v Košiciach, 2019, s. 363.

<sup>369</sup> Ne všechny virtuální měny jsou totiž spojeny s kryptografií.

<sup>370</sup> Pro vyčerpávající definici kryptoměny srov. LÁNSKÝ, J. *Kryptoměny*. Praha: C. H. Beck, 2018, s. 3.

<sup>371</sup> SZOSTEK, D. *Blockchain and the Law*. Baden-Baden: Nomos Verlagsges.MBH + Co., 2019, s. 55.

věcí bývá uváděna Gruzie a Švédsko.<sup>372</sup> Typickým užitím protokolu *blockchain* může být také mezinárodní přeprava zboží, kdy předávání zboží mezi různými přepravci a jinými osobami je evidováno prostřednictvím protokolu *blockchain*. Mohlo by být jeho prostřednictvím také chráněno autorské právo, resp. uzavírány licenční smlouvy. V *blockchainu* jsou však nejčastěji zaznamenávány transakce kryptoměn a dalších typů tzv. kryptoaktiv, kterými lze rozumět privátní aktiva, jejichž existence závisí na kryptografii, jejich vlastnictví je evidováno prostřednictvím protokolu *blockchain* a slouží pro investiční účely, přístup ke zboží či službám anebo jako prostředek směny.<sup>373</sup>

#### 8.4.2 Podstata smart kontraktů

Do *blockchainu* lze kromě záznamů o vlastnictví kryptoaktiv také uložit počítačový kód, který vykoná akce podle předem stanovených podmínek smlouvy mezi stranami. Tento kód, spíše než smlouva, kterou reprezentuje, je následně označován za výše zmíněnou „chytrou smlouvu“ (*smart contract*).<sup>374</sup> Po zdůraznění odlišení od pojmu smlouvy se tedy v následujícím textu raději uchylujeme k užití anglicismu „smart kontrakty“. Za autora tohoto pojmu je považován Nick Szabo.<sup>375</sup> Ten za jeho základní myšlenku považoval to, že pravidla vycházející ze smluvního ustanovení je možné binárně převést do pokynů zanesených do hardwaru či softwaru takovým způsobem, že jejich naplnění je algoritmicky automatizováno a smluvní protistrana se tak ve velké míře může spolehnout na jejich dodržení a naplnění. Jako základní příklad uváděl algoritmus fungování prodejního automatu, který přijme mince, a následně

<sup>372</sup> KACZOROWSKA, M. Blockchain-based Land Registration: Possibilities and Challenges. *Masaryk University Journal of Law and Technology*. 2019, roč. 13, č. 2, s. 352, SHANG, Q., PRICE, A. A Blockchain-Based Land Titling Project in the Republic of Georgia: Rebuilding Public Trust and Lessons for Future Pilot Projects. *Innovations: Technology, Governance, Globalization*. Roč. 12, č. 3–4, s. 77.

<sup>373</sup> Advice on “Initial Coin Offerings and Crypto-Assets”. ESMA [online]. S. 42 [cit. 7. 12. 2021]. Dostupné z: [https://www.esma.europa.eu/system/files\\_force/library/esma50-157-1391\\_crypto\\_advice.pdf?download=1](https://www.esma.europa.eu/system/files_force/library/esma50-157-1391_crypto_advice.pdf?download=1), Report with Advice for the European Commission on Crypto-Assets. EBA [online]. S. 11, [cit. 7. 12. 2021]. Dostupné z: <https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf>

<sup>374</sup> HALLER GROENBAEK, M. Blockchain 2.0, Smart Contracts and Legal Challenges. *Computers & Law* [online]. 2016, č. 6–7 [cit. 14. 8. 2021]. Dostupné z: <https://www.scl.org/articles/3668-blockchain-2-0-smart-contracts-and-legal-challenges>

<sup>375</sup> ALLEN, J. G., HUNN, P. *Smart legal contracts: computable law in theory and practice*. Oxford, United Kingdom: Oxford University Press, 2022, s. 26. ISBN 9780192858467.



skrze analogově či digitálně stanovený postup automaticky vydá požadované zboží či vrátí peníze nad rámec kupní ceny. Jeho pomocí tedy dochází k uzavření i plnění kupní smlouvy mezi zákazníkem a prodejcem.<sup>376</sup> Takový automat je dobrým příkladem pro vysvětlení fungování smart kontraktu, nepředstavuje nicméně smlouvu jako takovou, ale je pouze prostředkem k uzavření a vykonání smlouvy.<sup>377</sup> Na podobném principu fungují internetové obchody poskytující digitální obsah, jako jsou například elektronické knihy, software či hudba.<sup>378</sup> Tyto obchody také fungují pouze jako prostředek k uzavření „*click-wrap*“ či „*click-through*“ smluv. *Blockchain* je v tomto kontextu ještě základnějším prvkem. Neobsahuje sám o sobě srovnatelnou transakční platformou, jde pouze o podkladový protokol, ve kterém je umožněno zachycení záznamů důvěryhodným a jednostranně neměnným způsobem. To ovšem v kombinaci s možností zachytit širokou škálu digitálního obsahu, což zahrnuje i kód, a tudíž vyjádření postupu srovnatelné s programovým nastavením prodejního automatu, čímž je umožněno uložení smart kontraktů a operace s nimi v nadstavbových službách.

Allen pro svou pracovní definici volí vymezení smart kontraktu jako záznam textu ve formálním jazyce, který má obsahovat jak i) písemný dokument obsahující a zaznamenávající vzájemné závazky smluvních stran, tak ii) kód, který tyto závazky plní a/nebo vynucuje na digitálním počítači.<sup>379</sup>

Podobně Bejček definuje smart kontrakty jako „*počítačové kódy spojené s prohlášeními, jež počítačový software provede, naplní-li se podmínky předem definované v kódu.*“<sup>380</sup> Podle něj by ale spíše než „*smart contracts*“ měly být nazývány „*automated contracts*“, jelikož to, co „*v právních vztazích provádějí, je povytce kauzální deterministická automatizovaná reakce na splnění předem zadaných podmínek.*“ Jde tak z jeho pohledu především o soubor příkazů.<sup>381</sup> Pro jejich zcela automatizovanou

<sup>376</sup> SZABO, N. Formalizing and Securing Relationships on Public Networks. *First Monday* [online]. 1997, roč. 2, č. 9 [cit. 22. 7. 2020]. Dostupné z: <https://doi.org/10.5210/fm.v2i9.548>

<sup>377</sup> MIK, E. Smart contracts: terminology, technical limitations and real world complexity, *Law, Innovation and Technology*. Roč. 9, č. 2, s. 274.

<sup>378</sup> ALLEN, HUNN, 2022, op. cit., s. 29.

<sup>379</sup> ALLEN, HUNN, 2022, op. cit., s. 32.

<sup>380</sup> BEJČEK, 2019, op. cit., s. 364.

<sup>381</sup> *Ibid.*, s. 365.

podobu a vykonatelnost je ně některými autory nahlíženo jako na formu svépomoci.<sup>382</sup>

Savelyev popisuje smart kontrakty jako softwarový kód implementovaný v *blockchainu*, který sám zajišťuje vykonání a autonomní povahu jeho pravidel za pomoci dříve definovaných podmínek a prostřednictvím majetku evidovaného v *blockchainu*.<sup>383</sup> Tuto definici lze rozpracovat pomocí následujících aspektů smart kontraktů:

- Na rozdíl od klasických smluv nemohou být uzavřeny ústně nebo v „papírové“ podobě. Mají tedy výhradně elektronickou podobu a jejich podmínky jsou vyjádřeny v softwarovém kódu.<sup>384</sup>
- Jsou spojeny s digitálním majetkem (například kryptoměnou) nebo jiným majetkem, jehož vlastnictví je registrováno pomocí *blockchainu*.<sup>385</sup>
- Vyjádření podmínek smart kontraktu pomocí softwarového kódu znamená, že k jejich vykonání není třeba jakékoliv interpretace těchto podmínek ze strany stran smart kontraktu, soudu nebo nějaké další třetí osoby.<sup>386</sup>
- Stejně jako jiný software, je smart kontrakt založen na podmínkách (pokud se stane X, pak nastane Y). Ty pak musí být jednoznačně vyjádřitelné v podobě kódu, tak aby byl naplněn předchozí bod. Ne vždy lze však u smluvních podmínek k tomuto způsobu vyjádření dospět. Nadto je část smluvních podmínek či práv smluvních stran založena zákonem a podmíněna určitými okolnostmi, přičemž v případě, že tyto nejsou zachyceny v kódu smart kontraktu, nelze je po uzavření smart kontraktu bez součinnosti obou smluvních stran vzhledem k povaze zachycení kódu na protokolu *blockchain* realizovat.
- K následnému vykonání zachycených úkonů a jejich podmínek na základě smart kontraktu již zpravidla další aktivita smluvních stran,

<sup>382</sup> RASKIN, M. The Law And Legality Of Smart Contracts. *Georgetown Law Technology Review*. 2017, roč 1, č. 2, s. 333.

<sup>383</sup> SAVELYEV, A. Contract Law 2.0: «Smart» Contracts As the Beginning of the End of Classic Contract Law?. *Higher School of Economics Working Papers* [online]. 2016, No. WP BRP 71/LAW/2016, s. 5 [cit. 26. 9. 2020]. Dostupné z: <https://wp.hse.ru/data/2016/12/14/1111743800/71LAW2016.pdf>

<sup>384</sup> *Ibid.*, s. 12.

<sup>385</sup> *Ibid.*

<sup>386</sup> *Ibid.*, s. 13.

proces plnění smlouvy probíhá automatizovaně jako u vydání zboží prodejním automatem.<sup>387</sup>

Automatizace plnění smart kontraktu však není v realitě zdaleka absolutní, jelikož řada podmínek je vázána na datové vstupy o určité realitě, která v samotném smart kontraktu či *blockchainu*, na kterém je uložen, zachycena není. Již prosté plynutí času se odvíjí od vnějšího vstupu, s kterým si kód smart kontraktu ověřuje, zda byla naplněna zachycená časová podmínka. Splnění či nesplnění většiny podmínek zachycených ve smart kontraktu je tak nevyhnutelně založené na datovém vstupu, kterým je smart kontrakt provázán s prostředím mimo daný blockchain. K tomu jsou používány například veřejně dostupné zdroje a tzv. „*oracles*“ jako třetí nezávislé entity ověřující splnění podmínky, které tuto informaci předají do prostředí *blockchainu*.<sup>388</sup> V případě podmínek, který bude nutné splnit, je tedy třeba rozlišovat mezi událostmi, které se odehrají tzv. *on-chain* (tedy v prostředí *blockchainu* – například převod kryptoměny na určitou adresu) a *off-chain* (mimo jeho prostředí).<sup>389</sup>

#### 8.4.3 Závislost smart kontraktu na „*oracles*“ jako jeho základní limitace

Role těchto vnějších vstupů se liší podle charakteru smart kontraktu. V případě prostého smart kontraktu na převod kryptoměny vyjádřené příslušným blockchainem z účtu plátce na účet příjemce v určitém rozsahu k určitému časovému okamžiku za předpokladu splnění podmínky, že na účtu plátce je dostatek kryptoměny pro tuto transakci, je vnějším vstupem pouze vazba na vnější veřejně dostupný zdroj o čase, na který bude příslušná transakce vázána. Pokud však půjde například o komplexnější smart kontrakt ve formě pojistné smlouvy, bude předpokladem plnění mimo jiné kódem smart kontraktu předvídaný datový vstup od stanoveného „*oracle*“, kterým je potvrzen vznik nároku na plnění na základě pojistné události. Pouze na základě tohoto vstupu se pak odehrají automatizovaně další kroky v rámci automatizovaného postupu smart kontraktu, které vedou k vyplacení pojistného plnění. Stejně tak v případě, že výše uvedený příklad převodu bude složkou smart

<sup>387</sup> SAVELYEV, 2016, op. cit., s. 15.

<sup>388</sup> ALLEN, HUNN, 2022, op. cit., s. 217.

<sup>389</sup> MIK, E. Smart Contracts: Terminology, Technical Limitations And Real World Complexity. *Law, Innovation and Technology*. 2017, roč. 9, č. 2, s. 295.

kontraktu, který představuje kupní smlouvu s převodem podmíněným zpřístupněním určitého digitálního obsahu, bude podmínkou realizace kódem předvídaný vstup o této skutečnosti z určeného „oracle“. Z výše uvedeného je zjevné, pro není vhodné mezi smlouvou a smart kontraktem činit rovnítko. V řadě případů půjde u smart kontraktu o digitální obraz uzavřené smlouvy, jejíž ustanovení jsou jednoznačně zachycena do počítačového kódu (čímž je výrazně snížen prostor pro případný odlišný výklad smluvních podmínek, a tedy rozpor v obsahu projevené vůle stran), s (podmíněně) automatizovaným plněním, důvěryhodně zachyceném na protokolu *blockchain*.<sup>390</sup>

#### 8.4.4 Zákonnost zachycení smluvního jednání pouze formou smart kontraktu

S ohledem na výše uvedené limitace smart kontraktu je na jejich uplatnění pro právní jednání, které se váže na aktiva či činnosti mimo prostředí příslušného protokolu *blockchain*, vhodné nahlížet spíše ve formě Bejčkem formulované kombinace rámcové klasické smlouvy a realizačních smluv v podobě smart kontraktů, přičemž s ohledem na právní jistotu doporučuje kombinaci smart kontraktů se smlouvami v jejich tradiční písemné podobě.<sup>391</sup> S tím vzhledem k výzvám spojeným s plnohodnotným a platným zachycením smluvního ujednání do podoby počítačového kódu souhlasíme, předpokládáme však, že s rozvojem technologie *blockchain* a jejích nástaveb se bude potřeba „zálohy“ v podobě tradičního písemného zachycení smluvních ujednání snižovat. Pokládáme tedy za vhodné položit si otázku ohledně platnosti smluv zachycených pouze ve formě smart kontraktu v českém právu.

Vyjádření vůle prostřednictvím počítačového kódu by nemělo být na překážku vzhledem k tomu, že každý má právo si zvolit pro právní jednání libovolnou formu, pokud není tato volba omezena zákonem nebo ujednáním stran.<sup>392</sup> I požadavek písemnosti by mohl být smart kontrakty naplněn. Písemnost je podle občanského zákoníku zachována i při právních jednáních učiněných elektronickými prostředky.<sup>393</sup> K transakcím v rámci protokolu *blockchain* je potřeba kombinace tzv. veřejného a soukromého klíče,

<sup>390</sup> Blíže viz ALLEN, HUNN, 2022, op. cit., s. 43 a násl.

<sup>391</sup> BEJČEK, 2019, op. cit., s. 366–368.

<sup>392</sup> § 559 obč. zák.

<sup>393</sup> § 562 odst. 2 obč. zák.

kdy soukromý klíč plní určitou formu podpisu transakce. Podepsat elektronické právní jednání elektronicky lze podle § 561 odst. 1 obč. zák. Prostý elektronický podpis je v nařízení eIDAS definován záměrně široce.<sup>394</sup> Dle zák. o službách vytvářejících důvěru lze k podpisu právního jednání použít kteroukoliv úroveň elektronického podpisu, není-li jednáno vůči veřejnoprávnímu podepisujícímu či dalším osobám v rámci jejich působnosti.<sup>395</sup> Docházíme tedy k závěru, že podpis transakce v *blockchainu*, tedy i zápis smart kontraktu, naplňuje požadavky na elektronický podpis prostý podle nařízení eIDAS, a lze s ním podepsat soukromoprávní jednání v souladu s českým právním řádem.

Otázka je, zda bude podpis v rámci *blockchainu* možné považovat i za zaručený elektronický podpis. Ten podle čl. 26 nařízení eIDAS musí:

1. být jednoznačně spojen s podepisující osobou;
2. umožnit identifikaci podepisující osoby;
3. být vytvořen pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou; a
4. být k datům, která jsou tímto podpisem podepsána, připojen takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat.

Problematický je požadavek na umožnění identifikace podepisující osoby. Běžné veřejné *blockchainy* jsou zpravidla pseudonymní či přímo anonymní<sup>396, 397</sup>. To ale nemusí být na překážku. Konkrétní veřejný klíč je přiřazen v rámci sítě při transakci jen jednomu uživateli. V síti jím je uživatel jednoznačně identifikován. Veřejný klíč je možné užít pouze v kombinaci se soukromým klíčem konkrétního uživatele. Pokud bude možné za použití dalších kroků a technických prostředků uživatele provádějícího transakci identifikovat, neměla by být vyslovena neplatnost smlouvy.<sup>398</sup> Lze si také představit situaci, že by uživatelé měli v rámci sítě povinnost uvést, které adresy – tedy který veřejný klíč – užívají. Jednotlivé uživatele by pak bylo možné snadno identifikovat.

<sup>394</sup> Článek 3 odst. 10 eIDAS.

<sup>395</sup> Srov. § 7 zák. o službách vytvářejících důvěru.

<sup>396</sup> Anonymní je například *blockchain* Monero.

<sup>397</sup> ALLEN, HUNN, 2022, op. cit., s. 63.

<sup>398</sup> Shodně BEJČEK, 2019, op. cit., s. 370.

Docházíme tak k závěru, že mohou být naplněny podmínky kladené nařízením eIDAS na zaručený elektronický podpis. Je dodržena podmínka jednoznačného spojení s podepisující osobou a její identifikace i použití pod výhradní kontrolou podepisujícího. Domníváme se, že použití kryptografického páru klíčů bude představovat jedinečná data, která podepisující osoba používá k vytváření elektronických podpisů.<sup>399</sup> Jednou nahraná data do protokolu blockchain již nelze změnit a je tedy splněna i podmínka zjištitelnosti jakékoli následné změny dat.<sup>400</sup>

S ohledem na požadavek použití kvalifikovaného certifikátu a kvalifikovaného prostředku pro vytváření kvalifikovaných elektronických podpisů však nelze předpokládat, že by byl v dohledné době dostupný a rozšířený blockchain v rámci něhož by bylo možné transakci podepsat kvalifikovaným elektronickým podpisem.<sup>401</sup>

#### 8.4.5 Závěrem k využitelnosti smart kontraktů při uzavírání smluv online

Jak vyplývá z předchozích úvah, lze si však snadno představit, že by byla smlouva uzavřena mimo *blockchain* prostřednictvím listinné smlouvy podepsané vlastnoručně či kvalifikovaným elektronickým podpisem, a tato smlouva (či její část) by následně byla pouze formou kódem zachyceného postupu a podmínek přenesena do podoby smart kontraktu (jehož znění po vytvoření musejí obě smluvní strany potvrdit svým elektronickým podpisem, čímž dojde ke sjednocení výkladu obsahu zachycených smluvních ujednání) a následně by při splnění zachycených podmínek došlo automatizovaně k plnění.

Prostřednictvím smart kontraktů tak lze podle našeho názoru naplnit i požadavky občanského zákoníku na písemnou formu právního jednání. Ta je zachována i při užití elektronického prostředku umožňujícího zachycení obsahu právního jednání a určení jednající osoby. Podmínku určení jednající osoby bude možné s ohledem na výše uvedené splnit. Obsah právního

<sup>399</sup> Čl. 3 odst. 13 nařízení eIDAS.

<sup>400</sup> K tomu závěru blíže také KRUPIČKOVÁ, 2017, op. cit., s. 26.

<sup>401</sup> Bylo by však možné zvažovat propagaci dat o vytvoření kvalifikovaného elektronického podpisu dokumentu do *blockchainu*.

jednání (smlouvy) bude zachycen a vyjádřen prostřednictvím počítačového kódu. To, že účastníci smart kontraktu nemusí bezprostředně rozumět zápisu zdrojového kódu smart kontraktu není nutně překážkou, obsah právního jednání bude stále jednoznačně zachycen. Zároveň lze prostřednictvím blockchainu právní jednání podepsat.<sup>402</sup>

#### 8.4.6 Automatizace plnění smlouvy skrze smart kontrakt

V předchozím textu bylo pojednáno o smart kontraktech a jejich možném využití v souvislosti s uzavíráním smluv online. Za jeden z jejich stěžejních rysů lze považovat předpoklad k automatizaci plnění, které nelze jednostranně zvrátit jednáním smluvní strany. Pojí se s nimi tedy zvýšení důvěry nejen v zachycení obsahu smluvního ujednání, ale především v realizaci plnění protistranou, jelikož algoritmická povaha smart kontraktu vylučuje, aby protistrana nepřistoupila k plnění, byť jsou podmínky pro toto plnění naplněny. V tom ostatně spočívá i často zmiňovaná „samovykonatelnost“ smart kontraktů. Jak již ovšem bylo přiblíženo výše, tato automatizace je téměř nevyhnutelně podmíněna vnějšími datovými vstupy, které mohou při nevhodném nastavení či vymezení plnění smlouvy naopak zásadně limitovat, čímž tato technická inovace dosti ztrácí na atraktivitě nad rámec specifického prostředí světa kryptoměn. S tím dále souvisí, že smart kontrakt je zásadně pouze (dílčím) obrazem smluvních ujednání ve formě počítačového kódu, který může sloužit toliko k omezení prostoru pro výkladový spor mezi smluvními stranami a záruku automatizovaného plnění za splnění stanovených podmínek. Zásadní výzvou při formulaci obsahu a podmínek v rámci smart kontraktu je však povaha některých institutů a ustanovení, která jsou pro smluvní jednání běžná, či dokonce zákonem zakotvená.<sup>403</sup>

Za nejvýznamnější lze považovat pravidla smluvního práva, jejichž porušení může mít za následek neplatnost smlouvy anebo některých ujednání v ní obsažených. Příkladem budiž nedostatek právní způsobilosti, rozpor ustanovení s dobrými mravy či veřejným pořádkem, odchylka od zákonného

<sup>402</sup> Shodně též Krupičková: „I když tedy lze považovat smart contract za specifickou formu uzavírání smlouvy, která s ohledem na volnost smluvních stran při volbě formy právního jednání může být využita, může smart contract naplnit i požadavky písemné formy.“ KRUPÍČKOVÁ, 2017, op. cit., s. 26.

<sup>403</sup> ALLEN, HUNN, 2022, op. cit., s. 44.

ustanovení v neprospěch slabší strany apod. Tyto pojistky či způsoby ochrany nebudou často ve smlouvách výslovně uvedeny, budou ale mít na oprávněnost plnění a vymahatelnost závazků ze smluv často zásadní vliv. Naproti tomu je na smart kontrakt nutno nahlížet jako na uzavřený program, který bez odpovídajících propojení nereflektuje pravidla či povinnosti z vnějších zdrojů (zde tedy práva smluvní strany vyplývající přímo ze zákona) a vzhledem k podstatě svého algoritmičeského nastavení nemusí vůbec umožnit změnu v procesu bez úpravy smart kontraktu za součinnosti obou smluvních stran.<sup>404</sup>

Smart kontrakty tak lze vnímat jako formu autonomní regulace v podobě Lessigova „*code is law*“, tedy regulace prostřednictvím počítačového kódu.<sup>405</sup> Takto vytvořené prostředí sice formálně není odtrženo od regulatorního rámce právního řádu, svou podstatou technické determinovanosti a jurisdikční neukotvenosti v kyberprostoru však může být vynutitelnost práva do tohoto prostředí z vnějšku do značné míry znemožněna. Běžně rozšířené veřejné blockchainy s uživateli rozestými po celém světě jsou nejen technologicky, ale také právně specifické, a to s ohledem na možné obtíže s určením rozhodného práva a vymahatelností rozhodnutí. Budou-li tedy ke kontraktaci použity, mohou nastat obtíže v případech sporů řešených soudní cestou a vykonatelností případných rozhodnutí.

I pokud by tedy jedna ze smluvních stran úspěšně dosáhla soudního rozhodnutí, které by ukládalo změnu ve smart kontraktu, lze jí dosáhnout opět pouze za součinnosti obou smluvních stran. Allen, Lane a Poblet si ve vztahu k řešení sporů vyplývajících ze smart kontraktů všímají dvou přístupů. Podle prvního smart kontrakty fungují v prostředí běžného smluvního práva, a spory tak mohou být rozhodovány soudy či v rámci existujícího alternativního řešení sporů.<sup>406</sup> Tento přístup však může narážet na kontext fungování protokolu *blockchain* a obtížnou vymahatelnost rozhodnutí. Druhý přístup vychází z názoru, že smart kontrakty jsou spíše než běžnými smlouvami

<sup>404</sup> FILLIPPI, P. de, HASSAN, S. Blockchain technology as a regulatory technology: From code is law to law is code. *First Monday* [online]. 2016, roč. 21, č. 12 [cit. 25. 9. 2020]. Dostupné z: <https://doi.org/10.5210/fm.v21i12.7113>

<sup>405</sup> LESSIG, L. *Code: Version 2*. New York: Basic Books, 2006.

<sup>406</sup> ALLEN, D. W. E., LANE, A. M., POBLET, M. The Governance of Blockchain Dispute Resolution. *Harvard Negotiation Law Review*. 2019, roč. 25, č. 75, s. 82.



zvláštním právním institutem. Tento náhled vychází z automatické vykonatelnosti transakcí v *blockchainových* sítích, jejich anonymity či pseudonymity nebo nezměnitelnosti zápisů o transakcích provedených v síti. V návaznosti na to by měl vzniknout nový právní systém svého druhu, někdy nazývaný jako *Lex Cryptographia*.<sup>407</sup>

Problém může pro účastníky představovat i samotné vyjádření smart kontraktu ve formě počítačového kódu.<sup>408</sup> Strany jednak mohou v některých případech využít předem vytvořených šablon smart kontraktů. Také lze předpokládat, že minimum uživatelů smart kontraktů bude skutečně rozumět zdrojovému kódu, ve kterém budou napsány. Může se vyskytnout chyba v kódu. Jak podrobně nastiňuje Gleeson, automatizace plnění skrze smart kontrakt s sebou přináší řadu nových právních otázek např. ohledně důsledků chyby, resp. odlišení chyby jednajícího (*mistake*) a chyby strojové (*error*), ke kterým se teprve rozvíjí potřebný právní diskurz.<sup>409</sup> V nastíněných případech lze předpokládat rozpor mezi vůlí a jejím projevem prostřednictvím kódu. I za této situace může být smart kontrakt kvůli své automatické vykonatelnosti vykonán za předem stanovených podmínek i proti vůli některé nebo dokonce všech stran smart kontraktu (za předpokladu, že nedojde k řádnému a včasnému upravení jeho obsahu a jeho validace v rámci příslušného blockchainu). Jak zdůrazňují Maslin a Butler, je tedy nutné hledat nejen nové cesty k aplikaci existujících právních nástrojů pro řešení těchto situací, ale reflektovat i technické parametry smart kontraktů a reagovat na ně novými právními nástroji, vycházejícími z koordinovaného úsilí právních a technických expertů na tuto technologii.<sup>410</sup>

Pouze v takovém případě lze dosáhnout překonání nastíněných výzev a překážek, které brání širšímu uplatnění smart kontraktů a umožní plně využít benefitů, které se s tímto technologickým řešením pojí.

<sup>407</sup> ALLEN, LANE, POBLET, 2019, op. cit., s. 83.

<sup>408</sup> Blíže viz ALLEN, Jason Grant a HUNN, P. *Smart legal contracts: computable law in theory and practice*. Oxford, United Kingdom: Oxford University Press, 2022, s. 278 a násl.

<sup>409</sup> Srov. ALLEN, HUNN, 2022, op. cit., s. 397.

<sup>410</sup> ALLEN, HUNN, 2022, op. cit., s. 371.

## 9 DORUČOVÁNÍ ELEKTRONICKÝCH PRÁVNÍCH JEDNÁNÍ

V rámci elektronického právního jednání dochází také k virtualizaci doručování. Při osobní přítomnosti účastníků právního jednání nastanou typicky jeho právní následky ve chvíli, kdy bude projevena vůle jednajících osob. Při právním jednání vůči nepřítomné osobě však již bude mít právní jednání zamýšlené právní následky až ve chvíli, kdy projev vůle jeho adresátovi dojde takovým způsobem, aby se s ním měl možnost seznámit.<sup>411</sup> Běžně tak byla, a stále jsou, právní jednání doručována poštou či osobně. Doručování elektronických právních jednání má oproti těmto způsobům určitá specifika.

V případě soukromoprávního jednání je zásadní zabývat se otázkou doručování, mnohdy nikoli kvůli nutnosti a potřebě respektovat specifické procesní lhůty, ale zejména v souvislosti s jistotou týkající se doručení komunikace a související důkazní spolehlivosti. K doručení může dojít i za využití široké škály elektronických prostředků zahrnujících email, komunikační služby ve smyslu *instant messengerů* apod. Vzhledem k jejich ryze soukromoprávnímu charakteru a jen specifickým zmínkám, kdy s nimi právní úprava počítá, však považujeme otázky související s dodáním či doručením touto formou za specifické a nutné posuzovat především *ad hoc*, co se týče jejich spolehlivosti. Problematice užití elektronických dokumentů při dokazování se přímo věnujeme v rámci kapitoly věnované vymáhání závazků z elektronicky uzavřených smluv.<sup>412</sup> V rámci problematiky doručování však vyvstává řada zajímavých otázek v souvislosti s využitím datových schránek pro soukromoprávní jednání.

### 9.1 Evropské doporučené doručování

Před úvahami nad českými datovými schránkami považujeme za vhodné zmínit souvislosti s nařízením eIDAS, které specificky počítá s tzv. službou elektronického doporučeného doručování. Ta je vymezena jako „*služba, která*

<sup>411</sup> ZUKLÍNOVÁ, M. Komentář k § 570. In: ŠVESTKA, J., DVOŘÁK, J., FIALA, J. a kol. *Občanský zákoník. Komentář. Svazek I (obecná část)* [online]. 2020 [cit. 16. 5. 2021]. Praha: Wolters Kluwer. Dostupné z: <http://www.noveaspi.cz>

<sup>412</sup> Blíže viz kapitolu 12 této knihy.

*umožňuje přenášet data mezi třetími osobami elektronickými prostředky a poskytuje důkazy týkající se nakládání s přenášenými daty, včetně dokladu o odeslání a přijetí dat, a která chrání přenášena data před rizikem ztráty, odcizení, poškození nebo neoprávněných změn.*<sup>413</sup> Toto obecné vymezení naplní (i v rámci ostatních států EU) různé systémy pro doručování za předpokladu, že jsou schopny generovat spolehlivé logy a záznamy o jednotlivých aktivitách, které při nakládání s elektronickými dokumenty vznikají (což se bude týkat rovněž systému datových schránek). Nařízení eIDAS ovšem dle čl. 44 zavádí kvalifikovanou úroveň pro služby elektronického doporučeného doručování. Ta nad výše řečené musí být poskytována kvalifikovaným poskytovatelem služeb a mimo jiné umožňovat s vysokou mírou spolehlivosti identifikovat odesílatele a příjemce, odesílání zabezpečit využitím zaručeného elektronického podpisu, zajistit čas odeslání pomocí kvalifikovaného časového razítka apod. Systém datových schránek je technologicky konstruován zcela jinak a nelze ani v dohledné době předpokládat, že by došlo k naplnění požadavků kladených nařízením eIDAS. Tyto kvalifikované služby jsou dostupné například v Belgii, Itálii, Německu, Španělsku, Francii, Nizozemí, Polsku či Slovinsku.<sup>414</sup>

## 9.2 Soukromoprávní jednání prostřednictvím datových schránek<sup>415</sup>

Datové schránky jsou specifickým elektronickým prostředkem, který lze použít pro právní jednání v různých oblastech. Vzhledem k zaměření této monografie se budeme dále zaměřovat na oblast soukromoprávního jednání, ale pokusíme se na řešené otázky nahlížet v rámci rozebírané problematiky komplexně.

V dalším textu se tedy zaměřujeme nejprve na obecné výkladové otázky související s právním jednáním přes datové schránky a na podmínky kladené na takové jednání. Následně se věnujeme konkrétním, potenciálně

<sup>413</sup> Čl. 3 bod 36 nařízení eIDAS.

<sup>414</sup> Seznam všech dostupných poskytovatelů kvalifikovaných služeb elektronického doporučeného doručování je dostupný po vyhledání z: <https://esignature.ec.europa.eu/efda/tl-browser/#/screen/search/type/1>

<sup>415</sup> Tato podkapitola částečně vychází a rozvíjí závěry dřívějšího textu JAREŠ, A. Soukromoprávní doručování datovými schránkami a teorie dojití. *Obchodněprávní revue*. 2022, č. 2.

problematickým otázkám, a to zejména uplatnění fikce doručení, resp. teorie dojití v případě soukromoprávního jednání. Tuto otázku považujeme za významnou, jelikož povinnost využívat datovou schránku byla rozšířena na nové subjekty,<sup>416</sup> což podstatně rozšiřuje prostor pro využívání datových schránek rovněž v rámci soukromoprávního jednání.

### 9.2.1 Obecné výkladové otázky při doručování pomocí datových schránek

Datovou schránku zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů definuje jako elektronické úložiště určené k doručování orgány veřejné moci a provádění úkonů vůči nim, ale také k dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob.<sup>417</sup> Původním účelem zavedení datových schránek byla vzájemná komunikace mezi osobami soukromého práva a orgány veřejné moci či mezi orgány veřejné moci navzájem.<sup>418</sup> Možnost dodávat datovými schránkami dokumenty fyzických osob, podnikajících fyzických osob a právnických osob byla do zákona vložena až jeho novelou provedenou zákonem č. 190/2009 Sb. s účinností od 1. 1. 2010.

