

Elektronické podpisy a dokumenty v pracovním právu

JUDr. Bc. MICHAL PEŠKAR, Ph.D.,
advokátní kancelář Randl Partners

prof. JUDr. PETR HŮRKA, Ph.D.,
Právnická fakulta Masarykovy univerzity Brno



Pandemie covid-19 výrazně umocnila trend elektronizace a digitalizace pracovního práva v praxi. Zaměstnanci, jejichž činnost není fyzicky vyžadována přímo na pracovišti zaměstnavatele, již mnohdy vykonávají činnost na dálku. Na druhou stranu je ale potřeba reflektovat skutečnost, že ne každý zaměstnanec je technicky zdatný, a ne každý disponuje prostředky elektronické komunikace. Zároveň je třeba mít na paměti rizika, která vyplývají z relativní jednoduchosti zneužití elektronického jednání. V současné době je poměrně jednoduché zfalšovat např. identitu odesílatele e-mailové zprávy nebo autorství jiné elektronické zprávy. Byť se v oblasti občanského práva, a někdy i pracovního práva, objevují liberální názory, které prosazují snížení požadavků na elektronická jednání na minimum s tím, že potenciální spory o autorství a pravost elektronické zprávy se vyřeší v řízení před soudem (jak tomu je ostatně v současnosti při pochybnostech o pravosti „papírových“ listin), pracovní právo právě s ohledem na zvláštní ochranu zaměstnanců nemůže na takové požadavky zcela rezignovat, protože důsledkem by mohlo být podstatné ztížení postavení zaměstnanců, kteří by se museli vlastními prostředky vyrovnávat zejména se soudními spory.

I. Úvod

Tento článek proto stručně popisuje právní úpravu formy právních jednání, aby následně mohla být rozpracována písemná forma právního jednání v elektronické podobě. Písemná forma je v pracovním právu (na rozdíl od ostatních oblastí soukromého práva) značně rozšířená a vyžadována pro naprostou většinu nejenom těch nejdůležitějších, ale často i poměrně marginálních dokumentů.

Jelikož pro písemnou formu je zásadní podpis jednajícího, článek se podrobně zabývá právě elektronickými podpisy, které, na rozdíl od podpisů vlastnoručních, mají celou řadu podob a možností. Navíc neplatí, že by všechny elektronické podpisy byly zcela rovnocenné, tedy že by měly stejné vlastnosti a mohlo se s nimi zacházet shodně. Článek proto čtenářům vysvětlí základní rozdíly, aby jim pomohl rozhodnout, který bude pro ně ten nejvhodnější, pokud budou k elektronizaci pracovních dokumentů přistupovat.

Článek zároveň tvoří úvod k další oblasti – doručování v pracovním právu. Jeho velice rigidní a přísné pojetí podle zákoníku práce tvoří v současnosti největší překážku pro větší výraznější elektronizaci pracovního práva. Problematice doručování se proto bude věnovat navazující článek.

1.1 Písemná forma podle českých a evropských právních předpisů a vybraných českých soudních rozhodnutí

Občanský zákoník (zák. č. 89/2012 Sb.) se použije subsidiárně ve všech soukromoprávních vztazích, a to včetně pracovních vztahů, a to vždy v souladu se základními zásadami pracovních vztahů.¹ Zákoník práce (zák. č. 262/2006 Sb.) neobsahuje obecnou úpravu požadavků na formu právních jednání, ale pouze stanovuje, kdy je písemná forma povinná, a dále stanovuje speciální pravidla pro doručování některých pracovních dokumentů, která se však formy dokumentů a podpisů dotýkají (§ 334 a násl.). Přesto je nutno vycházet z obecných pravidel občanského zákoníku, popř. dalších právních předpisů, které upravují elektronické podpisy.

Současná soukromoprávní úprava stojí na zásadě tzv. bezformálnosti,² zatímco zákoník práce naopak vychází spíše z opačného principu, když pro mnohá

¹ Viz § 4 zákoníku práce.

² Viz § 559 občanského zákoníku.

právní jednání,³ ale nejenom pro ně⁴ stanovuje obligatorní písemnou formu.