Datové schránky tak slouží primárně jako nástroj doručování v oblasti veřejného práva, což je oblast, ke které je dostupná bohatá literatura i judikatura<sup>419</sup>. Je však možné (a stále běžnější) je využívat i pro doručování soukromoprávních dokumentů, a tedy prostřednictvím těchto dokumentů právně jednat i v oblasti soukromého práva. Této druhé oblasti je přitom věnována nepoměrně menší pozornost, což bychom rádi v rámci následujícího textu alespoň částečně kompenzovali.

Vzrůstající potenciál datových schránek pro veřejnoprávní i soukromoprávní styk lze spatřovat i ve vzrůstajícím zájmu nepodnikajících fyzických osob o zřízení datové schránky. V roce 2020 bylo nepodnikajícím fyzickým osobám na jejich žádost zřízeno přes 67 tisíc datových schránek. V roce 2021

<sup>416</sup> Podrobněji viz níže.

<sup>417</sup> § 2 Zák. o el. úkonech.

<sup>418</sup> LECHNER, T. Elektronické dokumenty. In: POLČÁK, R. a kol. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 256.

<sup>419</sup> Příkladem budiž Stanovisko Nejvyššího soudu ze dne 1. 5. 2017, sp. zn. PlsN 1/2015.

to již bylo 145 tisíc a v roce 2022 188 tisíc.<sup>420</sup> K lednu 2020 tak bylo cekem aktivních 900 169 datových schránek, přičemž ke květnu 2023 toto číslo vzrostlo na tři a půl milionu. Vzrůstá i počet odeslaných datových zpráv. V lednu 2020 jich bylo odesláno 9 908 029, v lednu 2023 bylo odesláno přes 13 milionů datových zpráv.<sup>421</sup>

Datové schránky nově zřizuje a spravuje Digitální a informační agentura<sup>422</sup>. Organům veřejné moci, právníkům osobám a dalším subjektům<sup>423</sup> je datová schránka zřizována povinně vždy poté, co jsou zapsáni do příslušného rejstříku či registru (datová schránka je zřizována bezplatně); od 1. 1. 2023 je povinnost zřídit datovou schránku stanovena *de facto* jakékoli osobě<sup>424</sup> s výjimkou osoby fyzické.<sup>425</sup>

Po novele provedené zákonem č. 190/2009 Sb. lze datové schránky využít nejen pro doručování orgánům veřejné moci a zpět, ale také – dikcí zákona – k dodávání dokumentů fyzických osob, podnikajících fyzických osob a právníků osob. Stát se v oblasti soukromého práva považuje za právníkou osobu.<sup>426</sup> Datovou schránku lze využít i při doručování veřejnoprávním osobám v rámci jejich vystupování v rovném postavení s účastníky právního jednání. Svou využitelnost a místo mají tak datové schránky i v oblasti soukromoprávních vztahů. Jako jejich výhody lze spatřovat identifikaci jednajících osoby a poskytnutí potvrzení o dodání a doručení dokumentu, u kterého

<sup>420</sup> Informační společnost v číslech 2023. *Český statistický úřad* [online]. 2023, s. 86 [cit. 27. 6. 2023]. Dostupné z: <https://www.czso.cz/documents/10180/191186455/06100423.pdf/879a3104-e54c-4f4e-b768-b0bd057ac006?version=1.3>

<sup>421</sup> Dle údajů České pošty dostupných z: <https://info.mojedatovaschranka.cz/info/cs/stats.html> [cit. 26. 6. 2023].

<sup>422</sup> A to na základě zákona č. 471/2022 Sb., kterým se mění zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů, a další související zákony.

<sup>423</sup> Viz § 4 odst. 3 Zák. o el. úkonech.

<sup>424</sup> § 4 a 5 Zák. o el. úkonech a dopad čl. CXLII, bod 3. zákona č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci.

<sup>425</sup> Možnost zřizovat datové schránky automatizovaně fyzickým osobám byla nicméně sáhodlouze diskutována. Od 1. 1. 2023 měla být fyzické osobě zřízena datová schránka ve chvíli, co tato osoba „*poprvé použila prostředek pro elektronickou identifikaci (například a naprosto typicky tzv. bankovní identitu) vydaný v rámci kvalifikovaného systému elektronické identifikace*“. Nakonec ale od takovéto automatické „předzřízení“ bylo upuštěno. Viz např. <https://www.mvcr.cz/clanek/datove-schranky-budou-pro-bezne-obcany-dobrovolne-nova-povinnost-zustala-jen-subjektum-vedenym-v-registru-osob.aspx>

<sup>426</sup> § 21 obč. zák.

je garantován jeho obsah. Rovněž spolehlivost metadat případně sloužících pro dokazování relevantních skutečností bude na vyšší úrovni, než je tomu v případě poskytovatelů například soukromých komunikačních služeb. Zároveň zachovávají datové schránky listovní tajemství, což zdaleka nemusí být vlastnost všech běžně užívaných elektronických komunikačních nástrojů. Jsou tedy důvěryhodným komunikačním nástrojem.<sup>427</sup>

Na jednu z výhod datových schránek nepřímou poukazují Donát s Tomíškem porovnáním s doporučeným dopisem zasílaným běžnou poštou. Doporučený dopis je podle nich z hlediska právní jistoty vhodnější než obyčejný dopis. Upozorňují ale na to, že u doporučeného dopisu je jisté pouze to, že obálka přijatá poštou bude s vyšší pravděpodobností doručena osobě, která má být příjemcem dopisu. To však ale příliš nevyovídá o prokazatelnosti obsahu samotné obálky a také o totožnosti osoby, která dopis odesílá. Tento deficit odstraňuje systém elektronického doporučeného doručování podle nařízení eIDAS.<sup>428</sup> To samé platí i pro české datové schránky. Informační systém datových schránek obsahuje totiž také nástroj pro porovnání zprávy se záznamem v informačním systému datových schránek, tedy potvrzení o tom, zda tato zpráva odpovídá zprávě přenesené informačním systémem datových schránek. Je důležité v této souvislosti upozornit na to, že český informační systém datových schránek lze sice považovat za službu elektronického doporučeného doručování dle nařízení eIDAS,<sup>429</sup> nejedná se však o kvalifikovanou službu doporučeného doručování a ani svým charakterem a technologickou konstrukcí by podmínky zejména dle článku 44 nařízení eIDAS systém datových schránek nesplnil. Právní účinky doručování prostřednictvím informačního systému datových schránek jsou tak relevantní jen v rámci vnitrostátního doručování v České republice.<sup>430</sup>

Dodávání soukromoprávních dokumentů v rámci systému datových schránek však není možné v každém případě. Právnícké osoby, ale také fyzické

<sup>427</sup> LECHNER, T. In: POLČÁK, R. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 256.

<sup>428</sup> DONÁT, TOMÍŠEK, 2016, op. cit., s. 143.

<sup>429</sup> Dle čl. 3 bod 36) je vymezena jako „služba, která umožňuje přenášet data mezi třetími osobami elektronickými prostředky a poskytuje důkazy týkající se nakládání s přenášenými daty, včetně dokladu o odeslání a přijetí dat, a která chrání přenášená data před rizikem ztráty, odcizení, poškození nebo neoprávněných změn.“

<sup>430</sup> Srov. DONÁT, PIFFL, MAISNER, 2017, op. cit., s. 163.

osoby a podnikající fyzické osoby musely mít do 31. 12. 2021 ve své datové schránce povolené dodávání dokumentů z datové schránky jiné fyzické osoby, podnikající fyzické osoby nebo právnické osoby.<sup>431</sup> S účinností od 1. 1. 2022 mohou pouze fyzické osoby svou datovou schránku znepřístupnit pro dodávání dokumentů z datové schránky fyzické osoby, podnikající fyzické osoby nebo právnické osoby.

K provedení právního jednání skrze datové schránky je tedy třeba splnit dvě podmínky – obě strany musí mít datovou schránkou zřízenou a zároveň je třeba, aby měly povolené dodávání dokumentů z datové schránky jiné fyzické osoby, podnikající fyzické osoby nebo právnické osoby.

Díky občanského zákoníku půjde v tomto případě o právní jednání vůči nepřítomné osobě. Občanský zákoník ho upravuje ve svém § 570 a násl., kde konstatuje, že právní jednání působí vůči nepřítomné osobě od okamžiku, kdy jí projev vůle dojde.<sup>432</sup> V případě právního jednání skrze datové schránky je také nutné zohlednit § 561 a § 562 obč. zák., podle kterých je písemná forma zachována i při právním jednání učiněném elektronickými prostředky umožňujícími zachycení jeho obsahu a určení jednatelce a zároveň je zde obsažen odkaz na jiný právní předpis, který má stanovit, jak lze při právním jednání učiněném elektronickými prostředky písemnost elektronicky podepsat.

Občanský zákoník tak nijak nevylučuje doručování datovou schránkou v soukromoprávních vztazích. Nijak se mu však ani nevěnuje. Výslovně upravuje pouze doručování s využitím provozovatele poštovních služeb.<sup>433</sup> Datové schránky tak lze použít i pro elektronickou kontraktaci a v souvislosti s ní. Výhodu mohou představovat například v případě prokazatelného doručení nabídky a její akceptace, ale samozřejmě i v případě doručování jiných právních jednání.<sup>434</sup> Dalším přínosem je zvýšení bezpečnosti, důvěrnosti a integrity přenášených dat. Datové schránky mohou také sloužit k identifikaci

<sup>431</sup> § 18a odst. 1 zák. o el. úkonech ve znění účinném do 31. 12. 2021: „*Ministerstvo umožní na žádost fyzické osoby, podnikající fyzické osoby nebo právnické osoby dodávání dokumentů z datové schránky jiné fyzické osoby, podnikající fyzické osoby nebo právnické osoby do datové schránky této osoby.*“

<sup>432</sup> § 570 odst. 1 obč. zák.

<sup>433</sup> § 573 obč. zák.

<sup>434</sup> Shodně např. HRDLIČKA, M. Datové schránky a možnosti jejich využití. In: *COFOLA 2010: the Conference Proceedings*. Brno: Masarykova univerzita, 2010, s. 58.

jednající osoby, a to vzhledem k procesu předcházejícímu jejich zpřístupnění jejich uživatelům. V této souvislosti například Ústavní soud konstatoval, že „*datová schránka není anonymním úložištěm dat, nýbrž je striktně individuálně přidělena.*“<sup>435</sup>

Vnímáme tak, že ač systém datových schránek nebyl primárně konstruován pro komunikaci a doručování v soukromoprávních vztazích, svou mírou spolehlivosti záznamů a legislativního zakotvení poskytuje vysoký stupeň důvěry ve spolehlivost komunikace, kterou obsahuje. Využití systému datových schránek pro soukromoprávní jednání tak skýtá velký potenciál, je nicméně nutno upozornit na to, že vzhledem ke svému specifickému charakteru a postavení pouze v rámci České republiky.

### 9.2.2 Fikce doručení

Právní jednání vůči nepřítomné osobě má zamýšlené právní následky až ve chvíli, kdy projev vůle jeho adresátovi dojde takovým způsobem, aby se s ním měl možnost seznámit (typicky osobním předáním, při vhození do schránky, oznámením o uložení zásilky na poště apod.).<sup>436</sup> Občanský zákoník výslovně zmiňuje domněnku dojití pro případy zásilek doručovaných prostřednictvím provozovatele poštovních služeb. Tato vyvratitelná právní domněnka se však uplatní pouze v případech, kdy byla zásilka doručena, jen není jasné, kdy přesně k tomu došlo.<sup>437</sup> Fikci dojití zná občanský zákoník pouze v případě, že zmaří dojití druhá smluvní strana vědomě. Pak platí, že právní jednání řádně došlo.<sup>438</sup>

Dále se tedy zaměřujeme na otázku, v jakém okamžiku lze považovat soukromoprávní jednání projevené prostřednictvím datové schránky za perfektní a jak se u něj projevuje teorie dojití.

Okamžik doručení právního jednání do datové schránky je možné určit s ohledem na zák. o el. úkonech. Ten rozlišuje mezi pojmy „dodání“ a „doručení“. Dodáním je okamžik, kdy je datová zpráva k dispozici v datové schránce

<sup>435</sup> Rozhodnutí Ústavního soudu ze dne 7. 3. 2016, sp. zn. II. ÚS 289/15.

<sup>436</sup> Srov. ZUKLÍNOVÁ, M. Komentář k § 570. In: ŠVESTKA, DVORÁK, FIALA a kol., 2020, op. cit.

<sup>437</sup> DOBROVOLNÁ, E. Komentář k § 573 [Domněnka doby dojití]. In: LAVICKÝ, P. a kol. *Občanský zákoník I. Obecná část* (§ 1–654). 2. vyd. Praha: C. H. Beck, 2022, s. 1830.

<sup>438</sup> § 570 odst. 1 obč. zák.



a je možné se s jejím obsahem seznámit. Doručením začne mít právní jednání své právní účinky (tedy typicky ve chvíli, kdy se se zprávou adresát seznámí). U právních jednání vůči orgánu veřejné moci judikatura dovozuje, že k doručení dochází již okamžikem dodání do datové schránky orgánu veřejné moci, tedy tyto dva pojmy v daném případě časově splývají.<sup>439</sup> Naopak při doručování orgány veřejné moci soukromým subjektům je dokument dodaný do datové schránky doručení okamžikem, kdy se do datové schránky přihlásí osoba, která má s ohledem na rozsah svého oprávnění přístup k dodanému dokumentu. Pokud se však do datové schránky osoba oprávněná k přístupu nepřihlásí ve lhůtě 10 dnů ode dne, kdy byl dokument dodán do datové schránky, považuje se tento dokument za doručení posledním dnem této lhůty – nastává tedy fikce doručení.<sup>440</sup>

Pro soukromoprávní jednání platí totéž – dokument dodaný do datové schránky je doručení okamžikem, kdy se do datové schránky přihlásí osoba, která má s ohledem na rozsah svého oprávnění přístup k tomuto dokumentu.<sup>441</sup> Zák. o el. úkonech však na rozdíl od doručování dokumentů orgánem veřejné moci do 1. 1. 2022 neurčoval, že by se při doručování v soukromoprávních vztazích, jakkoliv uplatnila fikce doručení. Pokud se tedy při soukromoprávním jednání prostřednictvím datové schránky neuplatnila fikce doručení, pak tento způsob doručování nemusel být příliš efektivní. Pokud by tak osoba doručovala prostřednictvím datové schránky druhé smluvní straně významné právní jednání vztahující se ke smlouvě (například její výpověď, odstoupení apod.), pak by mohl smluvní partner obstruovat účinnost taktového právního jednání jednoduše tím, že se do datové schránky nepřihlásí. Za této situace tak bylo z opatrnosti možné zvažovat výslovnou úpravu doručování datovou schránkou ve smlouvě.<sup>442</sup>

Je otázkou, proč zákonodárce neupravil fikci doručení i pro soukromoprávní jednání. Nejasnosti přitom mohlo mimo jiné vyvolávat doručování v případě právního jednání osob, které mají zřízenou datovou schránku, orgánu veřejné

<sup>439</sup> Např. usnesení Nejvyššího správního soudu ze dne 15. 7. 2010, sp. zn. 9 Afs 28/2010, nebo náleží Ústavního soudu ze dne 10. 1. 2012, sp. zn. II. ÚS 3518/11.

<sup>440</sup> § 17 odst. 3 a 4 zák. o el. úkonech.

<sup>441</sup> § 18a odst. 2 zák. o el. úkonech.

<sup>442</sup> Shodně např. ONDREJOVÁ, D. *Průvodce uzavíráním smluv*. 3. aktualizované vyd. Wolters Kluwer, 2020, kap. 36. Dostupné z: <http://www.noveaspi.cz> [cit. 13. 6. 2021]. Srov. také Rozhodnutí Vrchního soudu v Praze ze dne 16. 11. 2009, sp. zn. 5 Cmo 161/2009, nebo rozhodnutí Nejvyššího soudu ze dne 16. 1. 2013, sp. zn. 31 Cdo 1571/2010.

moci, avšak dokument byl doručován v rámci soukromoprávního jednání při rovném postavení s adresátem tohoto právního jednání.

Tento nedostatek se pokusil vyřešit zákon č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci (dále „DEPO“). Ten s účinností od 1. 1. 2022 vložil do § 18a zák. o el. úkonech nový odstavec číslo 3, podle kterého za situace, kdy se nepřihlásí do datové schránky osoba, která má s ohledem na rozsah svého oprávnění přístup k tomuto dokumentu ve lhůtě 10 dnů ode dne, kdy byl dokument dodán do datové schránky, považuje se tento dokument za doručení posledním dnem této lhůty.<sup>443</sup>

S účinností této změny stanovené k 1. 1. 2022 tedy došlo ke sjednocení fikce doručení skrze datovou schránku u dokumentů doručovaných orgánem veřejné moci a u dokumentů dodávaných v rámci soukromoprávního styku. To považujeme za správný přístup. Vzhledem k nevyřešenému vztahu k soukromoprávní úpravě právního jednání v občanském zákoníku a jeho teorii dojití je však otázka, zda zákonodárce pro vyloučení pochybností neměl zvolit jiné legislativní řešení a nevyjasnit poměr zák. o el. úkonech a občanského zákoníku.

### 9.2.3 Teorie dojití<sup>444</sup>

Na doručování soukromoprávních jednání prostřednictvím datových schránek lze totiž, stejně jako na ostatní způsoby doručování, nahlížet rovněž prostřednictvím teorie dojití. Podle § 570 obč. zák. právní jednání působí vůči nepřítomné osobě od okamžiku, kdy jí dojde. K dojití dojde v okamžiku, kdy se projev vůle dostane do sféry adresáta takovým způsobem, že za normálního běhu věcí je možné počítat s tím, že se adresát s tímto projevem vůle seznámil. Postačí navíc, aby měl adresát objektivní příležitost se s projevem vůle seznámit.<sup>445</sup>

<sup>443</sup> Čl. CXLII bod 28 zákona č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci.

<sup>444</sup> K otázce teorie dojití a doručování datovými schránkami viz také JAREŠ, A., Soukromoprávní doručování datovými schránkami a teorie dojití. *Obchodněprávní revue*. 2022, č. 2.

<sup>445</sup> DOBROVOLNÁ, 2022, op. cit., s. 1826; ZUKLÍNOVÁ, M. Komentář k § 570. In: ŠVESTKA, DVORÁK, FIALA a kol., 2020, op. cit.

K teorii dojití bylo vydáno větší množství soudních rozhodnutí. Z nich vyplývá, že projev vůle adresátovi dojde v okamžiku, kdy se dostane do sféry jeho dispozice. K tomu dochází ve chvíli, kdy adresát nabude objektivní možnost seznámit se s obsahem projevu vůle. To, aby se adresát přímo seznámil s obsahem právního jednání, není nezbytné, je přitom dostačující, že měl objektivně možnost seznat jeho obsah.<sup>446</sup> Možností seznámit se s právním jednáním se chápe nejen samotné převzetí písemného hmotněprávního jednání adresátem, ale i případy, kdy je dopis vložen do jeho poštovní schránky, popřípadě i pouhým vhozením oznámení do poštovní schránky o uložení takové zásilky.<sup>447</sup> Pouze výjimečně nemusí mít adresát objektivní možnost se seznámit s obsahem právního jednání při vhození oznámení o uložení zásilky s hmotněprávním jednáním do jeho schránky.<sup>448</sup>

Již dříve byl na teorii dojití postaven závěr, že byť byla dříve při doručování datovou schránkou při soukromoprávním styku vyloučena fikce doručení, měla se uplatnit soukromoprávní fikce podle § 45 odst. 1 občanského zákoníku z roku 1964 (nyní § 570 obč. zák.) okamžikem dojití zásilky do dispoziční sféry adresáta.<sup>449</sup> Tento názor prezentovaný Korbelem pochází z roku 2010, tedy z doby, kdy § 18a odst. 2 zák. o el. úkonech považoval dokument za doručený okamžikem, kdy jeho převzetí potvrdí odesílateli adresát prostřednictvím své datové schránky. Podle Korbela se měla uplatnit „výkladová soukromoprávní fikce podle § 45 odst. 1 občanského zákoníku okamžikem dojití zásilky do dispoziční sféry adresáta.“<sup>450</sup> Pokud by měla tato „výkladová soukromoprávní fikce“ nastoupit v takové situaci, měla by se podle našeho názoru uplatnit i po následujících novelizacích § 18a zák. o el. úkonech. Tedy i v době, kdy toto ustanovení upravovalo doručení pouze okamžikem přihlášení do datové schránky. A zároveň by tento závěr mohl být platný i nyní, kdy zákon předpokládá doručení okamžikem přihlášení nebo nejpozději do 10 dnů od dojití do datové schránky.

<sup>446</sup> Rozhodnutí Nejvyššího soudu ze dne 15. 1. 2004, sp. zn. 32 Odo 442/2003. Shodně např. rozhodnutí Nejvyššího soudu ze dne 8. 1. 2008, sp. zn. 29 Odo 805/2006.

<sup>447</sup> Rozhodnutí Nejvyššího soudu ze dne 27. 4. 2011, sp. zn. 23 Cdo 3951/2009.

<sup>448</sup> Rozhodnutí Nejvyššího soudu ze dne 1. 7. 2016, sp. zn. 26 Cdo 1239/2016 nebo rozhodnutí Ústavního soudu ze dne 1. 10. 2013, sp. zn. I. ÚS 2474/13.

<sup>449</sup> KORBEL, F. Lze doručovat fikci do datové schránky mezi soukromými osobami? *JINÉ PRÁVO* [online]. 2010 [cit. 4. 2. 2022]. Dostupné z: <https://jinepravo.blogspot.com/2010/01/f-korbel-lze-dorucovat-fikci-do-datove.html>

<sup>450</sup> Ibid.

### 9.2.4 Poměr teorie dojití k fikci doručení datové zprávy

Na základě výše řečeného se tedy k okamžiku účinnosti soukromoprávního projevu vůle doručovaného datovou schránkou nabízejí dva výkladové přístupy:

1. K účinnosti projevu vůle postačí dodání do datové schránky, faktické doručení není rozhodné a postačí objektivní možnost se s obsahem právního jednání seznámit. To by odpovídalo aktuálnímu nastavení občanského zákoníku a závěrům relevantní rozhodovací praxe k teorii dojití, podle které například nezáleží na tom, jestli si adresát skutečně vyzvedne zásilku na poště poté, co mu bylo do jeho schránky vhozeno oznámení o uložení na poště, protože již tímto okamžikem získal objektivní možnost se s obsahem zásilky seznámit. Určitá fikce doručení by se uplatnila ve smyslu výše uvedené Korbelovy „*soukromoprávní fikce okamžikem dojití do dispoziční sféry adresáta*“<sup>451</sup>, tedy okamžikem dodání do datové schránky.
2. Druhý přístup je založen na tom, že § 18a odst. 3 zák. o el. úkonech je *lex specialis* vůči § 570 odst. 1 obč. zák. a při doručování právního jednání prostřednictvím datových schránek se v soukromoprávním styku teorie dojití a dosavadní judikatura neuplatní. Projev vůle má v tomto případě účinky v okamžiku, kdy dojde k přihlášení do datové schránky, či nejpozději 10. den od dodání, pokud se oprávněná osoba do datové schránky nepřihlásí.

Přikláníme se k druhé možnosti, a tedy že § 18a odst. 3 zák. o el. úkonech je speciálním ustanovením a při doručování dokumentů se soukromoprávním jednáním zakládá právní účinky tohoto jednání až okamžikem doručení (bez ohledu na to, zda přihlášením uživatele, nebo fikcí po uplynutí 10 dní od dodání). Pokud by tento závěr neplatil, byla by novela zmíněného ustanovení nadbytečná a neměla by pro soukromoprávní doručování žádný dopad. Výsledkem tedy je, že účinné znění § 18a odst. 3 zák. o el. úkonech se při dodávání soukromoprávních dokumentů datovými schránkami zcela distancuje od teorie dojití užitě již v občanském zákoníku z roku 1964 a na ní navazující soudní praxe.

<sup>451</sup> KORBEL, 2010, op. cit.

Odchylná úprava doručování v soukromoprávní styku však není nic nového. Podobně zná zákoník práce vlastní úpravu doručování v pracovněprávních vztazích. Zákoník práce nicméně výslovně řeší pouhé subsidiární užití občanského zákoníku v rámci soukromoprávní úpravy pracovního poměru.<sup>452</sup> Naproti tomu zákon o el. úkonech však o svém vztahu k občanskému zákoníku mlčí. Důvodová zpráva k DEPO pouze konstatuje, že touto změnou „se předejde jak obstruování při doručování soukromoprávních dokumentů, ke kterému dochází podle současné právní úpravy, tak nutnosti rozlišovat mezi dokumenty doručovanými ve veřejnoprávním a soukromoprávním režimu.“<sup>453</sup> A zároveň, že „[p]ro určení okamžiku doručení veřejnoprávních i soukromoprávních dokumentů prostřednictvím datové schránky tak budou platit stejná pravidla.“<sup>454</sup> Zákonodárce tak při novele § 18a zák. o el. úkonech pro vyjasnění vzájemného vztahu tohoto ustanovení či zák. o el. úkonech jako celku k občanskému zákoníku mohl zvolit vhodnější způsob.

### 9.3 Specifika doručování v pracovním právu

Výše jsme otevřeli téma doručování v pracovněprávních vztazích. Byť je pracovní poměr specifickým vztahem upraveným zvláštním předpisem, platí, že jde o soukromoprávní vztah. To potvrzuje i důvodová zpráva k § 2401 obč. zák. svým konstatováním, že pracovní smlouva je institut soukromého práva a subjektivní práva a povinnosti založené touto smlouvou jsou právy a povinnostmi soukromoprávní povahy.<sup>455</sup> Vzhledem k zaměření této kapitoly a celé monografie tak považujeme za vhodné stručně zmínit specifika doručování v rámci pracovněprávního vztahu.

Zákoník práce pro pracovněprávní vztahy výslovně předpokládá užití občanského zákoníku jen v případech, kdy nelze zákoník práce použít,<sup>456</sup> a doručování právních jednání v pracovněprávních vztazích zákoník práce specificky upravuje. Pro některá právní jednání předpokládá zákoník práce jejich účinnost až okamžikem doručení. Typicky musí být do vlastních rukou

<sup>452</sup> § 4 zák. práce.

<sup>453</sup> Sněmovní tisk č. 756, Návrh zákona včetně důvodové zprávy. *Poslanecká sněmovna* [online]. [cit. 13. 6. 2021]. Dostupné z: <https://www.psp.cz/sqw/text/orig2.sqw?idd=171296>

<sup>454</sup> Ibid.

<sup>455</sup> Důvodová zpráva k občanskému zákoníku, § 2401.

<sup>456</sup> § 4 zák. práce.

zaměstnance doručeny písemnosti týkající se vzniku, změn a skončení pracovního poměru, důležité písemnosti týkající se odměňování apod.<sup>457</sup>

Pracovní právo se zdálo být dlouhá léta rezistentní vůči používání elektronických prostředků při doručování pracovněprávních písemností. To bylo někdy v diskuzích odůvodňováno potřebou zvýšené zákonné ochrany zaměstnance<sup>458</sup> jakožto jedné ze základních zásad pracovního práva (abychom ochránili zaměstnance, tak by doručování zaměstnavatelem mělo být co nejsložitější). O tom svědčila dlouho přetrvávající úprava elektronického podepisování a doručování prostřednictvím elektronických prostředků v zákoníku práce. Povinnost zaměstnavatele opatřit písemnost uznávaným elektronickým podpisem bylo možné akceptovat. Nicméně reálnému využívání elektronické komunikace ze strany zaměstnavatele bránila skutečnost, že aby byla písemnost považována za doručenou, musel zaměstnanec potvrdit převzetí písemnosti zprávou podepsanou svým uznávaným elektronickým podpisem.<sup>459</sup>

V kontextu pracovního práva se tak jevilo jako poměrně frivolní rozhodnutí Nejvyššího soudu ze dne 27. 4. 2022, sp. zn. 21 Cdo 2061/2021. Zde nejprve zaměstnanec obdržel výpověď z pracovního poměru, nicméně strany následně uzavřely elektronicky prostřednictvím e-mailové komunikace dohodu o narovnání, kterou byla uzavřena dohoda o rozvázání pracovního poměru a bylo dohodnuto odstupné. Toto odstupné však zaměstnavatel nevyplatil s tvrzením, že dohoda o narovnání nikdy nebyla uzavřena, jelikož nebyl dodržen požadavek písemné formy a dohoda nebyla nikdy doručena zaměstnanci do vlastních rukou. Dohoda o narovnání v této věci byla uzavřena tak, že zaměstnavatel nejprve odeslal zaměstnanci e-mailem sken dohody podepsané osobami jednajícími za zaměstnavatele. Právní zástupkyně zaměstnance následně zaměstnavateli opět e-mailem zaslala potvrzení o akceptaci dohody zaměstnavatele a o podpisu dohody.

Nejvyšší soud tak byl postaven před otázku, zda může být dohoda mezi zaměstnancem a zaměstnavatelem uzavřena tímto způsobem distančně při nedodržení pravidel pro doručování stanovených zákoníkem práce. Soud

<sup>457</sup> § 334 zák. práce.

<sup>458</sup> Srov. § 1a zák. práce.

<sup>459</sup> § 335 zák. práce.

v řízení následně dospěl k závěru, že dohoda byla uzavřena, jelikož vůči zaměstnanci byla platně doručena oferta dohody, která byla zaměstnancem následně bez výhrad přijata, byť k těmto projevům vůle došlo prostřednictvím e-mailu. Nejvyšší soud v této věci tedy konstatuje, že v případě dvoustranného právního jednání (byť se týká skončení pracovní poměru) není potřeba dodržet přísná pravidla zákoníku práce ohledně doručování. Zároveň měl dohodu za řádně podepsanou, přestože si strany vyměnily pouze sken podepsané dohody.

Na rozhodnutí navázaly nadšené reakce, které vítaly otevřenost Nejvyššího soudu vůči elektronickému podepisování a doručování. Z našeho pohledu je sice sken podpisu či jiné jeho grafické znázornění prostým elektronickým podpisem,<sup>460</sup> z rozhodnutí se však nejeví, že by se Nejvyšší soud v řízení jakkoliv zabýval otázkou elektronického podpisu. V předcházejícím řízení pouze Krajský soud v Brně jako odvolací soud konstatoval, že dohoda o narovnání byla uzavřena podle § 562 odst. 1 obč. zák., podle kterého je písemná forma zachována i při právním jednání učiněném elektronickými nebo jinými technickými prostředky umožňujícími zachycení jeho obsahu a určení jednajících osoby. Zároveň je otázka, zda lze vytištěný dokument, který byl vlastnoručně podepsán a následně naskenován, považovat za elektronicky podepsaný dokument.<sup>461</sup> Je také nutné vzít v úvahu specifikum této věci, a to, že byla projednávána v mantinelech pracovního práva. Nelze z něj tak bez dalšího vyvozovat obecné závěry k elektronickému podepisování. I odvolací soud v této věci totiž připomenul, že v rozhodované věci *„je třeba postupovat při posouzení řádného doručení a platnosti dohody o narovnání s přihlédnutím ke všem okolnostem a k základním zásadám pracovníprávních vztahů vymezených v § 1a zákoníku práce.“*

Podobným přístupem k elektronickému doručování a podepisování reagovala na dosavadní stav poslední novela zákoníku práce vyhlášená 19. 9. 2023 ve Sbírce pod číslem 281/2023 Sb.

Zákoník práce díky ní od 1. 10. 2023 nově pamatuje na uzavírání pracovníprávních smluv a dohod prostřednictvím sítě nebo služby elektronických

<sup>460</sup> Bylo rozebráno blíže v podkapitole 6.5.2 k úrovním elektronického podpisu a různých podpisových technik.

<sup>461</sup> Této otázce jsme se věnovali také podkapitole 6.5.2.

komunikací. V této souvislosti poskytuje zákoník práce zvýšenou ochranu zaměstnanci, jelikož v takovém případě je zaměstnavatel povinen zaslat vyhotovení smlouvy nebo dohody na elektronickou adresu zaměstnance, která však nesmí být v dispozici zaměstnavatele a zaměstnanec ji pro tyto účely sdělil zaměstnavateli. Vyloučeno je tedy zaslání pouze na e-mailovou adresu zřízenou zaměstnanci zaměstnavatelem.

Novela při uzavření smlouvy nebo dohody tímto způsobem také přináší další prvek podobný spotřebitelské ochraně při uzavírání smluv online. Zaměstnanec má totiž právo od takové smlouvy nebo dohody odstoupit ve lhůtě 7 dnů ode dne dodání jejího vyhotovení na elektronickou adresu zaměstnance. Odstoupení je však možné pouze do okamžiku, než bylo ze strany zaměstnance započato s plněním pracovního závazku.

Obě povinnosti jsou odůvodněny tím, že lze předpokládat uzavírání pracovních smluv a dohod v různých platformách a aplikacích v dispozici zaměstnavatele. Zaměstnanci tak má být tímto způsobem zajištěn dostatečný přehled a klid pro nezávislý a určitý projev vůle směřující k založení nebo změně pracovního závazku.

Výše jsme konstatovali, že elektronické doručování bylo v pracovním právu v podstatě nepoužitelné. Tuto situaci novela napravuje také. Zaměstnanci lze doručovat elektronicky i závažné pracovní právní dokumenty (např. výpověď a okamžité zrušení pracovního poměru, mzdový nebo platový výměr apod.), pokud k tomu zaměstnanec udělí souhlas. Zaměstnanec následně již nemusí potvrzovat doručení zprávou podepsanou uznávaným elektronickým podpisem.

Zaměstnanec a zaměstnavatel si mohou vzájemně doručovat písemnosti, včetně těchto významných také prostřednictvím datové schránky. Nově zaměstnanec nemusí dát k tomuto doručování souhlas, musí mít nicméně v datové schránce umožněné dodávání soukromoprávních dokumentů. V takovém případě zákoník práce sjednocuje doručování se zák. o el. úko- nech tím, že považuje písemnost za doručenu – pokud se dříve zaměstnanec nepřihlásí do datové schránky – ve lhůtě 10 dnů ode dne dodání písemnosti do datové schránky.





## 10 OCHRANA SPOTŘEBITELE PŘI UZAVÍRÁNÍ ELEKTRONICKÝCH SMLUV

Při úvahách o elektronickém právním jednání je dále nutné se také zabývat specifickou oblastí kontraktace přes internet – smlouvám uzavíraným se spotřebiteli. Jedná se v tomto případě o typ smluv uzavíraných distančním způsobem, u kterých občanský zákoník obecně spotřebitelům poskytuje zvýšenou míru ochrany. Je tak vhodné se na tomto místě věnovat specifikům elektronických smluv uzavřených se spotřebiteli (respektive smlouvám uzavřeným elektronickými prostředky). Spotřebitelé jsou dále chráněni prostřednictvím zákazu některých obchodních praktik podnikatelů zákonem č. 634/1992 Sb., o ochraně spotřebitele. S ohledem na zaměření této monografie se nicméně budeme dále soustředit především na aktuální právní úpravu obsaženou v občanském zákoníku.

### 10.1 Obecně k povinnostem podnikatele při uzavírání smlouvy se spotřebitelem

Občanský zákoník čerpá základ spotřebitelské ochrany ze směrnice Evropského parlamentu a Rady 2011/83/EU ze dne 25. října 2011 o právech spotřebitelů. Míří přitom na ochranu spotřebitele již v procesu uzavírání smlouvy. Podnikatel musí vůči spotřebiteli splnit širokou informační povinnost ohledně své osoby, nabízeného zboží, jeho dodání apod., a to v dostatečném předstihu před uzavřením smlouvy nebo před tím, než spotřebitel učiní závaznou nabídku.<sup>462</sup> O něco méně informací se spotřebitel musí dozvědět v případě, pokud se smlouva uzavírá výlučně výměnou elektronické pošty nebo obdobnou individuální komunikací.<sup>463</sup>

Podnikatel je následně povinen prostřednictvím některého prostředku komunikace na dálku neprodleně potvrdit spotřebiteli obdržení objednávky. To však neplatí při uzavírání smlouvy výlučně výměnou elektronické pošty nebo obdobnou individuální komunikací.<sup>464</sup> Uzavřená smlouva musí

<sup>462</sup> V podrobnostech viz § 1811 odst. 2 a § 1820 odst. 1 ve spojení s § 1824 obč. zák.

<sup>463</sup> 1826 odst. 3 obč. zák.

<sup>464</sup> § 1827 obč. zák.

obsahovat i údaje sdělené spotřebiteli před jejím uzavřením.<sup>465</sup> Uzavírá-li se smlouva za použití elektronických prostředků, poskytne podnikatel spotřebiteli v textové podobě kromě znění smlouvy i znění všeobecných obchodních podmínek.<sup>466</sup> S nesplněním této povinnosti nicméně občanský zákoník nespojuje neplatnost smlouvy. Například při porušení povinnosti § 1820 odst. 1 písm. c) obč. zák. však náleží právo odstoupit ve lhůtě 1 roku a 14 dní od počátku běhu lhůty pro odstoupení od smlouvy, resp. 14 dnů ode dne, kdy poučení spotřebitel v této lhůtě od podnikatele obdržel.

Při uzavírání smluv mezi podnikateli a spotřebiteli na internetu půjde často o adhezní smlouvy. Za smlouvu uzavřenou adhezním způsobem považuje občanský zákoník každou smlouvu, u níž byly základní podmínky určeny jednou ze smluvních stran nebo podle jejich pokynů, aniž slabší strana měla skutečnou příležitost obsah těchto základních podmínek ovlivnit.<sup>467</sup> Při jejich uzavření bude také pravidelně vyjadřován souhlas s obchodními podmínkami. Aby byly obchodní podmínky v rámci daného závazku platné, musí s nimi být slabší smluvní strana seznámena.<sup>468</sup> V případě „*click-wrap*“ smluv jsou často obchodní podmínky druhé smluvní straně poskytnuty tak, že se k nim musí prokliknout prostřednictvím hypertextového odkazu. Aby se tak druhá smluvní strana mohla s obchodními podmínkami seznámit, musí učinit další krok, a je otázka, kolik osob ho učiní a skutečně obchodní podmínky přečte.<sup>469</sup> Významu zde tedy nabývá ochrana před tzv. překvapivými obchodními podmínkami.

<sup>465</sup> § 1822 odst. 1 obč. zák.

<sup>466</sup> Specificky k tomu více viz dále také rozsudek Soudního dvora Evropské unie ze dne 5. 7. 2012 ve věci *Content Services Ltd proti Bundesarbeitskammer*, C-49/11.

<sup>467</sup> § 1798 odst. 2 obč. zák.

<sup>468</sup> § 1799 obč. zák.

<sup>469</sup> Například Dulak uvádí příklad smluvních podmínek, u kterých nikdo nerozporoval závazek prodat svou duši videoherní společnosti. Zmiňuje také jiný případ, kdy jen jeden ze tří tisíc uživatelů reagoval na výzvu k zaslání e-mailu zmíněnou v obchodních podmínkách, kdy po zaslání e-mailu měla být vyplacena odměna 1 000 USD. Na základě těchto a dalších příkladů se zaměřuje na to, zda nečíst obchodní podmínky není vlastně racionálním rozhodnutím. DULAK, A. Prečo (ne)čítat' zmluvy? In: RONOVSÁ, K., HAVEL, B., LAVICKÝ, P. (eds.) *Pocta prof. Janu Hurdíkovi k 70. narodeninám. Základní otázky života, práva a vübec...* / Brno: Masarykova univerzita, Právnická fakulta, 2021, s. 76 a 83.

## 10.2 Ochrana spotřebitele před překvapivými obchodními podmínkami

Občanský zákoník v § 1753 prohlašuje za neúčinné takové ustanovení obchodních podmínek, které druhá strana nemohla rozumně očekávat. Do předmětného ustanovení se promítá zásada poctivosti obsažená v § 6 obč. zák. Podle té má každý v právním styku povinnost jednat poctivě a nikdo nesmí těžit ze svého nepoctivého nebo protiprávního činu.<sup>470</sup> Překvapivost se může projevat například tak, že ustanovení obchodních podmínek bude směřovat na otázku, jež s danou smlouvou vůbec nesouvisí nebo sice souvisí, ale obvykle není v takové smlouvě řešeno.

Zda jde o překvapivé ustanovení, se posuzuje i podle způsobu jeho vyjádření, nejen jeho obsahu. Ochrana se zde tedy poskytuje i například proti provedení některých ustanovení obchodních podmínek tak malým písmem, že jsou téměř nečitelné.<sup>471</sup> Případnou překvapivost ustanovení bude třeba také posuzovat podle předmluvní komunikace stran. Pokud tedy bude reklama nebo jiný způsob návrhu způsobit v druhé straně nějakou představu, ale daná věc bude v obchodních podmínkách řešena naprosto odlišně, mělo by také jít o překvapivé ustanovení ve smyslu § 1753 obč. zák.<sup>472</sup>

Kromě překvapivých ujednání zakazuje občanský zákoník výslovně ujednání uvedená v § 1814 obč. zák. Jde například o ujednání, která:

- vylučují nebo omezují práva spotřebitele z vadného plnění nebo na náhradu újmy,
- zakládají podnikateli právo odstoupit od smlouvy bez důvodu, zatímco spotřebiteli tato možnost poskytnuta není,
- dovolují podnikateli, aby ze své vůle jednostranně měnil práva či povinnosti stran,
- odkládají určení ceny až na dobu plnění závazku, či
- zbavují spotřebitele práva podat žalobu.<sup>473</sup>

<sup>470</sup> Tato ochrana bude poskytována bez ohledu na to, zda dotčenou smluvní stranou bude podnikatel či spotřebitel.

<sup>471</sup> BEJČEK, J., Některá úskalí racionality obchodních podmínek. *Právní rozhledy* [online]. 2015, č. 18 [cit. 9. 7. 2020]. Dostupné z: <http://www.beck-online.cz>

<sup>472</sup> PELIKÁNOVÁ, I., PELIKÁN, R. Komentář k § 1753. In: ŠVESTKA, J., DVOŘÁK, J., FIALA, J. a kol. *Občanský zákoník. Komentář. Svazek V*. Praha: Wolters Kluwer, 2014, s. 75.

<sup>473</sup> Dle § 1815 obč. zák. se k těmto ujednáním nepřihlíží, ledaže se jich spotřebitel dovolá.

Obchodní podmínky druhé smluvní straně nicméně nebude možno poskytovat pouze proklikem přes hypertextový odkaz. Takový způsob by bez dalšího (jak rozebíráme dále) byl v rozporu se směrnicí Evropského parlamentu a Rady 2011/83/EU o právech spotřebitelů. Ta totiž vyžaduje, aby obchodní podmínky byly uloženy na trvalém nosiči, čímž rozumí jakýkoli přístup, který umožňuje spotřebiteli nebo obchodníkovi ukládat informace určené jemu osobně, a to způsobem vhodným pro jejich budoucí použití, po dobu přiměřenou jejich účelu, a který umožňuje reprodukci uložených informací v nezměněném stavu. Užití trvalého nosiče je důležité pro zajištění budoucí nezměnitelnosti obchodních podmínek, za kterých spotřebitel smlouvu uzavřel (a kterých se potenciálně s odstupem času poté dovolává).

### 10.3 Přípustnost poskytování obchodních podmínek hypertextovým odkazem

Poskytování obchodních podmínek pouze hypertextovým odkazem se věnoval Soudní dvůr Evropské unie v rozhodnutí C-49/11.<sup>474</sup> V této věci společnost Content Services poskytovala různé online služby na svých internetových stránkách. Prostřednictvím nich bylo zejména možné stáhnout bezplatný software nebo placené demoverze softwaru. Při odeslání své objednávky museli uživatelé zaškrtnutím políčka kontrolním znaménkem ve formuláři prohlásit, že souhlasí se všeobecnými obchodními podmínkami a že se vzdávají práva odstoupit od smlouvy. Informace týkající se práva odstoupit od smlouvy, se nezobrazovaly uživatelům přímo, ale mohli se s nimi seznámit až kliknutím na hypertextový odkaz nacházející se na stránce, kterou za účelem uzavření uvedené smlouvy vyplňují. Po odeslání objednávky uživatel obdržel e-mail potvrzující objednávku, avšak tento e-mail neobsahoval žádný údaj o právu odstoupit od smlouvy.<sup>475</sup>

Soudní dvůr dospěl k závěru, „že čl. 5 odst. 1 směrnice 97/7 musí být vykládán v tom smyslu, že obchodní počínání, které spočívá ve zpřístupnění informací uvedených v tomto ustanovení pouze prostřednictvím hypertextového odkazu na internetové stránky dotyčného podniku, nespĺňuje požadavky stanovené v uvedeném ustanovení, neboť tyto

<sup>474</sup> Rozsudek Soudního dvora Evropské unie ze dne 5. 7. 2012, ve věci *Content Services Ltd v. Bundesarbeitskammer*, C-49/11.

<sup>475</sup> Bod 18 až 20 rozhodnutí C-49/11.

*informace nejsou ani tímto podnikem ‚poskytnuty‘, ani spotřebitelem ‚obdrženy‘ ve smyslu téhož ustanovení, a že takové internetové stránky, jako jsou stránky dotčené v původním řízení, nelze považovat za ‚stálý komunikační prostředek‘ ve smyslu uvedeného čl. 5 odst. 1.*<sup>476</sup> Dané je tak i na základě tohoto rozhodnutí v praxi často zhojeno například tím, že k emailu potvrzujícího objednávku jsou rovněž přiloženy (a tudíž zafixovány) dané obchodní podmínky, případně prodávající rovněž transparentně konkrétní časové verze obchodních podmínek zveřejňuje v rámci přehledu na svém webu.

I po uzavření smlouvy občanský zákoník poskytuje spotřebitelům ochranu. Ti si při objednání zboží přes internet nemohou prohlédnout zboží v kamenném obchodě, a proto mají možnost odstoupit od smlouvy. Podnikatel se v případě těchto smluv tak může dostat do krátkodobě nejisté situace s ohledem na právo spotřebitele podle § 1829 odst. 1 obč. zák. odstoupit od smlouvy ve lhůtě 14 dnů ode dne uzavření smlouvy, resp. ode dne převzetí zboží v případě kupní smlouvy, ode dne převzetí poslední dodávky zboží u smluv, jejichž předmětem je několik druhů zboží nebo dodání několika částí, či ode dne převzetí první dodávky zboží u smluv, jejichž předmětem je pravidelná opakovaná dodávka zboží.<sup>477</sup> Tato lhůta k odstoupení od smlouvy se také může prodloužit až na jeden rok a 14 dní, pokud spotřebitel nebyl poučen o právu odstoupit od smlouvy – pokud však spotřebitel byl v této lhůtě poučen o právu odstoupit od smlouvy, běží čtrnáctidenní lhůta pro odstoupení od obdržení poučení. Podnikatel je tedy významně motivován, aby tuto informační povinnost vůči spotřebiteli dodržel.

## 10.4 Ochrana spotřebitele v souvislosti s digitálním obsahem

Nově je pak od 6. 1. 2023 specificky poskytnuta spotřebiteli ochrana v souvislosti s digitálním obsahem.<sup>478</sup> Předchozí právní úprava se dotýkala obecně nejen prodeje zboží, ale rovněž i poskytování služeb (což nebylo v rámci

<sup>476</sup> Bod 51 rozhodnutí C-49/11.

<sup>477</sup> Specificky k tomuto právu a některým důsledkům více viz LOUTOCKÝ, P. Ochrana spotřebitele při uzavírání smluv na internetu a možnost řešení vzniklých sporů online. In: POLČÁK, R. a kol. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 323 a násl.

<sup>478</sup> Změnu přinesla novela provedená zákonem č. 374/2022 Sb., kterým se mění zákon č. 634/1992 Sb., o ochraně spotřebitele, ve znění pozdějších předpisů, a zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

implementace do občanského zákoníku specificky reflektováno). Nyní, na základě směrnice o poskytování digitálního obsahu a digitálních služeb<sup>479</sup> a její implementace zejména do § 2389a až § 2389 obč. zák. (ale nikoli bezvýhradně), došlo přímo k zakotvení problematiky poskytování digitálních služeb a digitálního obsahu. To je příhodné i vzhledem k tomu, že tato oblast smluvního jednání online nabývá na stále větším významu a bylo nezbytné specificky reflektovat charakter těchto produktů.<sup>480</sup> Jedná se typicky o poskytování jakéhokoli softwarového řešení (včetně například počítačových her), *streamingových* služeb apod.

Jádrem celé této právní úpravy je především poskytnout subjektivní a objektivní předpoklady pro posouzení, jestli je poskytovaná služba v souladu se smlouvou či s indikovanými vlastnostmi produktu. Jedná se o předpoklady, které vzhledem ke specifickému charakteru softwaru a digitálních služeb dokážou poskytnout vhodné podmínky pro porovnání konformity služby či obsahu jak v rámci smluvních očekávání spotřebitele, tak případně pro porovnání s obdobnou konkurencí na trhu. V případě porušení stanovených podmínek je pak v rámci právní úpravy poskytnuta jak možnost nápravy,<sup>481</sup> snížení ceny za poskytovanou službu, tak i možnost ukončení smlouvy a v hraničním případě vrácení celé ceny za službu.<sup>482</sup>

<sup>479</sup> Směrnice Evropského parlamentu a Rady (EU) 2019/770 ze dne 20. května 2019 o některých aspektech smluv o poskytování digitálního obsahu a digitálních služeb.

<sup>480</sup> Viz bod odůvodnění 1 a násl. 23 apod. směrnice Evropského parlamentu a Rady (EU) 2019/770 ze dne 20. května 2019 o některých aspektech smluv o poskytování digitálního obsahu a digitálních služeb.

<sup>481</sup> Čl. 9 a 13 směrnice.

<sup>482</sup> Čl. 15 a násl. směrnice.

### **III. VYUŽITÍ DIGITÁLNÍCH TECHNOLOGIÍ PO UZAVŘENÍ SMLOUVY**





## 11 ROSTOUCÍ POTENCIÁL UPLATNĚNÍ DIGITÁLNÍCH TECHNOLOGIÍ PO UZAVŘENÍ SMLOUVY

V předchozí části bylo pojednáno o řadě kontextů, ve kterých dochází k elektronizaci procesu kontraktace a byly podrobně představeny stěžejní i doprovodné technologie typu elektronického podpisu, datových schránek či kontraktačních platforem, kterým se dostává stále širšího uplatnění i při soukromoprávním jednání. Současně byly nastíněny budoucí trendy, resp. další technologie či koncepty, se kterými je spojována možnost posunu k vyšší důvěře a bezpečnosti uzavírání smluv online, ať se jedná o technologii *blockchain* či Evropskou peněženku digitální identity.

Uzavřením smlouvy online však prostor pro uplatnění elektronických nástrojů nekončí. Již při představení smart kontraktů jsme zmiňovali možnosti automatizace plnění smlouvy a tím i mitigace klíčové právní nejistoty, která je se smluvním jednáním úzce spojena – neplnění závazku druhou smluvní stranou. Byť je tato záruka plnění vyzdvihována právě v kontextu smart kontraktů, algoritmizace,<sup>483</sup> či přímo automatizace plnění na základě uzavřené smlouvy prostupuje množství dalších procesů navazujících na uzavření smlouvy online. Zavedení postupů či nástrojů, které snižují pravděpodobnost, že smluvní strana nesplní svůj smluvní závazek, je totiž zcela přirozeně v zájmu všech smluvních stran uzavírajících příslušnou smlouvu v dobré víře.

S technologií *blockchain* a zajištěním plnění ze smlouvy skrze automatický algoritmus smart kontraktu se pojí myšlenka záruky, že k plnění protistrany dojde i bez potřeby spoléhat na její dobrou víru. Takové řešení si ovšem svou výhodnost udrží pouze při kontraktaci mezi smluvními stranami, které nepředpokládají, že druhá strana bude dobrovolně jednat v dobré víře, tzn. bude mít zájem a snahu plnit dle uzavřené smlouvy. Technologie jim

<sup>483</sup> Ve smyslu rozložení úlohy do etap a způsobu jejich řešení, které dává přesný návod k jejímu vyřešení a umožňuje tak řešení úlohy programovat, tedy vyjádřit v konkrétním programovacím jazyce způsobem, který bude pro srozumitelný pro recipienta. V kontextu elektronických technologií jde pak zpravidla o programovatelnost v podobě software pro dané výpočetní zařízení či systém zařízení.

pak nabízí záruku, že je možnost neplnit protistraně z podstaty fungování smart kontraktu v konečném důsledku upřena (to ovšem, jak bylo přiblíženo výše, zpravidla včetně situací, kdy neplnění protistrany mohlo být po právu). Nástroje, o kterých pojednáváme v této kapitole však v zásadě tuto kvalitu nemají, slouží zpravidla jedné či oběma stranám k optimalizaci procesů spojených s plněním, nikoliv ke garanci, že plněno bude.

Věříme, že pro významnou většinu běžného právního jednání v online prostředí platí a bude i do budoucna platit, že smluvní strany k uzavření smlouvy přistupují s přiměřenou opatrností. K té patří mj. i předsmluvní subjektivní vyhodnocení důvěryhodnosti protistrany a pravděpodobnosti, že do smlouvy vstupuje v dobré víře plnit a dostát svým závazkům. Přidaná hodnota nástrojů, které umožňují automatizovat či garantovat plnění je tak podle nás spíše v usnadnění a urychlení souvisejících procesů dané smluvní strany než v garanci plnění od protistrany bez ohledu na její vůli plnit.

Konkrétně například, v tomto smyslu očekáváme, že za běžných okolností k objednání zboží přistoupí zákazník na e-shopu až poté, co přiměřeně nabyl dojmu, že mu bude zboží ve sjednané kvalitě a ve sjednaném termínu skutečně zasláno. Pro usnadnění tohoto vyhodnocení mu slouží mj. rámec ochrany spotřebitele, ale je samozřejmě možné, že tento dojem bude i přesto mylný, to však podle nás bude spíše výjimka, nikoliv pravidlo. Není tedy z tohoto pohledu nezbytné či zásadně přínosné, aby proces zajištění plnění na základě sjednané smlouvy byl mimo kontrolu protistrany, protože neslouží k překonání nedůvěry v její jednání v dobré víře, ale především k zefektivnění či organizaci jednání protistrany na základě smlouvy a výsledně ve prospěch naplnění účelu a smyslu uzavřené smlouvy.

Možnost automatizace plnění je pak do značné míry vázána na jeho podobu; pro přiblížení zvažme rozdíly při zpřístupnění digitálního obsahu, doručení fyzické zásilky či poskytnutí personalizované služby.

## 11.1 Smlouvy o poskytování digitálního obsahu

V případě, že má plnění ze smlouvy nehmotnou podstatu vyjádřenou elektronicky, a jde tedy např. o převod záznamů mezi účty či zpřístupnění digitálního obsahu online, je přenesení potřebných kroků pro plnění dle příslušné smlouvy zpravidla přímočaré a ze své podstaty snadno algoritimizovatelné.

Plnění na základě příkazu k nákupu cenných papírů přes online *brokeru* tudíž v principu proběhne automaticky, stejně jako zpřístupnění zakoupeného digitálního obsahu na platformách jako je GOG.com.<sup>484</sup> I při složitějších právních strukturách pro přistoupení k digitálnímu obsahu, jako je například zakoupení přístupu k videohře na platformě Ubisoft Connect<sup>485</sup> skrze zprostředkovatele Humble Bundle<sup>486</sup>, ke které uživatel následně přistupuje přes přihlášení pomocí účtu registrovaného na platformě Steam<sup>487</sup>, jde o sekvenci automatizovaných procesů, které zajišťují plnění na základě uzavřených smluv v zásadě obratem na splnění potřebných kroků či vstupů ze strany zákazníka.

## 11.2 Smlouvy na nákup zboží přes e-shop

U nákupu hmotného zboží přes e-shop do plnění nevyhnutelně vstupuje řada limitací fyzické povahy, které jsou u digitálního obsahu přenášeného v kyberprostoru marginalizovány. Přesto dochází při plnění zpravidla k sekvenci kroků, které jsou předvídatelné a v současné době stále častěji strojově zajišťované. Příkladem je automatizovaná logistika u velkých hráčů v prostředí elektronického obchodu, jako je Amazon, který v tomto směru dosáhl v roce 2023 významných pokroků ve spolupráci s klíčovým hráčem AI technologií, společností NVIDIA<sup>488</sup>. Ta přitom stojí nejen na pokroku v automatizaci správy logistických center, ale i v odpovídající správě datových toků a koordinaci činností, což je také oblast, která doznává značných pokroků i díky stále rozsáhlejšímu využití strojového učení. Jako u řady služeb v moderní společnosti pak dochází vzhledem ke komplexnosti a náročnosti rozvoje a k tendenci zajištění těchto pokročilých služeb skrze dominantní

<sup>484</sup> Srov. GOG User Agreement. *GOG.com* [online]. 2020 [cit. 25. 10. 2023]. Dostupné z: <https://support.gog.com/hc/en-us/articles/212632089-GOG-User-Agreement?product=gog>

<sup>485</sup> Srov. UBISOFT TERMS OF USE. *UBISOFT* [online]. 2020 [cit. 25. 10. 2023]. Dostupné z: <https://legal.ubi.com/termsfuse/en-US>

<sup>486</sup> Srov. Terms and Conditions. *Humble Bundle* [online]. 2023 [cit. 25. 10. 2023]. Dostupné z: <https://www.humblebundle.com/terms>

<sup>487</sup> Linking your Steam and Ubisoft accounts. *UBISOFT* [online]. 2023 [cit. 25. 10. 2023]. Dostupné z: <https://www.ubisoft.com/en-gb/help/account/article/linking-your-steam-and-ubisoft-accounts/000066792>

<sup>488</sup> Viz NVIDIA's cutting-edge groundbreaking platform for AI-robotics. *Warehouse Automation* [online]. 2023 [cit. 25. 10. 2023]. Dostupné z: <https://www.warehouseautomation.ai/top-stories/nvidia-brings-advanced-autonomy-to-mobile-robots-9mn25>

či oligopolní platformy (podobně jako u online vyhledávání či služeb online reklamy)<sup>489</sup>.

### 11.3 Smlouvy na poskytování služeb či personalizovaného plnění

U poskytování služeb či personalizovaného plnění pak vyvstává řada dalších překážek a výzev, které činí plnou automatizaci plnění zpravidla nedosažitelnou či alespoň za současné technologické úrovně neekonomickou. To však neznamená, že nenarůstá spektrum a kvalita nástrojů, které i tento druh plnění usnadňují a část dříve manuálních činností nahrazují automatizovaným strojovým procesem. Nejzřetelnější role těchto nástrojů lze vnímat ve správě závazků, komunikaci smluvních stran a podpoře při vytváření předmětu plnění.

#### 11.3.1 Organizační a plánovací nástroje

Stále častější je, především v rámci rozsáhlejších entit či entit s velkým množstvím různorodých smluvních závazků, uplatnění podpůrných nástrojů na správu a organizaci smluvních závazků či jiných nástrojů, které řeší rozdělení úkolů mezi zaměstnanci, příp. třetími subjekty, ověřují dodržování harmonogramu plnění (např. v případě platebních závazků) a notifikují či informují relevantní strany o vývoji či případných překážkách s plněním. V této oblasti roste uplatnění strojového učení a nástrojů pro rozeznání a převod textu či obsahu do digitální podoby pro další automatizované zpracování. Je tak umožněno efektivně digitalizovat a následně zahrnout do procesů i dokumentaci, která nebyla subjektu zpřístupněna elektronicky, příp. má podobu grafického, nikoliv textového vyjádření (např. sken či fotografie faktury)<sup>490</sup>.

<sup>489</sup> Srov. PASUMARTI, M., MOHANTY, S., ZEKPA, N. Automate Document Processing in Logistics using AI. *AWS* [online]. 1. 8. 2021 [cit. 25. 10. 2023]. Dostupné z: <https://aws.amazon.com/blogs/architecture/automate-document-processing-in-logistics-using-ai/>

<sup>490</sup> Do velké míry synonymem pro tyto nástroje jsou nejen v evropském prostředí produkty německé softwarové společnosti SAP. Srov. Produkty SAP. *SAP* [online]. 2023 [cit. 25. 10. 2023]. Dostupné z: <https://www.sap.com/cz/products.html>. Další příklady nástrojů nabízí např. 5 Key Ways How Artificial Intelligence in Contract Lifecycle Management Brings Value. *DocuCollab* [online]. 2020 [cit. 25. 10. 2023]. Dostupné z: <https://docucollab.com/5-key-ways-how-ai-brings-value-to-contract-lifecycle-management/>

### 11.3.2 Asistenční komunikační nástroje a nástroje pro online řešení sporů

Vedle organizačních a plánovacích nástrojů nabývá rostoucím tempem na významu, především od zveřejnění první veřejné verze ChatGPT, využití asistenčních komunikačních nástrojů na bázi generativní AI. Své chatboty zákaznické podpory zajišťující (polo)automatizaci vyřizování reklamací, poskytování informací či řešení běžných požadavků protistrany – zejména spotřebitele – má stále více subjektů napříč sektory.<sup>491</sup> Při vhodném nastavení mají zřetelné výhody ve srovnání s personálním zajištěním srovnatelné zákaznické podpory, a to ať už v neomezené časové dostupnosti, nákladovosti či nikoliv nevýznamné konsistenci odpovědí na stejné dotazy, s čímž souvisí větší prostor pro zkvalitňování zákaznických služeb a zpřesňování informací, které jsou zákazníkům na vyžádání komunikovány. Jsou zde samozřejmě přetrvávající limity v podobě dotazů či formulací dotazů, na které chatbot není schopen adekvátně reagovat pro jejich vychýlení od naučeného algoritmu či dostupných vstupů. I proto zůstanou zřejmě i v dohledné době nejefektivnějším řešením hybridní modely, kdy chatbot představuje pouze první úroveň zákaznické podpory, která je doplněna o druhou v podobě specializovaného personálu.<sup>492</sup>

Související, ale často i specificky zřizované uplatnění nacházejí chatboti v řešení sporů online (ODR), kde je ovšem na místě reflektovat nejen přínosy spojené s charakteristickými vlastnostmi strojové konverzace na základě učícího algoritmu, ale též její přetrvávající či inherentní nedostatky, které, podobně jako u zákaznické podpory, vedou k preferenci hybridního uplatnění

<sup>491</sup> Analýzu prostředí nabízí např. KELLY, S., KAYE, S.-A., OVIEDO-TRESPALACIOS, O. A Multi-Industry Analysis of the Future Use of AI Chatbots. *Human Behavior and Emerging Technologies* [online]. 2022, č. 14 [cit. 25. 10. 2023]. Dostupné z: <https://doi.org/10.1155/2022/2552099>. Aktualizovaný přehled kontextů pro uplatnění chatbotů pak poskytuje např. DILMEGAMI, C. 30+ Chatbot Use Cases/Applications in Business (2023 Update). *AIMultiple* [online]. 12. 10. 2023 [cit. 25. 10. 2023]. Dostupné z: <https://research.aimultiple.com/business-chatbot/>

<sup>492</sup> Srov. DAUGHERTY, P., GHOSH, B., NARAINOS, K., GUAN, L., WILSON, J. A new era of generative AI for everyone. *Accenture* [online]. 2023, č. 23, s. 16 [cit. 25. 10. 2023]. Dostupné z: <https://www.accenture.com/us-en/insights/technology/generative-ai>

ve spojení s tradičnějšími přístupy<sup>493</sup>. Síla těchto nástrojů se pak projevuje zejména ve fázích automatizovaného vyjednávání mezi účastníky,<sup>494</sup> které má ale v rámci nezávazných forem ODR potenciál pro eliminaci velkého počtu sporů,<sup>495</sup> čemuž právě automatizované nástroje mohou dále přispět.

### 11.3.3 Nástroje pro vytváření či zajištění vlastního předmětu plnění

Třetí oblast, kde mají digitální nástroje stále dominantnější roli v jednotlivých krocích či celého procesu, je pak vytváření či zajištění vlastního předmětu plnění na základě uzavřené smlouvy. Zde je přitom možné snadno opominout, že digitální technologie prostupují moderní společnost natolik, že většina činností, které vycházejí (nejen) ze smluv uzavřených online, jsou zcela běžně (spolu)prováděny za pomoci digitálních technologií. Textové editory (např. Microsoft Word) slouží k vytváření nejrůznějších plnění ze smluv v textové podobě, grafické editory (např. Adobe Photoshop) jsou významným pracovním nástrojem pro vytváření graficky založených plnění, a ve stejném směru lze uvažovat množství dalších nástrojů, ať se jedná o nástroje pro tvorbu a editaci audiovizuálního obsahu (např. Riverside) či technické kreslení (např. AutoCAD). Všechny tyto nástroje jsou využívány na základě odpovídajících licenčních smluv a jejich využití pro smluvní plnění může vytvářet dílčí právní vazby (např. ukládání dat v cloudovém úložišti, popř. sdílení metadat či záznamů o užívání nástroje). Podobně lze nahlížet na stále častěji využívané online nástroje pro překlad (např. DeepL), které mají se svým užitím spojené podmínky, které mohou být pro využití dat v rámci plnění smlouvy relevantní<sup>496</sup>. Se strmým rozvojem nástrojů na bázi umělé

<sup>493</sup> Blíže viz ALESSA, H. The role of Artificial Intelligence in Online Dispute Resolution: A brief and critical overview. *Information & Communications Technology Law* [online]. 2022, roč. 31, č. 3, s. 319–342 [cit. 25. 10. 2023]. ISSN 1360-0834. DOI: <http://doi.org/10.1080/13600834.2022.2088060>

<sup>494</sup> Více viz: SUSSKIND, R. *Online Courts and the Future of Justice*. Oxford: Oxford University Press, 2019, č. 347, s. 98 a násl.