Písemná forma má dva základní požadavky,⁵ a to písemnost a připojení podpisu jednatelů.⁶ Občanský zákoník však podpis blíže nedefinuje. Úpravu podpisů pro elektronická právní jednání občanský zákoník ponechává jiným právním předpisům.⁷

1.2 Písemná forma a elektronická právní jednání

Podle § 562 odst. 1 občanského zákoníku je písemná forma zachována i při právním jednání učiněném elektronickými nebo jinými technickými prostředky, a to za předpokladu, že umožňují (a) zachycení jeho obsahu a (b) určení jednatelů.

Co se týče umožnění zachycení obsahu elektronického právního jednání, právní teorie se shoduje v tom, že se jedná o potřebu grafického znázornění souboru znaků.⁸

K požadavku umožnění určení jednatelů osoby je nutno zdůraznit, že se jedná o „pouhou“ určitelnost, nikoliv nutnost určení jednatelů osoby prokázáním totožnosti.⁹ Právní úprava ani nevyžaduje, aby určení bylo nutně vždy úspěšné.¹⁰ Určitelnost může být zajištěna různými způsoby – autentizací (přihlášení heslem), autentizací určitým předmětem (např. USB tokenem), biometrickou autentizací (otisk prstu nebo sken oční duhovky) nebo autentizací ve spojení s autorizací (zasláním unikátního hesla v SMS zprávě).¹¹ Je na subjektech právního jednání, jakou formu si zvolí. Zvláštní

zákon však může stanovit zvláštní požadavky na ověření osoby.¹²

Pro zachování písemné formy podle § 562 odst. 1 občanského zákoníku se nevyžaduje podpis, pokud jsou splněny zde uvedené dvě podmínky. Komentářová literatura uvedené dovoduje z toho, že zákon používá souloví „zachování písemné formy“ a zároveň výslovně nestanovuje požadavek podpisu: „Nevyžaduje se, aby právní jednání učiněné v elektronické podobě, které splňuje požadavky § 562 odst. 1, bylo podepsáno (samozřejmě za předpokladu, že jsou splněny obě podmínky, tj. především lze identifikovat jednatelů). Tím spíše se nevyžaduje právní jednání opatřené zaručeným elektronickým podpisem (čl. 3 odst. 11 eIDAS), kvalifikovaným elektronickým podpisem (čl. 3 odst. 12 eIDAS) nebo učiněné prostřednictvím datové schránky.“

Z hlediska následků § 562 odst. 1 ve spojení s § 561 odst. 1 tedy postačí, aby v prostém e-mailu bylo obsaženo jméno a příjmení v jeho textu a půjde o platné právní jednání buď ve variantě § 561 odst. 1 věty třetí, nebo z důvodu § 562 odst. 1 (Korbel, Melzer 2014 s. 32 a násl.).¹³

Je však nutné zmínit, že přístup českých soudů a kontrolních orgánů je poměrně konzervativní a prozatím se k výše uvedenému názoru plošně nepřiklání, jinak řečeno je vůči některým typům elektronických podpisů nedůvěřivý.

II. Elektronické podpisy

Níže budou popsány jednotlivé typy elektronických podpisů, jak je definují právní předpisy. Podrobnější odborné informace o elektronických podpisech, které jsou psány srozumitelným jazykem, a to včetně jejich technické stránky včetně kryptologie, lze nalézt např. v Kompendiu elektronického podpisu dostupném online: www.elektronicky-podpis.info

Kromě elektronických podpisů budou dále popsány i dva další pojmy, které se ve spojení s elektronizací v poslední době často spojují a uživatelé je s elektronickými podpisy (často mylně) zaměňují – datové schránky a bankovní identita.

2.1 Elektronické podpisy podle nařízení eIDAS

Nařízení eIDAS upravuje základní rámec pro elektronické podpisy, který je přímo účinný pro všechny členské státy Evropské unie a některé další státy Evropského hospodářského prostoru.¹⁴

Nařízení eIDAS rozlišuje tři druhy elektronických podpisů:

a) elektronický podpis bez přívlastku, také někdy

³ Požadavek písemné formy je zákonem práce stanoven např. pro pracovní smlouvu (§ 34 odst. 2), sjednání zkušební doby (§ 35 odst. 6) všechna právní jednání směřující k rozvázání pracovního poměru (dohoda – § 49 odst. 2; výpověď – § 50 odst. 1; okamžitě zrušení – § 60, věta druhá; zrušení ve zkušební době – § 66 odst. 2), mzdový výměr (§ 113 odst. 4), konkurenční doložku (§ 310 odst. 6), kvalifikační dohodu (§ 234), vnitřní předpisy (§ 305), dohoda agentury práce s uživatelem o dočasném přidělení (§ 308 odst. 2) a další.

⁴ Požadavek písemné formy je zákonem práce stanoven i pro další jednání a úkony např.: rozvrh pracovní doby (§ 84), rozvrh čerpání dovolené (§ 217 odst. 1 práce), určení čerpání dovolené (§ 217 odst. 1 a § 218 odst. 4), žádost o převod dovolené do následujícího kalendářního roku (§ 218 odst. 2), podmínky pracovní cesty (§ 153) a další.

⁵ Rozsudek Nejvyššího soudu ze dne 29. ledna 2009, sp. zn. 30 Cdo 1230/2007.

⁶ Ustanovení § 561 odst. 1 věta první občanského zákoníku.

⁷ Ustanovení § 561 odst. 1 věta třetí občanského zákoníku.

⁸ JANOUŠEK, Michal. § 562 [Písemná forma právního jednání učiněného elektronickými prostředky]. In: LAVICKÝ, Petr a kol. Občanský zákoník I. Obecná část (§ 1–654). 2. vydání. Praha: C. H. Beck, 2022, s. 1801, marg. č. 13.

⁹ K pojmům identifikace, totožnost, autentizace a autorizace blíže viz část 1.3.7.1.

¹⁰ KORBEL, František, MELZER, Filip. Písemnost, elektronický a biometrický podpis v elektronickém právním jednání. *Bulletin advokacie*, 2014, č. 12, s. 31–36.

¹¹ JANOUŠEK, Michal. § 562 [Písemná forma právního jednání učiněného elektronickými prostředky]. In: LAVICKÝ, Petr a kol. Občanský zákoník I. Obecná část (§ 1–654). 2. vydání. Praha: C. H. Beck, 2022, s. 1801–1802, marg. č. 15.

¹² Např. §§ 7 a 8 zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů.

¹³ JANOUŠEK, Michal. § 562 [Písemná forma právního jednání učiněného elektronickými prostředky]. In: LAVICKÝ, Petr a kol. Občanský zákoník I. Obecná část (§ 1–654). 2. vydání. Praha: C. H. Beck, 2022, s. 1801, marg. č. 8–9.

¹⁴ Island, Lichtenštejnsko a Norsko, srov.: www.efta.int/eea-lex/32014R0910

- označovaný jako prostý, či dokonce primitivní elektronický podpis – čl. 3 odst. 10) nařízení,
- b) zaručený elektronický podpis – čl. 3 odst. 11) nařízení, a
- c) kvalifikovaný elektronický podpis – čl. 3 odst. 12) nařízení.

2.1.1 Elektronický podpis

Elektronickým podpisem se rozumí data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která podepisující osoba používá k podepsání.

Pojem elektronického podpisu lze vnímat ve dvou kontextech. Jedná se o obecnou definici elektronického podpisu, která se uplatní i na zaručené a kvalifikované elektronické podpisy. Zároveň se jedná o „zbytkovou“ kategorii, do které spadají všechny elektronické podpisy, které nesplňují předpoklady kvalifikovaných ani zaručených elektronických podpisů, která se jinak nazývá i jako tzv. prostý elektronický podpis.

Podle čl. 25 odst. 1 nařízení eIDAS nesmějí být elektronickému podpisu upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické podpisy.

Z uvedené vyplývají dva účinky veškerých elektronických podpisů:

- elektronický podpis je vždy právně relevantní, a
- elektronický podpis má vždy důkazní funkci.

Z toho vyplývá, že pokud je k elektronickému právnímu jednání připojen elektronický podpis, byť prostý, vždy se jedná o podpis i ve smyslu běžného (ne-elektronického) písemného právního jednání.