<sup>495</sup> Více viz LOUTOCKÝ, P. *Výmahatelnost práva pomocí online řešení sporů*. 1. vyd. Praha: Woltes Kluwer, 2020, 217 s., s. 26 a násl. ISBN 978-80-7598-752-5.

<sup>496</sup> Srov. DeepL Pro – Terms and Conditions. *DeepL* [online]. 2023 [cit. 25. 10. 2023]. Dostupné z: <https://www.deepl.com/en/pro-license>

inteligence založené na strojovém učení rozsáhlých jazykových modelů<sup>497</sup> přibývá rozsah, ve kterém mohou být využity při plnění smluvních závazků. Nástroje, jako je Legito, slouží k automatizaci řady kroků při vytváření právních či jiných formalizovaných dokumentů, nástroje typu DALL-E<sup>498</sup> jsou užívány pro vytváření obrazového výstupu z textových vstupů, a například AudioCraft slouží pro vytváření audio obsahu. Všechny tyto nástroje mají transformativní charakter, který významně dopadá na celé spektrum činností a přináší přitom s sebou množství nových otázek a výzev pro právní rámce sahající od ochrany osobních údajů přes práva z duševního vlastnictví po ochranu obchodního tajemství a vnitropodnikové politiky pro přípustné využívání těchto nástrojů.

## 11.4 Rostoucí význam digitální stopy smluvního vztahu

Tyto technologické posuny přinášejí novou dynamiku i do oblastí, které šířeji souvisejí s uplatněním digitálních technologií ve vazbě na uzavřenou smlouvu online. S rostoucí centralitou digitálních nástrojů napříč celým cyklem smluvního vztahu nabývá na významu jeho digitální stopa, která při vhodném přístupu přináší zřetelné výhody pro smluvní strany a uplatnění jejich nároků. Vymáhání závazků z elektronicky uzavřených smluv má proto v důsledku svá specifika, resp. skýtá dodatečné možnosti, kterým se budeme podrobně věnovat dále. Předtím však pokládáme za vhodné přiblížit prostředí a možnosti elektronické archivace, jelikož ústředním elementem pro vymáhání závazků je shromáždění odpovídajících elektronických důkazů, ze kterých lze rekonstruovat potřebnou část digitální stopy relevantních událostí. Pro ty je přitom digitální archivace významným zdrojem a s ohledem na rostoucí digitalizaci činností napříč entitami, kterou jsme se snažili v této kapitole nastínit, její význam stále narůstá.

<sup>497</sup> K pojmu viz např. MEARIAN, L. What are LLMs, and how are they used in generative AI? A brief and critical overview. *ComputerWorld* [online]. 30. 5. 2023 [cit. 25. 10. 2023]. Dostupné z: <https://www.computerworld.com/article/3697649/what-are-large-language-models-and-how-are-they-used-in-generative-ai.html>

<sup>498</sup> DALL·E 3. *OpenAI* [online]. 2023 [cit. 25. 10. 2023]. Dostupné z: <https://openai.com/dall-e-3>





## 12 ELEKTRONICKÁ ARCHIVACE PRÁVNÍCH JEDNÁNÍ

### 12.1 Obecně k elektronické archivaci

Rozdíl mezi vlastnoručně a elektronicky podepsanou smlouvou lze spatřovat i v oblasti jejich dlouhodobého uchovávání. Listinné smlouvy mohou s plynutím času ztrácet svou informační hodnotu – inkoust bledne nebo se rozpíje, může dojít k mechanickému zničení listiny, ztrátě její části či celé listiny. Tomu se dá v případě smluv v podobě elektronických dokumentů s ohledem na libovolný počet jejich kopií předejít. Dlouhodobá použitelnost elektronických smluv však může narazit na záležitost, která by jinak byla vnímána pozitivně – na technologický vývoj. Mění se jak formáty elektronických dokumentů, tak i prostředky, na kterých jsou uloženy. Problém s různými formáty, jejich vývojem a změnami lze s určitým úsilím či náklady překlenout. Jinou otázkou jsou však prostředky, na nichž jsou dokumenty uloženy. Běžný uživatel nyní například nebude bez vynaložení dodatečných nákladů schopný otevřít dokument uložený na 3,5palcové disketě, natož na disketě o velikosti 5,25 palců nebo dokonce starší 8palcové. Málokdo již bude mít běžně k dispozici mechaniku pro zpřístupnění dat z CD. Dokumenty jsou nyní ukládány na různá záznamová zařízení uživatelů či cloudová úložiště. Další vývoj v této oblasti je podle našeho názoru předvídatelný pouze omezeně.<sup>499</sup> Je proto nutné při zvažování užití listin či elektronických dokumentů brát v úvahu i tyto souvislosti.

Archivaci a použitelnost dokumentů je třeba zvažovat i v souvislosti s možností dlouhodobě ověřovat jejich pravost. V případě listinného dokumentu je třeba vzít v úvahu zejména mechanické vlivy. Ověřovací doložka na listinné smlouvě může ztratit v důsledku času svou informační a důkazní hodnotu.

<sup>499</sup> Například soudce Easterbrook ve svém slavném článku o autorském právu v kyberprostoru *Cyberspace and the Law of the Horse* tvrdil, že přesvědčení právníků ohledně počítačů, a predikce, které ohledně nových technologií dělají, budou s vysokou pravděpodobností špatné. Také skromně uváděl: „*O kyberprostoru toho moc nevím; to, co vím, bude za pět let (ne-li za pět měsíců!) zastaralé; a mé předpovědi o směru změn jsou bezcenné, takže jakákoli snaha přizpůsobit zákon tomuto tématu je zbytečná.*“ EASTERBROOK, F. H. *Cyberspace and the Law of the Horse. The University of Chicago Legal Forum*. 1996, č. 207, s. 207.

U elektronicky podepsaných dokumentů může být ale závažnějším problémem ověření certifikátů elektronických podpisů v delším časovém horizontu. Pro něj je třeba, aby byla stále k dispozici certifikační autorita, která certifikát vydala, resp. aby byla k dispozici data, na základě kterých lze elektronický podpis ověřit. Navíc v současnosti vydávané kvalifikované certifikáty pro vytváření elektronických podpisů se z dnešního pohledu zdají bezpečné, nicméně optikou budoucího technického vývoje však jejich podvržení nemusí být tak složité.

## 12.2 Další relevantní služby vytvářející důvěru

Nařízení eIDAS a zák. o službách vytvářejících důvěru znají další služby vytvářející důvěru, kterými lze zvýšit důvěryhodnost elektronického právního jednání. Těmi jsou v kontextu této monografie elektronická pečeť a elektronické časové razítko. V případě elektronických pečeti je třeba vyjasnit jejich odlišnost oproti elektronickým podpisům, jelikož v praxi se lze příležitostně setkat s nepochopením jejich smyslu. Elektronické časové razítko má v elektronické kontraktaci také své místo, proto mu také dále krátce věnujeme pozornost.

### 12.2.1 Elektronická pečeť<sup>500</sup>

Před účinností nařízení eIDAS a zák. o službách vytvářejících důvěru byl v českém právním řádu pro elektronické pečeti používán pojem „elektronická značka“.<sup>501</sup> Tou zák. o el. podpisu rozuměl údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které splňovaly následující požadavky:

1. jednoznačné spojení s označující osobou a umožnění její identifikace prostřednictvím kvalifikovaného systémového certifikátu,
2. vytvoření a připojení k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba mohla udržet pod svou výhradní kontrolou,

<sup>500</sup> Následující text částečně vychází z textu JAREŠ, A. Nařízení eIDAS, elektronický podpis a pečeť v českém právním řádu. In: SEDLÁČEK, M., STŘELEČEK, T. a kol. *Právní jednání a procesní úkony (vzájemné vztahy a nové aspekty)*. Praha: Wolters Kluwer, 2019, s. 19–26.

<sup>501</sup> Pojem „elektronická značka“ byl tak zažitý, že jej lze stále příležitostně nalézt i v aktuální literatuře – viz např. LECHNER, T. *Nařízení eIDAS a české adaptační zákony. Komentář*. Praha: Wolters Kluwer, 2023, s. 316 a 338.

3. připojení k datové zprávě, ke které se vztahují, takovým způsobem, že bylo možné zjistit jakoukoli následnou změnu dat.<sup>502</sup>

Označující osobou mohla být podle této úpravy fyzická osoba, právnická osoba nebo organizační složka státu.<sup>503</sup>

Elektronické pečete bývají někdy chybně považovány za elektronický podpis právnické osoby – fyzické osoby by podle tohoto předpokladu měly používat elektronický podpis, právnické osoby elektronickou pečeť. Částečně by tomu sice mohl napovídat bod odůvodnění 58 nařízení eIDAS, podle kterého: „[v]yžaduje-li transakce kvalifikovanou elektronickou pečeť právnické osoby, měl by být stejně tak přijatelný kvalifikovaný elektronický podpis oprávněného zástupce této právnické osoby“. Elektronická pečeť se však nepoužívá k podepisování, ale zaručuje původ a integritu elektronického dokumentu, resp. elektronických dat.<sup>504</sup> S kvalifikovanou elektronickou pečeti je spojena domněnka integrity a správnosti dat.<sup>505</sup> Navíc vztah mezi elektronickým podpisem a pečeti nařízení eIDAS vyjasňuje v článku 3. V odstavci 9 rozumí podepisující osobou fyzickou osobu, která vytváří elektronický podpis. A v odstavci 24 tento článek rozumí pečeti osobou právnickou osobu, která vytváří elektronickou pečeť. Elektronickou pečeť lze tedy použít k autentizaci dokumentu, například k automatickému označování (pečetění) automaticky generovaných a vypravovaných dokumentů či jinému potvrzování původu dokumentu.<sup>506</sup>

Pokud by uvedené mělo být zjednodušeno, lze konstatovat následující:

- Elektronický podpis je součástí projevu vůle a podmínka platnosti písemného právního jednání<sup>507</sup> (pokud právní jednání nesplňuje podmínky dle § 562 odst. 1 obč. zák. a je třeba ho opatřit elektronickým podpisem dle § 561 odst. 1 obč. zák.).
- Elektronická pečeť potvrzuje, že určitý elektronický dokument (elektronická data) vznikla v prostředí určité právnické osoby a v podobě, která byla opatřena elektronickou pečeti.

<sup>502</sup> § 2 písm. c) zák. o el. podpisu.

<sup>503</sup> § 2 písm. f) zák. o el. podpisu.

<sup>504</sup> Srov. čl. 3 odst. 25 eIDAS: „[elektronickou pečeti se rozumí] data v elektronické podobě, která jsou připojena ke jiným datům v elektronické podobě nebo jsou s nimi logicky spojena s cílem zaručit jejich původ a integritu.“

<sup>505</sup> Čl. 35 odst. 2 eIDAS.

<sup>506</sup> POLČÁK, 2011, op. cit., s. 57.

<sup>507</sup> Srov. § 561 odst. 1 obč. zák.

Nicméně ve specifických situacích lze alternativně užít elektronickou pečeť nebo elektronický podpis. Tak je tomu například v případě zákona č. 125/2008 Sb., o přeměnách obchodních společností a družstev. Ten předepisuje povinnost podepsat uznávaným elektronickým podpisem nebo zapečetit uznávanou elektronickou pečeti dokumenty dle svého § 33b. Podobně dříve před 1. 10. 2023 zákoník práce považoval písemnost určenou zaměstnavateli doručovanou prostřednictvím sítě nebo služby elektronických komunikací za doručenu dnem, kdy její převzetí potvrdí zaměstnavatel zaměstnanci datovou zprávou podepsanou svým uznávaným elektronickým podpisem nebo zapečetěnou svou uznávanou elektronickou pečeti.

Narizení eIDAS podobně jako v případě elektronického podpisu nejdříve definuje elektronickou pečeť jako data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena s cílem zaručit jejich původ a integritu (čl. 3 odst. 25 eIDAS). Dále zavádí zaručenou elektronickou pečeť, která musí splňovat požadavky stanovené v čl. 36 eIDAS. V jejím případě musí být splněny podmínky:

- a) jednoznačného spojení s pečeti osobou;
- b) umožnění její identifikace;
- c) vytvoření pomocí dat pro vytváření elektronických pečeti, která může pečeti osoba s vysokou úrovní důvěry použít k vytváření elektronické pečeti pod svou kontrolou; a
- d) připojení k datům, ke kterým se vztahuje, takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat.

Podle čl. 3 odst. 27 eIDAS je pak kvalifikovanou elektronickou pečeti zaručená elektronická pečeť, která je vytvořena pomocí kvalifikovaného prostředku a je založena na kvalifikovaném certifikátu.

S elektronickými pečeti zák. o službách vytvářejících důvěru pracuje podobně jako s elektronickým podpisem – nejprve ve svém § 8 stanovuje, v jakých případech je nutné použít kvalifikovanou elektronickou pečeť. Poté v § 9 odst. 1 uvádí, kdy je třeba užít uznávanou elektronickou pečeť. Tou ale opět zákon v § 9 odst. 2 rozumí kvalifikovanou elektronickou pečeť a zaručenou elektronickou pečeť založenou na kvalifikovaném certifikátu.

### 12.2.2 Elektronické časové razítko

Technické pozadí mají elektronická časová razítka obdobně jako elektronické podpisy (a pečete), nicméně jejich účel je jiný – tím je prokázání existence určitých dat v daném okamžiku.<sup>508</sup> Tuto skutečnost pak technicky ani podpisy ani pečete nejsou schopny prokázat – přestože je v certifikátu uveden čas podepsání, jedná se jen o systémový čas (například počítače, ze kterého je podepisováno), který nemusí odpovídat realitě, a nikoli o čas objektivně platný.<sup>509</sup> Elektronickým časovým razítkem nařízení eIDAS rozumí data v elektronické podobě, která spojují jiná data v elektronické podobě s určitým okamžikem a prokazují, že tato jiná data existovala v daném okamžiku.<sup>510</sup> Stejně jako v případě podpisů a pečeti zná nařízení eIDAS i kvalifikované elektronické časové razítko, jehož smysl je v důvěryhodném spojení dat v elektronické podobě s přesným časovým okamžikem a zaručení existence těchto dat před tímto časovým okamžikem.<sup>511</sup>

Donát s Tomíškem poukazují na smysl elektronických časových razítek v právně nezpochybnitelném prokázání okamžiku, kdy právní úkon nastal, resp. že v daném okamžiku nějaký dokument existoval. Jejich smysl ukazují na příkladu odeslání a přijetí e-mailové zprávy. Mohlo by se totiž zdát, že e-mailový klient svým uživatelům zobrazí čas odeslání a doručení e-mailu, které nebude možné zpochybnit. Ve většině případů však bude e-mailový klient zobrazovat čas dle nastavení operačního systému konkrétního zařízení, který nemusí odpovídat realitě.<sup>512</sup> Elektronické časové razítko tedy podobně jako některé formy elektronického podpisu fixuje podobu dokumentu k určitému okamžiku. Není však na rozdíl od elektronického podpisu projevem vůle a podpis nijak nenahrazuje. Typicky jsou používány v rámci spisových služeb.<sup>513</sup>

<sup>508</sup> ZAJÍČEK a kol., 2021, op. cit., s. 83.

<sup>509</sup> Technicky je pak možné zažádat o kvalifikovaný elektronický podpis, který je spojen s kvalifikovaným časovým razítkem dohromady, jedná se pak o nástroj, který jednak spolehlivě prokazuje identitu podepisujícího, jednak pak rovněž prokazuje spolehlivě čas, ve které došlo k připojení podpisu/razítka k elektronickému dokumentu.

<sup>510</sup> Čl. 3 bod 33 nařízení eIDAS.

<sup>511</sup> DONÁT, PIFFL, MAISNER, 2017, op. cit., s. 159.

<sup>512</sup> DONÁT, TOMÍŠEK, 2016, op. cit., s. 142.

<sup>513</sup> POLČÁK, 2011, op. cit., s. 57.

Opatření elektronicky podepsaného dokumentu rovněž elektronickým časovým razítkem zajišťuje možnost dlouhodobě ověřovat elektronické podpisy a elektronické dokumenty.<sup>514</sup> Namísto opakovaného přerazítkování dokumentů se nicméně pro dlouhodobou archivaci a prokazatelnost dokumentů jeví jako vhodnější užití spolehlivých záznamů údajů o právních jednáních v elektronickém systému ve smyslu § 562 odst. 2 obč. zák. Na ty se zaměřuje další text.

### 12.3 Záznamy o právních jednáních při archivaci

Je třeba vzít v úvahu, že v současnosti vydávané kvalifikované certifikáty pro elektronický podpis mají omezenou platnost a po jejím skončení se při ověření elektronického podpisu jeví podpis jako neplatný. Neplatnost certifikátu je však třeba odlišit od neplatnosti podpisu či samotné smlouvy. Význam by totiž mělo mít to, zda byl podpis, resp. certifikát pro něj platný v okamžiku podepsání elektronickým podpisem.<sup>515</sup> Pokud tedy strany smlouvy nechtějí snížit důkazní spolehlivost elektronicky podepsaných smluv, je třeba technicky zajistit možnost dlouhodobě ověřit, že alespoň v okamžiku připojení podpisu byl certifikát platný. Jako nejjednodušší řešení se může nabízet pravidelné přerazítkování elektronických dokumentů elektronickými časovými razítky. V této souvislosti však Polčák varuje před „*bezbrhým optimismem vůči komerčním technickým řešením, která si kladou za cíl formou takzvaného přerazítkování uchovávat autenticitu elektronických dokumentů*“. Lze podle něj tento postup doporučit k uchovávání dokumentů nejdéle v řádu jednotek let.<sup>516</sup>

Za současného stavu poznání a legislativy se nám jako ideální řešení jeví využití elektronického systému se záznamy údajů o právních jednáních, které budou prováděny systematicky, posloupně a chráněny proti změnám, aby naplnily vyvratitelnou právní domněnku o spolehlivosti těchto záznamů podle § 562 odst. 2 obč. zák. Jejich úprava v občanském zákoníku z roku 1964 chyběla. Před účinností současného občanského zákoníku jako vhodné řešení tohoto problému nabízel Polčák kontraktační platformy, systémy pro vedení elektronické spisové služby či jiná datová uložiska. Konstatoval, že pravost

<sup>514</sup> DONÁT, PIFFL, MAISNER, 2017, op. cit., s. 130.

<sup>515</sup> Srov. KORBEL, MELZER, 2014, op. cit., s. 36.

<sup>516</sup> POLČÁK, 2011, op. cit., s. 59.

dokumentu se pak neprokazuje přímo, ale „prostřednictvím toho, že dokument ležel v příslušném standardně zabezpečeném úložišti“.<sup>517</sup>

Ke stejnému závěru dochází Korbel s Melzerem, kteří v § 562 odst. 2 obč. zák. vidí značný potenciál s ohledem na jeho preferenci uchovávání dat v profesionálním elektronickém systému spisové služby a obrácení důkazního břemene prokazování jejich spolehlivosti k tíži toho, kdo je napadá, a nikoli toho, kdo jimi dokazuje. To však za předpokladu, že bude takový systém schopen zajistit nezměnitelnost vložených dokumentů a pořizovat automaticky bez neautorizovaných zásahů a změn transakční protokol s uloženými údaji o všech operacích s dokumenty a o uživateli provádějících tyto operace. Za zbytečné pak v takovém případě považují další přepodepisování či přerazítkovávání, jelikož obdobnou činnost zajišťuje transakční protokol.<sup>518</sup>

Ustanovení § 562 odst. 2 obč. zák. považují z hlediska důkazní spolehlivosti za vhodné také Matejka a Güttler. Podle nich reflektuje moderní přístupy k podstatě elektronických písemných dokumentů a současně výrazně usnadňuje využívání typických a stále častějších forem elektronického uzavírání smluv. Hodnotí tento směr zvolený českým zákonodárcem v mnoha ohledech jako vhodnější než další autentizační mechanismy, jako přidávání je dalších kvalifikovaných podpisů, značek a razítek. Konstatují tak, že trend elektronického zpracování dokumentů vede k tomu, že jejich důkazní věrohodnost je zjišťována spíše kvalifikovaným způsobem a postupem, kterým byly vytvořeny nebo jsou dlouhodobě ukládány, než jednotlivými elektronickými podpisy v nich. Záruky zde poskytují funkční vlastnosti, architektura a design elektronického systému.<sup>519</sup>

## 12.4 Revize nařízení eIDAS a elektronická archivace

### 12.4.1 Elektronická archivace jako nová služba vytvářející důvěru

Evropská unie má prostřednictvím revize nařízení eIDAS ambice také zprostředkovat dlouhodobou důvěryhodnou archivaci elektronických dokumentů. Revize tak zavádí novou službu vytvářející důvěru spočívající v elektronické

<sup>517</sup> POLČÁK, 2011, op. cit., s. 59.

<sup>518</sup> KORBEL, MELZER, 2014, op. cit., s. 36.

<sup>519</sup> MATEJKA, GÜTTLER, 2018, op. cit., s. 46.



archivaci elektronických údajů. Elektronickou archivací schválený text revize rozumí službu zajišťující přijímání, uchovávání, zpřístupnění a výmaz elektronických dat a elektronických dokumentů s cílem zajistit jejich trvanlivost a čitelnost, jakož i zachovat jejich integritu, důvěrnost a důkaz původu po celou dobu uchovávání.

Rada ve svém obecném přístupu k návrhu revize blíže konstatovala důvody pro úpravu této služby. Odůvodňuje ji zájmem na zajištění právní jistoty, důvěryhodnosti a harmonizace ve všech členských státech. Směřováno je zde jak na dokumenty vytvořené elektronicky, tak dokumenty naskenované a digitalizované. Tato služby by měla mít také ambice adresovat potenciální problémy se změnami a zastaráváním formátů. Služby kvalifikované elektronické archivace by měly umožnit přenos uchovávaných elektronických dat na různá média nebo jejich převedení do různých formátů za účelem prodloužení jejich trvanlivosti a čitelnosti.<sup>520</sup>

Tato služba bude mít také svou kvalifikovanou úroveň. Kvalifikovanou službou elektronické archivace bude moci poskytovat pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru používající postupy a technologie, které zajistí důvěryhodnost elektronického dokumentu i po uplynutí doby technické platnosti.

Stejně jako tomu bylo dříve například u elektronických dokumentů, podpisů či pečeti, tak revize nově míří také na stanovení zásady nediskriminace i pro služby elektronické archivace. Z toho důvodu revize nařízení eIDAS stanoví, že elektronickým datům a elektronickým dokumentům uchovávaným s použitím služby elektronické archivace nesmějí být upírány právní účinky ani nesmějí být odmítány jako důkaz v soudním nebo správním řízení pouze z toho důvodu, že mají elektronickou podobu nebo že nejsou uchovávány s použitím kvalifikované služby elektronické archivace.

Domníváme se, že pro české právní prostředí návrh v této oblasti nepřináší nic nového, a to s ohledem na zásadu volného hodnocení důkazů a povinnost řádně odůvodnit odmítnutí některého důkazu, která na zásadu volného hodnocení důkazů navazuje a je pravidelně připomínána judikaturou.<sup>521</sup>

<sup>520</sup> Bod odůvodnění č. 33 obecného přístupu Rady.

<sup>521</sup> K tomuto závěru blíže v kapitole 12.2. této publikace.

Zároveň se revize blíže zaměřuje na právní účinky služby elektronické archivace.<sup>522</sup> Stanoví proto, že u elektronických dat a elektronických dokumentů uchovávaných s použitím kvalifikované služby elektronické archivace platí předpoklad integrity dat a jejich původu, a to po dobu uchovávání kvalifikovaným poskytovatelem služeb vytvářejících důvěru.

Zde se návrh dostává do určité kolize s naším občanským zákoníkem, když návrh počítá s domněnkou integrity dat a původu pouze po dobu uchovávání kvalifikovaným poskytovatelem služeb vytvářejících důvěru. To nicméně nemusí znamenat, že by se po uchovávání kvalifikovaným poskytovatelem stala data bezcenná. Bude podle nás stále platit domněnka podle § 562 obč. zák., jen bude zřejmě nutné vynaložit větší úsilí při dokazování.

#### 12.4.2 Využití protokolu blockchain a podobných technologií pro archivaci

Pro elektronickou archivaci také může být významný protokol *blockchain*, resp. obecněji DLT a jiné podobné technologie. Revize nařízení eIDAS tak mluví také na úpravu tzv. elektronické knihy záznamů (podle původního českého překladu návrhu Komise a obecného přístupu Rady mělo jít elektronické účetní knihy). Jejich smyslem je zaznamenávání dat způsobem, který zajistí jedinečnost, autenticitu, správné pořadí dat a odolnost proti neoprávněným zásahům. Kombinovat by měly časové razítkování dat s garancí původce dat podobnou elektronickému podpisu. Jejich zamýšleným přínosem je také decentralizovanější model správy vhodnější pro spolupráci více stran.<sup>523</sup>

Zaznamenávání elektronických dat do elektronické knihy záznamů je další návrhem nově zaváděnou službou vytvářející důvěru. Definice elektronické knihy záznamů a český překlad pojmu „*electronic ledger*“ prošly vývojem mezi návrhem Evropské komise, obecným přístupem Rady a textem schváleným Parlamentem.

Komise definovala elektronickou účetní knihu jako elektronický záznam údajů odolný proti neoprávněným zásahům, který zajišťuje pravost a integritu

<sup>522</sup> Srov. čl. 45g obecného přístupu Rady.

<sup>523</sup> Návrh nařízení Evropského Parlamentu a Rady, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu, op. cit., s. 19, bod odůvodnění 34.

údajů, jež obsahuje, přesnost jejich data a času a jejich chronologické řazení.<sup>524</sup> Rada pak nejprve definovala obecně účetní knihu jako pořadí elektronických datových záznamů, které zajišťuje jejich integritu a přesnost jejich chronologického řazení.<sup>525</sup> Elektronická účetní kniha měla následně naplnit požadavky, které jsou stanoveny pro její kvalifikovanou úroveň. Na základě těchto požadavků musely být kvalifikované účetní knihy vytvářeny jedním či více kvalifikovanými poskytovateli služeb vytvářejících důvěru, identifikovat původ datových záznamů v účetní knize, zajišťovat jedinečné sekvenční chronologické řazení datových záznamů v účetní knize a zaznamenávat údaje takovým způsobem, že je možné zjistit jakoukoliv následnou změnu údajů, čímž zajišťují jejich integritu v čase.

Podle schváleného textu je elektronickou knihou záznamů posloupanost elektronických datových záznamů zajišťující integritu těchto záznamů a přesnost chronologického pořadí těchto záznamů. Text zavádí také kvalifikovanou elektronickou knihou záznamů, kterou poskytuje kvalifikovaný poskytovatel služeb vytvářejících důvěru a která splňuje požadavky stanovené dále v textu revize. Podle nich musí identifikovat původ datových záznamů v knize záznamů, zajišťovat jedinečné sekvenční chronologické řazení datových záznamů v knize záznamů a zaznamenávat data takovým způsobem, že je možné okamžitě zjistit jakoukoliv následnou změnu dat, čímž zajišťují jejich integritu v čase.

Pro datové záznamy obsažené v kvalifikované elektronické účetní knize podle revize platí předpoklad jejich jedinečného a přesného sekvenčního chronologického řazení a jejich integrity.

Text revize také mluví na zákaz upírání právních účinků, nicméně i zde platí totéž, co bylo v této souvislosti uvedeno výše u služby elektronické archivace.

Rada ve svém obecném přístupu popisovala užití elektronických knih záznamů (resp. tehdy elektronických účetních knih) jako klasický *use case*

<sup>524</sup> Návrh nařízení Evropského Parlamentu a Rady, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu, op. cit., s. 23, čl. 1 odst. 3 písm. i).

<sup>525</sup> Čl. 2 bod. 53 obecného přístupu Rady. Stejným způsobem je definována i v předběžné politické dohodě. Viz ITRE. European Digital Identity – Provisional Agreement. *Evropský parlament* [online]. 2023 [cit. 20. 12. 2023]. Dostupné z: <https://www.europarl.europa.eu/committees/cs/european-digital-identity-provisional-ag/product-details/20231116CAN72103>

*blockchainu* nebo jiných DLT technologií.<sup>526</sup> Účelem má být vytvoření chronologické posloupnosti datových záznam, aby se zabránilo kopírování digitální aktiv a jejich prodeji několika různým příjemcům. Tím Rada v zásadě popisovala původní smysl *blockchainu* u kryptoměn, kterým je zabránění duplikace záznamu (*double spending*) při převodu jednotek kryptoměny. Jako další *use case* je zmíněn například dodavatelský řetězec nebo digitalizace práv duševního vlastnictví. Do budoucna může být zajímavé i užití pro elektronické volby nebo referenda ale také širší užití pro decentralizované katastry nemovitostí. Těmito příklady zmíněnými Radou se ale podle našeho názoru užití elektronických účetních knih zdaleka nevyčerpává. Své místo by si mohly najít i v rámci elektronického soukromoprávního jednání a elektronické kontraktace a mohly by být více užívány i pro elektronické podepisování nebo jako dobrý způsob archivace elektronicky uzavřených smluv a jiných právních jednání.

---

<sup>526</sup> Srov. bod odůvodnění č. 34 nařízení eIDAS v obecném přístupu Rady.



## 13 VYMÁHÁNÍ ZÁVAZKŮ Z ELEKTRONICKY PODEPSANÝCH SMLUV

### 13.1 Úvod

Dokazování je jednou z nejdůležitějších otázek spojených s elektronickou kontraktací.<sup>527</sup> Nařízení eIDAS vychází mimo jiné z hypotézy, že budování důvěryhodnosti online prostředí má pro hospodářský a sociální rozvoj klíčový význam a nedostatek právní jistoty vede k pomalejšímu rozvoji elektronických transakcí. Cílem nařízení je tak zvýšení důvěryhodnosti elektronických transakcí a tím krom dalšího posílit efektivnost elektronického podnikání a elektronického obchodu.<sup>528</sup> Aby se přispělo k přeshraničnímu využívání služeb vytvářejících důvěru, mělo by být možné použít je ve všech členských státech jako důkaz v soudním a správním řízení.<sup>529</sup>

Nařízení stanovuje, 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. Totéž platí obdobně pro elektronické podpisy, elektronické pečete a elektronická časová razítka. Na vnitrostátním právu podle nařízení je, aby vymezilo právní účinky služeb vytvářejících důvěru.<sup>530</sup> Český právní řád ale žádné konkrétní účinky či důkazní sílu u služeb vytvářejících důvěru nestanoví. Touto otázkou se tak dále zabýváme v souvislosti se zásadou volného hodnocení důkazů v civilním procesu.

### 13.2 Elektronické důkazy

V rámci českého civilního procesu není dokazování elektronickými důkazy nijak speciálně upraveno. Za důkaz však mohou sloužit všechny prostředky, jimiž lze zjistit stav věci. Výčet důkazů je v občanském soudním řádu pouze demonstrativní. Zároveň pokud není způsob provedení důkazu zákonem výslovně stanoven, určí ho soud.<sup>531</sup> Dokazování elektronickými dokumenty

<sup>527</sup> Srov. MATEJKA, CHUM, 2002, op. cit., s. 38.

<sup>528</sup> Srov. bod odůvodnění 1 a 2 nařízení eIDAS.

<sup>529</sup> Srov. bod odůvodnění 22 nařízení eIDAS.

<sup>530</sup> Bod odůvodnění 22 nařízení eIDAS.

<sup>531</sup> § 125 občanského soudního řádu.

tak sice není výslovně upraveno, občanský soud řád mu však zároveň ani nijak nebrání.

Elektronické důkazy mohou být často mnohem spolehlivější než jejich „analogové“ období. Na druhou stranu soudy při jejich předkládání stále narážejí na technické a odborné zázemí při jejich provádění a posuzování.<sup>532</sup> Jako elektronický důkaz bude v praxi především použit elektronický dokument, který je nařízením eIDAS široce definován jako jakýkoli obsah uchovávaný v elektronické podobě, zejména jako text nebo zvuková, vizuální nebo audiovizuální nahrávka.<sup>533</sup> Ideální pak bude jeho spojení s elektronickým podpisem, elektronickou pečetí nebo razítkem, resp. jeho řádnou archivací.

### 13.2.1 Volné hodnocení důkazů a další zásady

Soud hodnotí důkazy podle své úvahy, a to každý důkaz jednotlivě a všechny důkazy v jejich vzájemné souvislosti; přitom pečlivě přihlíží ke všemu, co vyšlo za řízení najevo, včetně toho, co uvedli účastníci.<sup>534</sup> Takto je upraven základ zásady volného hodnocení důkazů jako jedné z hlavních zásad civilního procesu, která dává soudci značný prostor pro jeho úvahu a zároveň jsou jí na soudce kladeny vysoké nároky.<sup>535</sup> Soud také podle své úvahy určí, které z navržených důkazů provede.<sup>536</sup> V obou zmíněných ustanoveních se promítá ústavní princip nezávislosti soudce.<sup>537</sup>

Soudce má tedy poměrně značný prostor pro hodnocení důkazů<sup>538</sup>, který však naráží na limity práva na spravedlivý proces, a toto hodnocení tedy nemůže být svévolné.<sup>539</sup> Zároveň soud musí dbát na dodržení zásady rovnosti

<sup>532</sup> MAISNER, M. Řešení sporů v oblasti informačních technologií. In: MAISNER, M. a kol. *Základy softwarového práva*. Praha: Wolters Kluwer, 2011, s. 156.