2.1.2 Prostý elektronický podpis

Prostý elektronický podpis nemusí mít podle mnohých odborných názorů jenom podobu digitálního podpisu (speciální data, která jsou připojena k danému dokumentu nebo jsou s ním logicky spojena – např. podpis vytvořený podpisovými aplikacemi,¹⁵ který nebude splňovat požadavky alespoň zaručeného elektronického podpisu), ale může se jednat třeba i o uvedení jména a příjmení na konci e-mailové, SMS či jiné elektronické zprávy nebo naskenovaný vlastnoruční podpis.¹⁶

¹⁵ Např. DocuSign, Adobe Sign, OBELISK Signing Portal nebo Signer od Software602.

¹⁶ Např. Korbelt P., Kovář D. a Amler P., Interpretace elektronického podpisu a související identifikace v soukromém právu, 15. 7. 2022 [online]. Dostupné z: www.pravniprostor.cz/clanky/obcanske-pravo/interpretace-elektronickeho-podpisu-souvisejici-identifikace-v-soukromem-pravu?fbclid=IwAR16X3fgJdNHtA-XDN1Qn7BsFmpLF9vISnbt9L-2CIom1rVdviNHamoQkzbo; Podaný J., Podepisování soukromých listin včera, dnes a zítra, 15. 7. 2022 [online]. Dostupné z <https://advokatnidenik.cz/2020/05/04/podepisovani-soukromych-listin-vcera-dnes-a-zitra/>; nebo Peterka J., eIDAS a elektronické podpisy: Nepřehnali jsme to s našimi výjimkami?, 15. 7. 2022 [online]. dostupné z:

2.1.3 Zaručený elektronický podpis

Zaručeným elektronickým podpisem se rozumí elektronický podpis, který:

- a) je jednoznačně spojen s podepisující osobou,
- b) umožňuje identifikaci podepisující osoby,
- c) je vytvořen pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou, a
- d) je k datům, která jsou tímto podpisem podepsána, připojen takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat.

Poslední požadavek, bod d), zaručuje neporušenost (integritu) obsahu datové zprávy od okamžiku, kdy byla podepsána. Zaručený elektronický podpis poskytuje oproti „prostému“ elektronickému podpisu větší bezpečnost před zneužitím. Zaručený elektronický podpis je vytvářen za pomoci certifikátu, který ovšem nemusí být splňovat žádné speciální náležitosti a může tedy být vydán jakoukoli certifikační autoritou nebo může být tzv. *self-signed*.¹⁷ V praxi se lze často setkat s tzv. „komerčními“ certifikáty, které vydávají jak specializovaní poskytovatelé, tak velcí zaměstnavatelé (např. IT společnosti nebo automobilky).¹⁸

2.1.4 Kvalifikovaný elektronický podpis

Kvalifikovaný elektronický podpis představuje „nejvyšší“ variantu elektronického podpisu. Rozumí se jím zaručený elektronický podpis, který je vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů a který je založen na kvalifikovaném certifikátu pro elektronické podpisy.

Kvalifikovaný elektronický podpis má účinky vlastnoručního podpisu¹⁹ a je uznáván napříč členskými státy Evropské unie (Evropského hospodářského prostoru).²⁰ Kvalifikovaný elektronický podpis však nemá účinky úředně ověřeného podpisu.²¹

Kvalifikované certifikáty může vydávat pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru.²² Seznam kvalifikovaných poskytovatelů služeb vytvářejících důvěru vede v České republice Ministerstvo vnitra ČR,²³ obdobně Evropská

www.lupa.cz/clanky/eidas-a-elektronicke-podpisy-neprehnali-jisme-to-s-nasimi-vyjimkami/

¹⁷ Certifikát podepsaný sám sebou, tedy certifikát který podepsal sám jeho tvůrce, který se tak zároveň stal certifikační autoritou.

¹⁸ Některé komerční certifikáty (např. velice častý od PostSignum) však slouží spíše pro bezpečnou komunikaci – pro přihlášení do datové schránky, pro bezpečný přístup do aplikací nebo třeba k šifrování komunikace. V praxi je využíván při provádění konverzí.

¹⁹ Čl. 25 odst. 2 nařízení eIDAS.

²⁰ Čl. 25 odst. 3 nařízení eIDAS.

²¹ Podle § 6 zákona č. 12/2020 Sb., o právu na digitální služby, ve znění pozdějších předpisů, elektronické podpisy za určitých podmínek slouží k úřednímu ověření podpisu.

²² Čl. 3 odst. 15 a 20 a čl. 24 nařízení eIDAS.

²³ Dostupné zde: www.mvcr.cz/clanek/seznam-kvalifikovanych-poskytovatelu-sluzeb-vytvarejicich-duveru-a-poskytovanych-kvali

komise pro celou EU (a Evropský hospodářský prostor).²⁴

V ČR v současnosti mohou vydávat kvalifikované certifikáty pro elektronické podpisy: Česká pošta, s.p. (její služba PostSignum), První certifikační autorita, a.s., eIdentity a.s. a Správa základních registrů prostřednictvím své certifikační autority Národní certifikační autorita. Pouze první tři však poskytují své služby veřejnosti na komerční bázi. Poslední slouží výhradně pro veřejnou správu.

Aby mohl být kvalifikovaný certifikát využíván pro účely kvalifikovaného elektronického podpisu, musí být uložen na kvalifikovaný prostředek pro vytváření elektronických podpisů, jakým je např. USB token, čipová karta, MicroSD karta nebo tzv. HSM modul v rámci serverového řešení. Kvalifikovaný certifikát též může být uložen na novější občanské průkazy, které jsou vybaveny strojeově čitelnými údaji a kontaktním elektronickým čipem.²⁵

2.2 Zákon o službách vytvářejících důvěru a uznávaný elektronický podpis

Na nařízení eIDAS navazuje český adaptační zákon o službách vytvářejících důvěru, který úpravu elektronických podpisů doplňuje a rozšiřuje o české specifikum tzv. uznávaného elektronického podpisu.

Zákon o službách vytvářejících důvěru upravuje další druh elektronického podpisu, kterým je zaručený elektronický podpis založený na kvalifikovaném certifikátu (§ 6 odst. 2 zákona). Rozdíl oproti kvalifikovanému podpisu spočívá v tom, že kvalifikovaný certifikát není uložen na kvalifikovaném prostředku pro vytváření elektronických podpisů, nýbrž může být uložen na odlišném, nezabezpečeném zařízení, např. na běžném počítači.

České právo také pracuje s pojmem tzv. uznávaného elektronického podpisu. Tento však nepředstavuje samostatný druh elektronického podpisu, ale jedná se o legislativní zkratku, která v sobě zahrnuje dva druhy elektronického podpisu:

- a) kvalifikovaný elektronický podpis (tj. „nejvyšší“ podpis podle nařízení eIDAS), a
- b) zaručený elektronický podpis založený na kvalifikovaném certifikátu (tj. „český druh“ elektronického podpisu, viz výše).

S pojmem uznávaného elektronického podpisu pracují i další právní předpisy – např. právě zákoník práce.²⁶

2.3 Datové schránky

Datové schránky upravuje zákon o elektronických úkonech. Datové schránky nepředstavují formu elek-

tronického podpisu, ale jedná se o elektronickou službu doručování (obdobně jako třeba pošta u „papirovo“ zásilek). Z působnosti nařízení eIDAS jsou přímo vyňaty.²⁷ Zákon o elektronických úkonech však datovým zprávám přiznává stejné účinky, jako kdyby se jednal o písemný a podepsaný úkon, pokud jsou učiněny vůči orgánům veřejné moci a pokud tak učinila oprávněná osoba.²⁸

Jelikož je používání datové schránky vysoce zabezpečeno – speciální přihlašovací údaje, šifrovaná komunikace atd., zákon o elektronických úkonech zavádí tzv. fikci podpisu.²⁹ Tato fikce se však ze zákona uplatňuje pouze při jednání vůči orgánům veřejné moci. Fikce se navíc týká jen vyjmenovaných osob³⁰ a pověřených osob a nevztahuje se na případy, kdy jiný právní předpis nebo vnitřní předpis požaduje společný úkon více z uvedených osob. Jedná se např. o situaci, kdy statutární orgán společnosti tvoří více jednatelů, přičemž musí vždy jednat alespoň dva společně.

Fikce podpisu není ze zákona stanovena u soukromých zpráv – např. mezi zaměstnancem a zaměstnavatelem. Přesto se autoři článku domnívají, že by tato fikce měla být i u soukromých zpráv dovozena, protože komunikace prostřednictvím datových schránek je vysoce bezpečná a s vysokou mírou jistoty identifikuje toho, kdo ji odeslal, a tedy i jednal – až na výjimku kdy jiný právní předpis nebo vnitřní předpis požaduje společný úkon více z uvedených osob (viz příklad výše).