<sup>533</sup> Čl. 3 odst. 35 nařízení eIDAS.

<sup>534</sup> § 132 občanského soudního řádu.

<sup>535</sup> JIRSA, J. Komentář k § 132. In: JIRSA, J. a kol. *Občanské soudní řízení (soudcovský komentář)*. Kniha II. Praha: Havlíček Brain Team, 2014, s. 348.

<sup>536</sup> § 120 občanského soudního řádu.

<sup>537</sup> Dle rozhodnutí Ústavního soudu ze dne 6. 1. 1997, sp. zn. IV. ÚS 191/96.

<sup>538</sup> „Hodnocením důkazů“ Nejvyšší soud rozumí „*mýšlenkovou* činnost soudu, kterou je provedeným důkazům přisuzována hodnota závažnosti (důležitosti) pro rozhodnutí, hodnota zákonosti, hodnota pravdivosti, popř. hodnota věrohodnosti“ (Rozhodnutí Nejvyššího soudu ze dne 19. 5. 2010, sp. zn. 33 Cdo 2441/2008).

<sup>539</sup> K pojmu „svévole“ srov. např. rozhodnutí Ústavního soudu ze dne 16. 6. 2015, sp. zn. II. ÚS 3588/14.

stran. Má tedy stranám zajistit rovnocenné možnosti k uplatnění jejich práv.<sup>540</sup> Při uplatnění zásady volného hodnocení důkazů musí soud zkoumat důkazy nikoliv pouze každý zvlášť, ale i ve vzájemných souvislostech. Jak k tomu uvádí Jirsa, „[ž]ádný důkaz, pokud by byl hodnocen jenom zvlášť, bez souvislosti s ostatními, nemůže být stoprocentní. Kouzlo zásady volného hodnocení však funguje v praxi téměř dokonale a většinou se i nejdokonalejší falzum ukáže ve světle ostatních důkazů jako podvrh. I proto může za důkaz posloužit vše.“<sup>541</sup>

Zásada volného hodnocení důkazů tak elektronickým důkazům do značné míry do občanského soudního řízení otevírá dveře. V odborné literatuře a judikatuře lze nalézt různé důvody k neprovedení důkazů. Jako příklad bývá uváděna skutečnost, že důkaz nemá relevantní souvislost s řízením či je zjevně nezpůsobilý k ověření či vyvrácení tvrzené skutečnosti. Dále také, že důkazy byly zjevně navrženy k účelovému prodloužení sporu. Může jít také o situace, kdy byly navrženy nezákonné důkazy anebo byly navrženy v rozporu se zásadou koncentrace řízení.<sup>542</sup> Naproti tomu nemůže soud odmítnout provést důkaz jen proto, že by jej považoval předem za nevěrohodný bez toho, aby provedl jeho hodnocení v souladu se zásadou volného hodnocení důkazů.<sup>543</sup>

Z uvedeného vyplývá, že elektronické dokumenty včetně elektronických podpisů či dalších služeb vytvářejících důvěru jsou přípustné jako důkazy.<sup>544</sup> Soud je sice může jako důkaz odmítnout, ale takové odmítnutí musí důkladným, transparentním a přezkoumatelným způsobem odůvodnit.

### 13.2.2 Nařízení eIDAS a elektronické důkazy

Pro elektronický podpis, elektronickou pečeť, elektronické časové razítko i elektronický dokument nařízení eIDAS stanovuje, že jim nesmějí být upírány právní účinky a nesmí být odmítány jako důkaz v soudním a správním řízení pouze z toho důvodu, že mají elektronickou podobu.<sup>545</sup> Nesmí být

<sup>540</sup> Blíže viz např. rozhodnutí Ústavního soudu ze dne 8. 1. 1997, sp. zn. II.ÚS 127/96.

<sup>541</sup> JIRSA, J. Komentář k § 125. In: JIRSA a kol., 2014, op. cit., s. 304.

<sup>542</sup> HRŮMADA, M. § 120 [Důkazní povinnost]. In: SVOBODA, K., SMOLÍK, P., LEVÝ, J., DOLEŽÍLEK, J. a kol. *Občanský soudní řád*. 3. vyd. Praha: C. H. Beck, 2021, s. 614.

<sup>543</sup> Rozhodnutí Nejvyššího soudu ze dne 9. 10. 2002, sp. zn. 29 Cdo 2893/2000.

<sup>544</sup> Shodně MATEJKA, GÜTTLER, 2018, op. cit., s. 44.

<sup>545</sup> Srov. čl. 25 odst. 1, čl. 35 odst. 1, čl. 41 odst. 1 a čl. 46 nařízení eIDAS.



také odmítány jen proto, že nesplňují požadavky na jejich kvalifikovanou úroveň.<sup>546</sup> Smyslem je přispět k obecnému přeshraničnímu využívání služeb vytvářejících důvěru a také umožnit jejich použití ve všech členských státech Evropské unie jako důkazu v soudním a správním řízení.<sup>547</sup>

Pro dokazování jsou také důležité domněnky založené nařízením eIDAS. U kvalifikované elektronické pečeti platí domněnka integrity dat a správnosti původu těch dat, s nimiž je kvalifikovaná elektronická pečeť spojena. Podobně u kvalifikovaného elektronického časového razítka platí domněnka správnosti data a času, které udává, a integrity dat, s nimiž jsou toto datum a čas spojeny. Zároveň je nařízením eIDAS stanoveno, že kvalifikovaný elektronický podpis má právní účinek rovnocenný vlastnoručnímu podpisu.

Nařízení pak nechává na vnitrostátním právu, aby vymezilo právní účinky služeb vytvářejících důvěru.<sup>548</sup> Český právní řád tak ale žádnou speciální úpravou nečiní. Do občanského soudního řádu se nařízení eIDAS při jeho adaptaci promítlo v podstatě jen novelizací § 42 odst. 3. To po její účinnosti zní takto: „*V případech podání v elektronické podobě podepsaného způsobem, se kterým zvláštní právní předpis spojuje účinky vlastnoručního podpisu<sup>103</sup>*), se nevyžaduje doplnění podání předložením jeho originálu podle odstavce 2.“ Poznámka pod čarou číslo 103 odkazuje na § 6 odst. 1 zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, který ale o účincích vlastnoručního podpisu neříká vůbec nic. To činí pouze zvláštní část důvodové zprávy k tomuto zákonu.<sup>549</sup>

### 13.2.3 Zásada nediskriminace

Pokud má mít právní, resp. obchodní praxe skutečnou důvěru v elektronické právní jednání a mohla jej využívat, je třeba, aby elektronické dokumenty bylo možné úspěšně uplatnit jako silné důkazy v rámci civilních sporů. Zmiňovali jsme, že nařízení eIDAS zapovídá odmítnutí elektronického podpisu

<sup>546</sup> O kvalifikované úrovni nelze hovořit pouze v případě elektronického dokumentu. Nařízení eIDAS jinak předpokládá kvalifikovaný elektronický podpis, pečeť i razítko.

<sup>547</sup> Srov. bod odůvodnění 22 nařízení eIDAS.

<sup>548</sup> Viz bod odůvodnění 22 nařízení eIDAS: „*Je na vnitrostátním právu, aby vymezilo právní účinky služeb vytvářejících důvěru, nestanoví-li se v tomto nařízení jinak.*“

<sup>549</sup> Blíže také JAREŠ, A. Nařízení eIDAS, elektronický podpis a pečeť v českém právním řádu In: SEDLÁČEK, M., STŘELEČEK, T. a kol. *Právní jednání a procesní úkony (vzájemné vztahy a nové aspekty)*. Praha: Wolters Kluwer, 2019, s. 19–26.

či elektronického dokumentu jako důkazu v soudním řízení jen kvůli tomu, že má elektronickou podobu a nelze je také odmítnout jen proto, že nespĺňují požadavky na jejich kvalifikovanou úroveň.

Tyto zákazy se mohou zdát jako zásadní, nicméně pouze konstatují, že elektronický dokument a další služby vytvářející důvěru nesmí být odmítnuty jako důkaz. Neodmítnutí důkazu pouze pro jeho elektronickou podobu však nevyovídá nic o jeho důkazní síle v rámci řízení a o závěru soudu o něm. Při platnosti zásady volného hodnocení důkazů jde zároveň spíše o deklaraci bez většího dopadu pro rozhodování soudů, která i bez nařízení eIDAS dává soudu značný prostor pro jeho úvahu při provádění a hodnocení důkazů. Soud sice podle své úvahy určí, který z navržených důkazů provede, nemůže tak ale učinit svévolně. Musí dodržet rovnost stran a zajistit jim rovnocenné možnosti k uplatnění jejich práv. Za tím účelem musí soud mimo jiné v odůvodnění rozsudku stručně a jasně uvést, o které důkazy opřel svá skutková zjištění, jakými úvahami se při hodnocení důkazů řídil a proč naopak některý důkaz neprovedl. Tento závěr platí pro všechny důkazy bez ohledu na jejich podobu. V tomto ohledu tak nebude rozdíl mezi papírovou a vlastnoručně podepsanou smlouvou a smlouvou ve formě elektronicky podepsaného dokumentu.

Odmítnout elektronický důkaz bez dalšího odůvodnění a jen pro jeho elektronickou podobu by soud neměl ani bez zákazů v nařízení eIDAS. Pokud by tak učinil bez odůvodnění či toto odůvodnění opřel pouze o elektronickou podobu důkazu, nenaplnil by požadavek na řádné odůvodnění rozhodnutí a v konečném důsledku by se mohl dopustit *denegatio iustitiae*.

Diskutované zákazy nařízení eIDAS tak podle nás nepřinesly do českého civilního procesu žádnou zásadní novinku. Přesto je nutné vnímat příslušná ustanovení nařízení eIDAS pozitivně. Význam mohou mít ve vztahu k soudcům, kteří by potenciálně měli tendence reagovat na elektronické právní jednání s nedůvěrou a obavami. I pokud by tedy šlo pouze o apel na soudce, aby se elektronickým důkazům nevyhýbali, měl by tento apel význam. Například Polčák totiž při svých úvahách o perspektivách elektronizace justice naráží na to, že pro její úspěšné provedení bude nutné také změnit některé návyky a stereotypy, typicky při volném hodnocení důkazů v elektronické formě. A apeluje na důkladné vzdělávání soudců a soudního personálu v technických

aspektech tvorby a používání elektronických dokumentů tak, aby byla adekvátně hodnocena jejich *ad hoc* autenticita a průkaznost.<sup>550</sup> Jinde upozorňuje na to, že virtualizovaný dokument (tedy elektronický dokument) není o nic méně reálným nebo spolehlivým důkazem než jeho tradiční formy, jen je třeba se adaptovat na jeho jiné formální parametry a z toho plynoucí jiné metody zpracování.<sup>551</sup>

### 13.3 Dokazování elektronickými podpisy, pečetěmi a razítky

Z některých ustanovení nařízení eIDAS o konkrétních službách vytvářejících důvěru, ale také z občanského zákoníku, vyplývají pravidla a domněnky, která mají význam pro dokazování.

Kvalifikovaný elektronický podpis má podle nařízení eIDAS stejné účinky jako podpis vlastnoruční. To je pravidlo se značným významem. Někteří mohou mít stále sklon více důvěřovat listinnému dokumentu s vlastnoručním podpisem než elektronickému dokumentu opatřenému elektronickým podpisem. A to i v případě, že je podepsán kvalifikovaným elektronickým podpisem. Díky asymetrické kryptografii používané při vytváření kvalifikovaného elektronického podpisu je však možné zjistit jakoukoliv následnou změnu podepsaného dokumentu. Jeho prostřednictvím se tak podepisující osoba vyhne situacím, kdy je například vlastnoručně podepsaná smlouva vyhotovená na více listech rozešita a některá strana vyměněna.

Může samozřejmě dojít k tomu, že dokument za vlastníka kvalifikovaného certifikátu a kvalifikovaného prostředku pro vytváření elektronického podpisu podepíše jiná osoba. Ale ani to není argument pro nedůvěru ke všem elektronicky podepsaným dokumentům. I někteří zaměstnanci advokátních kanceláří se možná setkali s praxí, kdy je za advokáta bez jeho osobní přítomnosti (avšak s jeho souhlasem) podepsána listina například jejím přiložením na originální vlastnoruční podpis advokáta na jiné listině a „obkreslení“ podpisu na tuto listinu. Šikovní zaměstnanci mohou také podpis na základě dlouholeté praxe napodobit bez dalšího. V úvahu lze vzít i datové schránky. V jejich případě se předpokládá, že za osobu, pro kterou byla datová schránka zřízena, přistupuje k datové schránce pověřená osoba. A některé úkony

<sup>550</sup> POLČÁK, 2012, op. cit., s. 255.

<sup>551</sup> POLČÁK, 2011, op. cit., s. 53.

provedené prostřednictvím datových schránek se považují za rovnocenné listinným a podepsaným dokumentům, i když úkon provedla pouze osoba pověřená.<sup>552</sup> I tyto skutečnosti je možné brát v úvahu při teoretickém srovnávání listinných a elektronických důkazů.

Dokazování elektronickým dokumentem s kvalifikovaným elektronickým podpisem by mělo být relativně jednoduché. Jakákoliv následná změna podepsaného dokumentu se projeví při ověření platnosti kvalifikovaného elektronického podpisu.<sup>553</sup> Proto by mělo v zásadě postačit, že bude ověřena platnost tohoto podpisu, a další zpochybnění integrity dokumentu či dalších skutečností bude záviset na tvrzení a dokazování stran sporu.<sup>554</sup>

Složitější je to v případě, že již certifikát pro kvalifikovaný elektronický podpis pozbyl platnosti. Tento problém lze jednoduše překlenout opatřením dokumentu elektronickým časovým razítkem<sup>555</sup> před skončením platnosti certifikátu pro podpis. Druhou možností je využití systematických záznamů o právních jednáních v elektronickém systému ve smyslu § 562 odst. 2 obč. zák. (jedná se pak *de facto* o dva základní přístupy k elektronické archivaci). V jeho důsledku osoba, která tyto záznamy vede, bude muset prokázat, že záznamy vede systematicky a posoupně a také, že jsou chráněny proti změnám. Pokud tyto předpoklady splní, bude je soud do prokázání opaku považovat za spolehlivé.<sup>556</sup> Požadavky § 562 odst. 2 obč. zák. mohou naplnit i záznamy internetového obchodu o provedených objednávkách, které by tedy měly být považovány za spolehlivé.<sup>557</sup>

Pro kvalifikovanou elektronickou pečeť platí podle nařízení eIDAS domněnka integrity dat a správnosti původu těch dat, s nimiž je kvalifikovaná elektronická pečeť spojena. Pokud tedy není prokázán opak, má se za to, že elektronický dokument byl vyhotoven právníkou osobou, které svědčí

<sup>552</sup> § 18 odst. 2 zák. o el. úkonech.

<sup>553</sup> Požadavky na ověřování platnosti kvalifikovaných elektronických podpisů jsou stanoveny v čl. 32 nařízení eIDAS.

<sup>554</sup> Srov. § 565 zákona č. 89/2012 Sb., občanský zákoník.

<sup>555</sup> Srov. čl. 41 odst. 2 nařízení eIDAS: „U kvalifikovaného elektronického časového razítka platí domněnka správnosti data a času, které udává, a integrity dat, s nimiž jsou toto datum a tento čas spojeny.“

<sup>556</sup> Srov. HRDLIČKA, M. Komentář k § 562. In: LAVICKÝ, P. a kol. *Občanský zákoník I. Obecná část (§ 1–654)*. 1. vyd. Praha: C. H. Beck, 2014. Dostupné z: <https://www.beck-online.cz> [cit. 5. 11. 2021].

<sup>557</sup> DONÁT, TOMÍŠEK, 2016, op. cit., s. 161.

kvalifikovaná elektronická pečeť spojená s tímto dokumentem. Má se rovněž za to, že dokument má totožnou podobu jako v okamžiku vytvoření této pečeti.<sup>558</sup> Pro ověření platnosti kvalifikované elektronické pečeti se použije přiměřeně postup pro ověření platnosti kvalifikovaného elektronického podpisu.

U kvalifikovaného elektronického časového razítka platí domněnka správnosti data a času, které udává. Platí také domněnka integrity dat, s nimiž jsou toto datum a tento čas spojeny. Elektronická časová razítka jsou v nařízení eIDAS upravena oproti podpisům a pečetím spoře. I tak je ale například Kment považuje za důkazně nejspolehlivější službu vytvářející důvěru vůbec.<sup>559</sup>

Pro elektronický dokument nařízení eIDAS pouze určuje – stejně jako pro podpisy, pečeti a časová razítka – zákaz upření právních účinků a odmítnutí jako důkazu jen pro jeho elektronickou podobu. Nic bližšího o jeho důkazních účincích nařízení ani český právní řád nestanoví. Elektronický dokument lze sice bez dalšího použít jako důkaz, na druhou stranu pro zvýšení důkazní spolehlivosti bude vhodné (či někdy nutné) opatřit jej elektronickým podpisem či pečeti (nejlépe jejich kvalifikovanými úrovněmi) ideálně v kombinaci s elektronickým časovým razítkem. O důkazních účincích elektronických dokumentů je možné vést debatu. Například Polčák považuje elektronické dokumenty, co do prokazování autenticity, za mnohem výhodnější než ty papírové. To zdůvodňuje tím, že namísto znaleckého zkoumání papíru postačí ve většině případů ke zjištění autenticity jen automatická početní operace provedená speciálním softwarem.<sup>560</sup> Naproti tomu Kment nepovažuje výklad o univerzální rovnocennosti elektronického dokumentu papírové listině a elektronického dokumentu s kvalifikovaným elektronickým podpisem vlastnoručně podepsané listině za správný. Tento výklad považuje dokonce za přepjatý.<sup>561</sup> Kment také dochází k závěru, že „*připuštění elektronického podpisu prostého pro platné právní jednání v písemné formě za určité obroženi*

<sup>558</sup> Pro vyvrácení domněnky integrity dat a správnosti původu dat, s nimiž je elektronická pečeť spojena srov. KMENT, 2018, op. cit., s. 239–242. Autor zde dokonce prezentuje tvrzení, že: „*důkazní presumpce u kvalifikované elektronické pečeti [...] má silnější důkazní účinek než kvalifikovaný elektronický podpis, pro nějž v eIDAS tento účinek vyjádřen není.*“

<sup>559</sup> KMENT, 2018, op. cit., s. 243.

<sup>560</sup> POLČÁK, 2012, op. cit., s. 255.

<sup>561</sup> KMENT, 2018, op. cit., s. 246.

*osob, které takto budou jednat, neboť pro elektronický vyhovují prakticky všechny druhy techniky elektronických podpisů, tedy i tzv. click-wrap podpis.*<sup>562</sup>

Přikláníme se k prve uváděnému názoru, tedy že elektronické dokumenty mohou při dokazování výhodnější než ty papírové, a to za situace, kdy bude elektronický dokument opatřen vyšší úrovní některé služby vytvářející důvěru či ideálně jejich kombinací nebo archivován v rámci záznamů údajů o právních jednáních v elektronickém systému ve smyslu § 562 odst. 2 obč. zák. Jeho autenticita pak bude ověřena prostřednictvím služeb vytvářejících důvěry či těchto záznamů.

### 13.4 Důkazní břemeno při dokazování pravosti podpisu

V civilních sporech není výjimečné, že některá ze stran namítá, že právní jednání nepodepsala. Domníváme se proto, že pro téma je také významné se krátce věnovat otázce, komu svědčí důkazní břemeno při prokazování pravosti podpisu. Závěry uváděné rozhodovací praxe byly dosaženy ve vztahu k vlastnoručně podepsaným listinám, nicméně nevidíme důvod, proč by se neměly uplatnit i elektronicky podepsané dokumenty.

Předchozí občanský zákoník z roku 1964 pravidla v tomto směru neobsahoval, musela je tedy dovodit judikatura. Ta obecně pro dokazování soukromými listinami dovodila, že je třeba rozeznávat jejich pravost (zda pochází od toho, kdo je v ní uveden jako vystavitel) a správnost (pravdivost). Jestliže vystavitel popíral pravost listiny, leželo důkazní břemeno ohledně pravosti na tom účastníkovi, který ze skutečností v listině uvedených pro sebe vyvozuje příznivé právní důsledky.<sup>563</sup>

Nejvyšší soud také dospěl k závěru, že pokud účastník řízení popře pravost či správnost soukromé listiny, pak toho účastníka, který listinu předložil jako důkaz, stíhá důkazní povinnost a důkazní břemeno. Tento účastník tedy nese procesně nepříznivé následky toho, že se v řízení nepodaří prokázat pravost či správnost soukromé listiny.<sup>564</sup>

Podobně Nejvyšší soud konstatoval, že ve sporu o zaplacení směnky, ve kterém popře žalovaný její pravost, leží důkazní břemeno ohledně pravosti

<sup>562</sup> KMENT, 2018, op. cit., s. 336.

<sup>563</sup> Rozhodnutí Nejvyššího soudu ze dne 9. 10. 2000, sp. zn. 22 Cdo 617/99.

<sup>564</sup> Rozhodnutí Nejvyššího soudu ze dne 17. 4. 1996, sp. zn. 3 Cdon 1031/96.

podpisu žalovaného na směnce na žalobci, který směnku k důkazu předložil a který ze skutečností v ní uvedených vyvozuje žalobou uplatněný nárok.<sup>565</sup>

Podle současného občanského zákoníku je na každém, kdo se dovolává soukromé listiny, aby dokázal její pravost a správnost.<sup>566</sup> Občanský zákoník také zavádí vyvratitelnou domněnku pro případ použití soukromé listiny proti osobě, která listinu zjevně podepsala (a některým dalším osobám). Pak se má za to, že pravost a správnost listiny byla uznána. Důkazní břemeno k prokázání opaku zde leží na osobě, která listinu podepsala. To má smysl v ochraně třetích osob a také se zde posiluje odpovědnost za vlastní právní jednání.<sup>567</sup>

Výše uvedené závěry potvrdil Nejvyšší soud také například v rozhodnutí ze dne 26. 11. 2019, kde konstatuje, že pokud žalovaná strana zpochybnila pravost podpisu žalobce na soukromé listině (v tomto případě převodní smlouvě), přesouvá se důkazní břemeno k prokázání pravosti podpisu na žalující stranu, která listinu v řízení předložila a vyvozuje z ní pro sebe příznivé právní následky.<sup>568</sup>

<sup>565</sup> Rozhodnutí Nejvyššího soudu ze dne 21. 12. 2009, sp. zn. 29 Cdo 3478/2007.

<sup>566</sup> § 565 obč. zák.

<sup>567</sup> MACKOVÁ, A. Komenář k § 565. In: ŠVESTKA, J., DVOŘÁK, J., FIALA, J. a kol. *Občanský zákoník. Komentář. Svazek I.* Praha: Wolters Kluwer, 2014, s. 1399.

<sup>568</sup> Rozhodnutí Nejvyššího soudu ze dne 26. 11. 2019, sp. zn. 24 Cdo 1110/2019.

## 14 ROZHODOVACÍ PRAXE Z POSLEDNÍCH LET

V následujícím textu se věnujeme konfrontaci dříve dosažených závěrů s rozhodovací praxí soudů. Z rozhodnutí některých nižších soudů vydaných v posledních letech se totiž jeví, že soudy k hodnocení elektronických právních jednání mohou přistupovat poměrně přísně a do jisté míry přispívat k nedůvěře v elektronické právní jednání. Pro kontext s rozhodnutími vydanými v poslední době se věnujeme i některým dřívějším rozhodnutím přijatým za účinnosti předchozího občanského zákoníku z roku 1964 a zák. o el. podpisu.

Coudert, Debet a de Hert uvádějí, že ve Francii nové technologie ovlivnily právní styk a výkon některých práv, což postupně vedlo k přijímání nových zákonných úprav, které mohou následovat řešení navržená rozhodovací praxí.<sup>569</sup> Na první pohled se však může zdát, že v České republice toto tvrzení neplatí a rozhodovací praxe je naopak pozadu za regulací. Dále tak rovněž provádíme reflexi rozhodovací praxe pro potvrzení či vyvrácení tohoto předpokladu.

V dalším textu pracujeme s některými rozhodnutími nižších soudů, která podle nás ilustrují trend v rozhodování v rozhodovací praxi nižších soudů. Rozebíráme jak rozhodnutí, která z našeho pohledu přistupují k elektronickým právním jednáním správným způsobem, tak i ty, které nikoliv. Rozhodnutí z obou skupin je třeba brát v úvahu při zvažování úrovně elektronického podpisu užívaného pro právní jednání či při designu byznysového modelu počítajícího s pravidelným uzavíráním většího množství smluv se spotřebiteli.

### 14.1 Nelze uzavřít smlouvou jen výměnou e-mailů

V rozsudku ze dne 29. 1. 2009, sp. zn. 30 Cdo 1230/2007 se Nejvyšší soud věnoval také otázce platnosti smlouvy o postoupení pohledávky, která měla vzniknout na základě výměny e-mailových zpráv neopatřených uznávaným elektronickým podpisem dle § 11 odst. 3 tehdejšího zák. o el. podpisu.

<sup>569</sup> COUDERT, F., DEBET, A., HERT, P. de. Constitutional Rights and New Technologies in France. In: LEENES, R. E., KOOPS, B.-J., HERT, P. de (eds.). *Constitutional Rights and New Technologies: A Comparative Study Covering Belgium, Canada, France, Germany, Sweden, and the United States*. Tilburg University, 2007, s. 90.



Nejvyšší soud posoudil smlouvu jako neplatnou. Podle jeho názoru sice žalobce zasláným e-mailem navrhl původnímu věřiteli uzavření smlouvy o postoupení pohledávky vůči žalovanému, tento návrh však nebyl opatřen elektronickým podpisem. Z toho důvodu je třeba podle soudu tuto smlouvu posuzovat jako neplatnou.

Za platnou tedy nebyla uznána smlouva, k jejímuž uzavření mělo dojít prostřednictvím e-mailových zpráv.

K podobnému závěru dospěl Nejvyšší soud i v rozhodnutí ze dne 10. 4. 2014, sp. zn. 23 Cdo 1593/2012. V něm se Nejvyšší soud zabýval mimo jiné otázkou platnosti dodatku k písemné smlouvě předpokládající uzavření dodatku v písemné formě, k jehož uzavření mělo dojít prostřednictvím e-mailových zpráv. Odvolací soud v této souvislosti konstatoval, že za změnu písemné smlouvy nelze považovat e-mailovou korespondenci, jelikož ve smlouvě se smluvní strany dohodly, že veškeré změny nebo doplňky této smlouvy je možno činit pouze písemně. Nejvyšší soud tento závěr potvrdil s odkazem na vymezení elektronického podpisu v zák. o el. podpisu, jehož součástí byl i požadavek na jednoznačné ověření identity podepsané osoby ve vztahu k datové zprávě.

Neznáme všechny skutkové okolnosti posuzované v těchto řízeních, předpokládáme nicméně, že e-mailové zprávy byly v závěru podepsány alespoň jménem a příjmením jednatelky osoby či jméno nebo příjmení byla součástí e-mailové adresy. Dříve jsme konstatovali závěr, že pouhé jméno a příjmení v závěru e-mailové zprávy či v e-mailové adrese lze považovat za elektronický podpis prostý. Zároveň jsme ale upozorňovali na dřívější úpravu zák. o el. podpisu, který elektronickým podpisem rozuměl 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.<sup>570</sup>

Elektronický podpis je v současnosti nařízením eIDAS definován jiným způsobem a toto nařízení nevyžaduje u elektronického podpisu prostého jednoznačné ověření identity. Zák. o službách vytvářejících důvěru navíc výslovně umožňuje použití jakékoliv úrovně elektronického podpisu (včetně

<sup>570</sup> § 2 písm. a) zák. o el. podpisu.

elektronického podpisu prostého) pro právní jednání vůči jiným osobám, než veřejnoprávním podepisujícím a dalším osobám v rámci jejich působnosti. Domníváme se tak, že tato rozhodnutí by měla být za současné právní úpravy považována za přežitá. Pokud by v rámci řízení mělo být zpochybněno, že původcem e-mailové zprávy je tvrzená jednající osoba, mohou účastníci řízení dokazovat provedení právního jednání touto osobou i prostřednictvím jiných tvrzení a důkazů. Za současného právního stavu by tak nyní soudy podle našeho názoru – samozřejmě s přihlédnutím ke všem skutečnostem, které v řízení vyjdou najevo – měly za platnou smlouvu uznat i takovou, která byla uzavřena podobně jako v předmětném řízení.<sup>571</sup>

## 14.2 Oferta a akceptace dle dřívější právní úpravy

Smlouvou, která měla být uzavřena prostřednictvím výměny e-mailových zpráv, se zabýval rozsudek Nejvyššího soudu ČR ze dne 30. 10. 2009, sp. zn. 33 Cdo 3210/2007.

V dovolacím a předchozích řízeních soudy vycházely ze zjištění, že žalovaná dne 16. 5. 2005 prostřednictvím e-mailové adresy zaslala žalobkyni vyplněný formulář označený jako „cestovní smlouva – závazná přihláška“. Žalobkyně poté žalované fakturovala cenu zájezdu. Od smlouvy následně žalovaná odstoupila nejdříve telefonicky a poté ještě dopisem.

Soud upozornil na to, že je nejprve se třeba věnovat otázce, zda smlouva mezi účastníky vůbec vznikla, tedy zda se setkaly dva shodné projevy vůle (oferta a její akceptace). Přitom připomněl, že u smlouvy, pro niž zákon předepisuje písemnou formu, musí mít podle výslovného znění § 46 odst. 2 občanského zákoníku z roku 1964 písemnou formu i oferta.

Podle dovolacího soudu formulář vystavený na webových stránkách žalobkyně nevyhovoval požadavku adresnosti návrhu na uzavření smlouvy ani nespĺňoval požadavek písemnosti právního úkonu učiněného elektronickými prostředky, protože nebyl opatřen elektronickým podpisem podle zvláštního předpisu (tehdy platného zák. o el. podpisu). Tento formulář vyplněný návštěvníkem webových stránek žalobkyně měl podle soudu sloužit cestovní kanceláři ke sdělení zájmu o zájezd do konkrétní lokality v blíže určeném

<sup>571</sup> Za překonané toto rozhodnutí považují i například Donát s Tomíškem (srov. DONÁT, TOMÍŠEK, 2016, op. cit., s. 160).

období a k získání osobních údajů zájemce, které byly nezbytné k předložení návrhu cestovní smlouvy. To mělo být impulzem k iniciativě cestovní kanceláře předložit adresovaný písemný návrh smlouvy zákazníkovi. Ten pak, pokud byl předložen prostřednictvím elektronického prostředku, měl být opatřen zaručeným elektronickým podpisem definovaným v § 2 písm. b) zák. o el. podpisu. Smlouva by podle soudu byla uzavřena, pokud bude návrh stejným způsobem akceptován.

S ohledem na současnou definici prostého elektronického podpisu a jeho výslovnému dovolení pro právní jednání vyjma styku s veřejnoprávními podepisujícími je i toto rozhodnutí podle našeho názoru již neaplikovatelné. Za překonané ho považuje i literatura.<sup>572</sup>

### 14.3 Elektronický podpis prostý ve formě unikátního ID

Otázkou platnosti prostého elektronického podpisu ve formě unikátního hesla a uživatelského jména se zabýval Krajský soud v Českých Budějovicích ze dne 27. 3. 2015, sp. zn. 24 Co 696/2015.

V této věci rozhodl soudní exekutor o zamítnutí exekučního návrhu na základě pokynu exekučního soudu, podle kterého byla rozhodčí smlouva uzavřena distančně prostřednictvím internetového uživatelského účtu povinné, a proto nesplňovala požadavek písemnosti.

K uzavření smlouvy a rozhodčí smlouvy v této věci mělo dojít tak, že se povinná zaregistrovala v systému Klikpujcka.cz, při registraci uvedla jméno, příjmení, číslo mobilního telefonu, adresu elektronické pošty a rodné číslo. Následně byl vytvořen její uživatelský účet a současně došlo k vygenerování přístupových údajů, tedy uživatelského jména (ID) a hesla. ID jako devítimístné náhodně vygenerované unikátní číslo bylo odesláno na email povinné, a osmimístné unikátní heslo složené z číslic a malých a velkých písmen, obdržela povinná formou SMS zprávy zaslané na číslo jejího mobilního telefonu. Po přihlášení pomocí ID a hesla povinná doplnila další osobní údaje a vyslovila souhlas s podmínkami rámcové smlouvy o úvěru a rozhodčí smlouvy.

<sup>572</sup> DONÁT, TOMÍŠEK, 2016, op. cit., s. 160.

První úvěr byl poskytnut pouze prostřednictvím poštovní poukázky, kdy povinná byla jakožto výhradní adresát specifikována dle osobních údajů uvedených v rámci registračního procesu. Její identita tak byla ověřena pracovníkem doručovatele poštovní poukázky – České pošty.

Soud zde vyšel z toho, že „*pojem písemnosti zahrnuje textové či obrazové informace zachycené nejen v listinné, ale též v elektronické či jakékoliv jiné podobě, která umožňuje trvalý a písemný záznam dané informace s možností její autentizace, tj. přičitatelnosti určitému subjektu*“. Výslovně pak konstatoval, že „*prostým elektronickým podpisem může být oskenovaný vlastnoruční podpis, specifický PIN kód či dokonce jen jméno a příjmení napsané pod textem emailu, obecně vzato tedy jakákoliv data označující původce elektronického dokumentu*.“

Závěr rozhodnutí je tedy takový, že povinná opatřila smlouvy včetně rozhodčí doložky prostým elektronickým podpisem. Po zadání unikátních identifikačních údajů vztahujících se výhradně k její osobě totiž mechanickým prostředkem „kliknutím na virtuální tlačítko“ vyslovila souhlas s jejich zněním. Soud zde konstatoval, že podobné smlouvy jsou označovány jako „*click-through*“ smlouvy, u kterých je typický kontraktační proces kombinující prostý elektronický podpis (zde ID a heslo) s mechanickými prostředky (klik myši na příslušné tlačítko). Zároveň soud v rozhodnutí také uvedl, že „*[p]ožadavek písemnosti je přitom splněn nejen prizmatem § 561 odst. 1 o. z., ale rovněž dle § 3 odst. 1 zákona o rozpočtím řízení, respektive § 562 odst. 2 o. z., dle nichž se i nepodepsané elektronické dokumenty považují za podepsané, pokud zachycují obsah dokumentu a umožňují identifikaci jednajících osoby*.“<sup>573</sup>

Ve věcech s obdobnými skutkovými okolnostmi pak shodně s rozebíraným rozhodnutím rozhodoval například Krajský soud v Ostravě v rozhodnutí ze dne 28. 1. 2016, sp. zn. 37 I C m 4495/2014, nebo rozsudek Krajského soudu v Brně ze dne 5. 6. 2017, sp. zn. 33 I C m 547/2016.

#### 14.4 Potvrzení smluvních podmínek a zadání kódu z SMS

Ke stejným závěrům jako dříve uvedená rozhodnutí, ve kterých soudy dospěly k závěru o naplnění požadavku písemnosti při užití „*click-through*“ smluv a jejich podepsání pomocí unikátního hesla a uživatelského jména,

<sup>573</sup> Otázce *click-through* a *click-wrap* smluv se věnujeme v kapitole 6.5.5 a otázce nepodepsaného elektronického jednání v kapitole 4.4.

dochází v současné době i některé nižší soudy. Jako příklad lze uvést rozhodnutí Okresního soudu v Hodoníně ze dne 31. 8. 2021, sp. zn. 13 C 90/2021. V tomto rozhodnutí nejsou skutkové okolnosti uzavření smlouvy nijak blíže rozvedeny. Soud v rozhodnutí pouze uvádí, že „[p]ředmětná smlouva o úvěru měla být mezi právním předchůdcem žalobkyně a žalovaným uzavřena za pomoci prostředků komunikace na dálku v souladu s § 561 odst. 1 občanského zákoníku [...] a s § 562 odst. 1 občanského zákoníku“. Následně pak soud konstatuje svůj závěr, 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 předchůdce žalobkyně a zadání unikátního SMS kódu v tomto rozhraní.“

Soud zde pak také odkázal na předchozí judikaturu (rozsudek Krajského soudu v Ostravě ze dne 28. 1. 2016, sp. zn. 37 ICm 4495/2014 nebo rozsudek Krajského soudu v Brně ze dne 5. 6. 2017, sp. zn. 33 ICm 547/2016), podle které je pro uzavření spotřebitelské smlouvy jiný typ elektronického podpisu postačující a nevyžaduje se kvalifikovaný elektronický podpis. Toto rozhodnutí navíc výslovně konstatuje, že citovaná rozhodnutí vycházela z právní úpravy zák. o el. podpisu, ale jejich závěry jsou platné i za současné právní úpravy zák. o službách vytvářejících důvěru.

#### 14.4.1 K písemnému právnímu jednání lze použít telefax

Nejvyšší soud se ve svém rozhodnutí ze dne 3. 5. 2016, sp. zn. 23 Cdo 4093/2015 zabýval otázkou, zda lze za písemné považovat právní jednání provedené a doručené prostřednictvím telefaxu. Rozhodnutí se na první pohled může zdát jako věcně nerelevantní, nicméně jeho závěry mohou být použitelné i pro právní jednání prováděná elektronickým prostředkem.

V této věci šlo o to, že výzva ke jmenování rozhodce byla doručena právnímu zástupci žalobkyně prostřednictvím telefaxu. Soud prvního stupně k tomu konstatoval, že „[d]oručení faxem má stejnou relevanci jako doručení poštou, námitka dlužníka, že vzhledem k důležitosti výzvy ke jmenování rozhodce, měla být tato výzva doručena do vlastních rukou poštou, je bezpředmětná.“ Ke stejnému závěru dospěl i odvolací soud, podle kterého faxová výzva žalované splňovala náležitosti platného právního úkonu učiněného v písemné formě – bylo možné

jednoznačně určit jejího odesílatele, adresáta i obsah. Součástí byl i vlastnoruční podpis právního zástupce žalované.

V dovolacím řízení pak Nejvyšší soud uzavřel: „*Vzhledem k tomu, že v případě telefaxu se skenuje psaný text z listu papíru a zasílá se na jiný faxový přístroj, který zprávu přijme a vytiskne její kopii na list papíru, je v případě podepsané textové zprávy dodržen požadavek písemné formy, neboť lze identifikovat osobu, která právní úkon učinila. Lze tedy přijmout závěr, že právní úkon učiněný prostřednictvím telefaxu splňuje požadavek písemné formy, jestliže je podepsán osobou, která tento úkon činí.*“

Nejvyšší soud také nepřisvědčil námitce dovolatele, že výzva ke jmenování rozhodce měla být (vzhledem k důležitosti) doručena minimálně doporučeně poštou. V této souvislosti konstatoval, že strany si ujednaly pouze požadavek písemnosti výzvy a ten byl naplněn. Žádná další dohoda stran ohledně způsobu doručení výzvy nebyla. Soud tak uzavřel, že nelze přikládat větší váhu písemnému právnímu úkonu, který byl doručen doporučeně poštou než písemnému právnímu úkonu učiněnému faxem.

Rozhodnutí je z našeho pohledu důležité s ohledem právě na toto závěrečné konstatování o rovnosti písemného právního úkonu v podobě vlastnoručně podepsané písemnosti s písemným právním úkonem provedeným telefaxem. Tento závěr by mělo být možné vztáhnout i na písemný právní úkon provedený prostřednictvím kteréhokoliv elektronického prostředku.

Klademe si však otázku, zda je třeba trvat na požadavku soudu na existenci podpisu na odesílané faxové zprávě i za situace, kdy je z ní patrný obsah právního jednání a lze určit jednající osobu. Naplnění požadavku písemnosti tímto způsobem konstatoval v této věci i odvolací soud („*Faxová výzva žalované splňuje náležitosti platného právního úkonu učiněného v písemné formě, neboť lze jednoznačně určit jejího odesílatele, adresáta i obsah.*“). Podpis tak zřejmě považoval jako „něco navíc“ („*Součástí je i vlastnoruční podpis právního zástupce žalované.*“). Nejvyšší soud však konstatoval, že podpis je nezbytnou součástí tohoto právního jednání.

## 14.5 Doručení předžalobní výzvy e-mailem

Považujeme za vhodné zmínit také rozhodnutí Krajského soudu v Brně ze dne 9. 11. 2017, sp. zn. 27 Co 86/2017, ve kterém byl soud postaven před otázku platnosti doručení předžalobní výzvy prostřednictvím e-mailu.

Soud prvního stupně v této věci rozhodl, že žádný z účastníků nemá právo na náhradu nákladů řízení.<sup>574</sup> To odůvodnil tím, že žalobce soudu nepředložil předžalobní upomínku ve smyslu § 142a odst. 1 o. s. ř. a neprokázal její odeslání žalovanému. Vyšel z toho, že krom stanovených náležitostí musí být předžalobní upomínka zaslána v písemné formě a prokazatelným způsobem. Zaslání e-mailové upomínky nepovažoval soud prvního stupně za dostačující.

Odvolací soud vyšel z toho, že v daném případě komunikovali účastníci řízení při uzavírání smlouvy výhradně elektronicky e-mailem. Šlo o komunikaci pro jejich obchodní styk obvyklou a vedenou prostřednictvím žalovaným udávané e-mailové adresy, kterou odvolací soud považoval za adresu pro doručování dle § 142a odst. 1 o. s. ř.<sup>575</sup> Soud proto uzavřel, 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.*“<sup>576</sup>

Význam uváděného rozhodnutí spočívá v uznání výzvy zasláné e-mailem za písemné právní jednání. Odvolací soud se zde ani nepouštěl do úvahy, zda lze takovou výzvu považovat za podepsanou. To však nepovažujeme za nedostatek rozhodnutí a zřejmě absence podpisu nebyla ani v řízení namítána. Zároveň lze z rozhodnutí dovodit, že odvolací soud při posouzení předmětné věci vycházel i z jednání stran předcházejícího zaslání předžalobní výzvy. Pokud bychom tento závěr zobecnili na smlouvy uzavřené prostřednictvím elektronických prostředků typu e-mailu, pak by některá ze stran neměla úspěšně namítat neplatnost smlouvy z důvodu absence elektronického podpisu či jiného důvodu souvisejícího s elektronickou podobou smlouvy, když následně strany dle této smlouvy plnily a dále komunikovaly prostřednictvím prostředku užitého pro uzavření smlouvy.

<sup>574</sup> Usnesení Městského soudu v Brně ze dne 13. 12. 2016, sp. zn. 294 C 52/2016.

<sup>575</sup> Bod 23 rozhodnutí Krajského soudu v Brně ze dne 9. 11. 2017, sp. zn. 27 Co 86/2017.

<sup>576</sup> Ibid., bod 25.

## 14.6 E-mail musí být podepsán elektronickým podpisem

Městský soud v Praze jako soud odvolací v rozsudku ze dne 4. 12. 2018, č. j. 15 Co 356/2018-162 dospěl k závěru, že námitky proti výpovědi z nájmu prostor sloužících k podnikání, které žalobkyně podala e-mailem, nelze považovat za námitky v písemné formě, jelikož tento e-mail nebyl podepsán elektronickým podpisem. K témuž závěru dospěl v rámci dovolacího řízení i Nejvyšší soud, který konstatoval, že „[n]ámitky jsou právním jednáním, pro které je zákonem vyžadována písemná forma (§ 2314 o. z.), proto není důvodu posuzovat požadavky na zachování písemné formy u námitek odlišným způsobem, než jak je tomu u jiných právních jednání. Vzněs-la-li žalobkyně Námitky e-mailem ze dne 14. 6. 2016, který nebyl opatřen elektronickým podpisem, je závěr odvolacího soudu, že nedodržela písemnou formu Námitek, v souladu s judikaturou Nejvyššího soudu.“<sup>577</sup>

Odůvodnění tohoto rozhodnutí je velmi stručné. Nevyplývají z něj bohužel další relevantní skutkové skutečnosti, například, zda e-mailová adresa žalobkyně obsahovala její jméno a příjmení, zda byl e-mail zakončen jménem a příjmením žalobkyně či jestli žalobkyně dříve z této e-mailové adresy s žalovanou komunikovala a žalované byla tato adresa známa. Z rozhodnutí tedy nelze učinit nějaký zobecňující závěr ve vztahu k tématu. Je nicméně vhodné na toto rozhodnutí upozornit a vzít jej v úvahu kvůli jeho závěru o nenaplnění požadavku na písemnou formu prostřednictvím e-mailu.

## 14.7 Elektronický podpis prostý sám neobstojí

Postoupením pohledávky v elektronické podobě se zabýval Městský soud v Praze ze dne 8. 7. 2020, sp. zn. 18 Co 187/2018. V této věci byla vymáhána pohledávka postoupená na žalobce smlouvou, která „byla podepsána pomocí myši do prázdného pole na obrazovce a podpis pak byl přenesen na formulář, který poškozená nepodepsala“.<sup>578</sup> Smlouva byla uzavřena tak, že poškozená, která svou pohledávku postoupila, postupně na webových stránkách žalobce odklikávala jednotlivé kroky kontraktace a v jednom z kroků vyplnila v poli za pomoci myši svůj podpis.

<sup>577</sup> Rozhodnutí Nejvyššího soudu ze dne 22. 5. 2019, sp. zn. 26 Cdo 1230/2019.

<sup>578</sup> Bod 3 rozsudku Městského soudu v Praze ze dne 8. 7. 2020, sp. zn. 18 Co 187/2018.



Nalézací soud tak byl postaven před otázku, zda došlo k platnému postoupení pohledávky na žalobce, tedy zda byla platně uzavřena smlouva, resp. jestli byla řádně podepsána. Nalézací soud pak konstatoval, že k platnému uzavření smlouvy o postoupení pohledávky vůbec nemohlo dojít. Uvedl, že předpokladem uzavření jakékoliv smlouvy je plné srozumění smluvních stran s obsahem smlouvy a tato smlouva musí být podepsána. Podle soudu tak nebyla žalobcem předložená smlouva uzavřena, jelikož během online uzavírání smlouvy nebyl tento dokument poškozenou akceptován a poškozená nikdy k tomuto dokumentu nepřipojila svůj podpis. Její podpis nebyl vyplněn na žalobcem předloženém dokumentu, ale „*byl přenesen datovou formou na předmětný dokument, který poškozenou vyhotoven nebyl*“.<sup>579</sup>

Toto rozhodnutí bylo poté potvrzeno i odvolacím soudem. Ten uvedl, že účastníci postupní smlouvy si ve smyslu § 559 obč. zák. zvolili písemnou formu postupní smlouvy, která ke své platnosti vyžadovala podpis jednající osoby. Odvolací soud k tomu dovodil, že podepsanou osobu může český soud identifikovat se „*značnou úrovní důvěry*“ pouze v případě kvalifikovaného a zaručeného elektronického podpisu a zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu. Všechny ostatní elektronické podpisy je třeba přijmout jako důkaz, ale podle soudu nelze bez dalších tvrzení a důkazů mít za prokázané, že jde o podpis jednající osoby. Ve vztahu k předmětné věci dokonce soud uvádí, že se fakticky vůbec nemuselo jednat o podpis postupitelky či obrázek podpisu mohl být dokonce sejmuto z jiného dokumentu a bez vůle uvedené osoby mohl být vložen do dokumentu označeného jako postupní smlouva.<sup>580</sup>

Na první pohled se toto rozhodnutí nemusí jevit jako příliš šťastné. Mohlo by se z něj zdát, že nalézací a odvolací soud zde zcela pominuly vymezení elektronického podpisu v nařízení eIDAS.<sup>581</sup> Podpis postupitelky totiž tuto definici podle informací vyplývajících z rozhodnutí splní. Postupitelka zřejmě vytvořila pomocí myši obraz svého podpisu, tedy data, která používá k podepsání. Ta byla následně připojena ke postupní smlouvě jakožto jiným datům.

<sup>579</sup> Bod 5 rozsudku Městského soudu v Praze ze dne 8. 7. 2020, sp. zn. 18 Co 187/202018.

<sup>580</sup> Ibid., body 22 a 23.

<sup>581</sup> Čl. 3 odst. 10 nařízení eIDAS.

Soud však nezpochybnil, že by použitá technika nepředstavovala elektronický podpis prostý. Podle § 565 obč. zák. je na každém, kdo se dovolává soukromé listiny, aby dokázal její pravost a správnost. I kdyby byla soukromá listina použita proti osobě, která listinu zjevně podepsala, zavádí toto ustanovení pouze vyvratitelnou právní domněnku, že pravost a správnost listiny byla podepisující osobou uznána. Z předmětného rozhodnutí vyplývá, že žalovaný zpochybnil podpis na postupní smlouvě a žalobce neunesl břemeno tvrzení a důkazní, že jde skutečně o podpis postupitelky. Že důkazní břemeno v této souvislosti tížilo žalobce, vyplývá i z judikatury Nejvyššího soudu zmiňované v předchozím textu.

Domníváme se, že by předmětné rozhodnutí nemělo být zobecnováno v tom smyslu, že by soud měl při každém předložení listiny podepsané elektronickým podpisem prostým vyžadovat i další důkazy pro prokázání pravosti podpisu. K tomu by mělo dojít pouze v případech, že pravost podpisu bude v řízení zpochybněna. Opačný závěr není podle nás správný – při dokazování listinou podepsanou vlastnoručním podpisem také soud nebude vyžadovat v každém jednotlivém případě předložení znaleckého posudku posuzujícího pravost podpisu.

## 14.8 Písemnost jen s uznávaným elektronickým podpisem

Další zajímavé rozhodnutí, které odmítá užití elektronického podpisu prostého, je rozhodnutí Okresního soudu v Kladně ze dne 31. 8. 2021, sp. zn. 208 C 115/2021. Zde se soud věnoval smlouvě uzavřené v elektronické podobě tak, že žalovaný se nejprve elektronicky registroval jako zájemce o půjčku vyplněním formuláře na internetových stránkách. V rámci toho vyplnil své identifikační údaje a 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.

Soud zde konstatoval, že smlouva o zápůjčce ke své platnosti nevyžaduje písemnou formu právního jednání a lze ji tedy uzavřít v libovolné formě. Proto se soud nezabýval tím, zda smlouva byla uzavřena elektronicky v písemné formě.

Soud však uvedl, že patrně nebyla uzavřena ani v souladu s § 562 obč. zák., „neboť ani podle tvrzení žalobkyně nebyly využity žádné elektronické služby důvěryhodné identifikace a autentizace žalovaného (v úrovni vysoké či alespoň značné) v souladu s Nařízením Evropského parlamentu a Rady (EU)“.<sup>582</sup>

I přes svůj závěr o možnosti uzavřít předmětnou smlouvu v libovolné formě se v rozhodnutí soud také zabýval úvahou, zda byl o právním jednání učiněn spolehlivý záznam v elektronickém systému provedený systematicky, poslopně a chráněný proti změnám dle § 562 odst. 2 obč. zák., či zda byla smlouva elektronicky podepsána. K tomu soud uvedl, že „[z] předložených dokumentů také nevyplývá, že by k danému právnímu jednání došlo v elektronickém systému, v němž jsou záležitosti prováděny systematicky a poslopně a jsou chráněny proti změnám. Z hlediska § 561 o. z. je také zřejmé, že smlouva nebyla žalovaným elektronicky podepsána, a to nejen kvalifikovaným elektronickým podpisem (podle čl. 25 Nařízení eIDAS), ale ani některou z nižších úrovní elektronického podpisu (uznávaným či jen zaručeným elektronickým podpisem).“<sup>583</sup>

V rozhodované věci však podle soudu nebylo pochyb o tom, jaké osobě a za jakých podmínek byly finanční prostředky zapůjčeny. Výplata finančních prostředků byla prokázána výpisem z účtu právního předchůdce žalobkyně, a tím byla potvrzena totožnost osoby, která registraci provedla, a také skutečnost, že podle sjednaných podmínek převzala půjčenou částku. Nedostatek písemné formy tak nebyl dle soudu relevantní.<sup>584</sup>

Soud tak v tomto rozhodnutí nevzal v úvahu možnost podepsat právní jednání v soukromém právním styku pouze elektronickým podpisem prostým. Z rozhodnutí se jeví, že by za řádně podepsané elektronické právní jednání považoval pouze elektronický dokument podepsaný kvalifikovaným elektronickým podpisem, zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu nebo zaručeným elektronickým podpisem. Soud však i přes tuto skutečnost dospěl k závěru, že deficit písemnosti v dané věci je bez významu, jelikož předmětnou smlouvu bylo možné uzavřít i v jiné než písemné formě.

<sup>582</sup> Bod 9 rozhodnutí Okresního soudu v Kladně se v rozhodnutí ze dne 31. 8. 2021, sp. zn. 208 C 115/2021.

<sup>583</sup> Ibid.

<sup>584</sup> Ibid., body 4 a 10.

## 14.9 PIN jako elektronický podpis smlouvy

Jako příklad rozhodnutí, ve kterém soud vzal v úvahu smlouvu uzavřenou elektronicky a podepsanou vložení PIN kódu na webové stránce, lze zmínit také rozhodnutí Obvodního soudu pro Prahu 6 ze dne 27. 10. 2021, sp. zn. C 375/2021.

V této věci byla smlouva uzavřena za použití prostředků komunikace na dálku. Žalovaný prostřednictvím těchto prostředků požádal elektronicky podepsaným návrhem smlouvy žalobkyni o její uzavření. Elektronický podpis tohoto návrhu byl připojen na základě zadaného kódu, který byl žalovanému zaslán prostřednictvím SMS. Žalobkyně tento návrh akceptovala opatřením smlouvy elektronickým podpisem pověřeného pracovníka žalobkyně.

K uvedenému způsobu elektronické kontraktace soud konstatoval, že elektronické podpisy stran byly učiněny v souladu se zák. o službách vytvářejících důvěru. Na základě tohoto závěru soud nejprve vystavil elektronický platební rozkaz, který byl však následně zrušen pro jeho nedoručení žalovanému. Následně vydal předmětné rozhodnutí, kterým žalobě vyhověl a žalobci přiznal úhradu dlužné částky.

## 14.10 Uznání pouze kvalifikovaných a zaručených podpisů

Zcela opačně však rozhodl Okresní soud v Karviné rozhodnutím ze dne 14. 1. 2022, sp. zn. 24 C 233/2021.

V této věci měl žalobce se žalovaným uzavřít smlouvu o zápůjčce, na základě které žalobce poskytl žalovanému převodem na jeho bankovní účet peněžní prostředky. Žalobce poskytl zápůjčku prostřednictvím své webové stránky. Na ni si žalovaný nejprve přečetl nabídku na uzavření smlouvy a nastavil si splatnost a výši zápůjčky. Poté žalovaný vyplnil na webové stránce žalobce formulář, do kterého zadal osobní údaje včetně svého telefonního čísla a emailové adresy. Následně žalovaný zaškrtl políčko potvrzující seznámení se zněním smlouvy a všeobecných obchodních podmínek a projevil souhlas s jejich zněním. Smlouva o zápůjčce měla být žalovaným podepsána elektronicky – PINem, který byl zaslán na jeho telefonní číslo.

Smlouva předložená žalobcem soudu obsahovala podpisy za žalobce, a za žalovaného místo vlastnoručního podpisu číslo PIN kódu. Soud se věnoval

otázce, zda lze uznat tento způsob podpisu za platný, přičemž konstatoval, že na smlouvě chybí podpis žalovaného. K tomu dospěl na základě úvahy, že podle nařízení eIDAS má účinky vlastnoručního podpisu jen kvalifikovaný elektronický podpis. Následně soud vyložil, jaké požadavky na kvalifikovaný elektronický podpis klade toto nařízení. Vyložil i požadavky kladené na zaručený elektronický podpis. V návaznosti na to konstatoval, že PIN kód uvedený na smlouvě kvalifikovaným či zaručeným elektronickým podpisem není, neboť tyto podmínky nesplňuje. Za situace, že ani z ostatních předložených důkazů nevyplývá, že by žalovaný smlouvu o zápůjčce uzavřel, dospěl soud k závěru, že pro absenci podpisu žalovaného je smlouva neplatná.

Soud sice shledal neplatnost i z dalšího důvodu souvisejícího s neposouzením schopnosti úvěr splácet. Rozhodnutí však v části věnované elektronickému podpisu nelze podle našeho názoru hodnotit jinak, než jako nepřilíš šťastné. Soudem citovaný čl. 25 odst. 2 nařízení eIDAS zakotvuje pravidlo, že napříč Evropskou unií a některými třetími zeměmi musí být kvalifikovaný elektronický podpis postaven naroveň vlastnoručnímu podpisu. To ale neznamená, že by za vlastnoruční podpis neměl být považován i jiný elektronický podpis, pokud příslušný právní řád takový účinek jinému elektronickému podpisu přiznává. To činí náš zák. o službách vytvářejících důvěru v § 7, který umožňuje použití jakéhokoliv elektronického podpisu, není-li právně jednáno vůči veřejnoprávnímu podepisujícímu či další osobě při výkonu působnosti. Zdá se také, že soud přehlédl odstavec 1 jím citovaného čl. 25 nařízení eIDAS. Zde totiž nařízení eIDAS konstatoje, že elektronickému podpisu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické podpisy. Z rozhodnutí se jeví, že by kromě kvalifikovaného elektronického podpisu uznal za platný i zaručený elektronický podpis. Byť soud v rozhodnutí zmínil § 7 zák. o službách vytvářejících důvěru, nevěnoval se již odůvodnění svého závěru, že za platný podpis lze uznat pouze zaručený a kvalifikovaný elektronický podpis.

### **14.11 Neplatnost smlouvy podepsané vložení SMS kódu**

Okresní soud v Berouně se v rozhodnutí ze dne 21. 12. 2021, sp. zn. 18 C 225/2021, zabýval otázkou platnosti úvěrové smlouvy podepsané

vložení SMS kódu zasláního na telefonní číslo žalovaného po jeho předchozí identifikaci.

K uzavření smlouvy v této věci mělo dojít tak, že žalovaný vyplnil požadované údaje a po automatizovaném schvalovacím procesu byla žádost o úvěr 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. Žalovaný poté kód z SMS vložil do zobrazeného pole a smlouva byla následně žalovanému zaslána na jeho e-mailovou adresu. Na základě toho byly žalovanému poukázány peněžní prostředky. Soud v rozhodnutí uvádí, že identita žalovaného byla ověřena kopií občanského průkazu a kopií záhlaví výpisu z bankovního účtu žalovaného vedeného na jeho jméno. Považoval za prokázanou časovou souslednost mezi žádostí o úvěr, prověřením žádosti, odsouhlasením žádosti ze strany žalobkyně, oznámením o schválení úvěru žalovanému a následným zasláním SMS kódu žalovanému za účelem podpisu úvěrové smlouvy. Smlouva měla být podepsána tak, že u jména žalovaného bylo ve smlouvě v podobě PDF dokumentu připojeno datum a čas podpisu spolu s IP adresou a kódem z SMS zasláního žalovanému. Za žalobkyni smlouvu podepsala osoba oprávněná jednat za žalobkyni připojením grafického znázornění jejího podpisu.

Soud však konstatoval, že k předložené smlouvě nejsou připojeny žádné elektronické podpisy. K tomuto závěru dospěl soud přesto, že neměl pochybnost o tom, že žalobkyně zaslala žalovanému SMS kód k potvrzení přijetí návrhu úvěrové smlouvy. Nepovažoval však za prokázáno, že žalovaný zasláním kódem podepsal právě smlouvu předloženou žalobkyní. Předložený PDF dokument neobsahoval „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 ve smyslu ustanovení článku 26 eIDAS).“ Nadto soud konstatoval, že „není soudu zjevné, jak je možné do elektronického dokumentu pojmout vlastnoruční podpis, tedy opět může jít pouze o grafickou podobu, tentokrát vlastnoručního podpisu, která byla vložena přímo do dat dokumentu, nikoliv k datům obsahujícím smlouvu připojený.“ Z rozhodnutí také vyplývá, že soud by za elektronický

podpis považoval pouze data připojená k jiným datum umožňujícím ověřit, že po jejich připojení již dokument nedoznal žádné změny.

V tomto rozhodnutí soud tedy opomíjí existenci elektronického podpisu prostého a zcela rezignuje na úvahu o tom, zda předložená smlouva nemohla být podepsána touto základní úrovní elektronického podpisu. Soud za elektronický podpis považoval pouze zaručený a kvalifikovaný elektronický podpis, což je závěr v rozporu s nařízením eIDAS a zák. o službách vytvářejících důvěru. Jako nesprávný se nám jeví také závěr o tom, že elektronický podpis musí zajistit integritu dat. Zajištění integrity dat je nepochybně přidaná hodnota zaručeného elektronického podpisu a vyšších úrovní elektronického podpisu. Lze jí však docílit i prostřednictvím jiných technik než elektronickým podpisem. Elektronický dokument bude možné například opatřit elektronickou pečetí, jejíž smyslem je kromě zaručení původu dat také zajištění jejich integrity. Lze také k záznamům o právním jednání užít takový systém, který bude ve smyslu § 562 odst. 2 obč. zák. zajišťovat provedení těchto záznamů systematicky, posloupně a s ochranou proti změnám. Ani vlastnoruční podpis nezaručí, že by s obsahem listinné smlouvy nebylo nijak manipulováno. Pokud nepůjde o listinný dokument o jednom listu papíru či nebude podepisován každý list, bude pro ochranu dokumentu proti výměně některých listů či jiné manipulaci s obsahem třeba užít dalších prostředků. Nedomníváme se tak, že by elektronický podpis měl bez dalšího zajišťovat integritu podepsané smlouvy. I pokud bychom přistoupili na závěr, že soud má v každém případě požadovat elektronický dokument se zajištěnou ochranou integrity obsahu, pak je třeba připustit naplnění tohoto požadavku i jiným způsobem, než pouze elektronickým podpisem.

#### **14.12 Prokázání identity podepisujícího a integrity dokumentu**

Vlastnostmi elektronických podpisů a dokumentů se zabýval také Okresní soud v Karviné ve svém rozhodnutí ze dne 27. 1. 2022, sp. zn. 109 C 380/2021.

V něm soud bohužel neuvádí, jakým způsobem měla být smlouva uzavřena. Konstatuje pouze, že žaloba byla odůvodněna tvrzením, že právní předchůdce žalobkyně a žalovaný uzavřeli smlouvu o úvěru prostřednictvím elektronických prostředků komunikace na dálku. Soud si položil otázku, jak lze smlouvu elektronicky podepsat. Konstatoval, že ve vztahu k písemně

uzavřené smlouvě je zřejmé, že lze smlouvu písemně uzavřít také prostřednictvím elektronických prostředků. Za podstatnou náležitost elektronicky uzavřené smlouvy považoval elektronický podpis jednající osoby. Pokud by žalovaný podle soudu smlouvu o úvěru podepsal připojením určitých dat sloužících k podpisu, vždy je z hlediska dokazování podstatné prokázat jednak identitu jednající osoby a jednak integritu (nezměnitelnost) podepsaného dokumentu. Dostatečnou míru věrohodnosti těchto vlastností však podle soudu poskytují pouze kvalifikovaný nebo uznávaný elektronický podpis. Všechny ostatní elektronické podpisy tyto záruky dle soudu neposkytují a je třeba v řízení výše uvedené skutečnosti prokázat dalšími věrohodnými důkazy. Na základě toho soud uzavřel, že písemná forma v řízení nebyla prokázána, písemná ani jiná smlouva nebyla uzavřena, a žalobu tak v celém rozsahu zamítl.

Z rozhodnutí se jeví, že by soud uznal za platný i elektronický podpis prostý. To však pouze za splnění požadavku prokázání identity podepisující osoby a zajištění integrity podepsaného dokumentu, přičemž oba by měl podle soudu zajistit užitý elektronický podpis. Prokázat identitu podepisující osoby je v řízení klíčové. Smysl dává i požadavek na prokázání, že smlouva byla podepsána v podobě předložené soudu. To, jak tyto požadavky vyložil soud, ale nemá oporu v zákonu. V této práci již bylo na více místech konstatováno, že elektronický podpis nemusí sloužit k prokázání totožnosti podepisující osoby, ale jde pouze o data používaná k podepsání. K identifikaci podepisujícího může dojít jiným způsobem než užitím elektronického podpisu. Rovněž se nedomníváme, že by musela být *a priori* zajištěna integrita elektronicky podepsané smlouvy. Pokud nebude integrita elektronického dokumentu technicky zajištěna, ale strany obsah smlouvy nebudou rozporovat, pak se domnívám, že není třeba zajištění integrity dokumentu dokazovat. Zároveň nám není jasné, z čeho vyplývá závěr soudu, že integritu smlouvy by měl zprostředkovat elektronický podpis. Integritu dokumentu lze totiž docílit i jinými prostředky, než pouze elektronickým podpisem.<sup>585</sup>

<sup>585</sup> Této otázce se věnujeme například v kapitole 6.5 o dynamickém biometrickém podpisu.