2.3.1 Doručování prostřednictvím datových schránek

Doručování mezi soukromými subjekty doznalo k roku 2022 zásadních změn. Od 1. ledna 2022 byl novelou zákona o elektronických komunikacích³¹ změněn §18a. Do novely bylo totiž doručování mezi soukromými subjekty možné jen, pokud příjemce ta-

²⁷ Srov. čl. 2 odst. 2.

²⁸ Jak jsou vymezeny v § 1 odst. 1 písm. a) zákona o elektronických úkonech.

²⁹ Ustanovení § 18 odst. 2 zákona o elektronických úkonech: „Úkon učiněný osobou uvedenou v § 8 odst. 1 až 4 nebo pověřenou osobou, pokud k tomu byla pověřena, prostřednictvím datové schránky má stejné účinky jako úkon učiněný písemně a podepsaný, ledaže jiný právní předpis nebo vnitřní předpis požaduje společný úkon více z uvedených osob.“

³⁰ Ustanovení § 8 odst. 1 až 4 zákona o elektronických úkonech: „(1) K přístupu do datové schránky fyzické osoby je oprávněna fyzická osoba, pro niž byla datová schránka zřízena.

(2) K přístupu do datové schránky podnikající fyzické osoby je oprávněna podnikající fyzická osoba, pro niž byla datová schránka zřízena.

(3) K přístupu do datové schránky právnické osoby je oprávněn statutární orgán právnické osoby, člen statutárního orgánu právnické osoby nebo vedoucí organizační složky podniku zahraniční právnické osoby zapsané v obchodním rejstříku, pro něž byla datová schránka zřízena.

(4) K přístupu do datové schránky orgánu veřejné moci je oprávněn vedoucí orgánu veřejné moci, pro něhož byla datová schránka zřízena.“

³¹ Zákonem č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci.

fikovanych-sluzeb-vytvarejicich-duveru.aspx

²⁴ Dostupné zde: <https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home>

²⁵ Dostupné zde: www.mver.cz/clanek/obcansky-prukaz-vydavany-od-1-7-2018-splnuje-pozadavky-na-kvalifikovany-prostředek-pro-vytvareni-elektronickyh-podpisu.aspx

²⁶ Zvláštní úprava doručování prostřednictvím sítě nebo služby elektronických komunikací – § 335 odst. 2 nebo § 337 odst. 2 *in fine*.

kové doručování povolil (výchozí nastavení datových schránek toto doručování zakazovalo).

Od začátku roku 2022 je však princip nastaven opačně. Ve výchozím stavu datové schránky soukromých subjektů umožňují přijímání datových zpráv z datových schránek fyzických, podnikajících fyzických a právnických osob. Pouze u datových schránek fyzických osob (tj. nepodnikajících) je možno žádat o znepřístupnění dodávání od ostatních soukromých subjektů.

Datová zpráva se považuje za doručenu okamžikem, kdy se do datové schránky přihlásí osoba, která má s ohledem na rozsah svého oprávnění přístup k tomuto dokumentu. Nově je také zavedena fikce doručení v případě soukromých zpráv, a to uplynutím 10denní lhůty od dodání zprávy do datové schránky, nepřihlásí-li se do schránky osoba dříve. Podle předchozí úpravy byla zpráva doručena tehdy, kdy se do datové schránky osoba přímo přihlásila – nebyla tedy žádná zákonná fikce doručení.

Zákoník práce však obsahuje dílčí zvláštní úpravu doručování v pracovněprávních vztazích, o níž bude pojednáno v navazujícím samostatném článku.

2.4 Bankovní identita

Bankovní identita, původně „BankID“, je vlastně online průkaz totožnosti („e-občanka“), který je osobě vytvořen automaticky při zřízení internetového bankovníctví u banky, která se do tohoto projektu zapojila. Umožňuje zabezpečené přihlášení s vysokou úrovní ověřitelnosti přihlašující se osoby do portálů banky, ale také ke službám eGovernmentu, tedy k elektronickému systému veřejné správy.

Největší výhodou využití bankovní identity je vysoká míra ověřitelnosti totožnosti osoby, jež se skrze bankovní identitu přihlásí. Zajišťuje to jednak to, že banka musí své klienty důsledně „offline“ ztotožnit, jednak vysoký stupeň zabezpečení přihlašování – přihlašovací údaje, ke kterým má přístup pouze klientova banka, ale také dvoufázové ověření, nejčastěji prostřednictvím mobilního klíče, či kódu z SMS zprávy, které aplikace internetového bankovníctví již běžně využívají.³² Samotné ověření totožnosti zadáním přihlašovacích údajů probíhá v prostředí banky, čímž se zaručuje vysoký standard zabezpečení.

Bankovní identita nabízí komerční zpoplatněné služby, mezi kterými je i možnost elektronického podpisu dokumentů. Neumožňuje ovšem využití kvalifikovaného podpisu ani zaručeného podpisu založeného na kvalifikovaném certifikátu. Nabízí tedy pouze zaručený elektronický podpis, který se opírá o silné ověření totožnosti prostřednictvím bankovní identity. Tyto služby jsou ovšem zpoplatněny.³³

2.5 Rozhodovací praxe k elektronickým podpisům

Rozhodovací praxe k předchozímu občanskému zákoníku byla v otázce právních jednání podepsaných elektronicky poměrně přísná.

V roce se 2019³⁴ Nejvyšší soud stručně vyjádřil k písemné formě námitek proti výpovědi z nájmu prostor sloužících k podnikání (podle § 2314 odst. 1 občanského zákoníku) zaslány nájemcem e-mailem. Nejvyšší soud uvedl: „...není důvodu posuzovat požadavky na zachování písemné formy u námitek odlišným způsobem, než jak je tomu u jiných právních jednání. Vznese-li žalobkyně Námitky e-mailem..., který nebyl opatřen elektronickým podpisem, je závěr odvolacího soudu, že nedodržela písemnou formu Námitek, v souladu s judikaturou Nejvyššího soudu.“

Podle dvou rozsudků Městského soudu v Praze z roku 2020³⁵ pouze kvalifikovaný elektronický podpis, zaručený elektronický podpis založený na kvalifikovaném certifikátu a zaručený elektronický podpis umožňují se značnou úrovní důvěry identifikovat (ztotožnit) podepsanou osobu. Jiné elektronické podpisy (tj. prosté elektronické podpisy) „je soud sice povinen přijmout jako důkaz (ve smyslu čl. 25 bod 1. Nařízení eIDAS), avšak bez dalších tvrzení a důkazů, které v dané věci nabídnuty nebyly, nelze mít za prokazané, že tyto ostatní elektronické podpisy jsou podpisem (údajně) jednající osoby“.³⁶

Určitým průlomem by pak mohl být rozsudek 31 ICdo 36/2020.³⁷ Velký senát Nejvyššího soudu zde, vedle výkladu adverbium „zjevně“, připustil využití uznávaného elektronického podpisu (ve spojení s využitím elektronické identifikace prostřednictvím kvalifikovaného systému elektronické identifikace) v situaci uzavření dvoudomé smlouvy, podle § 13 zákona č. 90/2012 Sb. o obchodních společnostech a družstvech (obchodních korporacích), kde zákon explicitně vyžaduje úředně ověřený podpis. Velký senát dovodil, že přes to, že dojde k nedodržení zákonem vyžadované formy, nepůjde o narušení veřejného pořádku, neboť „smysl a účel normy zůstává naplněn“.

Na druhou stranu praxe soudů nižších instancí je, jak se zdá, nadále k elektronickým podpisům značně rozkolísaná s tím, že prostý elektronický podpis v zásadě není prokazatelný, nebo dokonce není vůbec považován za dostatečný pro uzavírání písemných právních jednání.³⁸

³⁴ Usnesení Nejvyššího soudu ze dne 22. května 2019, sp. zn. 26 Cdo 1230/2019.

³⁵ Rozsudek ze dne 8. července 2020, sp. zn. 18 Co 187/2020, a rozsudek ze dne 2. září 2020, sp. zn. 18 Co 227/2020.