## 15 SOUDY, SMLOUVY UZAVŘENÉ ONLINE A ELEKTRONICKÉ DŮKAZY

Podle našeho názoru je na místě, aby se elektronickým smlouvám a důkazům více otevřely i soudy. Neplédujeme zde rozhodně za to, aby soudy považovaly za platné a řádně elektronicky podepsané jakékoliv smlouvy opatřené jen elektronickým podpisem prostým bez dalších úvah a dokazování. Je jistě třeba poskytnout ochranu těm účastníkům sporu, kteří smlouvu zjevně nepodepsali či ji podepsali s jiným obsahem než s tím, který byl předložen soudu. Nelze na základě požadavku na efektivitu právního styku (především v případě *e-commerce*) a bezformálnosti zcela rezignovat na požadavek určité formy pro některá právní jednání.<sup>586</sup> Na druhou stranu ale není na místě elektronicky podepsané smlouvy odmítat jen z toho důvodu, že nebyly podepsány některou z vyšších úrovní elektronického podpisu. Vhodné není ani přehnané adorování vlastnoručního podpisu oproti elektronickému. Ani vlastnoruční podpis nezaručuje bez dalšího pravost listiny. Lze v této souvislosti odkázat na konstatování Nejvyššího správního soudu:

*„Podpis, není-li úředně ověřen, totiž za běžných okolností není nic víc než omezeně spolehlivý autentifikační prostředek – jeho přítomnost na podání obvykle zvyšuje pravděpodobnost, že je učinil vskutku ten, kdo v něm je za podatele označen, ale málokdy o tom dává jistotu. Za normálních okolností, chovají-li se lidé rozumně a poctivě, z čehož je nutno vycházet, je nepochybně jakousi ‚originální značkou‘ toho, kdo se podepsal. Není však příliš obtížné běžný (neověřený) podpis padělat, napodobit či vytvořit (ať ve zlém či dobrém úmyslu) podání pouze navenek vypadající jako učiněné osobou, jež je v něm za podatele deklarována, a toto podání podepsat zcela jiným podpisem, než jaký skutečně užívá osoba, jíž je podání přičítáno. Proto je třeba za běžných okolností vycházet z toho, že ten, kdo je v podání jako podatel označen, jím je, ledaže vyvstanou rozumné důvody k jiné domněnce či pochybě, že tomu je či může být jinak; tuto domněnku či pochybu pak musí správní orgán prověřit a zařídít se podle výsledků svých zjištění.“<sup>587</sup>*

<sup>586</sup> Již v roce 1941 Fuller uváděl, že „[n]avzdory údajné moderní tendenci k ‚neformálnosti‘ není příliš důvodů domnívat se, že problém formy v budoucnu zmizí. Záměry, které jsou základem používání formálních náležitostí, si zachovají svou relevanci, dokud budou lidé jeden druhému skládat sliby.“ (FULLER, 1941, op. cit., s. 822).

<sup>587</sup> Rozhodnutí Nejvyššího správního soudu ze dne 27. 7. 2017, sp. zn. 2 As 80/2017.

Podobně Korbel s Melzerem uvádí, že listinná forma písemného právního jednání s vlastnoručním podpisem negarantuje stoprocentní určitost autora podpisu. Vytváří podle nich pouze důkaz, na jehož základě lze s určitou pravděpodobností předpokládat, že autorem projevu vůle na listině je osoba, která ji podepsala.<sup>588</sup> Mohlo by se zdát, že nejvyšší míru právní jistoty a důkazní síly bude představovat úředně ověřený vlastnoruční podpis. Ten by se dal považovat za nejvyšší formu vlastnoručního podpisu.<sup>589</sup> Jak ale upozorňuje Smejkal, nelze vyloučit nepravdivé ověření na základě protiprávního jednání úřední osoby, provedení ověření na základě odcizeného nebo padělaného dokladu, ani následné pozměnění listiny s ověřeným podpisem. Poukazuje také na spory o pravost podpisu, ve kterých písmoznalci přicházejí s protichůdnými posudky. Z těchto důvodů je podle něj „*třeba absolutizování podepsaných papírových dokumentů s úředně ověřeným podpisem a nezlomnou vírou v jejich nedotknutelnost odmítnout.*“<sup>590</sup>

Stále více se začínají objevovat rozhodnutí soudů, ve kterých soudy již vychází z občanského zákoníku a z jeho § 561 a § 562 či dalších relevantních ustanovení, zák. o službách vytvářejících důvěru v elektronické transakce anebo nařízení eIDAS. Některé soudy uznávají za platné smlouvy opatřené pouze elektronickým podpisem prostým. Objevují se však stále i rozhodnutí, ve kterých soudy konstatují neplatnost takto uzavřených smluv. Soudy v těchto rozhodnutích buď projevují názor, že za elektronický podpis by měl být akceptován pouze kvalifikovaný či zaručený elektronický podpis, případně kladou na dokazování elektronickým podpisem prostým nepřiměřené nároky. Při dokazování dokumenty, bez ohledu na to, zda listinnými či elektronickými, je třeba brát v úvahu i další skutečnosti. Důkazní spolehlivost dokumentu může být podle Polčáka konstatována až jako výsledná kombinace jednotlivých skutkových informací, tedy vztahu k prokazované skutečnosti, obsahových a formálních parametrů a koherence s ostatními prokazovanými skutečnostmi. Nelze tedy podle něj, až na výjimky, a to ani v případě znaleckého potvrzení pravosti dokumentu, bez dalšího jen sylogisticky vycházet z obsahu dokumentu a považovat jej za spolehlivě prokázanou pravdu.<sup>591</sup>

<sup>588</sup> KORBEL, MELZER, 2014, op. cit., s. 35.

<sup>589</sup> MATEJKA, CHUM, 2002, op. cit., s. 28.

<sup>590</sup> SMEJKAL, 2019, op. cit., s. 345.

<sup>591</sup> POLČÁK, 2011, op. cit., s. 54.

To odpovídá i závěrům Nejvyššího soudu. Ten v rozhodnutí ze dne 26. 11. 2019, sp. zn. 24 Cdo 1110/2019 konstatoval:

*„I nejednoznačný závěr znalce týkající se pravosti podpisu uvedenou osobou na posuzované listině ještě neznamená, že soud na podkladě dalších provedených důkazů a s přihlédnutím ke všemu, co v řízení vyšlo najevo, nemůže nakonec dospět k jednoznačnému závěru, že podpis na předmětné listině není pravým podpisem dotčené osoby. Soud je totiž povinen hodnotit nejen předmětný znalecký posudek včetně výsledku znalce, ale také další v řízení provedené důkazy, a to s přihlédnutím ke všemu, co v řízení vyšlo najevo. Teprve po takovém zhodnocení všech právně významných okolností může soud na podkladě přijatých důležitých skutkových zjištění formulovat závěr o skutkovém stavu, jenž posléze podrobí právnímu posouzení věci.“*

Soudy by v případě tvrzené neplatnosti elektronicky uzavřené smlouvy měly vycházet i z jednání stran následujícího po sporném uzavření smlouvy. Zejména při dokazování elektronickým podpisem prostým bude k prokázání jeho pravosti zřejmě potřeba dalších důkazů (k tomu také viz výše). Podobně například Krajský soud v Brně v dříve rozebíraném rozhodnutí vzal v úvahu i jednání stran předcházející zaslání předžalobní výzvy.<sup>592</sup> Pokud by strany sporné smlouvy následně dle ní plnily a dále spolu čile komunikovaly prostřednictvím prostředku užitého pro uzavření smlouvy, neměl by podle našeho názoru soud učinit závěr o neplatnosti smlouvy jen pro její elektronickou formu a podepsání elektronickým podpisem prostým. Pro tyto účely je například na Slovensku v rámci zvažované rekodifikace občanského práva navrženo zavedení vyvratitelné právní domněnky. Podle ní by se předpokládalo, že projev vůle podepsaný kvalifikovaným elektronickým podpisem uskutečnila tato osoba. Podobná domněnka by platila, pokud by byl projev vůle uskutečněný z elektronické adresy, kterou určitá osoba používala v předcházejícím styku s adresátem anebo kterou oznámila adresátovi či veřejně.<sup>593</sup>

<sup>592</sup> Rozhodnutí Krajského soudu v Brně ze dne 9. 11. 2017, sp. zn. 27 Co 86/2017.

<sup>593</sup> Pracovní návrhy paragrafových znění předkladané na veřejnou a odbornou diskusi. *ministerstvo spravodlivosti SR* [online]. [cit. 11. 2. 2022]. Dostupné z: <https://www.justice.gov.sk/aktualne-temy/rekodifikacia-sukromneho-prava/>

## 15.1 Shrnutí k aktuálním trendům soudního rozhodování

V soudní praxi se začínají stále více objevovat rozhodnutí, ve kterých se soudy musí potýkat s elektronicky podepsanými smlouvami. V některých z nich již vychází z příslušných ustanovení občanského zákoníku, zák. o službách vytvářejících důvěru a nařízení eIDAS. Lze nalézt rozhodnutí, ve kterých soudy uznávají za platné smlouvy opatřené pouze elektronickým podpisem prostým i v podobě zadání PINu zasláného přes SMS na telefonní číslo podepisující osoby, která byla předtím identifikována.

Na druhou stranu se lze však setkat také s rozhodnutími, ve kterých soudy tuto nejnižší úroveň elektronického podpisu odmítají. Trend v těchto rozhodnutích lze shrnout takto:

1. Soudy v nich mají tendenci připisovat platnost téměř výhradně zaručenému elektronickému podpisu a vyšším úrovním elektronického podpisu.
2. Elektronický podpis má prokázat identitu jednajících osoby.
3. Je třeba prokázat připojení dat představujících podpis k datům představujícím předloženou smlouvu.
4. Elektronický podpis má zajistit integritu dokumentu. Některé soudy v této souvislosti zkoumají, zda jsou smlouvy vedeny v elektronickém systému se záznamy údajů o právním jednání vedeném systematicky, poslušně a s ochranou proti změnám dle § 562 odst. 2 obč. zák.

Požadavky soudů v těchto rozhodnutích lze shrnout tak, že v nich soudy v zásadě vyžadují naplnění požadavků na zaručené elektronické podpisy v čl. 26 nařízení eIDAS.

Zcela souhlasíme se závěrem prezentovaným Korbelem, Kovářem a Jarošem, kteří konstatují: „*[N]ázor, že by soudy měly v soukromém právu uznávat pouze kvalifikované elektronické podpisy nebo zaručené podpisy založené na kvalifikovaném certifikátu, a nikoli běžné zaručené podpisy nebo prosté elektronické podpisy, považujeme za ničím nepodložený, přímo odporující § 7 ZSVD a tím pádem protiprávní a zcela neudržitelný. Požadavek podepisování pouze vyššími úrovněmi elektronického podpisu je s ohledem na digitální (ne)kompetence všech vrstev naší populace i praktické aspekty nenaplnitelný, zákon ho nevyžaduje a neměla by ho k samotné platnosti elektronického jednání nerealisticky vyžadovat ani judikatura.*“<sup>594</sup>

<sup>594</sup> KORBEL, KOVÁŘ, JAROŠ, 2021, op. cit., s. 13.

Na základě soudních rozhodnutí citovaných v této kapitole lze však konstatovat, že některé soudy by tento závěr zřejmě nesdílely a rozhodují v rozporu s ním. S odkazem na § 562 odst. 1 obč. zák. má právní jednání umožnit určení jednající osoby. Nesdílíme však závěr, že by elektronický podpis měl sám o sobě jednoznačně identifikovat jednající osobu, což je požadavek, který – zdá se – někteří soudci na elektronický podpis kladou. Z § 561 odst. 1 a § 562 odst. 1 obč. zák., ze zák. o službách vytvářejících důvěru či z nařízení eIDAS nelze dovodit, že by prostý elektronický podpis měl tuto funkci plnit. Takovou funkci neplní bez úředního ověření ani vlastnoručního podpisu.

Vlastnoruční podpis krom jiných plní také funkci důkazní, identifikační či pravostní. Žádnou z nich však nebude úředně neověřený vlastnoruční podpis plnit dokonale. Vlastnoruční podpisy stejné osoby ze své podstaty nikdy nebudou totožné. Podpisový stereotyp se v čase mění. Pokud odhlédneme například od podpisových vzorů, nemá nikdo povinnost podepisovat se stále stejně. V některých případech se podepisující může podepsat jménem a příjmením, jindy pouze příjmením nebo za použití odlišného grafického znázornění podpisu. Nečitelný podpis sám o sobě k identifikaci jednající osoby nestačí a dojde k ní pouze ve spojení s dalšími údaji uvedenými v právním jednání. Bude-li právně jednáno vůči jiné osobě – až již v rámci soukromého či veřejného práva – a tato osoba z předchozího styku podpis nebude znát, zřejmě se tato osoba bez dalšího nebude zabývat tím, zda jde skutečně o podpis tvrzené podepisující osoby. Totéž platí pro soud. Pokud v řízení nebude zpochybňován podpis na listině, soud sám o sobě jeho pravost také hodnotit nebude. Domníváme se tak, že požadavky kladené některými soudy na elektronicky podepsané právní jednání neodpovídají požadavkům, které by tyto soudy kladly na listinné vlastnoručně podepsané právní jednání.

Je také chybné číst čl. 25 odst. 2 nařízení eIDAS<sup>595</sup> tak, že jiný než kvalifikovaný elektronický podpis nemůže mít účinky vlastnoručního podpisu. Nařízení totiž také konstatuje, že jím není dotčeno vnitrostátní právo týkající se uzavírání a platnosti smluv či jiných právních nebo procesních povinností

<sup>595</sup> „Kvalifikovaný elektronický podpis má právní účinek rovnocenný vlastnoručnímu podpisu.“

týkajících se formy.<sup>596</sup> V návaznosti na to dává zák. o službách svobodu volby úrovně a typu elektronického podpisu při soukromoprávním jednáním.<sup>597</sup>

Posuzovaná soudní praxe okresních soudů se zpravidla týká poskytování tzv. spotřebitelských úvěrů. Mohlo by se tak zdát, že soudy mohou mít tendenci poskytovat ochranu slabší straně. To lze obecně hodnotit kladně. Občanský zákoník na ochraně slabší strany stojí. V souladu s literaturou lze přijmout závěr, že slabší postavení může vyplývat i z neobezřetnosti, lehkomyšlnosti, nepřipravenosti či z nutnosti přistoupit na nevýhodné podmínky ze sociálních či osobních důvodů. Odkazuje se pak na obecnou mravní zásadu, že zneužití neznalosti nebo tísně je nemravné.<sup>598</sup> Pokud by ale soudy skutečně při odmítání elektronického podpisu prostého byly vedeny snahou o ochranu slabší strany, měly by to transparentně konstatovat v odůvodnění rozhodnutí. V odůvodnění by se zároveň měli vypořádat s již zmíněnými ustanoveními zák. o službách vytvářejících důvěru a nařízením eIDAS, doktrinálními závěry k elektronickému podpisu prostému a zřejmě se také věnovat funkcím písemné formy a podpisu.

<sup>596</sup> Čl. 2 odst. 3 nařízení eIDAS.

<sup>597</sup> Srov. § 7 zák. o službách vytvářejících důvěru.

<sup>598</sup> RABAN, 2019, op. cit., s. 59.

## ZÁVĚR

Tato monografie se zaměřujeme na aktuální trendy a perspektivy elektronicky uzavřených smluv. V jejím textu stavíme na základech dříve dosažených závěrů právní vědy, které klademe do kontextu vývoje informačních technologií a vyvozujeme z nich aktuální závěry. Na nové otázky virtualizace kontrakčního procesu tak nahlížíme prizmatem civilistické právní vědy. Dříve přijaté doktrinální názory jsme se snažili kriticky zkoumat a klást do vzájemného kontextu s jinými názory, rozhodovací praxí a vývojem v oblasti elektronické kontraktace. Na tomto základě jsme formulovali vlastní závěry prezentované napříč textem této monografie.

Při zkoumání jednotlivých relevantních oblastí jsme vždy postupovali od obecných otázek ke konkrétním. Nejprve jsme se tak věnovali teoretickým východiskům uzavírání smluv online včetně významu uzavírání smluv online v současné digitalizované společnosti.

Následně jsme se přesunuli k roli digitálních technologií při vyjednávání a uzavírání smlouvy. Kromě závěrů, jakým způsobem jsou právním řádem upraveny elektronická kontraktace a podepisování, jsme se zaměřili na jednotlivé úrovně elektronických podpisů a vybrané techniky elektronického podepisování nebo některé elektronické nástroje a platformy využívané pro kontraktaci.

Na to jsme navázali částí věnovanou využití digitálních technologií po uzavření smlouvy. Základem této části byl text věnovaný dokazování prostřednictvím elektronických důkazů v civilním procesu. Veškeré dříve dosažené závěry byly následně konfrontovány s dřívější judikaturou vyšších soudů a současnou dostupnou rozhodovací praxí nižších soudů.

V monografii se věnujeme otázkám, které se na první pohled mohou zdát spíše jako otázky technologického charakteru – jsou diskutovány například jednotlivé typy elektronického podpisu vymezené nařízením eIDAS, různé druhy podpisových technik či způsoby archivace elektronicky uzavřených smluv. Nutnost věnovat se těmto otázkám však vyplývá z právních z předpisů, ať již z občanského zákoníku a jeho pravidel k naplnění písemné formy elektronickým prostředkem či domněnky spolehlivosti záznamů o právních



jednáních v elektronickém systému nebo z dalších speciálních unijních a vnitrostátních předpisů.

V rámci monografie také v dílčích částech rozebíráme moderní aspekty kontraktace, zaměřujeme se na související aspekty smart kontraktů, využití DLT (nejen ke kontraktaci, ale rovněž k archivaci) a také se věnujeme například specifickým aspektům kontraktace spotřebitelské (a to včetně souvislostí, kdy předmětem smlouvy je digitální obsah).

Konstatujeme závěr, že samotný právní řád uzavírání smluv prostřednictvím elektronického prostředku a elektronickému podepisování překážky neklade. Občanský zákoník vychází z principu autonomie vůle, smluvní svobody a bezformálnosti. Pokud to nezakazuje zákon či ujednání stran, lze pro smlouvu zvolit libovolnou formu a prostředek jejího uzavření. Občanský zákoník nedělá v běžných právních vztazích rozdíl mezi písemností v listinné podobě podepsané vlastnoručním podpisem a v podobě elektronického dokumentu opatřeného elektronickým podpisem. Při uzavírání smluv mají účastníci volnost ohledně typu a úrovně elektronického podpisu, který zvolí pro podepsání smlouvy. Nadto argumentujeme, že požadavek písemnosti naplní i nepodepsaná právní jednání provedená elektronickým prostředkem, bude-li takový prostředek umožňovat identifikaci jednající osoby a zjištění obsahu právního jednání.

Na základě zkoumání relevantních soudních rozhodnutí uzavíráme, že rozhodovací praxe nižších soudů je v této oblasti nejednotná a chybí zde rozhodnutí Nejvyššího soudu s řádně odůvodněným závěrem k užívání elektronického podpisu prostého. Takové rozhodnutí by mělo zásadní význam pro praxi. Nyní totiž účastníci smluv podepsaných elektronickým podpisem prostým nemají právní jistotu ohledně vymahatelnosti těchto smluv vzhledem k množství rozhodnutí, která se užití základní úrovně elektronického podpisu brání a spíše hledají důvody pro konstatování neplatnosti takto uzavřených smluv. Těmi jsou závěry soudu o nedostatečné identifikaci jednající osoby elektronickým podpisem prostým či skutečnost, že tento podpis nezařísťuje integritu podepsaného dokumentu.

Při elektronickém podepisování se bez dalších souvislostí jako nejvhodnější zdá užití kvalifikovaného elektronického podpisu či zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu. V případě

zaručeného elektronického podpisu se jeho důvěryhodnost odvíjí od důvěry v osobu, která vydává data pro vytváření tohoto podpisu. Z rozhodovací praxe se zdá, že každý z uvedených elektronických podpisů by české soudy akceptovaly jako důkaz. Lze se domnívat, že by se české soudy nebránily ani užití dynamického biometrického podpisu, pokud by byla současně zajištěna i integrita podepsaného dokumentu. V případech užití jiných typů elektronického podpisu prostého je třeba pamatovat na zajištění dalších důkazních prostředků, kterými bude účastník smlouvy schopen prokázat zejména identifikaci podepisující osoby, skutečnost, že svůj podpis ke smlouvě připojila, a že byla podepsána smlouva ve znění předloženém soudu. Toto konstatování má původ v závěrech o zákonnosti podepisování elektronickým podpisem prostým, jehož užití je v praxi vysoce frekventované. Je však třeba vnímat při jeho užití i rizika, která tato úroveň podpisu přináší a která byla v textu práce rozebrána.

Vymahatelnost závazků z elektronicky uzavřených smluv závisí rovněž na způsobu jejich dlouhodobé archivace. Jako ideální způsob se v praxi navrhuje užití záznamů údajů o právních jednáních v elektronickém systému prováděných systematicky, poslučně a s ochranou proti změnám.

Lze identifikovat oblasti (typicky *e-commerce*), ve kterých při zachování efektivit právního styku téměř není možné užít listinné, vlastnoručně podepsané smlouvy. Na druhou stranu u jiných smluv mohou účastníci naopak preferovat jejich uzavření prostřednictvím vlastnoručně podepsané smlouvy. Jako příklad lze uvést smlouvy podepsané před notářem či advokátem spolu s ověřením podpisu.

V literatuře lze identifikovat názory o mnohem větší bezpečnosti elektronických podpisů oproti vlastnoručním podpisům. S tím lze zřejmě minimálně v případě elektronických podpisů založených na kvalifikovaném certifikátu do jisté míry souhlasit. Opět je ale třeba vzít v úvahu dlouhodobou archivaci. Uchovávaní bude jednodušší v případě vlastnoručně podepsané smlouvy. U ní v zásadě není třeba užití nějakých dalších prostředků. Účastník je však vázán omezeným počtem stejnopisů smlouvy, resp. je závislý na vyhotovování ověřených kopií. U elektronicky podepsaných smluv naproti tomu bude možné užít libovolné množství kopií. Vytisknutý a vlastnoručně podepsaný dokument ztrácí výhodné vlastnosti elektronického dokumentu

a elektronického podpisu. U elektronického dokumentu jsou jednoduše dostupná metadata použitelná při dokazování. Vyšší úroveň elektronického podpisu krom dalších výhod přináší ochranu dokumentu proti jeho pozměnění. Naproti tomu vlastnoruční podpis má tu výhodu, že je individuálním a více či méně stálým projevem konkrétní osoby. Na druhou stranu ani ten nezaručuje bez dalšího pravost listiny a jde pouze o omezeně spolehlivý důkazní prostředek. Ani v případě úředně ověřeného podpisu nelze totiž zcela vyloučit podvodné jednání.

Elektronicky a vlastnoručně podepsaná smlouva bude mít pro své účastníky ve specifických situacích jiná pozitiva či negativa. Bude v souladu s autonomií vůle na jejich rozhodnutí, jakou formu pro svou smlouvu zvolí. Při podpisu smlouvy za současné přítomnosti všech smluvních stran v jednom okamžiku na jednom místě může být pro strany vhodnější a jednodušší smlouvu podepsat vlastnoručním podpisem. Strany se mohou vzájemně před podpisem identifikovat, bude tak složitě podpis zpochybnit a další archivace smlouvy nevyžaduje nějaké zvláštní postupy. Výhodu opatření smlouvy elektronickým podpisem lze v takovém případě spatřovat v tom, že ten může zajistit integritu dokumentu a zabránit tedy v budoucnu manipulaci s jejím obsahem. Naproti tomu při kontraktaci na dálku se jeví jako vhodnější užití elektronického podpisu, a to nejlépe kvalifikovaného elektronického podpisu. Strany pak disponují elektronickým dokumentem s metadaty použitelnými při dokazování. Elektronický podpis, elektronická pečeť či elektronické časové razítko může zajistit integritu dokumentu. Samotný kvalifikovaný certifikát pro elektronický podpis také obsahuje řadu dat použitelných při dokazování a bude jej možné použít jako podpis rovnocenný vlastnoručnímu podpisu napříč Evropskou unií a v některých třetích zemích.

## SUMMARY

This monograph focuses on current trends and perspectives of electronically concluded contracts. We rely on the foundations of earlier findings of legal scholarship, which we put in the context of the development of information technologies and recent conclusions. We thus view the new issues of virtualization of the contractual process through the lenses of civil law science. We have sought to critically examine previously concluded doctrinal opinions and place them in context with other opinions, decision-making practice, and developments in the field of electronic contracting. On this basis, we have formulated our own conclusions presented throughout the text of the book.

In exploring each relevant area, we have always progressed from general to more specific questions. Thus, we first addressed the theoretical foundations of online contracting, including the relevance of online contracting in today's digital society.

We then moved on to the role of digital technologies in negotiating and concluding a contract. In addition to concluding how electronic contracting and signing are regulated by law, we focused on the different levels of electronic signatures and selected electronic signing techniques or some electronic tools and platforms used for contracting.

We followed with a section on the use of digital technologies after the conclusion of the contract. The basis of this part is a text dedicated to the use of electronic evidence in civil proceedings. All the previous conclusions were then confronted with the earlier case law of the higher courts and the current available decision-making practice of lower courts.

The monograph deals with issues that at first sight may seem to be more of a technological nature – for example, the various types of electronic signatures defined by the eIDAS Regulation, various types of signature techniques or methods of archiving electronically concluded contracts are discussed. However, the need to address these issues arises from legal provisions, whether from the Civil Code and its rules on the completion of the written form by electronic means or the presumption of reliability of records

of legal transactions in an electronic system, or from other special EU and national regulations.

The monograph also discusses modern aspects of contracting and focuses on related aspects of smart contracts, the use of DLT (not only for contracting, but also for archiving) and also addresses, for example, specific aspects of consumer contracting (including the context where digital content is the subject of the contract).

We conclude that the legal order itself does not impose any obstacles to the conclusion of contracts by electronic means and electronic signing. The Civil Code is based on the principle of autonomy of will, freedom of contract and informality. Unless prohibited by law or by the parties' agreement, any form and means of conclusion may be chosen for a contract. In ordinary legal relations, the Civil Code makes no distinction between a document in paper form signed with a handwritten signature and an electronic document signed with an electronic signature. When concluding contracts, the parties are free as to the type and level of electronic signature they choose to sign the contract. Furthermore, we argue that unsigned legal acts executed by electronic means will satisfy the requirement of a writing, provided that such means enable the identification of the person acting and the content of the legal act to be identified.

Based on an analysis of the relevant court decisions, we conclude that the decision-making practice of the lower courts is inconsistent in this area and there is no Supreme Court decision with a properly reasoned conclusion on the use of electronic signatures. Such a decision would be of fundamental importance for practice. At present, the parties to contracts signed with a plain electronic signature do not have legal certainty as to the enforceability of such contracts, given the number of decisions which prevent the use of the basic level of electronic signature and rather seek grounds for declaring contracts concluded in this way null and void. These include the court's conclusions on the lack of identification of the person acting by a simple electronic signature or the fact that this signature does not ensure the integrity of the signed document.

In the case of electronic signing, without further context, the use of a qualified electronic signature or an advanced electronic signature based on a qualified

certificate seems to be the most appropriate. In the case of an advanced electronic signature, its trustworthiness depends on the trust in the person who issues the data for the creation of the signature. From the decision-making practice, it seems that each of these electronic signatures would be accepted as evidence by the Czech courts. It can be assumed that Czech courts would not oppose the use of dynamic biometric signatures either. In the case of the use of other types of electronic signatures, it is necessary to bear in mind the provision of other means of evidence by which the party to the contract will be able to prove, in particular, the identification of the signatory, the fact that he or she affixed his or her signature to the contract and that the contract was signed in the version submitted to the court. This conclusion is rooted in the findings on the legality of signing by electronic signature, the use of which is very frequent in practice.

However, it is also necessary to take into account the risks that this level of signature entails, which have been discussed in the text of the monograph. The enforceability of obligations arising from electronically concluded contracts also depends on the method of their long-term archiving. We propose the use of records of data on legal transactions in an electronic system, carried out systematically, sequentially and with protection against changes, as the ideal method.

It is possible to identify areas (typically e-commerce) in which it is almost impossible to use handwritten contracts while maintaining the efficiency of legal transactions. On the other hand, for other contracts, the parties may prefer to conclude them by signing a handwritten contract. Examples include contracts signed in front of a notary or lawyer, together with a certification of signature.

In the literature it is possible to identify opinions about the much greater security of electronic signatures compared to handwritten signatures. This can probably be agreed to some extent, at least in the case of electronic signatures based on a qualified certificate. Again, however, long-term archiving must be taken into account.

Storage will be easier in the case of a handwritten contract. In principle, there is no need to use any additional means. However, the participant is bound

by a limited number of copies of the contract or is dependent on the making of certified copies. For electronically signed contracts, on the other hand, it will be possible to use any number of copies. A printed and hand-signed document loses the advantages of an electronic document and electronic signature. In the case of an electronic document, metadata is easily available for use in evidence. Higher levels of electronic signature provide protection against tampering with the document, among other benefits.

By contrast, a handwritten signature has the advantage of being an individual and more or less permanent expression of a particular person. On the other hand, even this does not guarantee the authenticity of the document unconditionally and is only a limitedly reliable means of evidence. Even in the case of a certified signature, fraud cannot be avoided.

Whether electronically or manually signed, a contract will have different positives or negatives for its participants in specific situations. It will be consistent with the autonomy of the will to decide what form they choose for their contract. When a contract is signed in the presence of all parties at the same time in one place, it may be preferable and easier for the parties to sign the contract by handwritten signature. The parties can identify each other prior to signing, it will be difficult to challenge the signature and further archiving of the contract does not require any special procedures. The advantage of providing for an electronic signature in such a case is that it can ensure the integrity of the document and thus prevent future manipulation of its content.

In contrast, in the case of long-distance contracting, the use of an electronic signature, ideally a qualified electronic signature, seems preferable. The parties then have an electronic document with metadata that can be used in evidence. An electronic signature, electronic seal or electronic time stamp can ensure the integrity of the document. The qualified certificate for the electronic signature itself also contains a range of data applicable to evidence and will be usable as a signature equivalent to a handwritten signature across the European Union and in some third countries.

# LITERATURA A DALŠÍ POUŽITÉ ZDROJE

## Komentáře

- BEZOUŠKA, P., HAVEL, B. *Občanský zákoník: Srovnávací komentář*. Praha: Wolters Kluwer, 2021. Dostupné z: <http://www.noveaspi.cz> [cit. 14. 8. 2020].
- DONÁT, J., PIFFL, R., MAISNER, M. *Narřízení eIDAS. Komentář*. Praha: C. H. Beck, 2017. ISBN 978-80-7400-633-3.
- GAŇO, J., JIRSA, J., ZOUBEK, H. a kol. *Občanský zákoník – Komentář s judikaturou. Svazek XI – Závazky – obecná část (§ 1721–2054)*. Ostrava: CODEXIS publishing, 2018.
- HULMÁK, M. a kol. *Občanský zákoník V. Závazkové právo. Obecná část (§ 1721–2054). Komentář*. 1. vyd. Praha: C. H. Beck, 2014.
- JIRSA, J. a kol. *Občanské soudní řízení (soudcovský komentář). Kniha II*. Praha: Havlíček Brain Team, 2014. ISBN 978-80-87109-46-5.
- KINDL, M., KINDL, T., KINDLOVÁ, M., ŠÍMA, A. a kol. *Občanský zákoník – Komentář s judikaturou. Svazek V – Právní skutečnosti (§ 545–654)*. Ostrava: CODEXIS publishing, 2018. ISBN 978-80-906391-9-5.
- LAVICKÝ, P. a kol. *Občanský zákoník I. Obecná část (§ 1–654)*. 2. vyd. Praha: C. H. Beck, 2022. ISBN 978-80-7400-529-9.
- LECHNER, T. *Narřízení eIDAS a české adaptační zákony. Komentář*. Praha: Wolters Kluwer, 2023. ISBN 978-80-7598-924-6.
- MELZER, F., TÉGL, P. a kol. *Občanský zákoník – velký komentář. Svazek III*. Praha: Leges, 2014. ISBN 978-80-7502-003-1.
- NULÍČEK, M. a kol. *Obecné nařízení o ochraně osobních údajů (GDPR): Praktický komentář*. 2. vyd. Praha: Wolters Kluwer, 2018. ISBN 978-80-7598-068-7.
- PETROV, J., VÝTISK, M., BERAN, V. a kol. *Občanský zákoník. Komentář*. 2. vyd. Praha: C. H. Beck, 2019. ISBN 978-80-7400-747-7.
- SVOBODA, K., SMOLÍK, P., LEVÝ, J., DOLEŽÍLEK, J. a kol. *Občanský soudní řád*. 3. vyd. Praha: C. H. Beck, 2021. ISBN 978-80-7400-828-3.



- ŠVESTKA, J., DVOŘÁK, J., FIALA, J. a kol. *Občanský zákoník. Komentář. Svazek I.* Praha: Wolters Kluwer, 2014. ISBN 978-80-7478-370-8.
- ŠVESTKA, J., DVOŘÁK, J., FIALA, J. a kol. *Občanský zákoník. Komentář. Svazek V.* Praha: Wolters Kluwer, 2014. ISBN 978-80-7478-638-9.
- ŠVESTKA, J., DVOŘÁK, J., FIALA, J. a kol. *Občanský zákoník. Komentář. Svazek IV.* 2. vyd. Praha: Wolters Kluwer, 2019. ISBN 978-80-7598-412-8.
- ZAJÍČEK, Z. a kol. *Zákon o právu na digitální služby. Komentář.* Praha: C. H. Beck, 2021. ISBN 978-80-7400-822-1.
- ZUKLÍNOVÁ, M. *Právní jednání podle občanského zákoníku č. 89/2012 Sb. Komentář, srovnání se zahraničím a vybraná platná judikatura.* 1. vyd. Praha: Linde, 2013. ISBN 978-80-7201-918-2.