³⁶ Je však třeba upozornit, že obě věci rozhodoval tentýž senát, že v obou případech se soud zabýval postoupením pohledávky, že obě rozhodnutí dělí necelé dva měsíce a že text obsahující právní posouzení je takřka totožný (rozdílná je v něm pouze identifikace jedné ze stran sporů).

³⁷ Rozsudek Nejvyššího soudu ze dne 10. června 2020, sp. zn. 31 ICdo 36/2020.

³⁸ Viz Prostý elektronický podpis dle EIDAS v soudní praxi, JUDr. Vladimír Janošek, 22. 4. 2022 [online]. Dostupné z: www.epravo.cz/top/clanky/prosty-elektronicky-podpis-dle-eidas-v-soudni-praxi-114434.html

³² Jak funguje bankovní identita, [online]. Dostupné z: www.bankid.cz

³³ Nabídka BankID pro firmy, [online]. Dostupné z: www.bankid.cz/pro-firmy

III. Závěr

Pracovněprávní jednání a faktické úkony lze rozdělit do následujících kategorií:

- a) povinně písemná dvoustranná pracovněprávní jednání uvedená v § 334 zákoníku práce,
- b) ostatní povinně písemná dvoustranná pracovněprávní jednání,
- c) neformální (nepísemná) dvoustranná pracovněprávní jednání,
- d) jednostranná písemná pracovněprávní jednání a faktické úkony uvedené v § 334 zákoníku práce,
- e) ostatní povinně písemná jednostranná pracovněprávní jednání a faktické úkony a
- f) neformální (nepísemná) jednostranná pracovněprávní jednání a faktické úkony.

U dokumentů, které nevyžadují písemnou formu, elektronizaci prakticky nic nebrání, avšak je nutné dbát na to, aby zejména zaměstnavatel byl schopen důvěryhodně prokázat, že dokument skutečně zaměstnanec elektronicky podepsal (a to i prostým elektronickým podpisem), nebo že dokument zaměstnanec skutečně obdržel (u jednostranných dokumentů doručovaných zaměstnanci).

Elektronizace povinně písemných dokumentů je za současné právní úpravy a rozhodovací praxe soudů podle autorů bez rizik možná jen za použití alespoň uznávaného elektronického podpisu. To neznamená, že nižší formy elektronického podpisu jsou vyloučeny, ale hrozí nemalé riziko, že takový podpis bude považován za neprůkazný, anebo že některé formy prostých (primitivních) podpisů vůbec soudy a kontrolní orgány nebudou považovat za podpis.

Právním jednáním, která jsou uvedena v § 334 zákoníku a která proto podléhají speciální a nutno říci přísné úpravě doručování, se budeme věnovat v navazujícím článku. Už na tomto místě lze říci, že pro příslušná dvoustranná právní jednání v zásadě platí totéž jako je uvedeno pro písemné dokumenty výše. Pro příslušná jednostranná právní jednání je však nutné dodržet ještě přísná pravidla doručování, která na-

víc obsahují povinnost použít uznávaný elektronický podpis.

Zaměstnavatelům lze proto doporučit, aby pečlivě zvažovali, jaké dokumenty budou elektronizovat – zejména s ohledem na jejich formu, a taktéž na to, kdo je podepisuje – zda zaměstnavatel i zaměstnanec, nebo jenom jeden z nich a druhý buď vůbec, nebo jenom jako potvrzení, že dokument převzal. Pracovní právo je v tomto ohledu velice pestré a přináší celou řadu kombinací. Elektronizace pracovněprávních dokumentů je tak daleko zajímavější, ale i složitější, než např. elektronizace běžného obchodního styku nebo smluvní dokumentace.

Závěrem je ještě nutné upozornit, že elektronické podpisy a dokumenty mají další svá specifika – zejména co se týká jejich bezpečné archivace, kterou musí zaměstnavatel zajistit pro některé dokumenty i v délce 45 let.³⁹ K elektronizaci je proto potřeba přistoupit komplexně a obezřetně.

Seznam souvisejících předpisů a judikatury

- zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů („zákoník práce“)
- zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů („občanský zákoník“)
- 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 („nařízení eIDAS“)
- zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů („zákon o službách vytvářejících důvěru“)
- zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů („zákon o elektronických úkonech“)

³⁹ Viz ustanovení § 35a odst. 4 zákona č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, ve znění od 1. 1. 2023.