## Monografie a učebnice

- BASHIR, I. *Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained.* 2. vyd. Birmingham: Packt Publishing Ltd., 2018. ISBN 9781788839044.
- ČAPEK, J., BOGUSZAK, J. *Teorie práva.* Praha: Codex, 1997. ISBN 978-80-85963-38-0.
- DONÁT, J., TOMÍŠEK, J. *Právo v síti: průvodce právem na internetu.* 1. vyd. Praha: C. H. Beck, 2016. ISBN 978-80-7400-610-4.
- DVOŘÁK, J., ŠVESTKA, J., ZUKLÍNOVÁ, M. *Občanské právo hmotné. Svazek I. Díl první: Obecná část.* 2. vyd. Praha: Wolters Kluwer, 2016. ISBN 978-80-7552-187-3.
- D'HAENENS, L. (ed.). *Cyberidentities: Canadian & European Presence in Cyberspace.* Ottawa: University of Ottawa Press, 1999. ISBN 978-0-7766-0493-0. DOI: [https://doi.org/10.26530/OAPEN\\_578780](https://doi.org/10.26530/OAPEN_578780)
- HORA, V. *Československé civilní právo procesní.* Wolters Kluwer, 2010. ISBN 978-80-7357-540-3.
- HURDÍK, J. a kol. *Občanské právo hmotné. Obecná část. Absolutní majetková práva.* 3. vyd. Plzeň: Aleš Čeněk, 2018. ISBN 978-80-7380-718-4.

- KMENT, V. *Elektronické právní jednání: Analýza s důrazem na využití elektronického podpisu podle práva EU, České republiky a Německa*. Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-814-8.
- KNAPP, V. *Teorie práva*. 1. vyd. Praha: Beck, 1998. ISBN 978-80-7179-028-0.
- KOOPS, B.-J., LEENES, R., HERT, P. de (eds.). *Constitutional Rights and New Technologies: A Comparative Study Covering Belgium, Canada, France, Germany, Sweden, and the United States*. Tilburg University, 2007. DOI: <https://doi.org/10.1007/978-90-6704-553-7>
- KRČMÁŘ, J. *Právo občanské I. Výklady úvodní a část všeobecná*. Praha: Wolters Kluwer, 2014 (reprint IV. vydání z roku 1946). ISBN 978-80-7478-408-8.
- LÁNSKÝ, J. *Kryptoměny*. 1. vyd. Praha: C. H. Beck, 2018. ISBN 978-80-7400-722-4.
- LESSIG, L. *Code: Version 2*. New York: Basic Books, 2006. ISBN 9780465039142.
- MASON, S. *Electronic Signatures in Law*. 4. vyd. London: University of London, 2017. ISBN 978-1-911507-01-7.
- MAISNER, M. a kol. *Základy softwarového práva*. Praha: Wolters Kluwer, 2011. ISBN 978-80-7357-638-7.
- MCKENDRICK, E. *Contract Law: Text, Cases, and Materials*. 4. vyd. Oxford: Oxford Univ. Press, 2010. ISBN 978-0-19-957979-2.
- PAULUS, S., POHLMANN, N., REIMER, H. (eds.). *ISSE 2004 – Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2004 Conference*. Wiesbaden: Vieweg+Teubner Verlag, 2004. ISBN 978-3-322-84984-7. DOI: <https://doi.org/10.1007/978-3-322-84984-7>
- PETERKA, J. *Báječný svět elektronického podpisu*. Praha: CZ.NIC, 2011. ISBN 978-80-904248-3-8.
- POOLE, J., DEVENNEY, J., SHAW-MELLORS, A. *Contract law: Law Revision and Study Guide*. 3. vyd. Oxford: Oxford University Press, 2017. ISBN 978-0-19-880385-0.
- POLČÁK, R. *Internet a proměny práva*. Praha: Auditorium, 2012. ISBN 978-80-87284-2-3.

- POLČÁK, R. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018. ISBN 978-80-7598-045-8.
- RABAN, P. A kol. *Závazkové právo*. Brno: Václav Klemm, 2019. ISBN 978-80-87713-18-1.
- RONOVSKÁ, K., HAVEL, B., LAVICKÝ, P. (eds). *Pocť prof. Janu Hurdíkovi ke 70. narozeninám. Základní otázky života, práva a vůbec...!* Brno: Masarykova univerzita, Právnická fakulta, 2021. ISBN 978-80-210-9937-1.
- SEDLÁKOVÁ, J. a kol. *Softwarové smlouvy: Jejich specifika a kontraktační proces*. Praha: C. H. Beck, 2021. ISBN 978-80-7400-814-6.
- STONE, R. *The Modern Law of Contract*. 8. vyd. London; New York: Routledge-Cavendish, 2009. ISBN 978-0-415-48136-6.
- SUCHOŽA, J., HUSÁR, J., HUČKOVÁ, R. (eds.). *Právo, Obchod, Ekonomika IX. 2019*. Košice: Univerzita P. J. Šafárika v Košiciach. ISBN 978-80-8152-775-3. DOI: <https://doi.org/10.33542/POE2020-931-3>
- SVOBODA, E. *Obrany a útoky*. Praha: Nakladatelství Al. Srdce, 1926.
- SZOSTEK, D. *Blockchain and the Law*. Baden-Baden: Nomos Verlagsges, MBH + Co., 2019. ISBN 978-3-8487-5693-3.
- ŠAVELKA, J. a kol. *Právní informační systémy*. Brno: Tribun EU, 2011. ISBN 978-80-7399-248-4.
- TINTĚRA, T., PETR, P. *Základy závazkového práva. 1. díl*. 2. vyd. Praha: Leges, 2020, 288 s. ISBN 9788075024762.
- TREITEL, G. H. *The Law of Contract*. 11. vyd. London: Sweet & Maxwell, 2003. ISBN 978-0-421-78850-3.

## Články a elektronické zdroje

- Advice on “Initial Coin Offerings and Crypto-Assets”. *ESMA* [online]. 2019 [cit. 4. 11. 2020]. Dostupné z: [https://www.esma.europa.eu/system/files\\_force/library/esma50-157-1391\\_crypto\\_advice.pdf?download=1](https://www.esma.europa.eu/system/files_force/library/esma50-157-1391_crypto_advice.pdf?download=1)
- ALLEN, D. W. E., LANE, A. M., POBLET, M. The Governance of Blockchain Dispute Resolution. *Harvard Negotiation Law Review*. 2019, č. 25, s. 75–101. DOI: <https://doi.org/10.2139/ssrn.3334674>

- Article 29 Data Protection Working Party: Opinion 05/2014 on Anonymisation Techniques. *Evropská komise* [online]. 2014, 0829/14/EN [cit. 4. 2. 2021]. Dostupné z: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf)
- BEJČEK, J. K možnostem automatizace právního jednání a rozhodování socialistických hospodářských organizací. *Právník*. 1982, č. 5, s. 392–404.
- BEJČEK, Josef, Některá úskalí racionality obchodních podmínek. *Právní rozhledy*. 2015, č. 18.
- BOBEK, M. Výzkum v právu: reklama na Nike anebo kvantová fyzika. *Jurisprudence*. 2016, č. 6, s. 3–10.
- BOYKIN, D. D. Survey of E-Contracting Cases: Browsewrap, Clickwrap, and Modified Clickwrap Agreements. *The Business Lawyer*. 2012, roč. 68, č. 1, s. 257–262.
- EASTERBROOK, Frank H. Cyberspace and the Law of the Horse. *The University of Chicago Legal Forum*. 1996, č. 207, s. 207–216.
- European Digital Identity – Provisional Agreement. *Evropský parlament* [online]. 2023 [cit. 20. 12. 2023]. Dostupné z: <https://www.europarl.europa.eu/committees/cs/european-digital-identity-provisional-ag/product-details/20231116CAN72103>
- FILLIPPI, P. de, HASSAN, S. Blockchain technology as a regulatory technology: From code is law to law is code. *First Monday* [online]. 2016, roč. 21, č. 12 [cit. 25. 9. 2020]. Dostupné z: <https://doi.org/10.5210/fm.v21i12.7113>
- FINCK, M. Blockchains and Data Protection in the European Union. *Max Planck Institute for Innovation & Competition Research Paper* [online]. 2017, č. 18-01 [cit. 7. 2. 2022]. Dostupné z: <https://doi.org/10.2139/ssrn.3080322>
- FULLER, L. L. Consideration and Form. *Columbia Law Review*. Columbia Law Review Association, Inc., 1941, roč. 41, č. 5, s. 799–824. ISSN 0010-1958. DOI: <https://doi.org/10.2307/1117840>
- HRDLIČKA, M. Datové schránky a možnosti jejich využití. In: *COFOLA 2010: the Conference Proceedings*. Brno: Masarykova univerzita, 2010.

- Informační společnost v číslech 2023. *Český statistický úřad* [online]. 2023 [cit. 27. 6. 2023]. Dostupné z: <https://www.czso.cz/documents/10180/191186455/06100423.pdf/879a3104-e54c-4f4e-b768-b0bd057ac006?version=1.3>
- JAREŠ, Adam, Soukromoprávní doručování datovými schránkami a teorie dojití. *Obchodněprávní revue*. 2022, č. 2.
- KACZOROWSKA, M. Blockchain-based Land Registration: Possibilities and Challenges. *Masaryk University Journal of Law and Technology*. 2019, roč. 13, č. 2, s. 339–360. DOI: <https://doi.org/10.5817/MUJLT2019-2-8>
- KMENT, V. Nahradí elektronický podpis prostý ten tradiční vlastnoruční? *Bulletin advokacie*. 2016, č. 12, s. 31–35.
- KORBEL, F., MELZER, F. Písemnost, elektronický a biometrický podpis v elektronickém právním jednání. *Bulletin advokacie*. 2014, č. 12, s. 31–36.
- KORBEL, F. a kol. Elektronická identita při elektronickém (hmotně)právním jednání. *Právní rozhledy*. 2019, č. 18, s. 626–632.
- KORBEL, F., KOVÁŘ, D., JAROŠ, J. Aktuální právní přístup k dynamickému biometrickému podpisu. *Pojistný obzor*. 2021, č. 2, s. 12–17.
- KOŠČÍK, M. Pojem a obsah právních úkonů na internetu. *Revue pro právo a technologie*. 2011, č. 4.
- KRUPÍČKOVÁ, P. Smart contract – revoluce v smluvním právu 21. století? *Revue pro právo a technologie*. 2017, č. 15, s. 19–31. DOI: <https://doi.org/10.5817/RPT2017-1-2>
- KUČERA, Z. Uzavírání spotřebitelských smluv na internetu. *Rekodifikace & praxe*. 2015, č. 5.
- KUNZ, Ch. L. a kol. Browse-Wrap Agreements: Validity of Implied Assent in Electronic Form Agreements. *The Business Lawyer*. 2003, roč. 59, č. 1, s. 279–312.
- LAVICKÝ, P., POLIŠENSKÁ, P. *Vznik a obsah závazků*. Praha: Wolters Kluwer, 2015. ISBN 9788074787546.

- Legislativní usnesení Evropského parlamentu ze dne 29. února 2024 o návrhu nařízení Evropského parlamentu a Rady, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu (COM(2021)0281 – C9-0200/2021 – 2021/0136(COD)). *Evropský parlament* [online]. 2024 [cit. 15. 3. 2024]. Dostupné z [https://www.europarl.europa.eu/doceo/document/TA-9-2024-0117\\_CS.pdf](https://www.europarl.europa.eu/doceo/document/TA-9-2024-0117_CS.pdf)
- LOUTOCKÝ, P. eIDAS Regulation: A Step Forward? In: BALTHASAR, A. (ed.). *CEE e-Dem and e-Gov Days 2015: Independence day: time for a European Internet?* Wien: Österreichische Computer Gesellschaft, 2015. ISBN 978-3-85403-308-0.
- LOUTOCKÝ, P., KASL, F. Potenciál a úskalí identifikačních služeb bankovní identity. *Právník*. 2021, č. 12, s. 1038–1053.
- MAISNER, M., SMEJKAL, V., UŘIČAŘ, M. Je používání dynamického biometrického podpisu v rozporu s GDPR. *Bulletin advokacie*. 2019, č. 9, s. 20–31.
- MATEJKA, J. Úprava elektronického podpisu v právním řádu ČR. *Právník* [online]. 2001, č. 6, s. 557–586 [cit. 18. 2. 2022]. Dostupné z: <http://www.codexis.cz>
- MATEJKA, J., CHUM, V. K právní úpravě elektronického podpisu. *Bulletin advokacie*. 2002, č. 3, s. 27–41.
- MATEJKA, J., GÜTTLER, V. Electronic Written Documents and Biometric Options of Their Signing – Problem of Evidentiary Reliability and Personal Data Protection. *The Lawyer Quarterly*. 2018, č. 1, s. 38–50.
- MASON, S. Electronic signatures: the essentials. *InsideOut Magazine* [online]. [cit. 13. 10. 2019]. Dostupné z: <https://communities.lawsociety.org.uk/insideout-magazine/electronic-signatures-the-essentials/5052726.article>
- MASON, S. Informal Debate on the Issues Relating to Terminology and Clarification of Concept in Respect of the EU e-Signature Legislation. *SCRIPTed* [online]. 2012, roč. 9, č. 1. DOI: <https://doi.org/10.2966/script.090112.82>
- METZLER, J. The Importance Of Irac And Legal Writing. *University of Detroit Mercy Law Review*. 2003, roč. 80, č. 4, s. 501–503.

- MIK, E. Smart contracts: terminology, technical limitations and real world complexity. *Law, Innovation and Technology*. 2017, roč. 9, č. 2, s. 269–300. DOI: <https://doi.org/10.1080/17579961.2017.1378468>
- Seznam kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru. *Ministerstvo vnitra* [online]. [cit. 19. 11. 2021]. Dostupné z: <https://www.mvcr.cz/clanek/seznam-kvalifikovanych-poskytovatelu-sluzeb-vytvarejicich-duveru-a-poskytovanych-kvalifikovanych-sluzeb-vytvarejicich-duveru.aspx>
- Návrh nařízení Evropského parlamentu a Rady o trzích skryptoaktivy a o změně směrnice (EU) 2019/1937. COM(2020)593 final. *Evropská komise* [online]. [cit. 1. 2. 2020]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A52020PC0593&qid=1619174354936>
- Návrh nařízení Evropského Parlamentu a Rady, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu. *Evropská komise* [online]. [cit. 1. 2. 2022]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=COM%3A2021%3A281%3AFIN>
- Otázky, na které se často ptáte. *BankID.cz* [online]. [cit. 10. 12. 2021]. Dostupné z: <https://www.bankid.cz/faq>
- PAYNE, D. Metadata: The Good, the Bad, and the Misunderstood. *GPSolo*. 2013, č. 2, s. 51–53.
- PETERKA, J. Elektronický podpis na rozcestí. *Lupa.cz* [online]. 6. 6. 2011 [cit. 22. 2. 2022]. Dostupné z: <https://www.lupa.cz/clanky/elektronicky-podpis-na-rozcesti/>
- POLČÁK, R. Praxe elektronických dokumentů. *Bulletin advokacie*. 2011, č. 7–8, s. 53–61.
- POLČÁK, R. Nové směry v elektronické dokumentaci právního jednání. *Právní prostor* [online]. 19. 6. 2017 [cit. 24. 10. 2019]. Dostupné z: <https://www.pravniprostor.cz/clanky/obcanske-pravo/nove-smery-v-elektronicke-dokumentaci-pravniho-jednani>
- POLČÁK, R. Odpovědnost umělé inteligence a informační útvary bez právní osobnosti. *Bulletin advokacie*. 2018, č. 11, s. 23–30.

- POLČÁK, R., KASL, F., LOUTOCKÝ, P., MÍŠEK, J., STUPKA, V. Virtualizace právních vztahů a nové regulační metody v pozitivním právu. *Právník*. 2019, č. 1, s. 86–98.
- POLČÁK, R. Protiprávní jednání a škoda online. *Bulletin advokacie*. 2021, č. 6, s. 16–22.
- Pracovní návrhy paragrafových znění predkladané na verejnú a odbornú diskusiu. *Ministerstvo spravodlivosti SR* [online]. [cit. 11. 2. 2022]. Dostupné z: <https://www.justice.gov.sk/Stranky/Ministerstvo/Rekodifikacia-OZ/Navrhy.aspx>
- RASKIN, M. The Law And Legality Of Smart Contracts, *Georgetown Law Technology Review* [online]. 2017, roč. 1, č. 2 [cit. 20. 10. 2020]. Dostupné z: <https://georgetownlawtechreview.org/the-law-and-legality-of-smart-contracts/GLTR-04-2017/>
- SCHWALM, S., ALBRECHT, D., ALAMILLO-DOMINGO, I. *eIDAS 2.0: Challenges, perspectives and proposals to avoid contradictions between eIDAS 2.0 and SSI*. 2022. DOI: [https://doi.org/10.18420/OID2022\\_05](https://doi.org/10.18420/OID2022_05)
- SHANG, Q., PRICE, A. A Blockchain-Based Land Titling Project in the Republic of Georgia: Rebuilding Public Trust and Lessons for Future Pilot Projects. *Innovations: Technology, Governance, Globalization* [online]. MIT Press, roč. 12, č. 3–4, s. 72–78 [cit. 11. 10. 2020]. DOI: [https://doi.org/10.1162/inov\\_a\\_00276](https://doi.org/10.1162/inov_a_00276)
- SMEJKAL, V., KODL, J. Development Trends of Electronic Authentication. In: *Proceedings of the 42nd Annual Conference 2008 IEEE International Carnahan Conference on Security Technology*. 2008, s. 2. DOI: <https://doi.org/10.1109/CCST.2008.4751267>
- SMEJKAL, V. Dynamický biometrický podpis a nařízení GDPR. *Revue pro právo a technologie*. 2017, roč. 8, č. 16, s. 89–112. DOI: <https://doi.org/10.5817/RPT2017-2-5>
- SMEJKAL, V. Kryptografický a dynamický biometrický podpis podle platné právní úpravy. *Právní rozhledy*. 2019, č. 10, s. 343–351.
- SMEJKAL, V., KODL, J., UŘIČAŘ, M. Elektronický podpis podle nařízení eIDAS. *Revue pro právo a technologie*. 2015, č. 11, s. 189–235.



- ŠČERBA, T. Právně teoretické aspekty elektronické kontraktace. *Revue pro právo a technologie*. 2012, č. 5, s. 36–120.
- VOSTOUPAL, J. Vybrané slabiny právní úpravy elektronických forem komunikace v obchodních korporacích v kontextu kybernetické bezpečnosti. *Obchodněprávní revue*. 2022, č. 1, s. 35–41.
- WOOD BRALEY, S. Why Electronic Signatures Can Increase Electronic Transactions and the Need for Laws Governing Electronic Signatures. *Law and Business Review of the Americas*. 2001, č. 7.
- WIMS, M. D. Introduction to the Utah Digital Signature Act Editorial. *EDI Law Review*. 1995, roč. 2, č. 3, s. 155–156.
- YEUNG, K. Blockchain, Transactional Security and the Promise of Automated Law Enforcement: The Withering of Freedom Under Law? *King's College London Law School Research Paper* [online]. 2017, č. 2017-20 [cit. 18. 4. 2021]. DOI: <http://doi.org/10.2139/ssrn.2929266>
- ZIMMER, J., FÜRST, T., HAUSER, T. Důkazní váha biometrického podpisu závisí na kvalitě použitého dotykového zařízení a na dostupnosti úplných podpisových dat. *Právní rozhledy*. 2021, č. 13–14.

## Koncepční dokumenty Evropské unie

- Sdělení Komise Evropskému parlamentu, Evropské radě, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů Zelená dohoda pro Evropu. *Evropská komise* [online]. 2019 [cit. 11. 3. 2023]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A52019DC0640&qid=1678544467235>
- Evropské prohlášení o digitálních právech a zásadách pro digitální dekádu 2023/C 23/01. *Evropská komise* [online]. 2023 [cit. 11. 3. 2023]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32023C0123%2801%29&qid=1678546597447>
- Rozhodnutí Evropského parlamentu a Rady (EU) 2022/2481 ze dne 14. prosince 2022, kterým se zavádí politický program Digitální dekáda 2030. *Evropský parlament a Rada* [online]. 2022 [cit. 11. 3. 2023]. Dostupné z: <http://data.europa.eu/eli/dec/2022/2481/oj/ces>

## Rozhodovací praxe

### Zahraniční

Court of Appeal. *Pharmaceutical Society of Great Britain v. Boots Cash Chemists (Southern) Ltd* [1953] EWCA Civ 6.

Divisional Court. *Fisher v. Bell* [1961] 1 QB 394.

House of Lords. *Grainger & Son v. Gough* [1896] AC 325 HL.

Supreme Court of New South Wales. *Stuart v Hisbon* [2013] NSWSC 766.

Soudní dvůr Evropské unie ze dne 5. 7. 2012, ve věci *Content Services Ltd v. Bundesarbeitskammer*, C-49/11.

Soudní dvůr Evropské unie ze dne 19. 10. 2016, ve věci *Patrick Breyer v Bundesrepublik Deutschland*, C-582/14.

United States Court of Appeals, District of Columbia Circuit. *U.S. v. Miller*, 70 F.3d 1353, 1355 (D.C. Cir. 1995).

### Česká a Československá

Rozhodnutí Nejvyššího soudu Československé republiky ze dne 3. 11. 1926, sp. zn. Rv II 161/26.

Rozhodnutí Ústavního soudu ze dne 20. 6. 1995, sp. zn. III. ÚS 84/94.

Rozhodnutí Nejvyššího soudu ze dne 17. 4. 1996, sp. zn. 3 Cdon 1031/96.

Rozhodnutí Ústavního soudu ze dne 6. 1. 1997, sp. zn. IV. ÚS 191/96.

Rozhodnutí Ústavního soudu ze dne 8. 1. 1997, sp. zn. II. ÚS 127/96.

Rozhodnutí Nejvyššího soudu ze dne 9. 10. 2000, sp. zn. 22 Cdo 617/99.

Rozhodnutí Nejvyššího soudu ze dne 28. 8. 2001, sp. zn. 29 Odo 14/2001.

Rozhodnutí Nejvyššího soudu ze dne 9. 10. 2002, sp. zn. 29 Cdo 2893/2000.

Rozhodnutí Nejvyššího soudu ze dne 15. 1. 2004, sp. zn. 32 Odo 442/2003.

Rozhodnutí Ústavního soudu ze dne 8. 12. 2005, sp. zn. I. ÚS 729/2000.

Rozhodnutí Ústavního soudu ze dne 12. 1. 2006, sp. zn. I. ÚS 437/03.

Rozhodnutí Okresní soudu v Kutné Hoře ze dne 29. 8. 2006, sp.zn. 10 C 60/2006.

Rozhodnutí Krajského soudu v Praze ze dne 23. 1. 2007, sp. zn. 28 Co 797/2006.

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

Rozhodnutí Nejvyššího soudu ze dne 8. 1. 2008, sp. zn. 29 Odo 805/2006.

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

Rozhodnutí Nejvyššího správního soudu ze dne 4. 2. 2009, sp.zn. 1 As 90/2008.

Rozhodnutí Nejvyššího soudu ČR ze dne 30. 10. 2009, sp.zn. 33 Cdo 3210/2007.

Rozhodnutí Vrchního soudu v Praze ze dne 16. 11. 2009, sp.zn. 5 Cmo 161/2009.

Rozhodnutí Nejvyššího soudu ze dne 21. 12. 2009, sp. zn. 29 Cdo 3478/2007.

Rozhodnutí Nejvyššího soudu ze dne 19. 5. 2010, sp. zn. 33 Cdo 2441/2008.

Rozhodnutí Nejvyššího soudu ze dne 27. 4. 2011, sp. zn. 23 Cdo 3951/2009.

Rozhodnutí Ústavního soudu ze dne 1. 10. 2013, sp. zn. I. ÚS 2474/13.

Rozhodnutí Nejvyššího soudu ze dne 16. 1. 2013 sp. zn. 31 Cdo 1571/2010.

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

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

Rozhodnutí Ústavního soudu ze dne 16. 6. 2015, sp. zn. II.ÚS 3588/14.

Rozhodnutí Ústavního soudu ze dne 23. 7. 2015, sp. zn. II.ÚS 3496/13.

Rozhodnutí Krajského soudu v Ostravě ze dne 28. 1. 2016, sp. zn. 37 Icm 4495/2014.

Rozhodnutí Ústavního soudu ze dne 7. 3. 2016 sp. zn. II. ÚS 289/15.

Rozhodnutí Nejvyššího soudu ze dne 3. 5. 2016, sp. zn. 23 Cdo 4093/2015.

Rozhodnutí Nejvyššího soudu ze dne 1. 7. 2016, sp. zn. 26 Cdo 1239/2016.

- Rozhodnutí Městského soudu v Brně ze dne 13. 12. 2016, sp.zn. 294 C 52/2016.
- Stanovisko Nejvyššího soudu ze dne 1. 5. 2017, sp. zn. Plsn 1/2015.
- Rozhodnutí Krajského soudu v Brně ze dne 5. 6. 2017, sp. zn. 33 Icm 547/2016.
- Rozhodnutí Nejvyššího správního soudu ze dne 27. 7. 2017, sp.zn. 2 As 80/2017.
- Rozhodnutí Nejvyššího soudu ze dne 1. 11. 2017, sp. zn. 20 Cdo 4016/2017.
- Rozhodnutí Krajského soudu v Brně ze dne 9. 11. 2017, sp. zn. 27 Co 86/2017.
- Rozhodnutí Úřadu pro ochranu hospodářské soutěže ze dne 21. 3. 2019, č. j. UOOU-10138/18-8.
- Rozhodnutí Nejvyššího soudu ze dne 22. 5. 2019, sp. zn. 26 Cdo 1230/2019.
- Rozhodnutí Nejvyššího soudu ze dne 30. 7. 2019, sp. zn. 29 NSCR 133/2017
- Rozhodnutí Nejvyššího soudu ze dne 26. 11. 2019, sp. zn. 24 Cdo 1110/2019.
- Rozhodnutí Nejvyššího soudu ze dne 22. 1. 2020, sp. zn. 26 Cdo 3501/2019.
- Rozhodnutí Nejvyššího soudu ze dne 27. 10. 2020, sp. zn. 27 Cdo 143/2020.
- Příkaz Úřadu pro ochranu osobních údajů ze dne 3. 3. 2021, č. j. UOOU-00982/21-5
- Rozhodnutí Okresního soudu v Hodoníně ze dne 31. 8. 2021, sp.zn. 13 C 90/2021.
- Rozhodnutí Okresního soudu v Kladně se v rozhodnutí ze dne 31. 8. 2021, sp. zn. 208 C 115/2021.
- Rozhodnutí Obvodního soudu pro Prahu 6 ze dne 13. 9. 2021, sp. zn. 18 C 198/2021-49.
- Rozhodnutí Obvodní soud pro Prahu 6 ze dne 27. 10. 2021, sp. zn. C 375/2021.
- Rozhodnutí Okresního soudu v Berouně ze dne 21. 12. 2021, sp.zn. 18 C 225/2021.
- Rozhodnutí Okresního soudu v Karviné ze dne 14. 1. 2022, sp.zn. 24 C 233/2021.

Rozhodnutí Okresního soudu v Karviné ze dne 27. 1. 2022, sp.zn. 109 C 380/2021.

Rozhodnutí Nejvyššího soudu ze dne 27. 4. 2022, sp. zn. 21 Cdo 2061/2021.

Rozhodnutí Ústavního soudu ze dne 4. 4. 2023, sp. zn. III.ÚS 752/23.

Rozhodnutí Vrchního soudu v Praze ze dne 28. 6. 2023, sp. zn. 3 VSPH 610/2023-A-122.

## **Právní předpisy**<sup>599</sup>

### **Zahraniční a unijní**

Bürgerliches Gesetzbuch.

Zákon č. 40/1964 Zb., občiansky zákonník.

Směrnice Evropského parlamentu a Rady 2011/83/EU ze dne 25. října 2011 o právech spotřebitelů, kterou se mění směrnice Rady 93/13/EHS a směrnice Evropského parlamentu a Rady 1999/44/ES a zrušuje směrnice Rady 85/577/EHS a směrnice Evropského parlamentu a Rady 97/7/ES.

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

RADA EVROPSKÉ UNIE. *Návrh nařízení Evropského parlamentu a Rady, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu – obecný přístup*

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.

Public Contracts Regulations 2015.

The Electronic Identification and Trust Services for Electronic Transactions Regulations 2016.

---

<sup>599</sup> Pokud není v textu výslovně uvedeno jinak, jsou všechny předpisy citovány v jejich znění účinném ke dni 31. 12. 2023.

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 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).

Směrnice Evropského parlamentu a Rady (EU) 2019/770 ze dne 20. 5. 2019 o některých aspektech smluv o poskytování digitálního obsahu a digitálních služeb.

## Vnitrostátní

Zákona č. 99/1963 Sb., občanský soudní řád.

Zákon č. 101/1963 Sb., o právních vztazích v mezinárodním obchodním styku (zákoník mezinárodního obchodu).

Zákon č. 40/1964 Sb., občanský zákoník.

Zákon č. 103/1990 Sb., kterým se mění doplňuje hospodářský zákoník.

Zákon č. 21/1992 Sb., o bankách.

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

Zákon č. 634/1992 Sb., o ochraně spotřebitele.

Zákon č. 1/1993 Sb., Ústava České republiky.

Usnesení Předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky.

Zákon č. 85/1996 Sb., o advokacii.

Zákon č. 222/1999 Sb., o zajišťování obrany České republiky.

Zákon č. 61/2000 Sb., o námořní plavbě.

Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu).

Zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů.

Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti).

Zákon č. 21/2006 Sb., o ověřování shody opisu nebo kopie s listinou a o ověřování pravosti podpisu a o změně některých zákonů (zákon o ověřování).

Vyhláška Ministerstva vnitra č. 36/2006 Sb., o ověřování shody opisu nebo kopie s listinou a o ověřování pravosti podpisu.

Zákon č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon).

Zákon č. 262/2006 Sb., zákoník práce.

Zákon č. 125/2008 Sb., o přeměnách obchodních společností a družstev.

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

Zákon č. 111/2009 Sb., o základních registrech.

Zákon č. 89/2012 Sb., občanský zákoník.

Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.

Zákon 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.

Zákon č. 460/2016 Sb., kterým se mění zákon č. 89/2012 Sb., občanský zákoník, a další související zákony.

Zákon č. 250/2017 Sb., o elektronické identifikaci.

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

Zákon 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.

Zákon č. 300/2021 Sb., kterým se mění zákon č. 358/1992 Sb., o notářích a jejich činnosti (notářský řád), ve znění pozdějších předpisů, a zákon č. 634/2004 Sb., o správních poplatcích, ve znění pozdějších předpisů.

Zákon č. 374/2022 Sb., kterým se mění zákon č. 634/1992 Sb., o ochraně spotřebitele, ve znění pozdějších předpisů, a zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.



## **Vědecká redakce MU**

prof. PhDr. Jiří Hanuš, Ph.D. (předseda);  
doc. Ing. Pavel Bobál, CSc.; doc. Mgr. Pavel Caha, Ph.D.;  
Mgr. Michaela Hanousková; prof. PhDr. Vít Hloušek, Ph.D.;  
doc. RNDr. Petr Holub, Ph.D.; prof. MUDr. Lydie Izakovičová Hollá, Ph.D.;  
prof. PhDr. Tomáš Janík, Ph.D., M.Ed.; prof. PhDr. Tomáš Kubíček, Ph.D.;  
PhDr. Alena Mizerová; doc. Mgr. Markéta Munzarová, Dr. rer. nat.;  
doc. RNDr. Lubomír Popelínský, Ph.D.; Ing. Zuzana Sajdlová, Ph.D.;  
Mgr. Kateřina Sedláčková, Ph.D.; prof. RNDr. Ondřej Slabý, Ph.D.;  
doc. Ing. Rostislav Staněk, Ph.D.; prof. PhDr. Jiří Trávníček, M.A.;  
doc. JUDr. PhDr. Robert Zbíral, Ph.D.

## **Ediční rada PrF MU**

doc. JUDr. PhDr. Robert Zbíral, Ph.D. (předseda);  
Mgr. Bc. Luboš Brim, Ph.D.; Mgr. David Čep, Ph.D.;  
JUDr. Mgr. Jakub Harašta, Ph.D.; doc. JUDr. Michal Janovec, Ph.D.;  
JUDr. Bc. Terezie Smejkalová, Ph.D.; doc. JUDr. Ing. Josef Šilhán, Ph.D.;  
JUDr. Dominik Židek, Ph.D.

## **SOUČASNÉ VÝZVY A PŘÍLEŽITOSTI UZAVÍRÁNÍ SMLUV ONLINE**

**JUDr. Adam Jareš, Ph.D., JUDr. Ing. František Kasl, Ph.D.,  
JUDr. Pavel Loutocký, Ph.D., BA (Hons)**

Vydala Masarykova univerzita  
Žerotínovo nám. 617/9, 601 77 Brno  
v roce 2024

Spisy Právnické fakulty Masarykovy univerzity  
Edice Scientia, sv. č. 757

1. elektronické vydání, 2024

ISBN 978-80-280-0523-8 (online ; pdf)  
DOI <https://doi.org/10.5817/CZ.MUNI.M280-0523-2024>  
[www.law.muni.cz](http://www.law.muni.cz)

**MUNI**  
PRESS

**MUNI**  
LAW



ISBN 978-80-280-0523-8



9 788028 005238